Quantum Series™
ENGINEERING

QUANTUM Series

Semester - 6 Computer Science & IT

Computer Networks

Session 2018-19 Even Semester

- Topic-wise coverage of entire syllabus in Question-Answer form.
- Short Questions (2 Marks)

Includes solution of following AKTU Question Papers:

2013-14 • 2014-15 • 2015-16 • 2016-17 • 2017-18

Includes Detailed Analysis of Previous AKTU Question Papers.

CONTENTS

RCS 601 : Computer Networks

ANALYSIS OF AKTU PAPERS (2013-14 TO 2017-18) (A–1 A to A–6 A)

UNIT-1 : INTRODUCTION CONCEPTS (1–1 A to 1–33 A)

Goals and Applications of Networks, Network structure and architecture, The OSI reference model, services, Network Topology Design - Delay Analysis, Back Bone Design, Local Access Network Design, Physical Layer Transmission Media, Switching methods, ISDN, Terminal Handling.

UNIT-2 : MEDIUM ACCESS SUB LAYER (2–1 A to 2–36 A)

Medium Access sub layer - Channel Allocations, LAN protocols - ALOHA protocols - Overview of IEEE standards - FDDI. Data Link Layer - Elementary Data Link Protocols, Sliding Window protocols, Error Handling.

UNIT-3 : NETWORK LAYER (3–1 A to 3–33 A)

Network Layer - Point - to Pont Networks, routing, Congestion control Internetworking -TCP / IP, IP packet, IP address, IPv6.

UNIT-4 : TRANSPORT LAYER (4–1 A to 4–30 A)

Transport Layer - Design issues, connection management, session Layer-Design issues, remote procedure call. Presentation Layer-Design issues, Data compression techniques, cryptography - TCP - Window Management.

UNIT-5 : APPLICATION LAYER (5–1 A to 5–21 A)

Application Layer: File Transfer, Access and Management, Electronic mail, Virtual Terminals, Other application. Example Networks - Internet and Public Networks.

SHORT QUESTIONS (SQ-1A to SQ-15A)

SOLVED PAPERS (2013-14 TO 2017-18) (SP-1A to SP-15A)

Analysis of Previous AKTU Papers

Unit-1 : Introduction Concepts							
Part	Topics	2017-18	2016-17	2015-16	2014-15	2013-14	Que. No.
1.	Introduction	0	0	0	0	0	0
2.	OSI reference model	1	1	1	1	1	1.3*, 1.4*, 1.5
3.	Services	0	0	0	1	0	1.8
4.	Network topology design	1	1	0	1	1	1.9*, 1.10
5.	Backbone design	0	0	0	0	1	1.12
6.	Local access network design	0	0	0	0	0	0
7.	Physical layer transmission media	1	0	0	1	1	1.14*, 1.16
8.	Switching method	0	0	0	0	1	1.17
9.	ISDN and terminal handling	0	0	0	3	1	1.19, 1.21, 1.22, 1.23
	Total Questions	3	2	1	7	6	

* = Asked in different years

Unit-2 : Medium Access Sublayer							
Part	Topics	2017-18	2016-17	2015-16	2014-15	2013-14	Que. No.
1.	Channel allocation	1	0	0	2	1	2.4*, 2.6, 2.7
2.	ALOHA protocols	0	0	1	2	1	2.11*, 2.12, 2.13
3.	FDDI	0	1	0	0	1	2.17, 2.19
4.	Data link layer	1	1	0	0	0	2.20*
5.	Sliding window protocol	3	2	0	4	2	2.21*, 2.23, 2.24*, 2.25*, 2.26, 2.27, 2.29, 2.30
6.	Error handling	0	0	1	2	1	2.35, 2.36, 2.37, 2.38
	Total Questions	5	4	2	10	6	

Unit-3 : Network Layer							
Part	Topics	2017-18	2016-17	2015-16	2014-15	2013-14	Que. No.
1.	Network layer	0	0	0	0	0	0
2.	Routing	1	1	1	0	1	3.5, 3.6*, 3.10
3.	Congestion control	1	0	1	0	1	3.11*, 3.13
4.	Internetworking	0	0	0	0	0	0
5.	IP address	1	0	3	2	2	3.20*, 3.26, 3.27, 3.28*, 3.29, 3.30
	Total Questions	3	1	5	2	4	

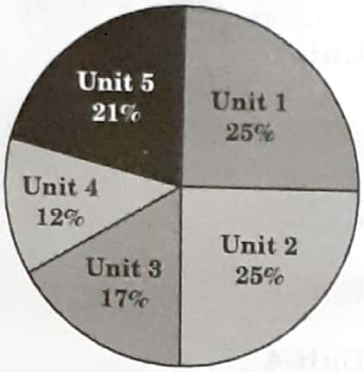
*** = Asked in different years**

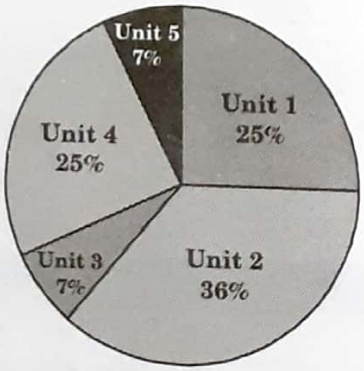
Unit-4 : Transport Layer							
Part	Topics	2017-18	2016-17	2015-16	2014-15	2013-14	Que. No.
1.	Transport layer	1	1	0	0	0	4.3*
2.	Connection management	2	2	1	1	1	4.8*, 4.9*, 4.10, 4.11
3.	Session layer	0	0	0	1	0	4.16
4.	Presentation layer	0	0	0	0	0	0
5.	Data compression	0	0	0	1	1	4.19, 4.20
6.	Cryptography	1	0	1	3	1	4.22, 4.26, 4.27, 4.28*, 4.29
7.	Window management	0	0	2	1	0	4.30, 4.31 4.32
	Total Questions	4	3	4	7	3	

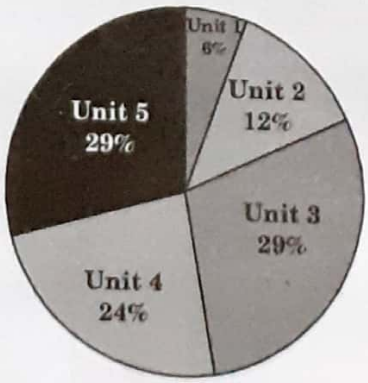
Unit-5 : Application Layer							
Part	Topics	2017-18	2016-17	2015-16	2014-15	2013-14	Que. No.
1.	Application layer	1	1	1	0	2	5.2*, 5.3, 5.4
2.	Access and management	1	0	2	0	1	5.5*, 5.6
3.	Electronic mail	0	0	1	0	1	5.8*
4.	Virtual terminals	2	2	1	2	1	5.13*, 5.14, 5.15, 5.16*, 5.17
5.	Public network	0	0	0	0	0	0
	Total Questions	4	3	5	2	5	

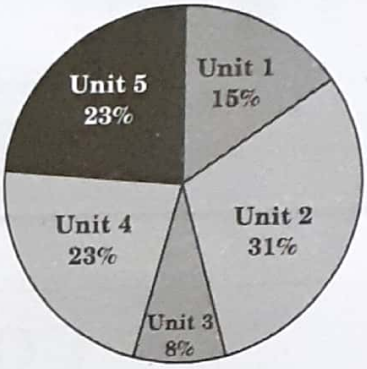
*** = Asked in different years**

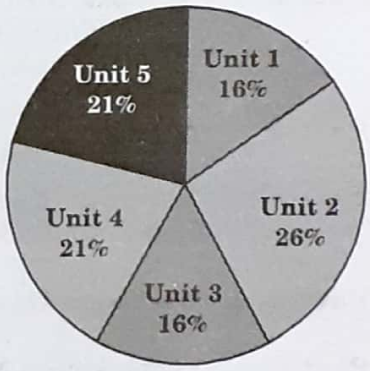
2 Marks Questions						
Units \ Year	2017-18	2016-17	2015-16	2014-15	2013-14	Total Questions
Unit-1	3	2	2	0	0	7
Unit-2	2	3	2	0	0	7
Unit-3	3	2	6	0	0	11
Unit-4	1	1	0	0	0	2
Unit-5	1	2	0	0	0	3

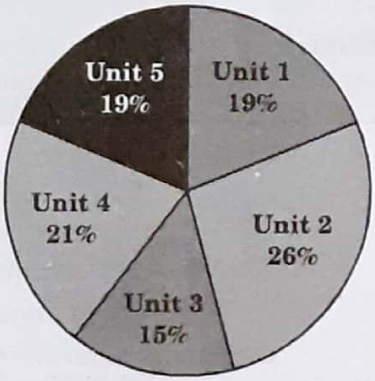
Units	Ques. Asked (2013-14)	% Weightage of Units (2013-14)
Unit-1	6	
Unit-2	6	
Unit-3	4	
Unit-4	3	
Unit-5	5	

Units	Ques. Asked (2014-15)	% Weightage of Units (2014-15)
Unit-1	7	
Unit-2	10	
Unit-3	2	
Unit-4	7	
Unit-5	2	

Units	Ques. Asked (2015-16)	% Weightage of Units (2015-16)
Unit-1	1	
Unit-2	2	
Unit-3	5	
Unit-4	4	
Unit-5	5	

Units	Ques. Asked (2016-17)	% Weightage of Units (2016-17)
Unit-1	2	
Unit-2	4	
Unit-3	1	
Unit-4	3	
Unit-5	3	

Units	Ques. Asked (2017-18)	% Weightage of Units (2017-18)
Unit-1	3	
Unit-2	5	
Unit-3	3	
Unit-4	4	
Unit-5	4	

Units	Total Questions (2013-14 to 2017-18)	% Weightage of Units (2013-14 to 2017-18)
Unit-1	19	
Unit-2	27	
Unit-3	15	
Unit-4	21	
Unit-5	19	

1 UNIT

Introduction Concepts

CONTENTS

Part-1	:	Introduction Concepts : Goals and Applications of Network	1–2A to 1–3A
Part-2	:	Network Structure and Architecture The OSI Reference Model	1–3A to 1–12A
Part-3	:	Services	1–13A to 1–14A
Part-4	:	Network Topology Design : Delay Analysis	1–14A to 1–19A
Part-5	:	Backbone Design	1–19A to 1–20A
Part-6	:	Local Access Network Design	1–20A to 1–21A
Part-7	:	Physical Layer Transmission Media	1–22A to 1–26A
Part-8	:	Switching Methods	1–27A to 1–29A
Part-9	:	ISDN Terminal Handling	1–29A to 1–33A

Introduction Con

Long Answer Ty

Que 1.1. Write a sh

Answer

1. A computer networ
2. A node can be any
3. The communicating
4. Categories of netw
5. The three basic cat
   - **a. Local Area N**
     - i. LAN is us
     - ii. It may be office on network
   - **b. Wide Area N**
     - i. WAN is area.
     - ii. The netw WAN.
   - **c. Metropolita**
     - i. MAN is
     - ii. It is larg
     - iii. It may co

Que 1.2. Describe

Answer

Goals of network ar

1. Cost reduction by
2. High reliability by
3. Greater flexibilit
4. Increase producti users.

PART-1

Introduction Concepts : Goals and Application of Network.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.1. Write a short note on computer network.

Answer

1. A computer network can be defined as a collection of nodes.
2. A node can be any device capable of transmitting or receiving data.
3. The communicating nodes have to be connected by communication links.
4. Categories of network are categorized on the basis of their size.
5. The three basic categories of computer networks are :

a. Local Area Network (LAN) :

i. LAN is usually limited to a few kilometers of area.

ii. It may be privately owned and could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in an entire building.

b. Wide Area Network (WAN) :

i. WAN is made of all the networks in a (geographically) large area.

ii. The network in the entire state of Maharashtra could be a WAN.

c. Metropolitan Area Network (MAN) :

i. MAN is of size between LAN and WAN.

ii. It is larger than LAN but smaller than WAN.

iii. It may comprise the entire network in a city like Mumbai.

Que 1.2. Describe the goals and application of network.

Answer

Goals of network are :

1. Cost reduction by sharing hardware and software resources.
2. High reliability by having multiple sources of supply.
3. Greater flexibility because of possibility to connect devices.
4. Increase productivity by making it easier to access data by the several users.

5. To increase the systems performance, as the work load increases, by just adding more processors.
6. Computer networks provide a powerful communication medium.

Applications of network are :

1. **Marketing and sales :**
   i. Marketing professional use to collect, exchange and analyze data relating to customer needs and product development cycles.
   ii. Sales application includes teleshopping, which uses order entry computers or telephone connected to an order processing network, and online reservation services for railways, hotels, airlines, restaurants, theatre etc.
2. **Financial services :** It include credit history searches, foreign exchange and investment services and Electronic Fund Transfer (EFT), which allow a user to transfer money without going to bank.
3. **Electronic messaging :**
   i. Emails transfer the messages between two and more users in a network.
   ii. With this application user can transfer the information in the form of text, picture and voice.
4. **Directory services :** It allows list of files to be stored in central location to speed up the world wide search operation.
5. **Information services :**
   i. It includes bulletin boards and data bank.
   ii. A 'www' site offering the technical specification for a new product in an information services.

PART-2

Network Structure and Architecture, the OSI Reference Model.

CONCEPT OUTLINE

- OSI model consists of seven layers :
  i. Physical layer
  ii. Data link layer
  iii. Network layer
  iv. Transport layer
  v. Session layer
  vi. Presentation layer
  vii. Application layer

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.3. **Describe OSI reference model in detail.**

OR

Discuss the services of each layer of OSI reference model.

AKTU 2014-15, Marks 05

OR

Explain functionalities of every layer in OSI reference model with neat block diagram.

AKTU 2016-17, Marks 7.5

Answer

a. OSI reference model is a seven layer architecture which defines seven levels or layers in a complete communication system. The lowest layer is physical layer and highest one is called as the application layer.

b. It is called as OSI (Open System Interconnection) reference model because it is designed to deal with open systems *i.e.*, the systems which are open for communication with other systems.

c. The OSI model suggested by IEEE has seven layers :

1. Physical layer :

i. The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

ii. It deals with the mechanical and electrical specifications of the interface and transmission medium.

iii. Fig. 1.3.1 shows the position of the physical layer with respect to the transmission medium and the data link layer.

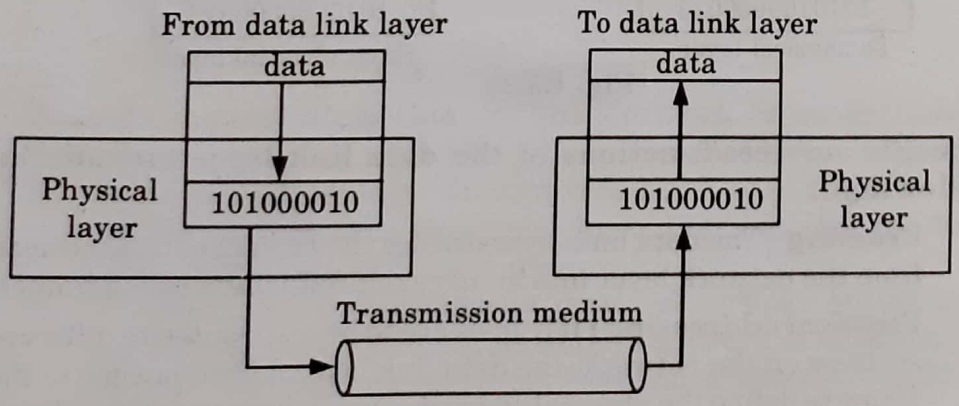


Fig. 1.3.1.

Specific services/functions of the physical layer are :

i. **Physical characteristics of interfaces and media :** The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

ii. **Representation of bits :** The physical layer defines the type of encoding (how 0s and 1s are changed to signals) of bit which is to be transmitted.

iii. **Data rate :** The transmission rate, the number of bits sent per second, is also defined by the physical layer.

iv. **Synchronization of bits :** The sender and receiver must be synchronized at the bit level.

v. **Line configuration :** The physical layer is concerned with the connection of devices to the medium. In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.

2. **Data link layer :**

i. The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery.

ii. It makes the physical layer appear error free to the upper layer (network layer).

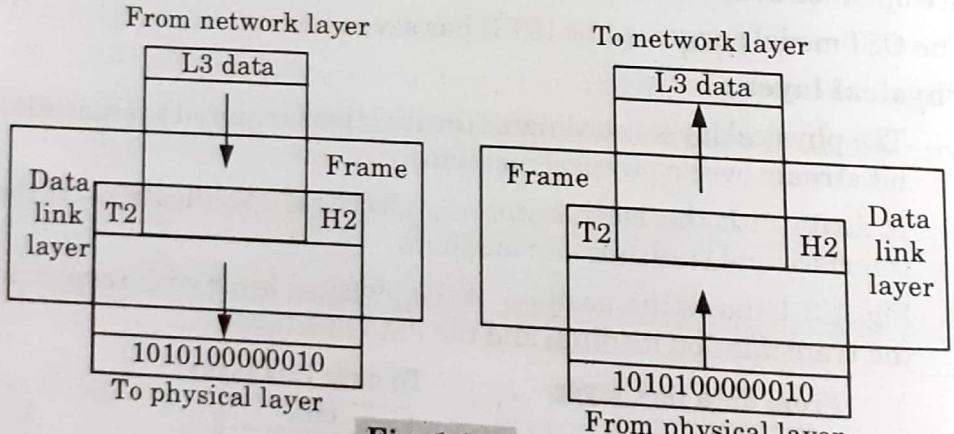


Fig. 1.3.2.

Specific services/functions of the data link layer include the following :

i. **Framing :** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

ii. **Physical addressing :** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender (source address) and/or receiver (destination address) of the frame.

iii. **Flow control :** If the rate at which the data are absorbed by the receiver is less than the rate produced by the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

iv. **Error control :** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to prevent duplication of frames.

v. **Access control :** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

3. **Network layer :**

i. The network layer is responsible for the source to destination delivery of a packet possibly across multiple networks (links).

ii. The network layer ensures that each packet gets from its point of origin to its final destination.

iii. If two systems are connected to the same link, there is no need for a network layer. However, if the two systems are attached to different networks (links), there is a need for the network layer to accomplish source-to-destination delivery.

iv. Fig. 1.3.3 shows the relationship of the network layer to the data link and transport layers.

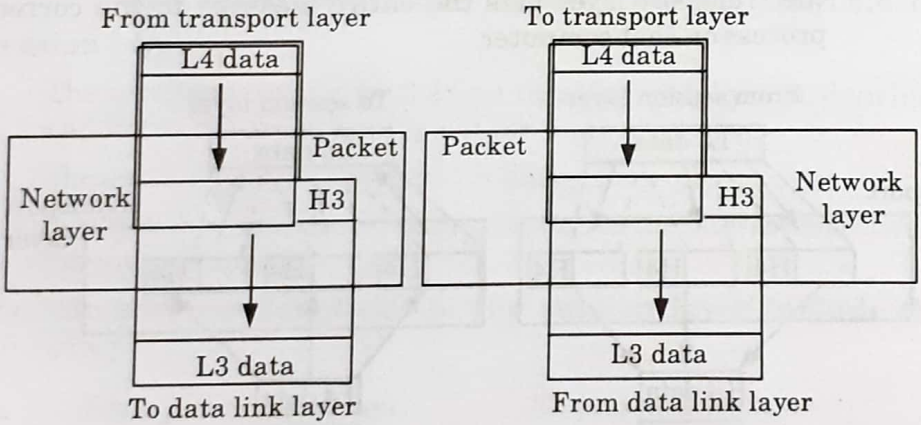


Fig. 1.3.3.

Specific services/functions of the network layer include the following :

i. **Logical addressing :** The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.

ii. **Routing :** When independent networks or links are connected together to create an internetwork (a network of networks) or a large network, the connecting devices (called routers or gateways) route the packets to their final destination.

4. Transport layer :

i. The transport layer is responsible for source-to-destination (end-to-end) delivery of the entire message.

ii. The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

iii. Fig. 1.3.4 shows the relationship of the transport layer to the network and session layers.

iv. For added security, the transport layer may create a connection between the two end ports.

Specific services/functions of the transport layer include the following :

i. Service point addressing :

a. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.

b. The transport layer header therefore must include a type of address called a service-point address (or port address).

c. The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

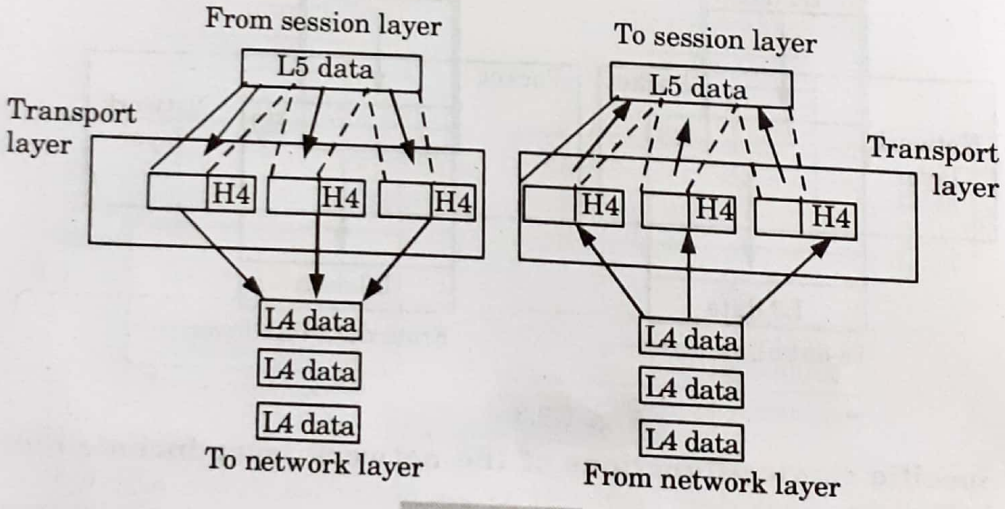


Fig. 1.3.4.

ii. Segmentation and reassembly :

a. A message is divided into transmittable segments, each segment containing a sequence number.

b. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in the transmission.

iii. Conne

a. Th or

b. A in de

c. A th th

d. Af

iv. Flow respon perfor

v. Error

a. E ac

b. T m (d

c. E

5. Session la

i. The se and ne

ii. The se

iii. It estal commu

Specific s following

Fro

Session layer

iii. **Connection control :**

a. The transport can be either connectionless or connection-oriented.

b. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.

c. A connection-oriented transport layer makes a connection with the transport layer at the destination machine before delivering the packets.

d. After all the data are transferred, the connection is terminated.

iv. **Flow control :** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end-to-end rather than across a single link.

v. **Error control :**

a. Error control at this layer is performed end-to-end rather than across a single link.

b. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss or duplication).

c. Error correction is usually achieved through retransmission.

5. Session layer :

i. The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes.

ii. The session layer is the network dialog controller.

iii. It establishes, maintains, and synchronizes the interaction between communicating systems.

Specific services/functions of the session layer include the following :

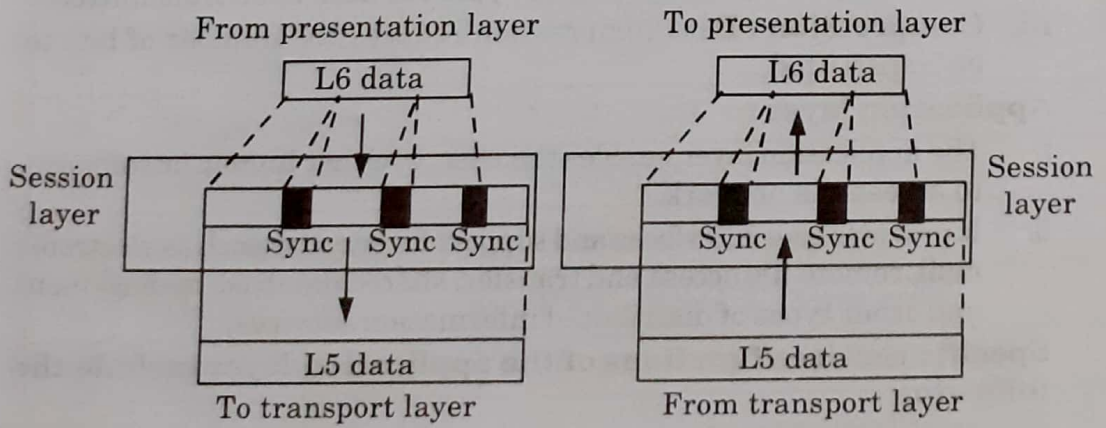


Fig. 1.3.5.

i. **Dialog control :**
   a. The session layer allows two systems to enter into a dialog.
   b. It allows the communication between two processes to take place either in half-duplex (one way at a time) or full-duplex (two ways at a time).

ii. **Synchronization :** The session layer allows a process to add checkpoints (synchronization points) into a stream of data.

6. **Presentation layer :**

i. The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

ii. Fig. 1.3.6 shows the relationship between the presentation layer, application layer and session layer.

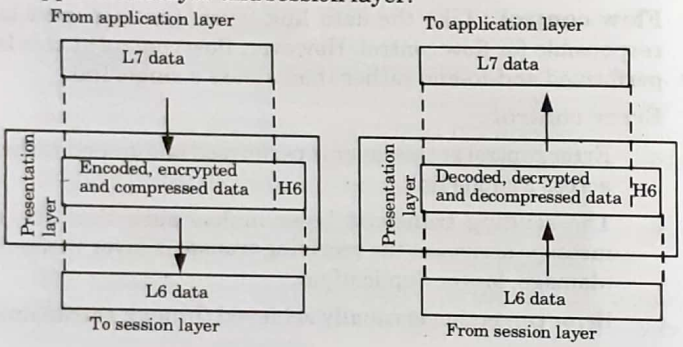


Fig. 1.3.6.

Specific services/functions of the presentation layer include the following :

i. **Translation :** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information should be changed to bit streams before being transmitted.

ii. **Encryption :** To carry sensitive information a system must be able to assure privacy. This layer encrypts the data to be transmitted.

iii. **Compression :** Data compression reduces the number of bits to be transmitted.

7. **Application layer :**

i. The application layer enables the user, whether human or software, to access the network.

ii. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information services.

Specific services/functions of the application layer include the following :

i. **Network virtual terminal :** A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host.

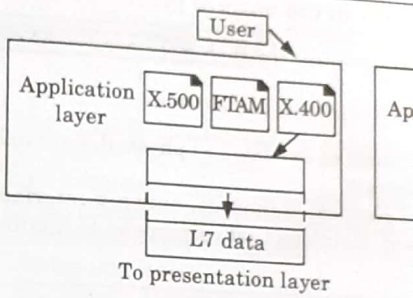


Fig. 1.

ii. **File Transfer, Access and** application allows a user to acces retrieve files from a remote com files in a remote computer.

iii. **Mail services :** This applicatio forwarding and storage.

iv. **Directory services :** This applicat sources and access for global infor services.

Que 1.4. **What is OSI model ? Expl and services of each layer.** AK

Answer

OSI model its function and services : R

Protocols of each layer :

S. No.	Layers	
1.	Application layer	TELNET HTTP, NI
2.	Presentation layer	LLC, MA
3.	Session layer	PSAP, SS
4.	Transport layer	TCP, UD
5.	Network layer	IP (Interr
6.	Data link layer	HDLC, S
7.	Physical layer	RS – 232

Que 1.5. **List the layers in the TCP/**

OR

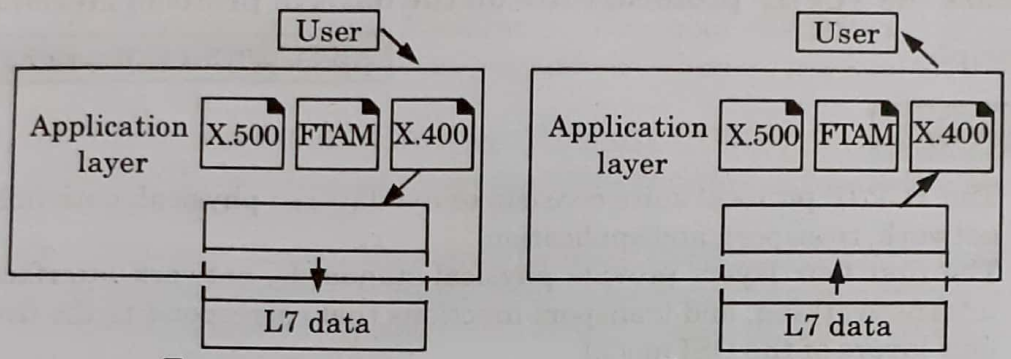


Fig. 1.3.7.

ii. **File Transfer, Access and Management (FTAM) :** This application allows a user to access files in a remote computer, to retrieve files from a remote computer, and to manage or control files in a remote computer.

iii. **Mail services :** This application provides the basis for email forwarding and storage.

iv. **Directory services :** This application provides distributed database sources and access for global information about various objects and services.

Que 1.4. **What is OSI model ? Explain the functions, protocols and services of each layer.** **AKTU 2015-16, 2017-18; Marks 10**

Answer

OSI model its function and services : Refer Q. 1.3, Page 1–4A, Unit-1.

Protocols of each layer :

S. No.	Layers	Protocols
1.	Application layer	TELNET, FTP, SMPTP, DNS HTTP, NNTP
2.	Presentation layer	LLC, MAC
3.	Session layer	PSAP, SSAP
4.	Transport layer	TCP, UDP
5.	Network layer	IP (Internet Protocols)
6.	Data link layer	HDLC, SDLC, X.25 protocols
7.	Physical layer	RS – 232 or RS – 449 standards

Que 1.5. **List the layers in the TCP/IP model.**

OR

Discuss the TCP/IP protocol suite on the basis of protocol layering principle.

AKTU 2013-14, Marks 05

Answer

1. The TCP/IP protocol suite consists of five layers : physical, data link, network, transport, and application.
2. The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model.

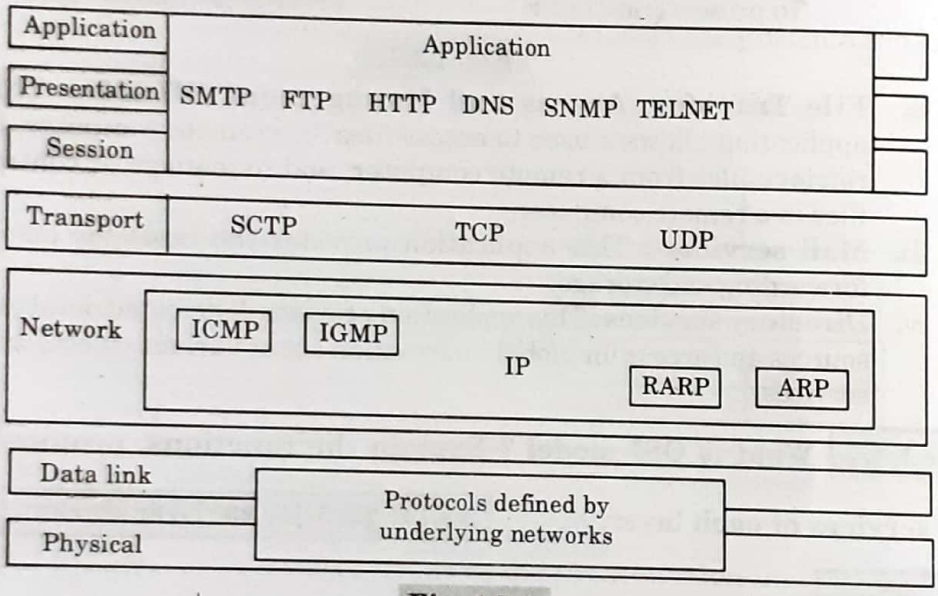


Fig. 1.5.1.

3. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer as shown in Fig. 1.5.1.
4. At the transport layer, TCP/IP defines three protocols : Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).

Layers of TCP/IP model :

1. **Physical and data link layers :**
   a. At the physical and data link layers, TCP/IP does not define any specific protocol.
   b. It supports all of the standard and proprietary protocols.
   c. A network in a TCP/IP internetwork can be a Local Area Network (LAN) or a Wide Area Network (WAN).
2. **Network layer :** At the network layer, TCP/IP uses four supporting protocols : ARP, RARP, ICMP, and IGMP.
   a. **Internet Protocol (IP) :** It is an unreliable and connectionless protocol offering a best effort delivery service.
   b. **Address Resolution Protocol (ARP) :** It is used to associate an IP address with the physical address.

c. **Reverse Address Resolution Protocol (RARP) :** It allows a host to discover its internet address when its physical address is known.

d. **Internet Control Message Protocol (ICMP) :** It is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

e. **Internet Group Message Protocol (IGMP) :** It is used to facilitate the simultaneous transmission of a message to a group of recipients.

3. **Transport layer :** Transport layer is represented in TCP/IP by following three protocols :

   a. **User Datagram Protocol (UDP) :** It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

   b. **Transmission Control Protocol (TCP) :** It provides full transport layer services to applications.

   c. **Stream Control Transmission Protocol (SCTP) :** It provides support for newer applications such as voice over the internet.

4. **Application layer :** Many protocols like Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP), Telnet, etc., are defined at application layer.

Que 1.6. What is the difference between TCP/IP and OSI model ?

Answer

S. No.	TCP/IP model	OSI model
1.	TCP/IP model contains five layers.	OSI model has seven layers.
2.	It does not distinguish between service, interface and protocol.	It distinguishes between service, interface and protocol.
3.	Protocol comes first and description of model later.	Firstly description of model and then protocol came next.
4.	TCP/IP has only one mode in network layer but supports both modes in transport layer.	It supports connectionless and connection-oriented communication in network layer and only connection-oriented communication in transport layer.
5.	Protocols in TCP/IP are not hidden and thus cannot be replaced easily.	Protocols in OSI model are hidden and can be replaced easily.
6.	It is the implemented model.	It is a reference model.

PART-3

Services.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.7. Explain the services offered by layer.

Answer

Two types of services are offered by the layer :

1. **Connection-oriented service :**
   a. The connection-oriented service is similar to the one provided in the telephone system.
   b. The services user of the connection-oriented service undergo the following sequence of operation :
      i. Establish a connection.
      ii. Use the connection.
      iii. Release the connection.
   c. The connection acts like a tube. The sender pushes bits from one end of the tube and the receiver takes them out from the outer end.
   d. The order is generally preserved. That means the order in which the bits are sent is same as the order in which they are received.
   e. Sometimes after establishing a connection, the sender and receiver can discuss and negotiate about parameters to be used such as maximum message size, quality of service and some other issues.
2. **Connectionless service :**
   a. The connectionless service is similar to the postal service.
   b. Each message (analogous to a letter) carries the full address of the destination. Each message is routed independently from source to destination through the system.
   c. It is possible that the order in which the messages are sent and the order in which they are received may be different.

Que 1.8. What do you mean by service primitives ?

AKTU 2014-15, Marks 05

Answer

1. A service is specified by a set of primitives available to a user process to access the service.
2. These primitives tell the service to perform some action or report on an action taken by a peer entity.
3. The primitives for connection-oriented service are different from the connectionless service.
4. The five different service primitives for implementing a simple connection-oriented service are :
   a. **Listen :** The server executes LISTEN to indicate that it is prepared to accept the incoming connection.
   b. **Connect :** The client executes a CONNECT call to establish the connection with the server and also specify the address.
   c. **Receive :** The server executes RECEIVE to prepare the first request. This call blocks the server.
   d. **Send :** The client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply.
   e. **Disconnect :** The client use DISCONNECT to end the connection.

PART-4

Network Topology : Delay Analysis.

CONCEPT OUTLINE

- Different types of delay are :
  i. Processing delay
  ii. Queueing delay
  iii. Transmission delay
  iv. Propagation delay

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.9. What do you mean by topology ? Explain in brief any three such network topologies.

OR

Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.

AKTU 2016-17, 2017-18; Marks 10

OR

Define topology and explain the advantage and disadvantage of bus, star and ring topologies.

AKTU 2013-14, Marks 05

Answer

Network topology is the arrangement of the various elements of a communication network. Network topology is a topological structure of network and may be depicted physically or logically.

Some network topologies are as follows :

1. Bus topology :

i. In a bus topology, all stations are attached to the same cable.
ii. In the bus network, messages are sent in both directions from a single point.
iii. In a bus topology, signals are broadcasted to all stations.
iv. Each computer checks the address on the signal (data frame) as it passes along the bus.
v. If the signal's address matches that of the computer, the computer processes the signal. If the address does not match, the computer takes no action and the signal travels on down the bus.

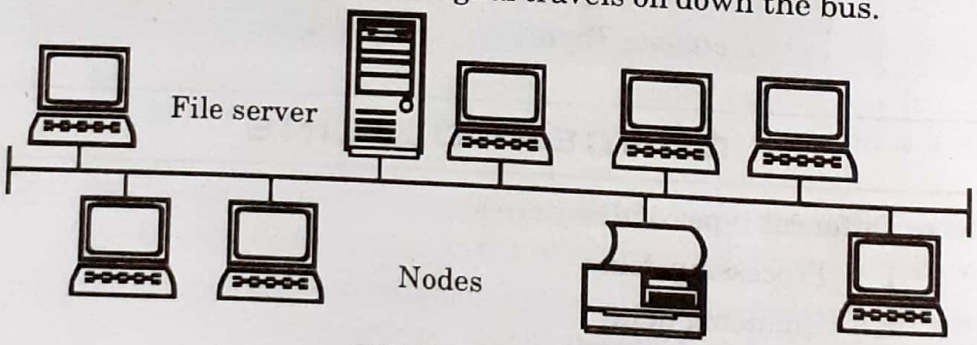


Fig. 1.9.1.

Advantages of bus topology are :

i. Bus topologies are relatively easy to install.
ii. It requires less cable length.
iii. It is simple and easy to implement and extend.

Disadvantages of bus topology are :

i. Maintenance costs may be higher in the long run.
ii. More expensive cabling.

2. Star topology :

i. In a star network, all the nodes (PCs, printers and peripherals) are connected to the central server.

ii. It has a central connection point, like a hub or switch.

iii. A star topology is designed with each node connected directly to a central network as shown in Fig. 1.9.2.

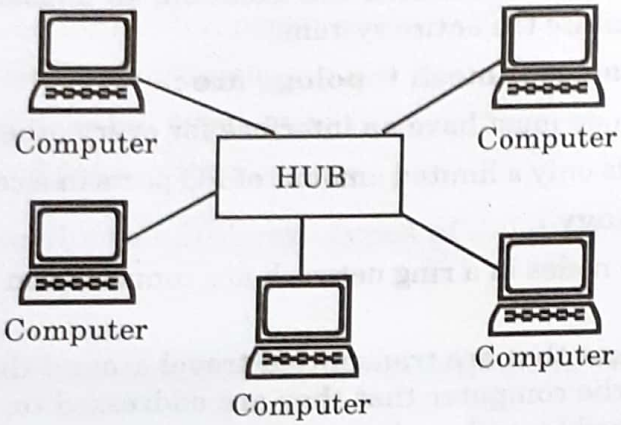


Fig. 1.9.2. Star topology.

Advantages of star topology are :

i. Easy to install and wire.

ii. It can accommodate different wiring.

Disadvantages of star topology are :

i. Star networks can require more cable length than a linear topology.

ii. More expensive cabling.

3. Mesh topology :

i. In a mesh topology, every device has a dedicated point-to-point link to every other device.

ii. Such a network is called complete because between any two devices there is a special link and no any non-redundant links can be added to mesh network.

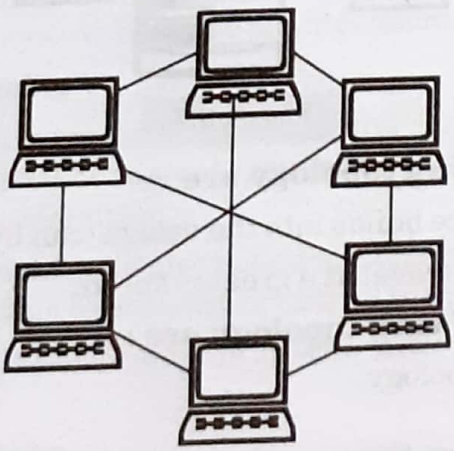


Fig. 1.9.3.

iii. In mesh topology, if we have to connect 'n' computers then we need of $n^*(n-1)/2$ cables and each computer must have $(n-1)$ Ethernet cards.

Advantages of mesh topology are :

i. Redundant links between devices.

ii. Easy fault identification and isolation, an unusable link does not incapacitate the entire system.

Disadvantages of mesh topology are :

i. Each node must have an interface for every other device.

ii. There is only a limited amount of I/O ports in a computer.

4. Ring topology :

i. All the nodes in a ring network are connected in a closed circle of cable.

ii. Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node.

iii. In a ring network, every device has exactly two neighbours for communication purposes.

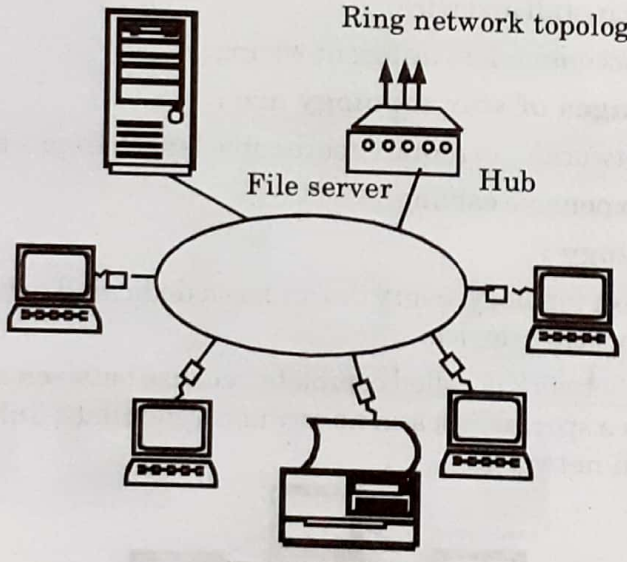


Fig. 1.9.4.

Advantages of ring topology are :

i. Fault tolerance builds into the design (can bypass damaged nodes).

ii. Data packets travel at a greater speed.

Disadvantage of ring topology are :

i. Expensive topology.

Que 1.10. What are the number of cable links required for *n* devices connected in mesh, ring, bus and star topology ?

AKTU 2014-15, Marks 05

Answer

For n connected device,

Cable link required for mesh topology = $n(n-1)/2$

Cable link required for ring topology = n

Cable link required for bus topology = $n-1$

Cable link required for star topology = n

Que 1.11. Describe the different types of delay in network.

Answer

In a packet switched network, the packets undergo different types of delays, such as :

1. **Processing delay :**
   a. A packet consists of a header and a data fields as shown in Fig. 1.11.1. The header contains the destination address.
   b. The time required to examine the packet header and determine where to direct the packet is a part of the processing delay.
   c. The processing delay is of the order of microseconds or less.

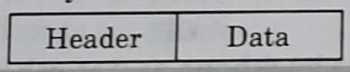


Fig. 1.11.1. Format of a packet.

2. **Queueing delay :**
   a. At the queue, the packet experiences a queueing delay, when they wait to transmit on the links.
   b. The queueing delay depends on the number of packets arrived earlier in the queue.
   c. Queueing delays can be of the order of microseconds or milliseconds.
3. **Transmission delay :**
   a. The packets are transmitted on the first come first served basis. So a particular packet can get transmitted only after all the earlier packets are transmitted.
   b. Transmission delay is also called as store and forward delay. It is the time required to push (transmit) all the packet bits into the link.
   c. The transmission delay is of the order of microseconds or milliseconds.
4. **Propagation delay :**
   a. The time required for the packet bits to reach from the beginning of the link to the desired router is called as propagation delay.
   b. Propagation delay is the ratio of the distance to be travelled by the signal to the speed of propagation.

c. The propagation delays are of the order of few milliseconds.

PART-5

Backbone Design.

CONCEPT OUTLINE

- Two architecture of backbone design are :
  i. Star backbone
  ii. Bus backbone

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.12. Discuss backbone LAN. Explain different types of backbone LAN.

OR

Explain briefly the bus backbone and star backbone.

AKTU 2013-14, Marks 05

Answer

1. The alternative of using a single LAN is to use low cost low capacity LANs in each building or department and then to interconnect all these LANs with a higher capacity LAN. Such a network is called as the backbone LAN.
2. The backbone network allows several LANs to be interconnected.
3. In the backbone network no station is directly connected to the backbone, instead each station is a part of LAN, and the LANs are connected to backbone.
4. The backbone itself is a LAN. It uses a LAN protocol such as Ethernet. So each connection to the backbone is itself another LAN.
5. The two very commonly used architectures are :

   a. Bus backbone :

   i. In a bus backbone, the backbone of topology is a bus.

   ii. Bus backbones are normally used as a distribution backbone to connect different buildings in an organization.

   iii. Each building can comprise either a single LAN or another backbone (normally a star backbone).

iv. The backbone itself can use one of the protocols that support a bus topology such as 10Base5 or 10Base2.

v. A good example of a bus backbone is one that connects single or multiple-floor buildings on a campus.

vi. Each single-floor building usually has a single LAN.

vii. Each multiple-floor building has a backbone (usually a star) that connects each LAN on a floor.

b. Star backbone :

i. In a star backbone, sometimes called a collapsed or switched backbone, the backbone of topology is a star.

ii. In this configuration, the backbone is just one switch that connects the LANs.

iii. Star backbones are mostly used as a distribution backbone inside a building.

iv. In a multi-floor building, we usually find one LAN that serves each particular floor.

v. A star backbone connects these LANs.

vi. The backbone network, which is just a switch, can be installed in the basement or the first floor, and separate cables can run from the switch to each LAN.

vii. If the individual LANs have a physical star topology, then either the hubs (or switches) can be installed in a close to the corresponding floor, or all can be installed close to the switch.

PART-6

Local Access Network Design.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.13. Discuss local access network. What are the different types of access network ?

Answer

Local access networks :

a. The access network is defined as the physical link which connects an end system to its edge router. An edge router is the first router met while travelling from one end system to the other.

b. The access network thus provides the infrastructure to connect the customers in a network.

c. The access network technology is closely tied to the physical media technology, such as optical fibers, coaxial cables, twisted pair line, RF links etc.

Different types of access network are :

i. Residential access :

1. The residential access refers to connecting a home end system to an edge router.
2. Access network is simply a pair of modems along with a point dial up line.
3. There are two types of broadband residential access :
   a. Digital Subscriber Line (DSL)
   b. Hybrid Fiber-coaxial Cable (HFC).
4. The DSL uses Frequency Division Multiplexing (FDM), where as HFC requires a special type of modem called cable modem.

ii. Company access network :

1. In companies or on the university campus, the LANs are used for connecting an end system to the edge router.

   Out of many technologies, the ethernet technology is used for network.
3. It operates at 10 Mbps or 100 Mbps or 1 Gbps and uses either twisted pair copper wire or coaxial cable for connecting a number of end systems with each other and with the edge router.
4. Like HFC, the Ethernet also uses a shared medium (coaxial plus optical fiber cable).

iii. Wireless access :

1. In a wireless LAN, the wireless users will transmit and receive packets to and from the base stations (also called as wireless access point) which is stationed within a radius of a few meters.
2. The IEEE standard had to work in two different modes :
   a. **In the presence of a base station :** In the network with base station, all the communication is passed through the base station. The Base Station (BS) is also called as the Access Point (AP) in 802.11 terminology.
   b. **In the absence of base station :** In the network without base station, the computers will communicate among each other. This mode is also called as adhoc networking.

PART-7

Physical Layer Transmission Media.

CONCEPT OUTLINE

- Transmission medium is a physical path between transmitter and receiver in a data transmission system.
- Transmission media can be classified as :
  i. Guided media
  ii. Unguided media

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.14. **What do you mean by transmission media ? Discuss the types of transmission media.**

OR

Discuss the different physical layer transmission media.

AKTU 2017-18, Marks 10

AKTU 2014-15, Marks 05

Answer

Transmission media is a pathway that carries the information from sender to receiver.

1. We use different types of cables or waves to transmit data.
2. Data is transmitted normally through electrical or electromagnetic signals.
3. An electrical signal is in the form of current.
4. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies.
5. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum.
6. Different media have different properties like bandwidth, delay, cost and ease of installation and maintenance.
7. Transmission media is also called communication channel.

Types of transmission media are :

1. **Wired or guided media or bound transmission media :**
   a. Guided transmission media are the cables that are tangible or have physical existence and are limited by the physical geography.
   b. Popular guided transmission media in use are twisted pair cable, co-axial cable and optical fiber cable.
   c. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.
2. **Wireless or unguided media or unbound transmission media :**
   a. Unguided transmission media are the ways of transmitting data without using any cables.
   b. These media are not bounded by physical geography.
   c. This type of transmission is called wireless communication.
   d. This transmission uses microwave, radiowave, infrared which are some of popular unguided transmission media.

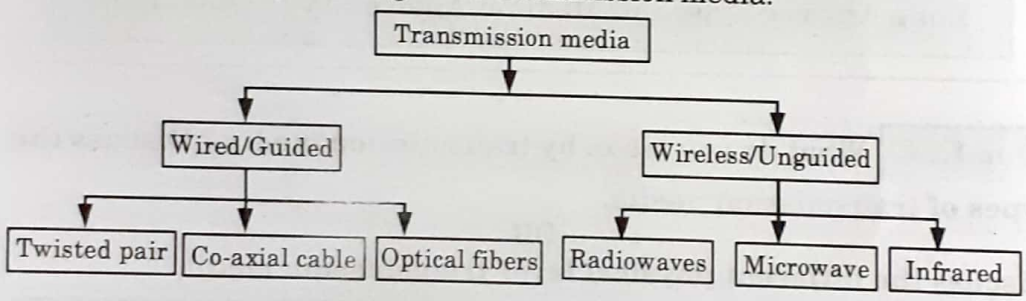


Fig. 1.14.1.

Que 1.15. Write a short note on following :

a. Twisted pair cable
b. Co-axial cable
c. Optical fiber cable

OR

What are the different types of guided media ?

Answer

a. Twisted pair cable :

Fig. 1.15.1. Twisted pair cable

i. The wires are twisted together in pairs.
ii. Each pair would consist of wire used for the positive data signal and a wire used for the negative data signal. Any noise that appears on positive/negative wire of the pair would occur on the other wire.

iii. Because the wires are opposite polarities, they are 180 degrees out of phase (180 degree phases or definition of opposite polarity) when the noise appears on both wires, it cancels or nulls itself out at the receiving used.

iv. Twisted pair cables are most effectively used in a system that uses a balanced line method of transmission.

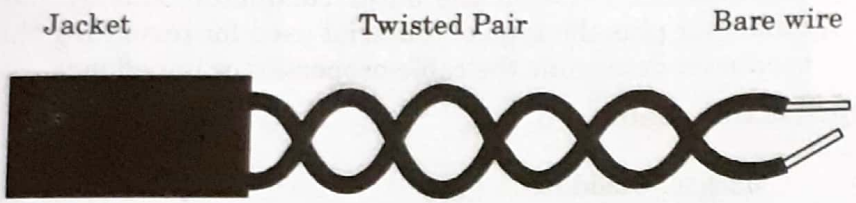


Fig. 1.15.2. Unshielded twisted pair cable.

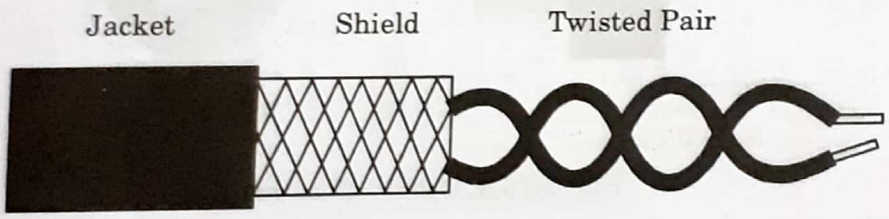


Fig. 1.15.3. Shielded twisted pair cable.

v. Cables with the shield are called shielded twisted pair and commonly abbreviated STP.

vi. Cables without a shield are called unshielded twisted pair or UTP.

vii. Twisting the wires together results in characteristics impedance for the cable.

viii. UTP or unshielded twisted pair cable is used on Ethernet.

ix. UTP cables are used for Ethernet cabling where four twisted pair cables (a total of 8 wires are used).

b. Co-axial cable :

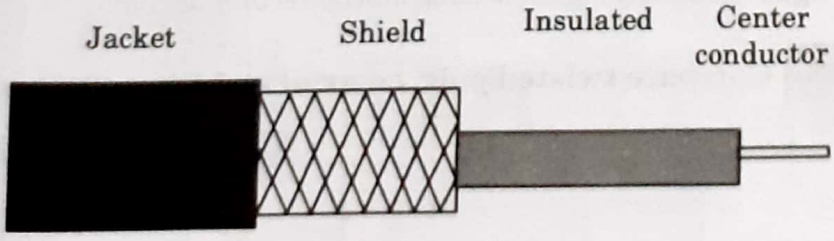


Fig. 1.15.4. Co-axial cable.

i. Co-axial cable consists of two conductors.

ii. The inner conductor is contained inside the insulator with the other conductor weaves around it providing a shield.

iii. An insulating protective coating called a jacket covers the outer conductor.

iv. The outer shield protects the inner conductor from outside electrical signals.

v. The distance between the outer conductor (shield) and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties or impedance.

c. Optical fiber cable :

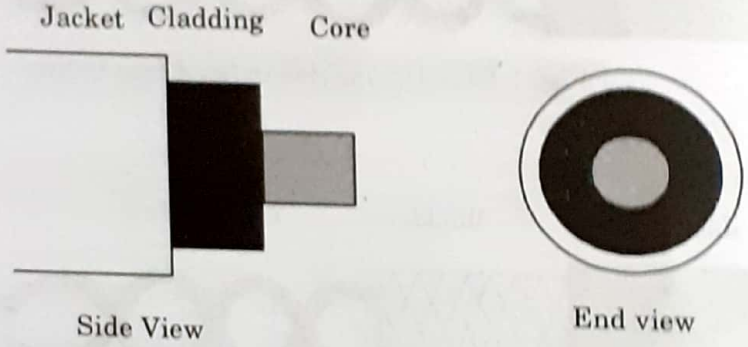


Fig. 1.15.5. Optical fiber cable.

i. Optical fiber consists of thin glass fiber that can carry information at frequencies in the visible light spectrum.

ii. The typical optical fiber consists of a very narrow strand of glass called the cladding.

iii. A typical core diameter is 62.5 microns.

iv. Typically cladding has a diameter of 125 minors. Coating the cladding is a protective coating consisting of plastic, it is called the jacket.

v. The device generating the message has it in electromagnetic form (electrical signal); this has to be converted into light (*i.e.*, optical signal) to send it on optical fiber cable. The process of converting light to electric signal is done on the receiving side.

Que 1.16. Compare twisted pair, co-axial and fiber optic cable.

AKTU 2013-14, Marks 05

Answer

S.No.	Characteristic	Twisted pair cable	Co-axial cable	Optical fiber cable
1.	Signal transmission	Takes place in the electrical form over the metallic conducting wires	Takes place in the electrical form over the inner conductor of cable	Takes place in an optical form over a glass fiber
2.	Noise immunity	Low	Higher	Highest
3.	External magnetic field	Affected due to external magnetic field	Less affected	Not affected
4.	Bandwidth	Low bandwidth	Moderately high	Very high
5.	Attenuation	Very high	Low	Very low
6.	Cause of power loss	Power loss due to conduction and radiation	Power loss due to conduction	Power loss due to absorption, scattering and bending
7.	Installation	Easy	Fairly easy	Difficult
8.	Cost	Cheapest	Moderately expensive	Expensive
9.	Data rate	Support low data rate	Moderately high data rate	Very high data rate
10.	Electromagnetic interference (EMI)	EMI can take place	EMI is reduced to shielding	EMI is not present

PART-8

Switching Method.

CONCEPT OUTLINE

- The three basic methods of switching are :
  i. Circuit switching
  ii. Packet switching
  iii. Message switching

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.17. Explain the types of switching.

OR

Explain the various types of switching methods with suitable examples.

AKTU 2013-14, Marks 05

Answer

Types of switching :

A. Circuit switching :

1. Circuit switching is a transfer mode of a network that involves setting up a dedicated end-to-end connection.
2. In circuit switching, the routing decision is made when the path is set up across the network.
3. After the link has been set between the sender and receiver, the information is forwarded continuously over the link. After the link has been set up no additional address information about the receiver or destination machine is required.
4. In circuit switching, a dedicated path is established between the sender and the receiver which is maintained for the entire duration of conversion, as shown in Fig. 1.17.1.

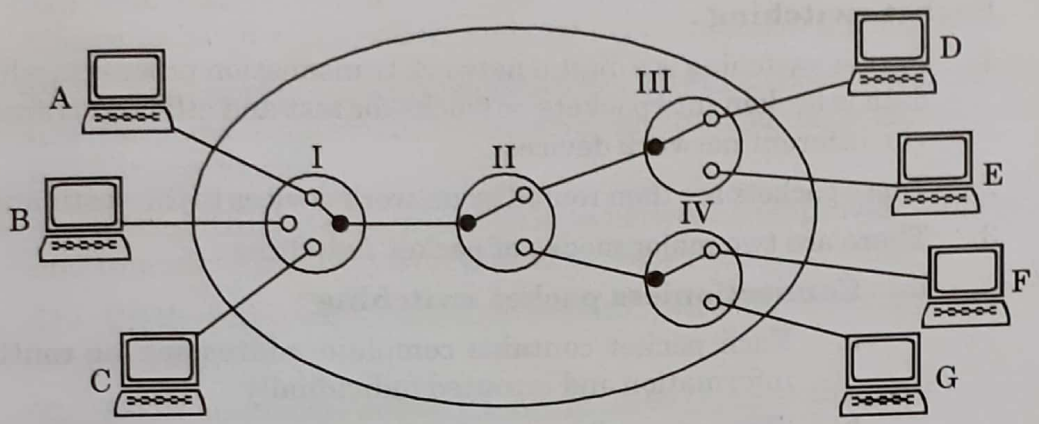


Fig. 1.17.1.

5. I, II, III and IV are the circuit switches or nodes. Nodes I, III, and IV are connected to the communicating devices while II is only routing node.
6. In telephone systems, circuit switching is used.

B. Message switching :

1. Message switching does not establish a dedicated path between two communicating devices.
2. In message switching, each message is treated as an independent unit and includes its own destination and source address.
3. In message switching, each complete message is then transmitted from device to device through the internetwork as shown in Fig. 1.17.2.
4. In message switching, each intermediate device receives the message, stores it, until the next device is ready to receive it and then forwards it to the next device. For this reason, a message switching network is sometimes called as a store and forward network.

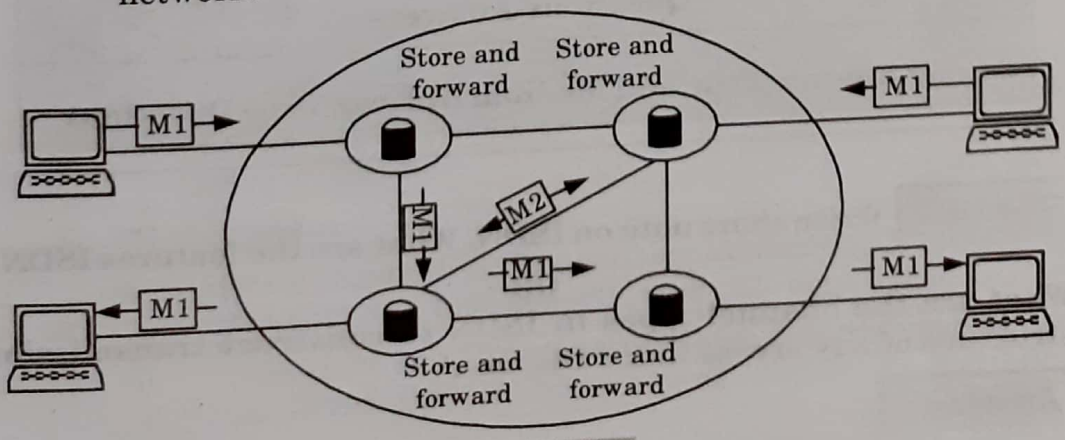


Fig. 1.17.2.

C. Packet switching :

1. Packet switching is a digital network transmission process in which data is broken into packets or blocks for fast and efficient transfer via different network devices.
2. These packets are then routed by network devices to the destination.
3. There are two major modes of packet switching :

i. Connectionless packet switching :

a. Each packet contains complete addressing or routing information and is routed individually.

b. This can result in out-of-order delivery and different paths of transmission, depending on the variable loads on different network nodes (adapters, switches and routers) at any given time.

c. After reaching the destination through different routes, the packets are rearranged to form the original message.

ii. Connection-oriented packet switching :

a. Data packets are sent sequentially over a predefined route.

b. Packets are assembled, given a sequence number and then transported over the network to a destination in order.

c. In this mode, address information is not required. This is also known as virtual circuit switching.

PART-9

ISDN, Terminal Handling.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.18. Write short note on ISDN. What are the features ISDN ?

OR

What are the channel types in ISDN to construct transmission structure of any access link ? Discuss.

Answer

1. Integrated Services Digital Network (ISDN) is a set of protocols that combines digital telephony and data transport services.

2. The whole idea is to digitize the telephone network to permit the transmission of audio, video, and text over existing telephone lines.
3. ISDN is an effort to standardize subscriber services, provide user/network interfaces and facilitate the internetworking capabilities of existing voice and data networks.
4. The goal of ISDN is to form a wide area network that provides universal end-to-end connectivity over digital media.
5. The ISDN integrates customer services with the integrated digital networking.
6. The ISDN standards define following three types of channels :

i. B channels :

a. A bearer channel (B channel) is defined at a rate of 64 kbps.

b. It is the basic user channel and can carry any type of digital information in full-duplex mode as long as the required transmission rate does not exceed 64 kbps.

c. For example, a B channel can be used to carry digital data, digitized voice or other low data-rate information.

d. Several transmissions can be accommodated at once if the signals are multiplexed first.

ii. D channels :

a. A data channel (D channel) can be either 16 or 64 kbps, depending on the needs of the user. Although the name says data, the primary function of a D channel is to carry control signaling for the B channels.

b. Control information (such as call establishment, ringing, call interrupt, or synchronization) is carried by the same channel that carries the message data.

c. The ISDN separates control signals onto a channel of their own, the D channel.

d. A D channel carries the control signaling for all of the channels in a given path, using a method called common-channel (out-of-band) signaling.

iii. H channels :

a. Hybrid channels (H Channels) are available with data rates of 384 kbps (H0), 1536 kbps (H11) or 1920 kbps (H12).

b. These rates suit H channels for high data-rate applications such as video, teleconferencing and so on.

Salient features of ISDN :

i. The ISDN is supported by a wide range of voice and non-voice applications of the same networks.

ii. It provides a range of services using a limited set of connections and multipurpose user-network interface arrangements.

iii. It supports a variety of applications that include both switched and non switched connections. The switched connection, include both circuit switched and packet switched connections.

iv. ISDN contains intelligence for providing service feature, maintenance and network management.

Que 1.19. Explain the user access in ISDN.

AKTU 2013-14, Marks 05

Answer

1. ISDN user access is done by devices that enables the user to access the service of Basic Rate Interface (BRI) or Primary Rate Interface (PRI) are described by their functional duties.
2. Functional duties are divided into two groups :
   a. **Functional grouping :** Functional grouping is a model that can be implemented using devices or equipment chosen by subscriber (user).
   b. **Reference points :** Reference point corresponds to conceptual points used in order to separate groups of functions.
3. The architecture on the subscriber premises is divided into small groups. Such a grouping is done on the basis of the functions and the groups are separated by reference points.

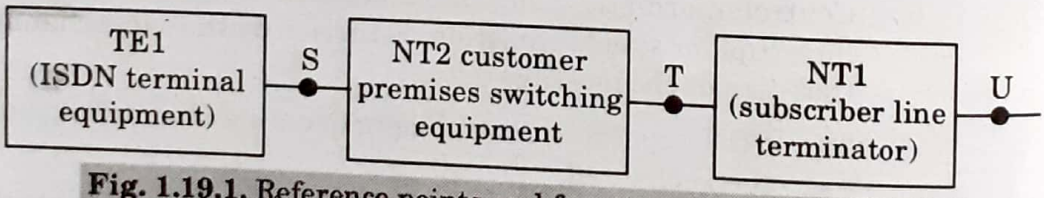


Fig. 1.19.1. Reference points and functional grouping in ISDN.

4. NT1 is the network termination which includes the functions associated with the physical and electrical termination of the ISDN on the user's premises which correspond to layer 1 of OSI.
5. NT2 is a customer premises switching equipment and it is an intelligent device which performs switching and concentration functions.
6. TE1 is the device which supports the standard ISDN interface.

Que 1.20. Write a short note on terminal handling.

Answer

1. A computer terminal is an electronic or electromechanical hardware device that is used for entering data into, and displaying data from, a computer or a computing system.
2. The function of a terminal is confined to display and input of data; a device with significant local programmable data processing capability may be called a "smart terminal" or fat client.
3. A terminal that depends on the host computer for its processing power is called a dumb terminal or thin client.
4. A personal computer can run software that emulates the function of a terminal, sometimes allowing concurrent use of local programs and access to a distant terminal host system.

Que 1.21. Differentiate between bit rate and baud rate. A modem constellation diagram has data point at coordinates : (1, 1), (1, –1), (–1, 1) and (–1, –1). How many bps can a modem with these parameters achieve at 1200 baud ? State two reason for using layered protocols. **AKTU 2014-15, Marks 05**

Answer

Basis for comparison	Bit rate	Baud rate
Basic	Bit rate is the number of bits per second.	Baud rate is the number of signal units per second.
Meaning	It determines the number of bits travelled per second.	It determines how many times the state of a signal is changing.
Term usually used	While the emphasis is on computer efficiency.	While data transmission over the channel is more concerned.
Bandwidth determination	Cannot determine the bandwidth.	It can determine how much bandwidth is required to send the signal.
Equation	Bit rate = baud rate × the number of bits per signal unit	Baud rate = bit rate / the number of bits per signal unit

Numerical :

Since there are four legal values per band. Therefore, bit rate is twice of baud rate. At 1200 baud, the data rate will be

$$= 2 \times 1200 = 2400 \text{ bps}$$

The two reasons for using layered protocols are :

a. It breaks up the design problem into smaller and more manageable pieces.

b. Protocols can be changed easily without affecting higher or lower layers.

Que 1.22. Calculate the required bandwidth, if in a communication channel the signal power is 10W, and the information transmission rate is 10 kbps.

AKTU 2014-15, Marks 05

Answer

$$R = 10 \text{ kbps}$$
$$S = 10 \text{ W}$$
$$R = B \log_2 \left[1 + \frac{S}{N}\right]$$

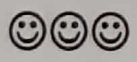
Since N is not given so bandwidth cannot be calculated.

Que 1.23. It is required to transmit a data at a rate of 64 kbps over a 3 kHz telephone channel. What is the minimum SNR required to accomplish this ?

AKTU 2014-15, Marks 05

Answer

$$R = 64 \text{ kbps} = 64 \times 1000 \text{ bps}$$
$$B = 3 \text{ kHz} = 3000 \text{ Hz}$$
$$R = B \log_2 \left[1 + \frac{S}{N}\right]$$
$$\log_2 \left[1 + \frac{S}{N}\right] = \frac{64 \times 1000}{3000} = \frac{64}{3}$$
$$1 + \frac{S}{N} = 2^{64/3}$$
$$\frac{S}{N} = 2^{64/3} - 1 \approx 2^{64/3} \text{ dB}$$



2
UNIT

Medium Access Sub Layer

CONTENTS

Part-1	:	Medium Access Sub Layer – Channel Allocations	**2–2A to 2–7A**
Part-2	:	LAN Protocols – ALOHA Protocols	**2–8A to 2–11A**
Part-3	:	Overview of IEEE Standards – FDDI	**2–11A to 2–15A**
Part-4	:	Data Link Layer – Elementary Data Link Protocols	**2–15A to 2–17A**
Part-5	:	Sliding Window Protocols	**2–17A to 2–27A**
Part-6	:	Error Handling	**2–27A to 2–36A**

PART-1

Medium Access Sub Layer – Channel Allocations.

CONCEPT OUTLINE

- Two different schemes used for channel allocation are :
  i. Static channel allocation
  ii. Dynamic channel allocation
- Types of CSMA are :
  i. Non-persistent CSMA
  ii. 1-persistent CSMA
  iii. P-persistent CSMA

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.1. Explain medium access control sublayer.

Answer

1. The MAC sublayer is very important in LANs because it is a broadcast network. Fig. 2.1.1, show the position of MAC sublayer.

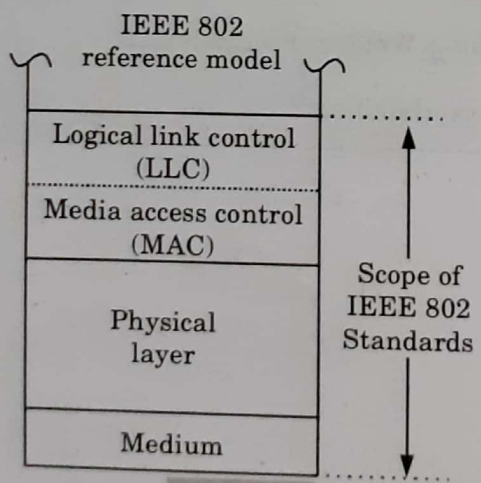


Fig. 2.1.1.

2. It is called as IEEE 802 reference model.

Functions of Media Access Control (MAC) sublayer :

1. To perform the control of access to media.
2. It performs the unique addressing to stations directly connected to LAN.

3. Detection of errors.

Functions of Logical

1. Error recovery.
2. It performs the flow
3. User addressing.

Que 2.2. Explain ch
schemes used for char

Answer

1. In a broadcast netw
allocated to one tran
to this medium shoul
2. There are two differe
   a. **Static channel**
      i. The traditio
      users is by
      ii. In these me
      slot is allott
      bandwidth
      iii. The Frequen
      Multiplexing
   b. **Dynamic chann**
      i. In this meth
      allotted to th
      their require
      ii. Following as
      this method :
         1. **Station**
         stations
         frames f
         2. **Single**
         commun
         3. **Collisio**
         two or m
         resulting
         4. **Continu**
         used to d
         can begin
         For a slo
         slots.

3. Detection of errors.

Functions of Logical Link Control (LLC) sublayer :

1. Error recovery.
2. It performs the flow control operations.
3. User addressing.

Que 2.2. Explain channel allocation. What are the two different schemes used for channel allocation ?

Answer

1. In a broadcast network, the single communication channel is to be allocated to one transmitting user at a time. The other users connected to this medium should wait. This is called as channel allocation.
2. There are two different schemes used for channel allocation :
   - **a. Static channel allocation :**
     - i. The traditional way of allocating a single channel, among many users is by means of Frequency Division Multiplexing (FDM).
     - ii. In these methods either a fixed frequency band or a fixed time slot is allotted to each user. Thus either the entire available bandwidth or entire time is shared.
     - iii. The Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are the example of static channel allocation.
   - **b. Dynamic channel allocation :**
     - i. In this method neither a fixed frequency nor fixed time is allotted to the user. The user can use the single channel as per their requirements.
     - ii. Following assumptions are made for the implementation of this method :
       1. **Station model :** This model consists of N independent stations such as a PC, computer etc. which can generate frames for transmission.
       2. **Single channel :** A single channel is available for all communication.
       3. **Collision :** If frames are transmitted at the same time by two or more stations, there is an overlap in time and the resulting signal is disconnected. This is called as collision.
       4. **Continuous or slotted time :** There is no master clock used to divide time into discrete time intervals. So, frames can begin at any random instant. This is continuous time. For a slotted time, the time is divided into discrete time slots.

5. **Carrier or no carrier sense :** Stations sense the channel before transmission or they directly transmit without sensing the channel.

Que 2.3. **Write a short note on random access.**

Answer

1. In the random access technique, there is no control station.
2. Each station will have the right to use the common medium without any control over it.
3. With increase in number of stations, there is an increased probability of collision or access conflict.
4. The collisions will occur when more than one user tries to access the common medium simultaneously.
5. As a result of such collisions some frames can be either modified (due to errors) or destroyed.
6. In order to avoid collisions, we have to set up a procedure like CSMA/CD and CSMA/CA.

Que 2.4. **Explain Carrier Sense Multiple Access (CSMA) protocol.**

OR

Discuss different carrier sense protocols. How are they different than collision protocols ? **AKTU 2014-15, Marks 05**

AKTU 2017-18, Marks 10

Answer

The CSMA protocol operates on the principle of carrier sensing. In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Different carrier sense protocols are :

1. **CSMA/CA :**
   a. Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is a network contention protocol used for carrier transmission in networks using the 802.11 standard.
   b. CSMA/CA works to avoid collisions prior to their occurrence.
2. **CSMA/CD :**
   a. Carrier Sense Multiple Access / Collision Detection is a set of rules which determine how network devices respond when two devices attempt to use a data channel simultaneously.
   b. CSMA/CD protocol works to handles transmissions only after a collision has taken place.

CSMA is different from collisio
for the channel without any
performance.

Que 2.5. **Explain the con**

Answer

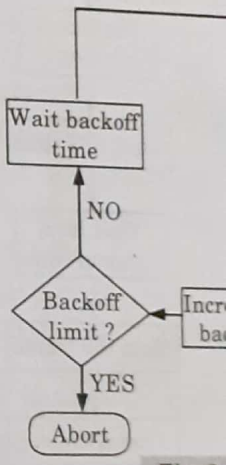


Fig. 2.

Explanation :

1. The station having ready
2. Then it senses the line u
3. It then sends the frame, i to one complete frame, t
4. Otherwise (in the event inform the other station
5. The station then increm backoff time and sends t
6. If the backoff has rea transmission.
7. CSMA/CD is used for th

Que 2.6. **Discribe CSM**

Write a short note on coll

CSMA is different from collision free protocol as it resolves the contention for the channel without any collision and does not affect the system performance.

Que 2.5. Explain the concept of CSMA/CD.

Answer

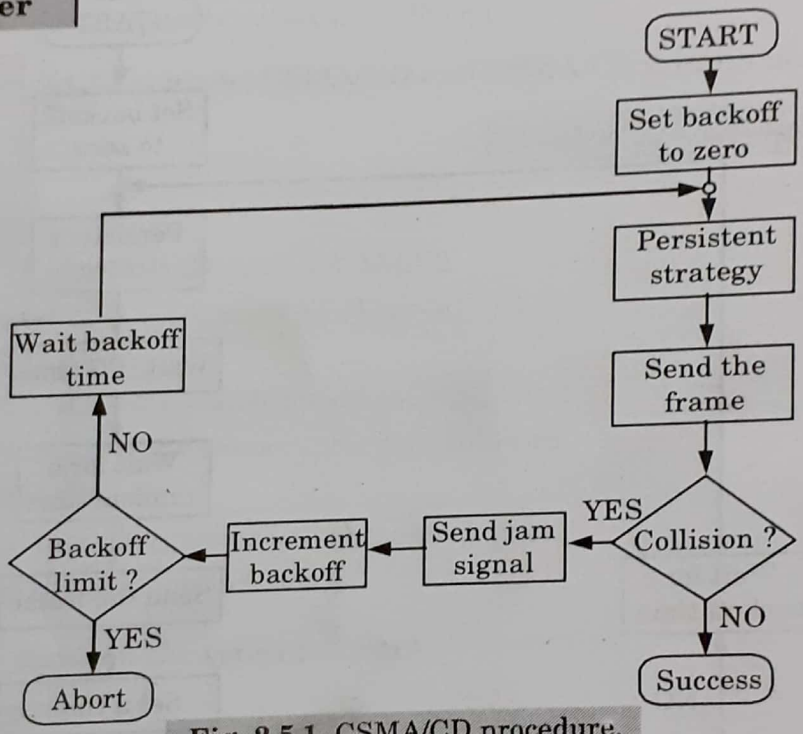


Fig. 2.5.1. CSMA/CD procedure.

Explanation :

1. The station having ready frame sets the backoff parameter to zero.
2. Then it senses the line using one of the persistent strategies.
3. It then sends the frame, if there is no collision for a period corresponding to one complete frame, then the transmission is successful.
4. Otherwise (in the event of collision) the station sends the jam signal to inform the other stations about the collision.
5. The station then increments the backoff time and waits for a random backoff time and sends the frame again.
6. If the backoff has reached its limit then the station aborts the transmission.
7. CSMA/CD is used for the traditional Ethernet.

Que 2.6. Discribe CSMA / CA in brief.

OR

Write a short note on collision avoidance.

AKTU 2014-15, Marks 2.5

Answer

1. The long form of CSMA / CA is CSMA protocol with collision avoidance. Fig. 2.6.1 shows the flow chart explaining the principle of CSMA / CA.

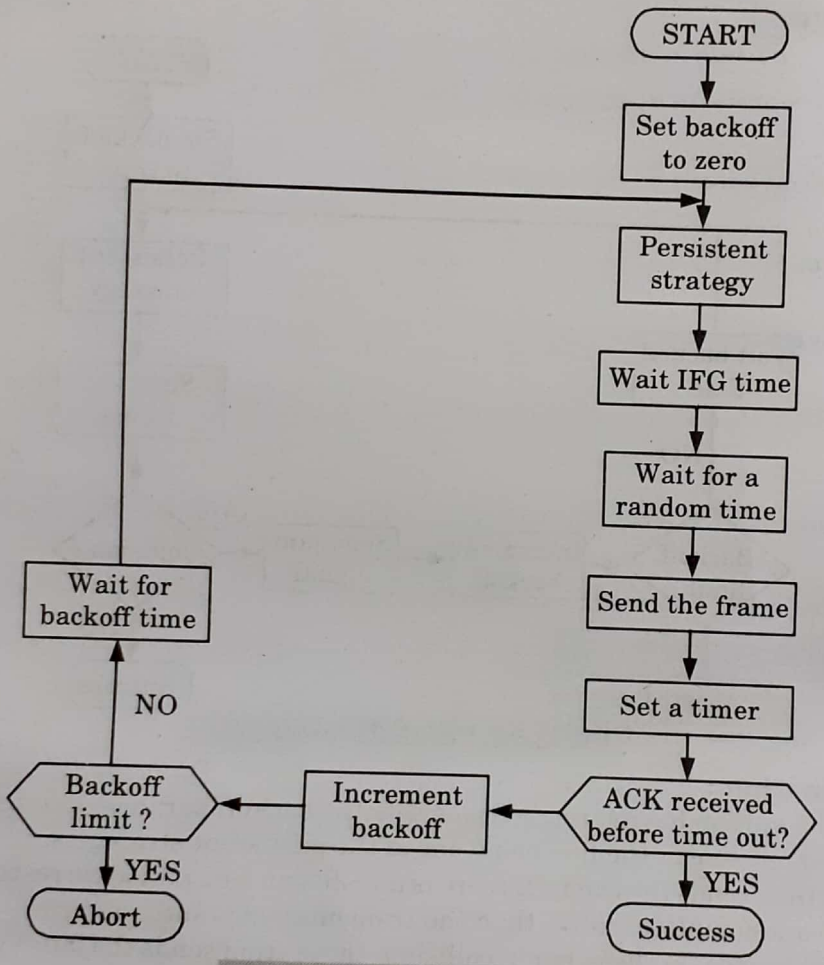


Fig. 2.6.1. CSMA / CA procedure.

2. The station ready to transmit, senses the line by using one of the persistent strategies.
3. As soon as it finds the line to be idle, the station waits for a time equal to an Interframe Gap (IFG).
4. It then waits for some more random time and sends the frame.
5. After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.

6. If the acknowledgeme transmission is succe
7. But if the transmit acknowledgement bef parameter, waits fo CSMA / CA completel

Que 2.7. **Explain abo**

Answer

CSMA/CD : Refer Q. 2.5, P

CSMA/CA : Refer Q. 2.6, P

Uses of CSMA/CD :

1. CSMA/CD is used for t
2. It uses MAC protocol t

Uses of CSMA/CA :

1. It is used to avoid collis
2. It is used in channel uti

Que 2.8. **Explain the t**

Answer

Types of CSMA :

a. Non-persistent CSMA

1. In this scheme, if a that the channel is b will wait for fixed in
2. After this time, it ag channel is free it wi

b. 1-persistent CSMA : In continuously monitors th immediately.

c. P-persistent CSMA :

1. The possibility of suc the p-persistent CSM
2. In this scheme, all th simultaneously as so

6. If the acknowledgement is received before expiry of the time, then the transmission is successful.
7. But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the backoff parameter, waits for the backoff time and senses the line again, CSMA / CA completely avoids the collision.

Que 2.7. Explain about CSMA/CD and CSMA/CA and its uses.

AKTU 2013-14, Marks 05

Answer

CSMA/CD : Refer Q. 2.5, Page 2–5A, Unit-2.

CSMA/CA : Refer Q. 2.6, Page 2–5A, Unit-2.

Uses of CSMA/CD :

1. CSMA/CD is used for traditional Ethernet.
2. It uses MAC protocol to encounter data collision.

Uses of CSMA/CA :

1. It is used to avoid collision between data frames.
2. It is used in channel utilization.

Que 2.8. Explain the types of CSMA.

Answer

Types of CSMA :

a. Non-persistent CSMA :

1. In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
2. After this time, it again checks the status of the channel and if the channel is free it will transmit.

b. 1-persistent CSMA : In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately.

c. P-persistent CSMA :

1. The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA.
2. In this scheme, all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.

PART-2

LAN Protocols – ALOHA Protocols.

CONCEPT OUTLINE

- ALOHA system has two versions :
  i. **Pure ALOHA :** It does not require global time synchronization
  ii. **Slotted ALOHA :** It require time synchronization.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.9. Write a short note on pure ALOHA.

Answer

1. In pure ALOHA, the stations transmit frames whenever they have data to send.
2. When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
3. In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
4. If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
5. If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
6. Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help to avoid more collisions.

Assumption for analysis :

1. All frames are of the same size/length to maximize the output.
2. Packet transmission time is the unit time.
3. The number of packets successfully transmitted per unit time is '*S*'.
4. Load for channel offered is '*G*' for transmission, which is Poisson's distribution (arrival).
   a. If $S < G$ then at high load, there will be frames from most of the users and hence many collisions.

b. If $G < S$ then at low load, there will be few or no collision, hence fewer retransmissions.

c. If $S > 1$, then the number of frames generated are more than the channels can handle, and every time probability of collision is 1.

d. If $G \approx S$, throughput is just the offered load, G times the probability of transmission being successful *i.e.*, $S = GP_0$

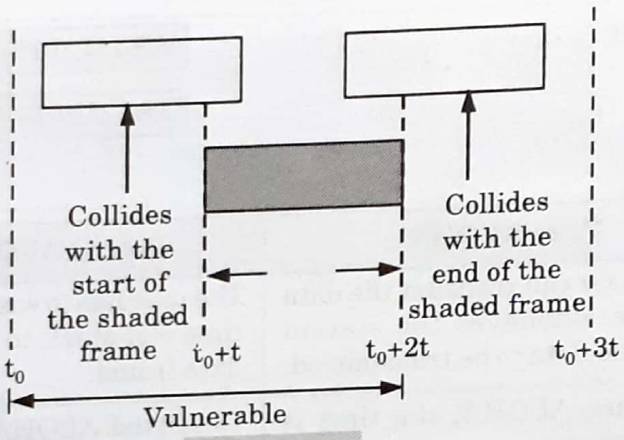


Fig. 2.9.1.

where P_0 is the probability, when the frames do not suffer from collision.

Que 2.10. Discuss slotted ALOHA.

Answer

1. It follows a synchronous transmission system, with time divided into slots.
2. Each slot size is equal to a fixed packet transmission time.
3. When the packet is ready for transmission, it needs to wait until the previous slot is over.
4. It uses the common clock at each station and satellite.
5. Fig. 2.10.1 shows packets completely or without any overlap.

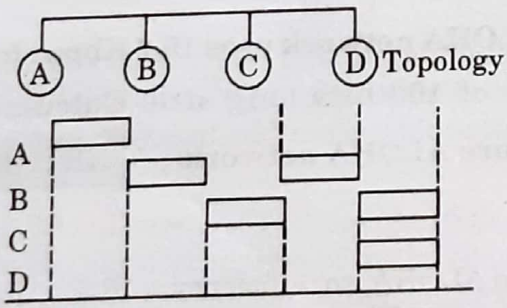


Fig. 2.10.1. Slotted ALOHA.

Performance of slotted ALOHA :

$S = G \times$ probability of no other transmission/overlap/arrival in previous slot

$\therefore S = Ge^{-G}$

Its peak at $G = 1$ with a throughput 0.368 (twice that of pure ALOHA). Operation at higher G reduces the number of empty slots but increases collision.

Que 2.11. **How can you compare pure ALOHA and slotted ALOHA ?**

AKTU 2013-14, Marks 05

AKTU 2014-15, Marks 2.5

Answer

S. No.	Pure ALOHA	Slotted ALOHA
1.	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
2.	In pure ALOHA, the time is continuous.	In slotted ALOHA, the time is discrete.
3.	The time is not globally synchronized.	The time is globally synchronized.

Que 2.12. **A pure ALOHA network transmits 200 bit frames on shared channel of 200 kbps. What is the throughput if the system (all station together) produces 250 frames per second ?**

AKTU 2014-15, Marks 2.5

Answer

If the system creates 250 frames per second, that is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$

This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

Que 2.13. **An ALOHA network uses 19.2 Kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput for pure ALOHA network.** **AKTU 2015-16, Marks 05**

Answer

The network is pure ALOHA, so, efficiency = 18 %

Usable bandwidth for 19.2 Kbps = $19.2 \times 0.18 = 3.456$ Kbps

Therefore, the maximum throughput of pure ALOHA

$$= \frac{1}{2e} \times 3.456 = \frac{18.4 \times 3.456}{100} = 0.635\ \%$$

PART-3

Overview of IEEE Standard – FDDI.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.14. Explain the IEEE 802.3 MAC sublayer frame format.

Answer

IEEE 802.3 specifies one type of frame containing seven fields : preamble, SFD, DA, SA, length/type of PDU, 802.2 frame and the CRC. The format of the MAC frame in CSMA/CD is shown in Fig. 2.14.1.

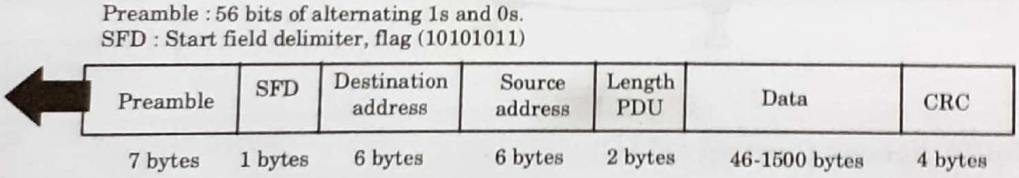


Fig. 2.14.1.

1. **Preamble :** The first field of the 802.3 frame, the preamble, contains seven bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enable it to synchronize its input timing.
2. **Start Frame Delimiter (SFD) :** The second field (one byte : 10101011) of the 802.3 frame signals at the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.
3. **Destination Address (DA) :** The Destination Address (DA) field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its Network Interface Card (NIC).
4. **Source Address (SA) :** The source address (SA) field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router to receive and forward the packet.

Performance of slotted ALOHA :

$S = G \times$ probability of no other transmission/overlap/arrival in previous slot

$$\therefore S = Ge^{-G}$$

Its peak at $G = 1$ with a throughput 0.368 (twice that of pure ALOHA). Operation at higher G reduces the number of empty slots but increases collision.

Que 2.11. **How can you compare pure ALOHA and slotted ALOHA ?**

AKTU 2013-14, Marks 05

AKTU 2014-15, Marks 2.5

Answer

S. No.	Pure ALOHA	Slotted ALOHA
1.	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
2.	In pure ALOHA, the time is continuous.	In slotted ALOHA, the time is discrete.
3.	The time is not globally synchronized.	The time is globally synchronized.

Que 2.12. **A pure ALOHA network transmits 200 bit frames on shared channel of 200 kbps. What is the throughput if the system (all station together) produces 250 frames per second ?**

AKTU 2014-15, Marks 2.5

Answer

If the system creates 250 frames per second, that is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$

This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

Que 2.13. **An ALOHA network uses 19.2 Kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput for pure ALOHA network.** **AKTU 2015-16, Marks 05**

Answer

The network is pure ALOHA, so, efficiency = 18 %

Usable bandwidth for 19.2 Kbps = $19.2 \times 0.18 = 3.456$ Kbps

Therefore, the maximum throughput of pure ALOHA

$$= \frac{1}{2e} \times 3.456 = \frac{18.4 \times 3.456}{100} = 0.635\ \%$$

PART-3

Overview of IEEE Standard – FDDI.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.14. Explain the IEEE 802.3 MAC sublayer frame format.

Answer

IEEE 802.3 specifies one type of frame containing seven fields : preamble, SFD, DA, SA, length/type of PDU, 802.2 frame and the CRC. The format of the MAC frame in CSMA/CD is shown in Fig. 2.14.1.

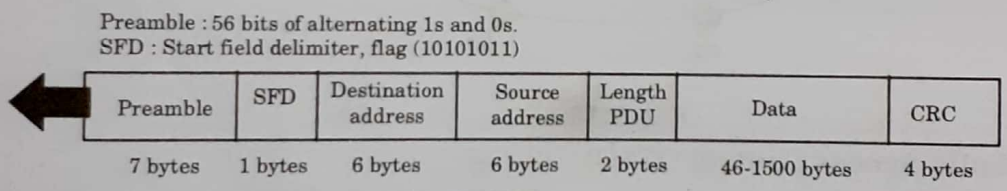


Fig. 2.14.1.

1. **Preamble :** The first field of the 802.3 frame, the preamble, contains seven bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enable it to synchronize its input timing.
2. **Start Frame Delimiter (SFD) :** The second field (one byte : 10101011) of the 802.3 frame signals at the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.
3. **Destination Address (DA) :** The Destination Address (DA) field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its Network Interface Card (NIC).
4. **Source Address (SA) :** The source address (SA) field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router to receive and forward the packet.

5. **Length/Type of Protocol Data Unit (PDU) :** These next two bytes indicate the number of bytes in the coming PDU. If the length of the PDU is fixed, this field can be used to indicate type, or as a base for other protocols.
6. **Data :** This field can be split up into two parts Data (0-1500 bytes) and padding (0-46 bytes).
7. **CRC :** The last field in the 802.3 frame contains the error detection information, in this case a CRC-32.

Que 2.15. How does in IEEE standard 802.5 LAN operates ? Discuss.

Answer

1. IEEE standard 802.5 LAN is a token ring system which is as shown in Fig. 2.15.1. It consists of a number of stations connected to the ring through a Ring Interface Unit (RIU).
2. The RIU is basically a repeater, therefore it regenerates the received data frames and sends them to the next station after some delay.

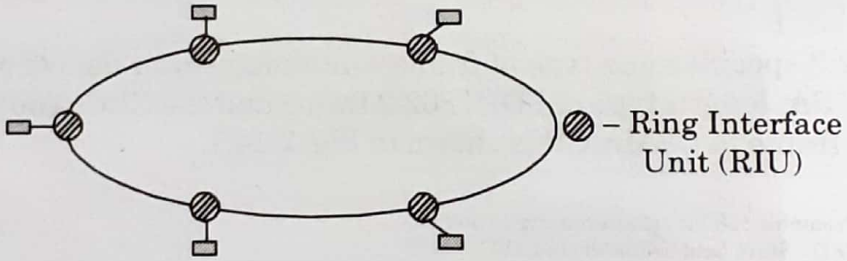


Fig. 2.15.1.

Media Access Control (MAC) :

1. The access to the medium (*i.e.*, who will transmit) is controlled by the special control frame called token.
2. The token is passed from one station to the other round the ring. The sequence of token passing is dependent on the physical location of the stations connected to the ring. It is not dependent on logical number as in case of token bus system.
3. A station which is in possession of the token only can transmit the frames. It may transmit one or more data frames but before the expiry of Token Holding Time (THT). Thus every station gets a fixed time to transmit its data.
4. Typically this time is of 10 msec. After the THT, the token frame must be handed over to some other station.

Que 2.16. How does IEEE standard 802.4 LAN operates ?

Answer

1. The IEEE 802.4 standard for Media Access Control (MAC) is known as token bus.

2. Logically the interconnected stations form a ring as shown in Fig. 2.16.1. The physical topology is bus topology as shown in Fig. 2.16.1.

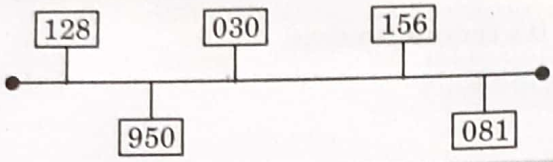


Fig. 2.16.1. Physical topology in token passing.

Media access control :

The operation of token bus taken place as follows :

1. At any time, the station which holds the token only can transmit its data frames on the bus. Every frame contains source and destination address.
2. All the other stations are ready to receive these data frames.
3. As soon as the transmission time of a station is over, it passes the token to the next station in the logical sequence. That station is allowed to transmit its data now.
4. In one cycle of operation, each station will get an opportunity to transmit once. The same station can get more number of chances to transmit in one cycle if more than one address is assigned to it.

Que 2.17. Differentiate between 802.3, 802.4, and 802.5 IEEE standards. **AKTU 2013-14, Marks 05**

Answer

S. No.	Parameters	802.3 Ethernet Bus	802.4 Token Bus	802.5 Token Ring
1.	Physical topology	Linear	Linear	Ring
2.	Logical topology	None	Ring	Ring
3.	Contention	Random chance	By token	By token
4.	Maintenance	No central maintenance	Distributed algorithm provides maintenance.	A designated monitor station performs maintenance.
5.	Cable used	Twisted pair, co-axial fiber optic	Co-axial	Twisted pair and fiber optic.
6.	Cable length	50 m to 2000 m	200 m to 500 m	50 m to 1000 m
7.	Frequency	10 Mbps to 100 Mbps	10 Mbps	4 to 100 Mbps
8.	Frame structure	1500 bytes	8191 bytes	5000 bytes

Que 2.18. Define Fiber Distributed Data Interface (FDDI) in detail with the help of its frame format.

Answer

FDDI :

1. Fiber Distributed Data Interface (FDDI) is a local area network protocol.
2. It supports data rates of 100 Mbps and provides a high speed alternative to Ethernet and token ring.
3. The copper version of FDDI is known as CDDI.
4. In FDDI, access is limited by time.
5. A station may send as many frames as it can within its allotted access period, with the provision that real time data be sent first.

Frame format :

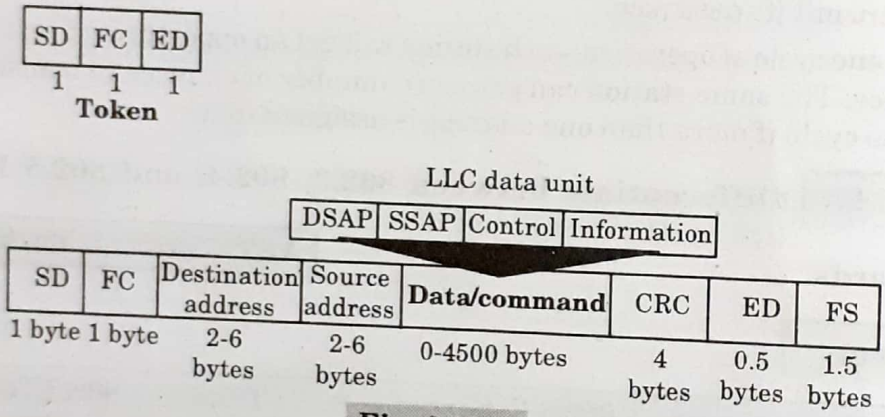


Fig. 2.18.1.

Frame fields :

1. **Start Delimiter (SD) :** The first byte of the field is the frame's starting flag.
2. **Frame Control (FC) :** The second byte of the frame identifies the frame type.
3. **Addresses :** The next two fields are the destination and source addresses. Each address consists of two to six bytes.
4. **Data :** Each data frame can carry up to 4500 bytes of data.
5. **Cyclic Redundancy Check (CRC) :** The field consists of 4 bytes.
6. **End Delimiter (ED) :** This field consists of half a byte in the data frame or a full byte in the token frame. It is changed in the physical layer with one *T* violation symbol in the data/command frame or two *T* symbols in the token frame.
7. **Frame Status (FS) :** The FDDI FS field is similar to that of token ring. It is included only in the data/command frame and consists of 1.5 bytes.

Que 2.19. **Brief about how line coding implemented in FDDI and describe its format.** **AKTU 2016-17, Marks 10**

Answer

Line coding implementation :

1. FDDI line coding use NRZI scheme in transition of data.
2. In this scheme, 4B/5B method is used in group encoding strategy.
3. The 4B/5B encoding scheme takes data in four bits codes and maps them to corresponding five bit codes.
4. For example, the four bit data code for the letter F (1111) corresponding to the five bit encoding 11101. These five bit codes are then transmitted using NRZI. By transmitting five bit codes using NRZI, a logical 1 bit is transmitted at least once every five sequential data bits, resulting in a signal transition.

Frame format for FDDI : Refer Q. 2.18, Page 2–14A, Unit-2.

PART-4

Data Link Layer – Elementary Data Link Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.20. **Discuss the issues in the data link layer and about its protocol on the basis of layering principle.** **AKTU 2016-17, 2017-18; Marks 10**

Answer

Data link layer issues are :

1. **Services provided to the network layer :**
   a. The data link layer act as a service interface to the network layer.
   b. The principle service is transferring data from the network layer on sending machine to the network layer on destination machine. This transfer always takes place via DLL (Dynamic Link Library).
2. **Frame synchronization :**
   a. The source machine sends data in the form of blocks called frames to the destination machine.

b. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. **Flow control :**
   a. Flow control is done to prevent the flow of data frame at the receiver end.
   b. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. **Error control :**
   a. Error control is done to prevent duplication of frames.
   b. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Data link layer protocol on the basis of layering principle :

1. **Serial Line Internet Protocol (SLIP) :**
   a. This protocol is used to connect a workstation to the internet over a dial-up line using a modem.
   b. It is connection-oriented protocol.
   c. The protocol is very simple. The workstation sends raw IP packets over the line with a flag byte at the end for framing purpose.

2. **Point-to-Point Protocol (PPP) :**
   a. This protocol is used by a lot of internet users to connect their home computers to the server of an Internet Service Provider (ISP).
   b. Most of these users have a traditional modem and they are connected to the internet through a telephone line or a TV cable.
   c. The PPP is used for controlling and managing the data transfer.

3. **High Level Data Link Control (HDLC) Protocol :**
   a. HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.
   b. For the HDLC protocol the following three types of stations have been defined :
      i. **Primary station :** A primary station takes care of the data link management.
      ii. **Secondary station :** A secondary station operates under the control of a primary station.
      iii. **Combined station :** A combined station can act as both primary and secondary stations.

4. **Ethernet :**
   a. Ethernet supports nearly every protocol, and can operate with any networking equipment that adheres to the IEEE standard.

b. This openness, combined with the ease of use, has made Ethernet dominant in the local area network.
c. The Ethernet system consists of three basic elements :
   i. The physical medium used to carry Ethernet signals between computers.
   ii. A set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly access to the shared Ethernet channel.
   iii. An Ethernet frame that consists of a standardized set of bits used to carry data over the system.

PART-5

Sliding Window Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.21. Explain sliding window protocol.

OR

Write short note on sliding window protocol.

AKTU 2014-15, Marks 2.5

AKTU 2017-18, Marks 05

Answer

1. Sliding window protocol is a feature of packet based data transmission protocols.
2. Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.
3. In sliding window method, multiple frames are sent by sender at a time before an acknowledgement is needed.
4. To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based on the size of the window.
5. The frames are numbered modulo-n, which means they are numbered from 0 to $n - 1$. For example, if $n = 8$, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, ... The size of the window is $n - 1$ (*i.e.*, 7).
6. When the receiver sends an ACK, it includes the number of the next frame it expects to receive. In other words, to acknowledge the receipt of a string of frames ending in frame 4, the receiver sends an ACK containing the number 5.

7. When the sender sees an ACK with the number 5, it knows that all frames up to number 4 have been received.
8. The window can hold $n-1$ frames at either end; therefore, a maximum of $n-1$ frames may be sent before an acknowledgement is required.

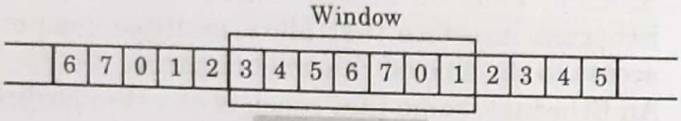


Fig. 2.21.1.

Sender window : At the beginning of a transmission, the sender's window contains $n-1$ frames. As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window.

1. Given a window of size w, if three frames have been transmitted since the last acknowledgement, then the number of frames left in the window is $w-3$.
2. Once an ACK arrives, the window expands to allow in a number of new frames equal to the number of frames acknowledged by that ACK. Fig. 2.21.2 shows a sender sliding window of size 7.

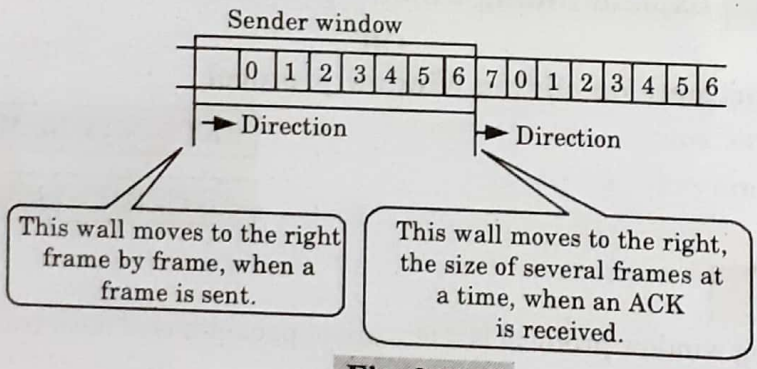


Fig. 2.21.2.

Receiver window : At the beginning of transmission, the receiver window contains not $n-1$ frames but $n-1$ spaces for frames.

1. As new frames come in, the size of the receiver window shrinks. The receiver window therefore represents not the number of frames received but the number of frames that may still be received before an ACK must be sent.
2. Given a window of size w, if three frames are received without an acknowledgement being returned, the number of spaces in the window is $w-3$.
3. As soon as an acknowledgement is sent, the window expands to include places for a number of frames equal to the number of frames acknowledged. Fig. 2.21.3 shows a receiving window of size 7.

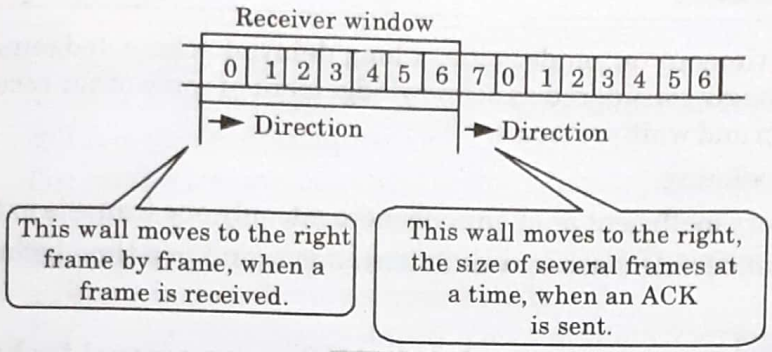


Fig. 2.21.3.

Que 2.22. Discuss stop and wait technique for flow control.

Answer

1. Stop and wait technique is the simplest form of flow control where a sender transmits a data frame.
2. After receiving the frame, the receiver indicates its willingness to accept another frame by sending back an ACK frame acknowledging the frame just received.
3. The sender must wait until it receives the ACK frame before sending the next data frame.
4. This technique is simple to understand and easy to implement, but not very efficient.
5. Fig. 2.22.1 illustrates the operation of the stop and wait protocol.

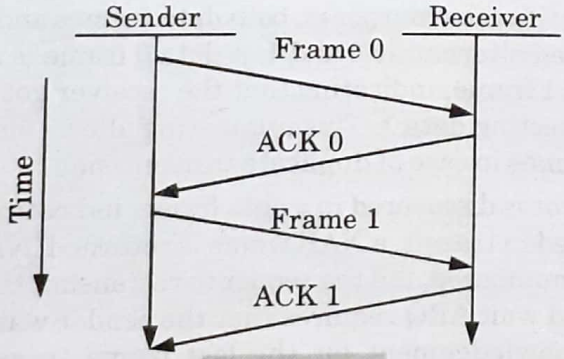


Fig. 2.22.1.

Que 2.23. State drawbacks of stop and wait protocols.

AKTU 2013-14, Marks 05

Answer

Drawbacks of stop and wait protocols are :

1. Data is lost due to processing or storage that occurs between the last backup and the subsequent disk crash, system crash, or some other such disaster.

2. After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet in stop and wait protocols.
3. No pipelining.
4. It is very inefficient as at any one moment, only one frame is in transition.
5. The sender will have to wait at least one round trip time before sending next.

Que 2.24. Discuss stop and wait ARQ error control technique.

OR

Write a short note on stop and wait ARQ. **AKTU 2014-15, Marks 2.5**

AKTU 2017-18, Marks 05

Answer

1. Stop and wait ARQ is a form of stop and wait flow control extended to include retransmission of data in case of lost or damaged frames.
2. For retransmission to work, four features are added to the basic flow control mechanism :

   The sending device keeps a copy of the last frame transmitted until it receives an acknowledgement for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.

   b. For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1. A data 0 frame is acknowledged by an ACK 1 frame, indicating that the receiver got the data 0 and is now expecting data 1. This numbering allows for identification of data frames in case of duplicate transmission.

   c. If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to retransmit the last frame sent. Stop and wait ARQ requires that the sender wait until it receives an acknowledgement for the last frame transmitted before it transmits the next one. When the sending device receives a NAK, it resends the frame transmitted after the last acknowledgement regardless of number.

   d. The sending device is equipped with a timer. If an expected acknowledgement is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again.

Following are the operations of protocol under certain conditions :

a. Operation in case of damaged frames :

1. When a frame is discovered by the receiver to contain an error, it returns a NAK frame and the sender retransmits the last frame.

2. For example, the sender transmits a data frame : data 0. The receiver returns an ACK 1, indicating the data 0 arrived undamaged and it is now expecting data 1.
3. The sender transmits its next frame : data 1. It arrives undamaged, and the receiver returns ACK 0.
4. The sender transmits its next frame : data 0. The receiver discovers an error in data 0 and returns a NAK.
5. The sender retransmits data 0. This time data 0 arrives intact, and the receiver returns ACK 1.

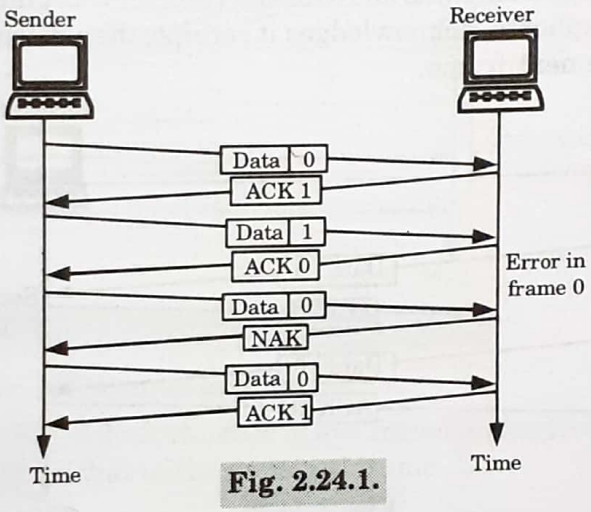


Fig. 2.24.1.

b. Operation in case of lost frame :

1. Any of the three frame types can be lost in transit. Fig. 2.24.2 shows how stop and wait ARQ handles the loss of a data frame.
2. The sender is provided with a timer that starts every time when a data frame is transmitted. If the frame never makes it to the receiver, the receiver can never acknowledge it, positively or negatively.
3. The sending device waits for an ACK or NAK frame until its timer goes off, at which point it tries again. It retransmits the lost data frame, restarts its timer, and waits for an acknowledgement.

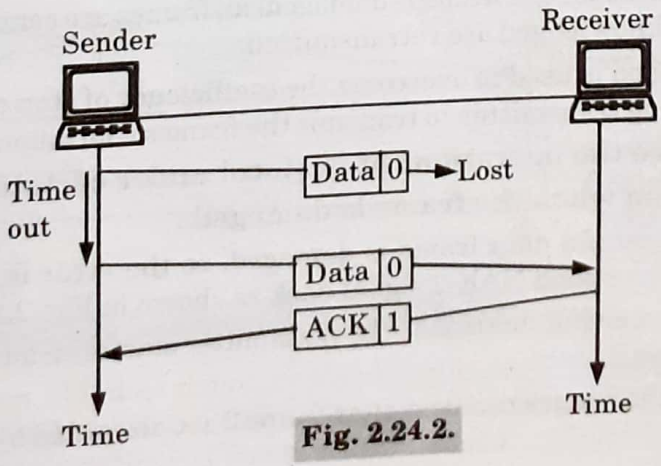


Fig. 2.24.2.

c. Operation in case of lost acknowledgement :

1. In this case, the data frame has made it to the receiver and has been found to be either acceptable or not acceptable. But the ACK or NAK frame returned by the receiver is lost in transit.
2. The sending device waits until its timer goes off, then retransmits the data frame.
3. The receiver checks the number of the new data frame. If the lost frame was a NAK, the receiver accepts the new copy and returns the appropriate ACK.
4. If the lost frame was an ACK, the receiver recognizes the new copy as a duplicate, acknowledges it receipt, then discards it and waits for the next frame.

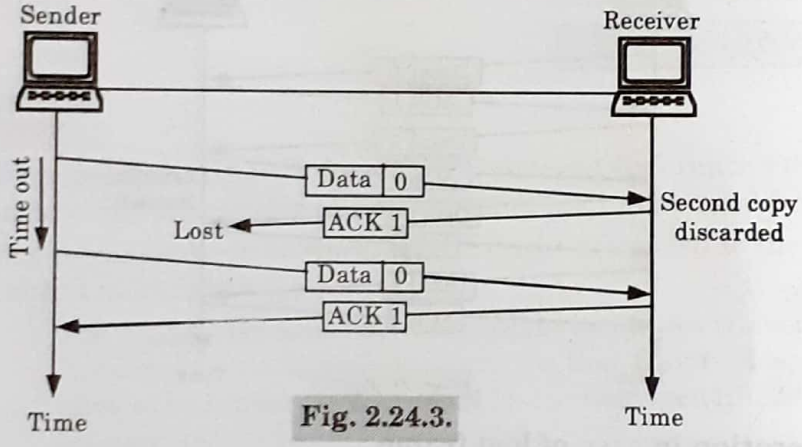


Fig. 2.24.3.

Que 2.25. Describe the Go-back-N ARQ protocol.

OR

Write a short note on Go-back-N ARQ. **AKTU 2014-15, Marks 2.5**

AKTU 2017-18, Marks 05

Answer

1. In this method if one frame is damaged, all frames are sent since the last frame acknowledged are retransmitted.
2. This method is used to overcome the inefficiency of stop and wait ARQ by allowing transmitter to transmit the frames continuously.

Following are the operations of protocol under certain condition :

1. Operation when the frame is damaged :

a. The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back as shown in Fig. 2.25.1.

b. On receiving this signal, the transmitter starts retransmission from frame 2.

c. All the frames received after frame 2 are discarded by the receiver.

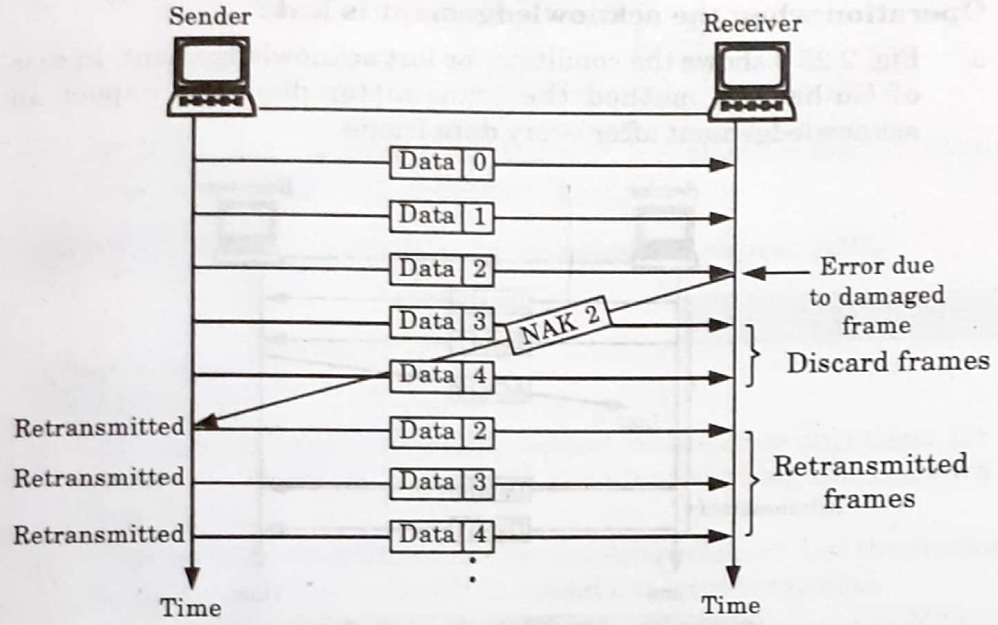


Fig. 2.25.1. Go-back-N, damaged data frame.

2. Operation when a frame is lost :

a. As shown in Fig. 2.25.2, the case of lost frame is also treated in the same manner as that of the damaged frame.

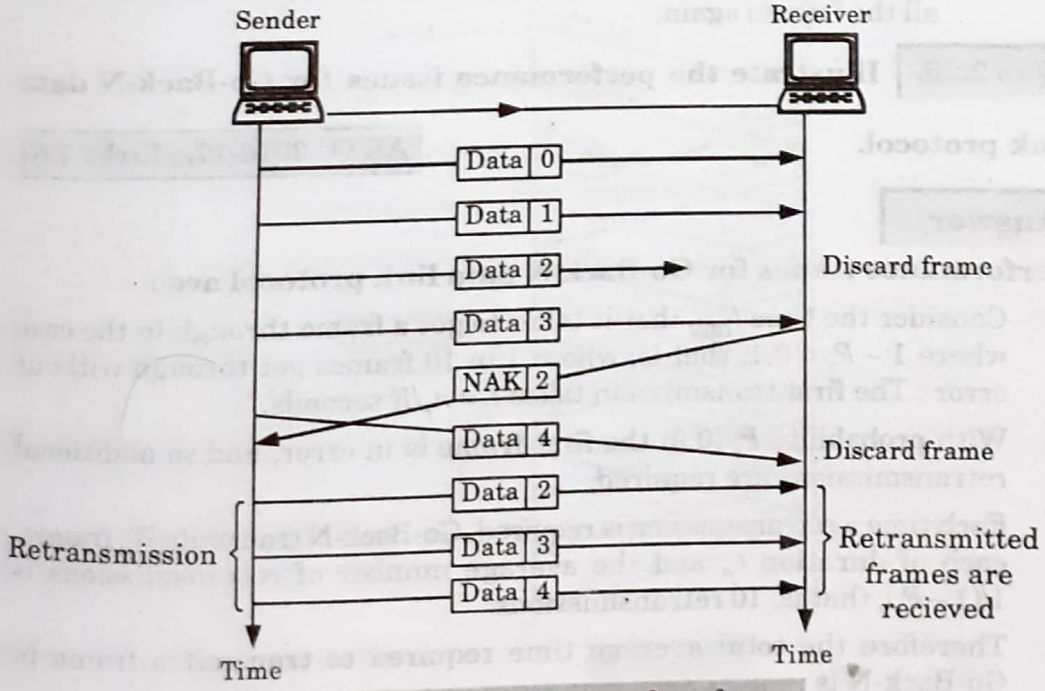


Fig. 2.25.2. Go-back-N, lost data frame.

b. The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

3. Operation when the acknowledgement is lost :

a. Fig. 2.25.3 shows the condition for lost acknowledgement. In case of Go-back-N method the transmitter does not expect an acknowledgement after every data frame.

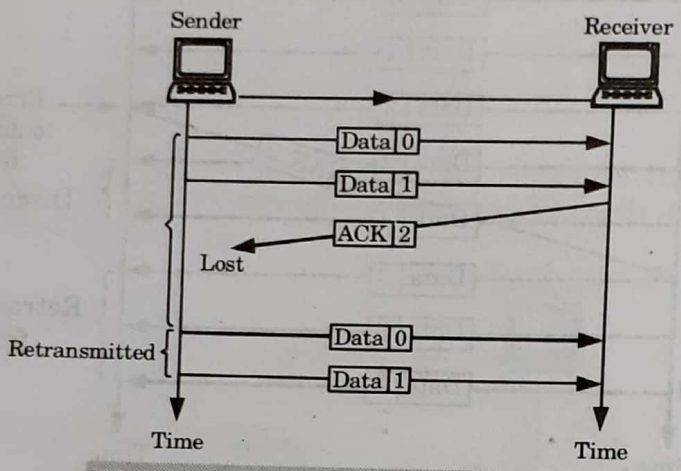


Fig. 2.25.3. Go-back-N, lost ACK frame.

b. The transmitter can send as many frames as the window allows before waiting for an acknowledgement.

c. Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and retransmit all the frames again.

Que 2.26. Illustrate the performance issues for Go-Back-N data link protocol.

AKTU 2016-17, Marks 7.5

Answer

Performance issues for Go-Back-N data link protocol are :

1. Consider the time t_{GBN} that it takes to get a frame through in the case where $1 - P_f = 0.1$, that is, where 1 in 10 frames get through without error : The first transmission takes $t_f = n_f/R$ seconds.
2. With probability P_f (0.9) the first frame is in error, and so additional retransmissions are required.
3. Each time a retransmission is required, Go-Back-N transmits W_s frames, each of duration t_f, and the average number of retransmissions is $1/(1-P_f)$, that is, 10 retransmissions.
4. Therefore the total average time required to transmit a frame in Go-Back-N is :

$$t_{GBN} = t_f + P_f \frac{W_s t_f}{1 - P_f}$$

Thus for the example, we have $t_{GBN} = t_f + 9W_s t_f$.

5. The efficiency for Go-Back-N is given by :

$$\eta_{GBN} = \frac{\frac{n_f - n_0}{t_{GBN}}}{R} = \frac{1 - \frac{n_0}{n_f}}{1 + (W_s - 1)P_f}(1 - P_f)$$

If the channel is error-free, that is $P_f = 0$, then Go-Back-N attains the best possible efficiency, namely, $1 - n_0/n_f$

Que 2.27. Write a short note on selective repeat ARQ.

AKTU 2014-15, Marks 2.5

Answer

1. The selective repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired, this is shown in the Fig. 2.27.1.
2. This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames.
3. The receiver also must have storage space to store the post NAK frames and processing power to reinsert frames in proper sequence.
4. In selective repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NAK for only frame which is missing or damaged.

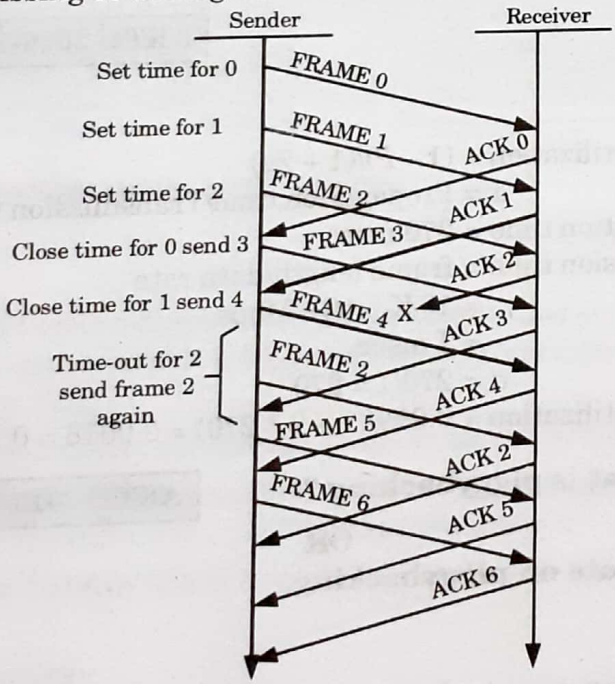


Fig. 2.27.1.

Que 2.28. Compare two data link layer protocols : Go-back-N and selective repeat in terms of flow control, error recovery and packet loss.

Answer

S. No.	Criteria	Go-back-N	Selective repeat
1.	Flow control	Flow control is done by storing frame of window size (N) in buffer at receiver end.	Flow control is done by storing continuous occurring frame in buffer at receiver end.
2.	Error recovery	It detects and controls the error during transmission of packets.	It detects and corrects the error during transmission of packets.
3.	Packet loss	If packet is lost during transmission then it discards all the packets after receiving NAK acknowledgement for the lost packet.	If packet is lost during transmission then it discards only the packet which is lost and continues to send other packets.

Que 2.29. Consider the use of 10 K-bit size frames on a 10 Mbps satellite channel with 270 ms delay. What is the link utilization for stop-and-wait ARQ technique assuming $P = 10^{-3}$?

AKTU 2016-17, Marks 10

Answer

Link utilization = $(1 - P)/(1 + 2a)$

where, a = Propagation time/Transmission time

Propagation time = 270 msec

Transmission time = frame length/data rate

= 10 K-bit/10 Mbps

= 1 msec

Hence, $a = 270/1 = 270$

Link utilization = $0.999/(1 + 2 * 270) = 0.0018 = 0.18\%$

Que 2.30. What is piggybacking ?

AKTU 2013-14, Marks 05

OR

Write a short note on piggybacking.

Answer

1. Piggybacking is a technique of temporarily delaying outgoing acknowledgments. So, that they can be hooked into the next outgoing data frame.
2. A better solution would be to use each channel (forward and reverse) to transmit frames both ways, with both channels having the same capacity.

3. Let *A* and *B* be the users. Then the data frames from *A* to *B* are intermixed with the acknowledgements from *A* to *B*. By checking the kind field in the header of the received frame, the received frame can be identified as either data frame or acknowledgement.
4. When a data frame arrives, the receiver waits, does not send the control frame (acknowledgement) back immediately.
5. The receiver waits until its network layer passes in the next data packet.
6. The acknowledgement is then attached to this outgoing data frame. Thus the acknowledgement travels along with next data frame.

PART-6

Error Handling.

CONCEPT OUTLINE

- Three error detecting methods :
  i. Parity checking
  ii. Checksum error detection
  iii. Cyclic redundancy check

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.31. Discuss error and its types.

Answer

1. Whenever an electromagnetic signal flows from one point to another, it is subject to unpredictable interference from heat, magnetism, and other forms of electricity.
2. This interference can change the shape or timing of the signal.
3. If the signal is carrying encoded binary data, such changes can alter the meanings of the data. This condition results in error.

Depending on the number of bits in error we can classify the errors into two types as :

1. **Single bit error :**
   a. The term single bit error suggests that only one bit in the given data unit such as byte is in error.
   b. That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 2.31.1.

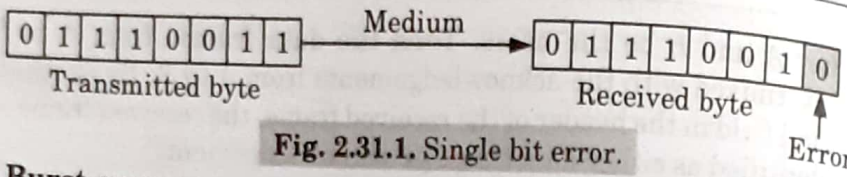


Fig. 2.31.1. Single bit error.

2. **Burst errors :**

   a. If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.

   b. The length of the burst error extends from the first erroneous bit to the last erroneous bit. Even though some of the bits in between have not been corrupted the length of the burst error is shown to be 5 bits.

   c. Burst errors are illustrated in Fig. 2.31.2.

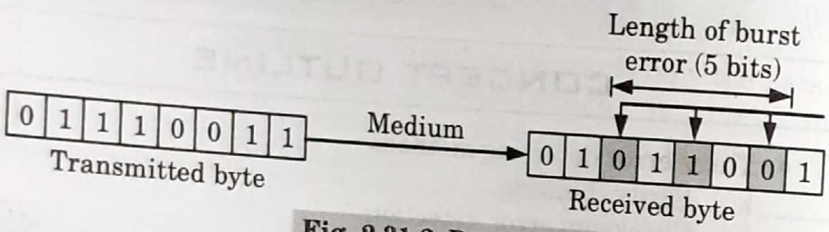


Fig. 2.31.2. Burst error.

Que 2.32. How does parity checking is helpful in error detection ?

Answer

1. The parity checking at the receiver can detect the presence of an error if the parity of the received signal is different from the expected parity.
2. That means if it is known that the parity of the transmitted signal is always going to be "even" and the received signal has an odd parity then the receiver can conclude that the received signal is not correct. This is as shown in Fig. 2.32.1.

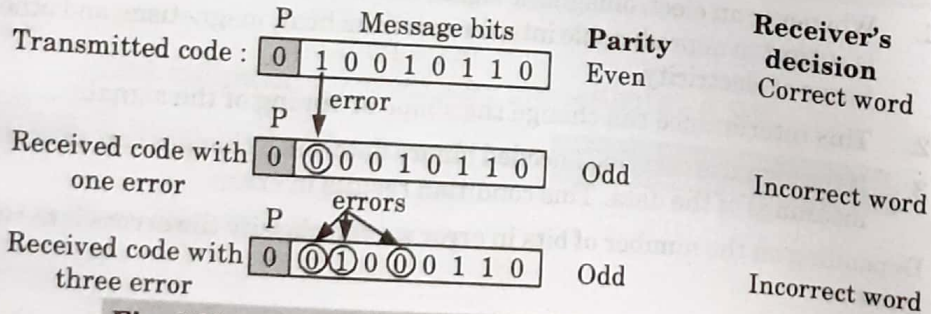


Fig. 2.32.1. The receiver detects the presence of error if the number of errors is odd *i.e.*, 1, 3, 5.

3. If a single error or an odd number of bits change due to errors introduced during transmission the parity of the codeword will change.
4. Parity of the received codeword is checked at the receiver and if there is change in parity then it is understood that error is present in the received word. This is as shown in Fig. 2.32.1.
5. If presence of error is detected then the receiver will ignore the received byte and request for the retransmission of the same byte to the transmitter.

Que 2.33. Explain the concept of checksum. How error is detected using the checksum byte ?

Answer

1. A checksum is a value used to verify the integrity of a file or a data transfer.
2. It is a sum that checks the validity of data.
3. A checksum is a simple type of redundancy check that is used to detect errors in data.
4. Checksums are typically used to compare two sets of data to make sure they are the same.
5. At the receiver end, the checksum function is applied to the message frame to retrieve the numerical value.
6. If the received checksum value matches the sent value, the transmission is considered to be successful and error free.

Error detection using checksum byte :

1. In checksum error detection scheme, the data is divided into k segments each of m bits.
2. In the sender's end the segments are added using 1's complement arithmetic to get the sum.
3. The sum is complemented to get the checksum.
4. The checksum segment is sent along with the data segments.
5. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
6. If the result is zero, the received data is accepted otherwise discarded.

Let consider following data

10011001111000100010010010000100

Original data

10011001	11100010	00100100	10000100
1	2	3	4

k = 4, m = 8

Sender

```
1   10011001
2   11100010
    ---------
    (1)01111011
       1
    ---------
    01111100
3   00100100
    ---------
    10100000
4   10000100
    ---------
    (1)00100100
       1
    ---------
Sum :  00100101
    ---------
Checksum : 11011010
```

Receiver

```
1   10011001
2   11100010
    ---------
    (1)01111011
       1
    ---------
    01111100
3   00100100
    ---------
    10100000
4   10000100
    ---------
    (1)00100100
       1
    ---------
    00100101
    11011010
    ---------
Sum :  11111111
Complement : 00000000
```

Conclusion : Accept data

Que 2.34. Write a short note on CRC.

Answer

1. CRC is a type of polynomial code in which a bit string is represented in the form of polynomials with coefficients of 0 and 1 only.
2. Polynomial arithmetic uses a modulo-2 arithmetic *i.e.*, addition and subtraction are identical to EX-OR.
3. For CRC code the sender and receiver should agree upon a generator polynomial $G(x)$. A codeword can be generated for a given dataword (message) polynomial $M(x)$ with the help of long division.
4. CRC works on the principle of binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of the message. This word is called appended message word.
5. The appended word thus obtained becomes exactly divisible by the generator word corresponding to $G(x)$.

CRC generator :

1. The CRC generator is shown in Fig. 2.34.1.

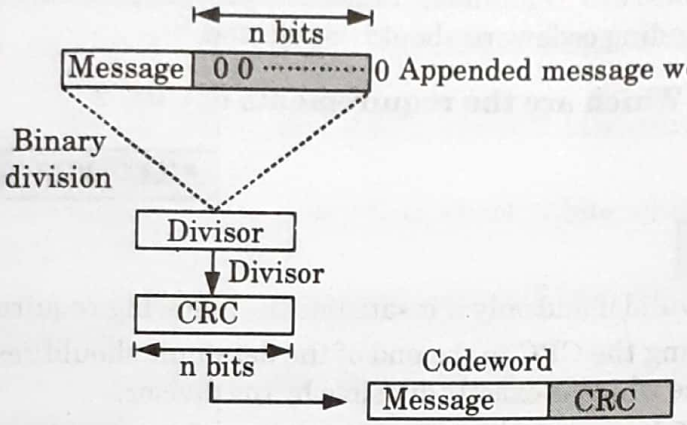


Fig. 2.34.1. CRC generator.

2. The stepwise procedure in CRC generation is as follows :

   Step 1 : Append a train of n 0s to the message word where n is 1 less than the number of bits in the predecided divisor (*i.e.*, generator word). If the divisor is 5-bit long then we have to append 4-zeros to the message.

   Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.

   Step 3 : The remainder obtained after the division in step 2 is the n bit CRC.

   Step 4 : This CRC will replace the n 0s appended to the data unit in step 1, to get the codeword to be transmitted as shown in Fig. 2.34.1.

CRC checker :

1. Fig. 2.34.2 shows the CRC checker.

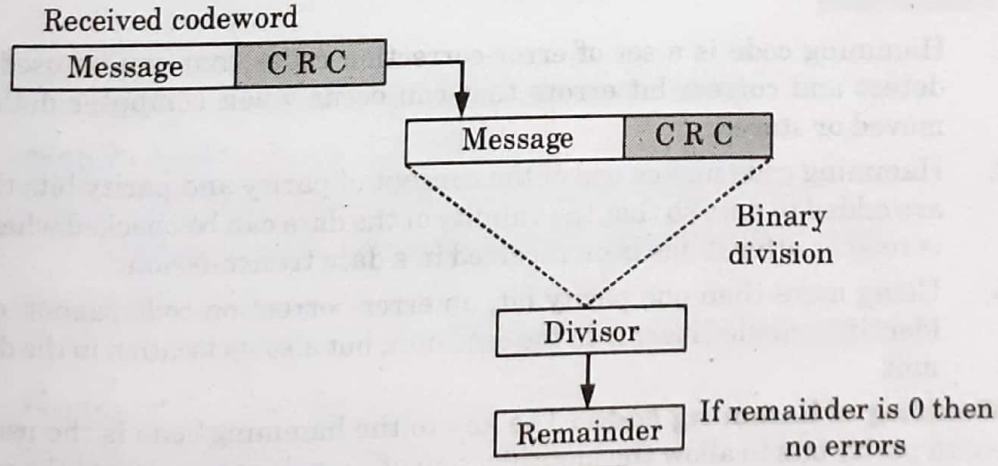


Fig. 2.34.2. CRC checker.

2. The codeword received at the receiver consists of message and CRC.
3. The receiver treats it as one unit and divides it by the same $(n + 1)$ bit divisor (generator word) which was used at the transmitter.
4. The remainder of this division is then checked.

5. If the remainder is zero, then the received codeword is error free and hence should be accepted.
6. But a non-zero remainder indicates presence of errors hence the corresponding codeword should be rejected.

Que 2.35. Which are the requirements of CRC ?

AKTU 2013-14, Marks 05

Answer

CRC will be valid if and only if it satisfies the following requirements:

1. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.
2. The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of $n + 1$ bit.
3. At the destination, the incoming data unit *i.e.*, data + CRC should be divided by the same number (predetermined binary divisor).
4. If the remainder after division is zero then there should be no error in the data unit and receiver accepts it.

Que 2.36. Describe hamming code. How it is used for error detection and correction ? Illustrate with the help of suitable example.

OR

What is hamming code ? Explain its working with suitable example.

AKTU 2015-16, Marks 7.5

Answer

1. Hamming code is a set of error-correction codes that can be used to detect and correct bit errors that can occur when computer data is moved or stored.
2. Hamming code makes use of the concept of parity and parity bits that are added to data so that the validity of the data can be checked when it is read or after it has been received in a data transmission.
3. Using more than one parity bit, an error-correction code cannot only identify a single bit error in the data unit, but also its location in the data unit.

Working of hamming code : The key to the hamming code is the use of extra parity bits to allow the identification of a single error. Create the code word as follows :

1. Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64, etc.)
2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)

3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.

   Position 1 : Check 1 bits, skip 1 bits, check 1 bits, skip 1 bits, etc. (1,3,5,7,9,11,13,15,...)

   Position 2 : Check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11,14,15,...)

   Position 4 : Check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15,20,21,22,23,...)

   Position 8 : Check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31,40-47,...)

   Position 16 : Check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc., (16-31,48-63,80-95,...)

   Position 32 : Check 32 bits, skip 32 bits, check 32 bits, skip 32 bits, etc., (32-63,96-127,160-191,...)

4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd.

5. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

For example : If the 7-bit hamming codeword received by a receiver is 1 0 1 1 0 1 1. Assuming the even parity state whether the received codeword is correct or wrong. If wrong, locate the bit in error.

	D_7	D_6	D_5	P_4	D_3	P_2	P_1
Received codeword :	1	0	1	1	0	1	1

Step 1 : Analyze bits 4, 5, 6 and 7 :

$$P_4\, D_5\, D_6\, D_7 = 1\,1\,0\,1 \rightarrow \text{Odd parity.}$$

$\therefore$ Error exists here.

$\therefore$ Put $P_4 = 1$ in the 4's position of the error word.

Step 2 : Analyze bits 2, 3, 6 and 7 :

$\therefore$ $P_2\, D_3\, D_6\, D_7 = 1\,0\,0\,1 \rightarrow$ Even parity so no error.

Hence put $P_2 = 0$ in the 2's position of the error word.

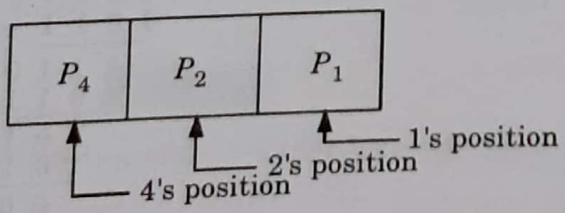
Step 3 : Check the bits 1, 3, 5, 7 :

$\therefore$ $P_1 D_3 D_5 D_7 = 1\,0\,1\,1 \rightarrow$ Odd parity so error exists.

Hence put $P_1 = 1$ in the 1's position of the error word.

Step 4 : Write the error word :

Error word $E =$



Substituting the values of P_4, P_2 and P_1 obtained in steps 1, 2 and 3 we get

$E =$ | 1 | 0 | 1 |

$= (5)_{10}$

Hence, bit 5 of the transmitted codeword is in error.

7	6	5	4	3	2	1
1	0	1	1	0	1	1

Incorrect bit

Step 5 : Correct the error :

Invert the incorrect bit to obtain the correct codeword as follows :
Correct codeword = [1 0 0 1 0 1 1]

Que 2.37. **Given a 10-bit sequence 1010011110 and a divisor of 1011. Find the CRC. Check your answer.** **AKTU 2014-15, Marks 05**

Answer

```
          1 0 0 1 0 0 0 1 1 1
      ____________________________
1 0 1 1 | 1 0 1 1 0 0 1 1 1 1 0 0 0 0
        | 1 0 1 1
        | ---------
        |   0 0 1 0
        |   0 0 0 0
        |   -------
        |     0 1 0 1
        |     0 0 0 0
        |     -------
        |       1 0 1 1
        |       1 0 1 1
        |       -------
        |         0 0 0 1
        |         0 0 0 0
        |         -------
        |           0 0 1 1
        |           0 0 0 0
        |           -------
        |             0 1 1 0
        |             0 0 0 0
        |             -------
        |               1 1 0 0
        |               1 0 1 1
        |               -------
        |                 1 1 1 0
        |                 1 0 1 1
        |                 -------
        |                   1 0 1 0
        |                   1 0 1 1
        |                   -------
        |                     0 0 1
```

Here, since remainder is 001. So, CRC will be 001.
We will add CRC to data and send it over network. At destination we have to check it if remainder is 000 then the data is right.

```
                1 0 0 1 0 0 0 1 1 1
          ┌─────────────────────────
1 0 1 1   │ 1 0 1 1 0 0 1 1 1 1 0 0 0 1
          │ 1 0 1 1
          │ ---------
          │   0 0 1 0
          │   0 0 0 0
          │   -------
          │     0 1 0 1
          │     0 0 0 0
          │     -------
          │       1 0 1 1
          │       1 0 1 1
          │       -------
          │         0 0 0 1
          │         0 0 0 0
          │         -------
          │           0 0 1 1
          │           0 0 0 0
          │           -------
          │             0 1 1 0
          │             0 0 0 0
          │             -------
          │               1 1 0 0
          │               1 0 1 1
          │               -------
          │                 1 1 1 0
          │                 1 0 1 1
          │                 -------
          │                   1 0 1 1
          │                   1 0 1 1
          │                   -------
          │                   0 0 0 0
```

Que 2.38. **Sketch the Manchester and differential Manchester encoding for the bit stream: 0001110101.** **AKTU 2014-15, Marks 05**

Answer

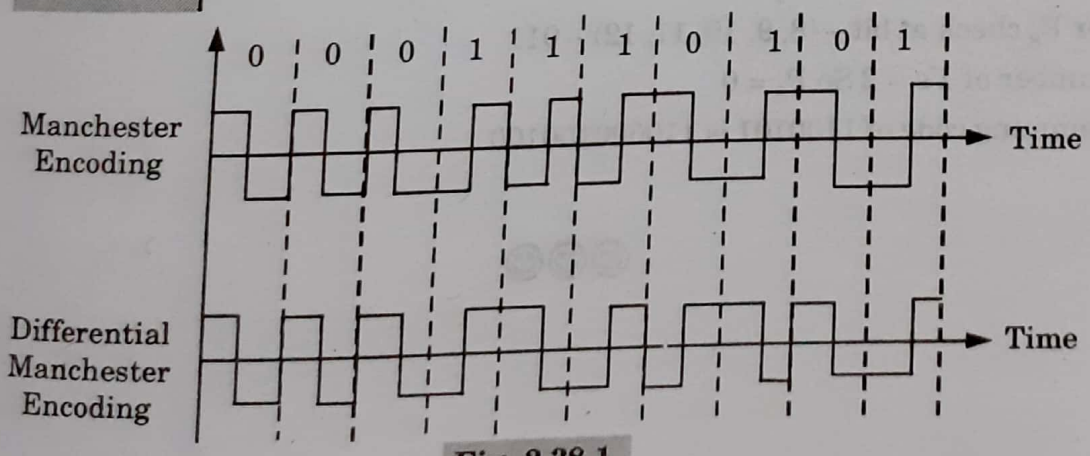


Fig. 2.38.1.

Que 2.39. **What is hamming code ? Calculate the hamming code for following message string : 1100101 with each and every step explained clearly.**

Answer

Hamming code : Refer Q. 2.36, Page 2–32A, Unit-2.

Numerical :

First check the number of parity bit used by using

$$2^x \geq k + x + 1$$

Number of data bit $(k) = 7$

$$2^x \geq 7 + x + 1$$

if $x = 4$

$$2^4 > 13$$

Number of parity bit = 4

Data/Parity	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
Data code	1	1	0		0	1	0		1		
Parity code				0				0		0	0
Code received	1	1	0	0	0	1	0	0	1	0	0

For P_1 check at bit – (1, 3, 5, 7, 9, 11) – 10001

Number of 1's = 2 So $P_1 = 0$

For P_2 check at bit – (2, 3, 6, 7, 10, 11) – 11011

Number of 1's = 4 So $P_2 = 0$

For P_4 check at bit – (4, 5, 6, 7, 12) – 011

Number of 1's = 2 So $P_4 = 0$

For P_8 check at bit – (8, 9, 10, 11, 12) – 011

Number of 1's = 2 So $P_8 = 0$

Hamming code of 1100101 is 110000100100.

3
UNIT

Network Layer

CONTENTS

Part-1	:	Network Layer : Point-to-Point Networks	**3–2A to 3–3A**
Part-2	:	Routing	**3–3A to 3–10A**
Part-3	:	Congestion Control	**3–10A to 3–17A**
Part-4	:	Internetworking-TCP/IP	**3–17A to 3–18A**
Part-5	:	IP Packet IP Address IPv6	**3–18A to 3–33A**

PART-1

Network Layer : Point-to-Point Network.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.1. What are the duties of network layer ?

Answer

Duties of network layer are :

1. **Internetworking :** This is the main duty of network layer. It provides the logical connection between different types of networks.
2. **Addressing :**
   a. Addressing identify each device on the internet. This is similar to a telephone system.
   b. The addresses used in the network layer should be able to uniquely define the connection of a computer to the internet universally.
3. **Routing :**
   a. In a network, there are multiple roots available from a source to a destination and one of them is to be chosen.
   b. The network layer decides which root is to be taken. This is called as routing and it depends on various criterions.
4. **Packetizing :**
   a. The network layer receives the packets from upper layer protocol and encapsulates them to form new packets.
   b. This is called as packetizing. A network layer protocol called IP (Internetworking Protocol), does the job of packetizing.
5. **Fragmenting :** The sent datagram can travel through different networks. Each router decapsulates the IP datagram from the received frame. Then the datagram is processed and encapsulated in another frame.

Que 3.2. Describe design issues in network layer.

Answer

1. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are wired into the network and rarely changed. They can also be highly dynamic,

being determined as new for each packet, to reflect the current network load.

2. If too many packets are present in the subnet at the same time, they will get into one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer.
3. Moreover, the quality of service provided (delay, transmit time, jitter, etc) is also a network layer issue.
4. When a packet has to travel from one network to another to get to its destination, many problems can arise such as:
   a. The addressing used by the second network may be different from the first one.
   b. The second one may not accept the packet at all because it is too large.
   c. The protocols may differ, and so on.
5. It is upto the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

PART-2

Routing.

CONCEPT OUTLINE

- Various types of routing algorithm :
  i. Dynamic/Adaptive routing
  ii. Static/Non-adaptive routing

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.3. Write down class of routing algorithms.

OR

What is adaptive routing algorithm ? Explain various types of adaptive routing algorithm.

Answer

Various types (class) of routing algorithm are :

1. **Dynamic / Adaptive algorithms :**
   a. Adaptive algorithms (dynamic routing) use such dynamic information as current topology, load, delay, etc., to select routes.

b. A dynamic algorithm can be run either periodically or in direct response to topology or link cost change.

c. While dynamic algorithms are more responsive to network changes, they are also more susceptible to problems such as routing loops and oscillation in routes.

d. Adaptive algorithms can be further divided in the following types :

i. **Isolated :** Each router makes its routing decisions using only the local information that it store. Specifically, routers do not even exchange information with their neighbours.

ii. **Centralized :** A centralized node makes all routing decisions. Specifically, the centralized node has access to global information.

iii. **Distributed :** Algorithms that uses a combination of local and global information.

2. **Static / Non-adaptive algorithms :**

a. In non-adaptive algorithms, routes never change, once initial routes have been selected, also called static routing.

b. In static routing algorithms, routes change very slowly over time, often as a result of human intervention (for example, a human manually editing a router's forwarding table).

c. Non-adaptive algorithms do not handle failed links.

Que 3.4. Differentiate between adaptive and non-adaptive routing algorithms.

Answer

S. No.	Adaptive routing algorithm	Non-adaptive routing algorithm
1.	In adaptive algorithm, routers exchange and update router table information.	In non-adaptive algorithm, network administrator manually enters routing paths into the router.
2.	In this algorithm, routers adjust automatically in response to changes in network topology.	In this algorithm, adjustments to changes in network topology require manual update.
3.	It prevents packet delivery failure and improves network performance.	It provides granular control over packet paths.
4.	It is dynamic routing.	It is static routing.
5.	It uses dynamic protocols to update the routing table and to find the optimal path between the source and the destination computers.	It manually sets up the optimal paths between the source and the destination computers.

Que 3.5. **What is meant by unicast and multicast routing with suitable diagrams ?** **AKTU 2013-14, Marks 05**

Answer

Unicast routing :

1. In unicast routing, there is one-to-one relation between the source and the destination. That means only one source sends packets to only one destination.
2. The type of source and destination addresses included in the IP datagram are unicast addresses assigned to the hosts as shown in Fig. 3.5.1.
3. In unicast routing, when a router receives a packet, it forwards that packet through only one of its ports which corresponds to the optimum path.

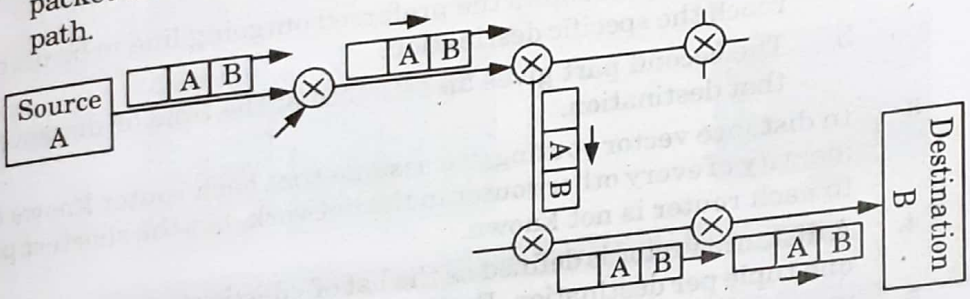


Fig. 3.5.1.

Multicast routing :

1. In multicasting, a message from a sender is to be sent to a group of destinations but not all the destinations in a network.
2. A process has to send a message to all other processes in the group. For a small group it is possible to send a point-to-point message.
3. But this is expensive if the group is large. So, we have to send messages to a well defined group which are small compared to the network size.
4. Sending message to such a group is called multicasting and the routing algorithm used for multicasting is multicast routing.
5. Multicast routing is a special class of broadcast routing as shown in Fig. 3.5.2.

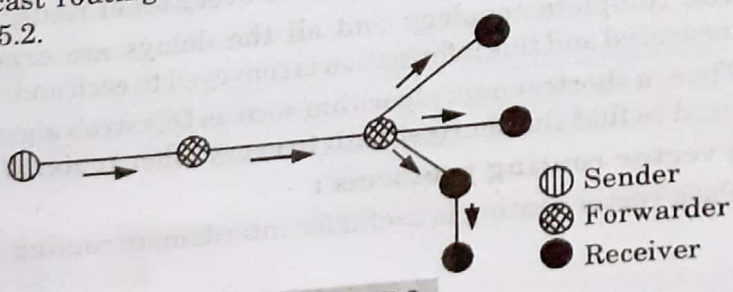


Fig. 3.5.2.

Que 3.6. **What is unicast routing ? Discuss unicast routing protocols.**

AKTU 2017-18, Marks 10

AKTU 2015-16, Marks 05

OR

Explain path vector routing protocol.

Answer

Unicast routing : Refer Q. 3.5, Page 3–5A, Unit-3.

Unicast routing protocols are :

i. Distance vector routing protocol :

1. In distance vector routing, each router maintains a routing table.
2. Routing table contains one entry for each router in the subnet. This entry has two parts :
   a. The first part shows the preferred outgoing line to be used to reach the specific destination.
   b. The second part gives an estimate of the time or distance to that destination.
3. In distance vector routing, we assume that each router knows the identity of every other router in the network, but the shortest part to each router is not known.
4. A distance vector is defined as the list of <destination, cost> tuples, one tuple per destination. Each router maintains a distance vector.
5. The cost in each tuple is equal to the sum of costs on the shortest path to the destination.

ii. Link state routing protocols :

1. The link state routing is simple and each router has to perform the following five operations :
   a. Discover its neighbours and learn their network address.
   b. Measure the delay or cost to each of its neighbours.
   c. Construct a packet containing the network addresses and the delays of neighbours.
   d. Send this packet to all other routers.
   e. Compute the shortest path to every other router.
2. The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.
3. Then, a shortest path algorithm such as Dijkstra's algorithm can be used to find the shortest path to every other router.

iii. Path vector routing protocols :

1. Path vector routing is useful for interdomain routing.

2. In path vector routing, there is one node in each Autonomous System (ASs) that acts on behalf of the entire ASs.
3. This single node is called the speaker node. The speaker node in an authentication server creates a routing table and advertises it to speaker nodes in the neighbouring ASs.

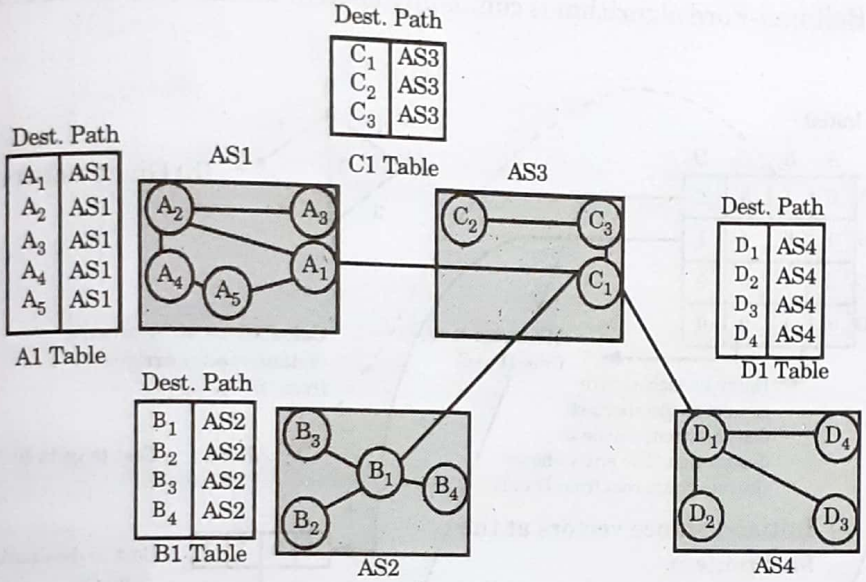


Fig. 3.6.1. Initial routing tables in path vector routing.

4. The principle of path vector routing is same as for distance vector routing except that only speaker nodes in each AS can communicate with each other.
5. A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems.

Que 3.7. Explain distance vector routing algorithm and how it updates the routing tables with the help of example.

Answer

Distance vector routing algorithm : Refer Q. 3.6, Page 3–6A, Unit-3.

Updation of router tables :

1. A router periodically sends a copy of its distance vector to all its neighbours.
2. When a router receives a distance vector from its neighbours, it tries to find out whether its cost to reach any destination would decrease if it routed packets to that destination through the particular neighbouring router.
3. Fig. 3.7.1 shows how the D.V. at *A* is automatically modified when a D.V. is received from *B*.
4. A similar calculation takes place at the other routers as well. So, the entries at every router can change. In Fig. 3.7.1 the initial distance

vector is shown. The entries in each source represent the shortest distance between the routers.

5. For example, $AC = 3$ indicates the cost corresponding to the shortest path in terms of number of hops from A to C.
6. Even if nodes asynchronously update their distance vectors the routing tables eventually converge.
7. Bellman-Ford algorithm is commonly used in distance vector routing.

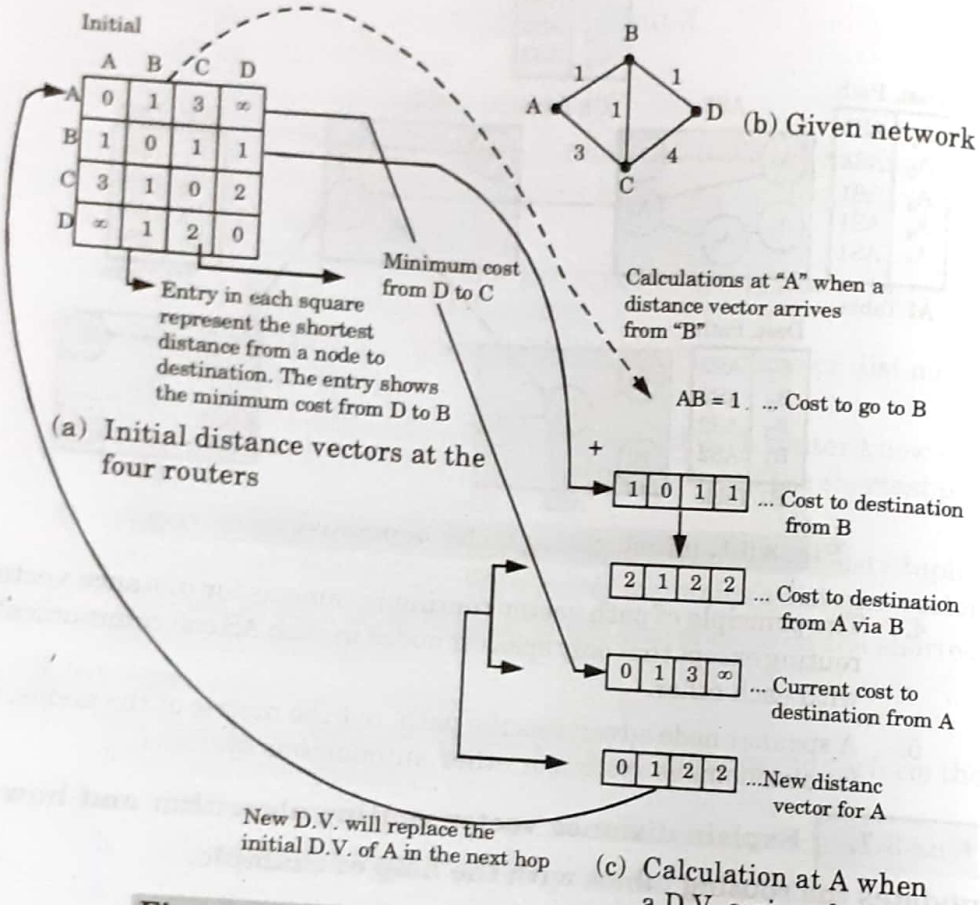


Fig. 3.7.1. Distance vector algorithm at router A.

Que 3.8. **Discuss link state routing. Compare distance vector routing with link state routing.**

Answer

Link state routing : Refer Q. 3.6, Page 3–6A, Unit-3.

Comparison :

S. No.	Distance vector routing	Link state routing
1.	Each router maintains routing table indexed by and containing one entry for each router in the subnet.	It is advanced version of distance vector routing.
2.	Algorithm is slower.	Algorithm is faster.
3.	Bandwidth is less.	Bandwidth is high.
4.	Router measure delay directly with special ECHO packets.	All delays measured and distributed to every router.
5.	It does not consider line bandwidth into account when choosing the routes.	It considers the line bandwidth into account when choosing the routes.

Que 3.9. Discuss Dijkstra algorithm.

Answer

1. The Dijkstra algorithm calculates the shortest path between two points on a network using a graph made up of nodes and arcs. Nodes in the graph may contain networks and routers.
2. Arcs are the connections between a router and a network (router to network and network to router). Cost is applied only to the arc from router to network.
3. The Dijkstra algorithm follows four steps to discover the shortest path tree (routing table) for each router :
   a. The algorithm begins to build the tree by identifying its root. The root of each router's tree is the router itself. The algorithm then attaches all nodes that can be reached from that root. Nodes and arcs are temporary at this step.
   b. The algorithm compares the tree's temporary arcs and identifies the arc with the lowest cumulative cost. This arc and the node to which it connects are now a permanent part of the shortest path tree.
   c. The algorithm examines the database and identifies every node that can be reached from its chosen node. These nodes and their arcs are added temporarily to the tree.
   d. The last two steps are repeated until every node in the network has become a permanent part of the tree. The only permanent arcs are those that represent the shortest (lowest-cost) route to every node.

Que 3.10. Describe the problem of count-to-infinity associated with distance vector routing technique. **AKTU 2016-17, Marks 7.5**

Answer

Count-to-infinity problem :

1. The main issue with Distance Vector Routing (DVR) protocols is routing loops.
2. This routing loops in DVR network causes count-to-infinity problem.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. Routing loops usually occur when any interface goes down or two routers send updates at the same time.

Explanation :

1. Consider a network connected with three routers as shown in Fig. 3.10.1.

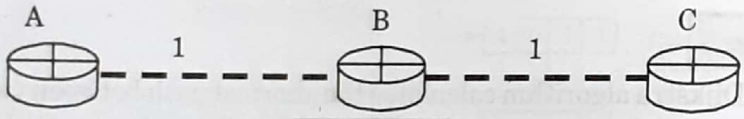


Fig. 3.10.1.

2. Let the matrices (weight or cost) between the routers is the number of jumps to reach the neighbour router.
3. In the Fig. 3.10.1 cost between B and C is 1 and cost between A and C is 2.
4. Now suppose the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
5. Before it can send any updates, it may be possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2.
6. B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3.
7. A will then receive updates from B later and update its cost to 4.
8. This will slowly propagates through the network until it reaches infinity. This will cause count-to-infinity problem.

PART-3

Congestion Control.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.11. What is congestion and congestion control ? Discuss open-loop congestion control techniques.

OR

What is congestion ? Name the techniques that prevent congestion.

AKTU 2015-16, Marks 05

OR

What is congestion ? Briefly describe the techniques that prevent congestion.

AKTU 2017-18, Marks 10

Answer

Congestion : Congestion is a situation which may occur if users send data into the network at a rate greater than that allowed by network resources.

Congestion control : Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

Techniques to prevent congestion :

1. **Open-loop congestion control :** In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. Following are the policies that can prevent congestion :
   - i. **Retransmission policy :** The retransmission policy is designed to optimize efficiency and at the same time prevent congestion.
   - ii. **Window policy :** The type of window at the sender may also affect congestion. The selective repeat window is better than the Go-Back-N window for congestion control.
   - iii. **Acknowledgement policy :** The acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help to prevent congestion.
2. **Closed-loop congestion control :** Closed-loop congestion control mechanisms try to reduce congestion after it happens. Several mechanisms have been used by different protocols which are as follows :
   - i. **Backpressure :** The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.

ii. **Choke packet :** A choke packet is a packet sent by a node to the source to inform about congestion. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly.

iii. **Implicit signaling :** In implicit signaling, there is no communication between the congested node or nodes and the source.

iv. **Explicit signaling :** The node that experiences congestion can explicitly send a signal to the source or destination.

Que 3.12. **What is the difference between open-loop congestion control and closed-loop congestion control ?**

Answer

S. No.	Open-loop congestion control	Closed-loop congestion control
1.	Open-loop congestion control is based on prevention of congestion.	Closed-loop congestion control is based on the solution for removing the congestion.
2.	It prevents the congestion from happening.	It removes the congestion after it took place.
3.	It does not need end to end feedback.	It adjusts its data rate depending on some kind of feedback.
4.	Mechanisms are as follow : i. Retransmission policy ii. Window policy iii. Acknowledgement policy iv. Admission policy	Mechanisms are as follow : i. Backpressure ii. Choke packet iii. Implicit signaling iv. Explicit signaling

Que 3.13. **Define traffic shaping. Elaborate leaky bucket algorithm used for congestion control.**

OR

What is the congestion in network layer ? Discuss at least one algorithm used for congestion control.

OR

Write a short note on leaky bucket algorithm.

AKTU 2013-14, Marks 05

Answer

Traffic shaping : Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network.

Congestion in network layer : Refer Q. 3.11, Page 3–11A, Unit-3.

Leaky bucket algorithm :

1. If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket.
2. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty.
3. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket which can smooth out bursty traffic.
4. Bursty chunks are stored in the bucket and sent out at an average rate.
5. A simple leaky bucket implementation is shown in Fig. 3.13.1, a FIFO queue holds the packets. If the traffic consists of fixed size packets the process removes a fixed number of packets from the queue at each tick of the clock.

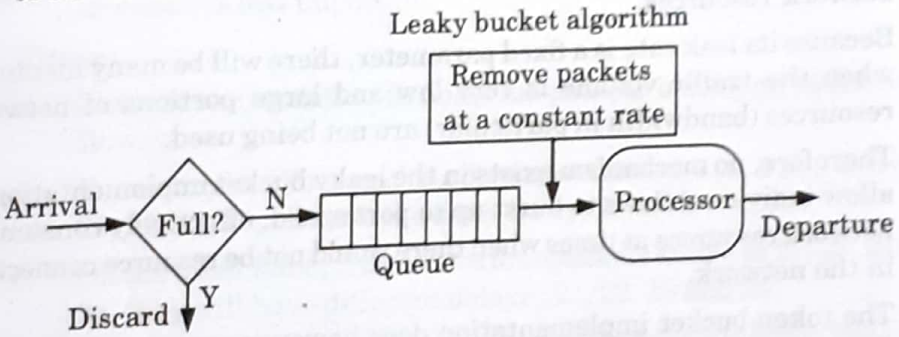


Fig. 3.13.1.

6. If the traffic consists of variable length packets, the fixed output rate must be based on the number of bytes or bits.
7. The following is an algorithm for variable length packets :
   i. Initialize a counter to n at the tick of the clock.
   ii. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
   iii. Reset the counter and go to step (i).

Que 3.14. Write a short note on token bucket algorithm. What are the limitations of leaky bucket algorithm ?

Answer

Token bucket :

1. Token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens.
2. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent.

3. In other words, the host can send bursty data as long as the bucket is not empty.
4. The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1.
5. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.
6. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick.

Limitation of leaky bucket algorithm :

1. The leaky bucket implementation does not efficiently use available network resources.
2. Because its leak rate is a fixed parameter, there will be many instances when the traffic volume is very low and large portions of network resources (bandwidth in particular) are not being used.
3. Therefore, no mechanism exists in the leaky bucket implementation to allow individual flows to burst up to port speed, effectively consuming network resources at times when there would not be resource connection in the network.
4. The token bucket implementation does however accommodate traffic flows with bursty characteristics.
5. The leaky bucket and token bucket implementations can be combined to provide maximum efficiency and control of the traffic flow into a network.

Que 3.15. What do you mean by congestion control and QoS ? What are the parameters of QoS ? Explain.

Answer

Congestion control : Refer Q. 3.11, Page 3–11A, Unit-3.

Quality of Service : Quality of Service (QoS) refers to a network's ability to achieve maximum bandwidth and provide better service to selected network traffic.

There are four types of QoS parameters :

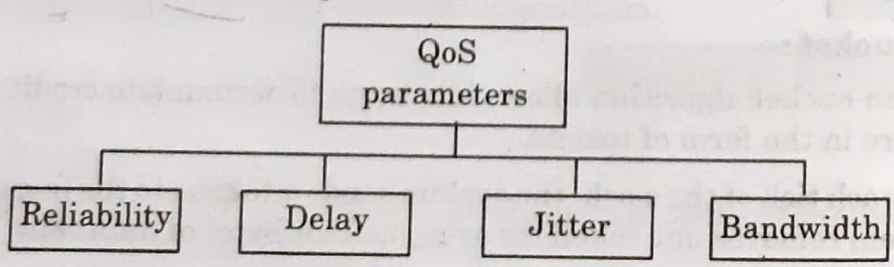


Fig. 3.15.1.

1. **Reliability :**
   a. Reliability is a characteristic that a flow needs.
   b. Lack of reliability means losing a packet or acknowledgement, which entails retransmission.
   c. However, the sensitivity of application programs to reliability is not the same.
   d. For example, it is more important that electronic mail, the transfer, and internet access have reliable transmission than telephony or audio conferencing.
2. **Delay :**
   a. Source to destination delay is another flow characteristic.
   b. Applications can tolerate delay in different degrees.
   c. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.
3. **Jitter :**
   a. Jitter is the variation in delay for packets belonging to the same flow.
   b. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time.
   c. On the other hand, if the above four packets arrive at 21, 23, 21 and 28, they will have different delays : 21, 22, 19 and 24.
   d. High jitter means that difference between delays is large; low jitter means that variation is small.
4. **Bandwidth :**
   a. Different applications need different bandwidths in video conferencing.
   b. We need to send millions of bits per second to refresh a colour screen while the total numbers of bits in an email not reach even a million.

Que 3.16. Write short note on ARP. How it works ?

Answer

Address Resolution Protocol (ARP) :

1. The address resolution protocol (ARP) is a protocol used by the internet protocol, specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.
2. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Ethernet.

3. For two machines on a given network to communicate, they must know the other machine's physical addresses.
4. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC layer address corresponding to a particular IP network layer address.
5. The term address resolution refers to the process of finding an address of a computer in a network.
6. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer.
7. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address.
8. The address resolution procedure is completed when the client receives a response from the server containing the required address.
9. An ethernet network uses two hardware addresses, which identify the source and destination of each frame, sent by the Ethernet.

Working of Address Resolution Protocol (ARP) :

When a host *A* needs to find the MAC address of another host *B* the sequence of events taking place is as follows :

1. The host *A* who wants to find the MAC address of some other host, sends an ARP request packet. This packet consists of IP and MAC addresses of the sender *A* and the IP address of the receiver *B*.
2. This request packet is broadcasted over the network as shown in Fig. 3.16.1.

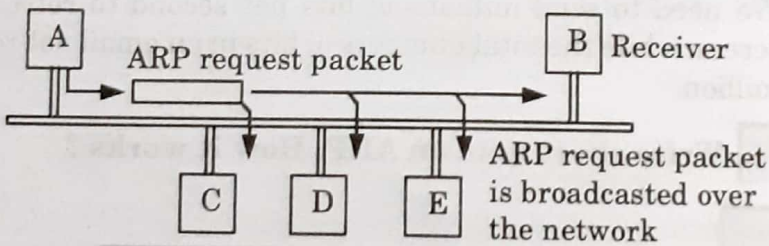


Fig. 3.16.1. ARP request is broadcast.

3. Every host on the network will receive the ARP request packet and process it. But only the intended receiver *B* will recognize its IP address in the request packet and will send an ARP response packet back to *A*.
4. The ARP response packet has the IP and MAC addresses of the receiver *B* in it. This packet is delivered only to *A* (unicast using *A*'s physical address in the ARP response packet). This is shown in Fig. 3.16.2. Thus host *A* has obtained the MAC address of *B* using ARP.

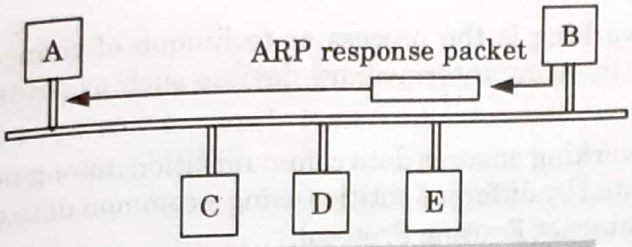


Fig. 3.16.2. ARP response unicast.

Que 3.17. **Write a short note on RARP.**

Answer

1. RARP (Reverse Address Resolution Protocol) is the logical inverse of ARP that resolves hardware address (MAC) to IP address.
2. RARP relies on the presence of a RARP server with table entries of MAC layer to IP address mappings.
3. RARP allows a physical machine in a local area network to request its IP address from a gateway server's address resolution protocol (ARP) table or cache.
4. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or media access control-MAC address) addresses to corresponding Internet Protocol addresses (IP address).
5. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address.
6. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine, which can store it for future use.
7. RARP is available for ethernet, fiber distributed data interface and token ring LANs.

PART-4

Internetworking – TCP/IP.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.18. **Write a short note on internetworking.**

Answer

1. Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.
2. Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol.
3. Internetworking is only possible when all the connected networks use the same protocol stack or communication methodologies.

Three units of internetworking :

1. **Extranet :** An extranet is a network of internetwork or internetworking that is limited in scope to a single organisation or entity.
2. **Intranet :** An intranet is a set of interconnected networks or internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and FTP tools, that is under the control of a single administrative entity.
3. **Internet :** The internet is the largest pool of networks geographically located throughout the world and these networks are interconnected using the same protocol stack, TCP/IP.

PART-5

IP Packet, IP Address, IPv6.

CONCEPT OUTLINE

- Each TCP/IP host is identified by a logical IP address.
- Classification of IP address :
  - i. Class A
  - ii. Class B
  - iii. Class C
  - iv. Class D
  - v. Class E
- Various types of IP addresses :
  - i. IPv4 (Internet Protocol Version 4)
  - ii. IPv6 (Internet Protocol Version 6)

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.19. Explain IP addressing.

Answer

1. IP addressing is the process of finding unique IP address. A unique IP address is required for each host and network component that communicates using TCP/IP.
2. The IP address is a network layer address and has no dependence on the data link layer address (such as a MAC address of a network interface card).
3. Each TCP/IP host is identified by a logical IP address.
4. The IP address is a network layer address and has no dependence on the data link layer address (such as a MAC address of a network interface card).
5. A unique IP address is required for each host and network component that communicates using TCP/IP.
6. The IP address identifies a system's location on the network. An IP address must be globally unique and have a uniform format.
7. Each IP address includes a networkID and a hostID.
   i. The networkID (also known as a network address) identifies the systems that are located on the same physical networkID. The networkID must be unique to the internetwork.
   ii. The hostID (also known as a host address) identifies a workstation, server, router, or other TCP/IP host within a network. The address for each host must be unique to the networkID.
8. The use of the term networkID refers to any IP networkID, whether it is class-based, a subnet, or a supernet.

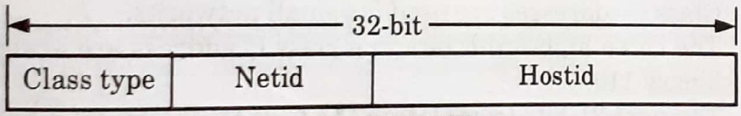


Fig. 3.19.1.

9. An IP address is 32-bits long. It is a common practice to segment the 32-bits of the IP address into four 8-bit fields called octets.
10. Each octet is converted to a decimal number (the base 10 numbering system) in the range 0-255 and separated by a period (a dot). This formal is called dotted decimal notation.

Que 3.20. Give the classification of different IP address.

OR

What is IP addressing? How it is classified? How is subnet addressing is performed? **AKTU 2015-16, 2017-18; Marks 10**

Answer

IP addressing : Refer Q. 3.19, Page 3–18A, Unit-3.

Classification of IP address :

1. **Class A :**
   - i. Class A addresses are assigned to networks with a very large number of hosts.
   - ii. The high-order bit in a class A address is always set to 0.
   - iii. The next seven bits (completing the first octet) complete networkID. The remaining 24-bits (the last three octets) represent the hostID.
2. **Class B :**
   - i. Class B addresses are assigned to medium-sized to large-sized networks.
   - ii. The two high-order bit in a class B address are always set to binary 10.
   - iii. The next 14-bits (completing the first two octets) complete the networkID. The remaining 16-bits (last two octets) represent the hostID.

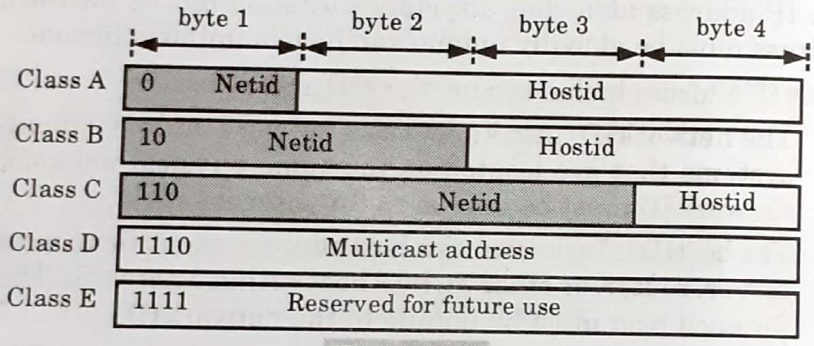


Fig. 3.20.1.

3. **Class C :**
   - i. Class C addresses are used for small networks.
   - ii. The three high-order bits in a class C address are always set to binary 110.
   - iii. The next 21-bits (completing the first three octets) complete the networkID. The remaining 8-bits (last octet) represent the hostID.

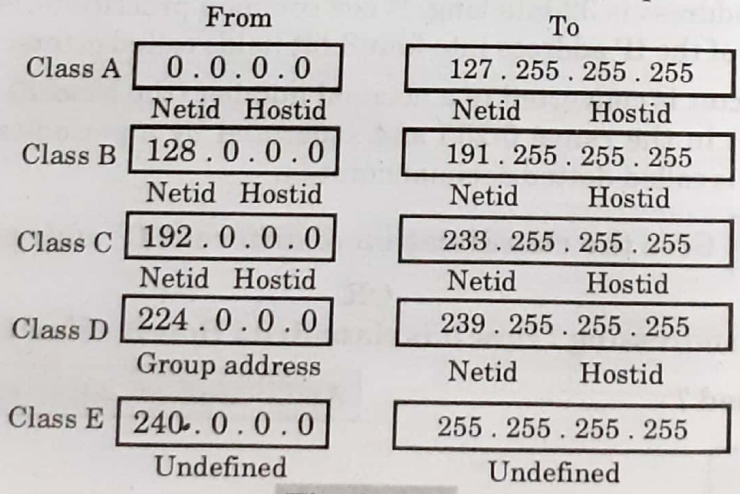


Fig. 3.20.2.

4. **Class D :**
   i. Class D addresses are reserved for IP multicast addresses.
   ii. The four high-order bits in a class D address are always set to binary 1110.
   iii. The remaining bits are for the addresses that interested hosts will recognize.
5. **Class E :**
   i. Class E addresses are experimental addresses reserved for future use.
   ii. The high-order bits in a class E address are set to 1111.

Steps for performing subnetting :

Step 1 : Check the IP address and the host's subnet mask.

Step 2 : Find the broadcast address.

Step 3 : Obtain the quantity of subnets : Find the number of subnets by using the following formula : 2^n, where, n is the number of subnet bits in the mask.

Step 4 : Acquire the number of hosts : Find the number of hosts by using the following formula : $2^n - 2$, where, n is the number of host bits in the mask.

Step 5 : Access the mask we need for the network : Find the number of sub-networks as well as the hosts for each network, by using formula $2^n - 2$.

Step 6 : Refer to the class C, mask to create sub-networks : To create sub-networks is to memorize class C masks. The default subnet mask is 255.255.255.0. There are other subnet masks that make up class C.

Step 7 : Decide which class mask to use for our sub-networks : Perform this step after we determined our networks and host.

Que 3.21. Explain the types of IP address.

Answer

There are two types of IP addresses :

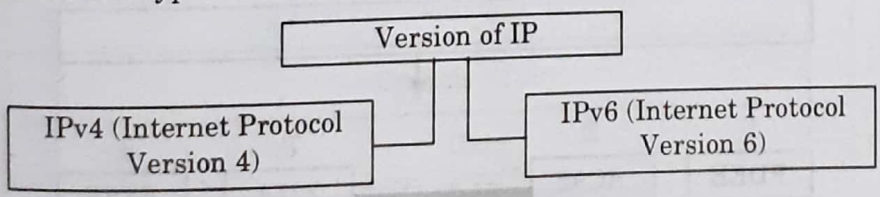


Fig. 3.21.1.

1. **IPv4 (Internet Protocol Version 4) :**
   i. IP addresses are 32-bit long and they are used in the source address and destination address fields of the IP header.

ii. Fig. 3.21.1 shows the IP address format. It consists of two fields called networkID and hostID. The IP numbers (addresses) for the hosts are assigned by the network administrator.

iii. An IP address consists of two parts. The first part of the address, called the network number, identifies a network on the internet, and the second part of address, called the hostID, identifies an individual host on that network.

iv. The IPv4 protocol has an address space. It is defined as the total number of addresses used by the protocol.

v. If N numbers of bits are used for defining an address then the address space will be 2^N addresses.

IPv4 address format :

i. The 32-bit IPv4 address is grouped into groups of 8-bits, separated by dots. Each 8-bit group is then converted into its equivalent binary number as shown in Fig. 3.21.2

ii Thus each octet (8-bit) can take value from (0 to 255). The IPv4 in the dotted decimal notation can range from 0.0.0.0 to 255.255.255.255.

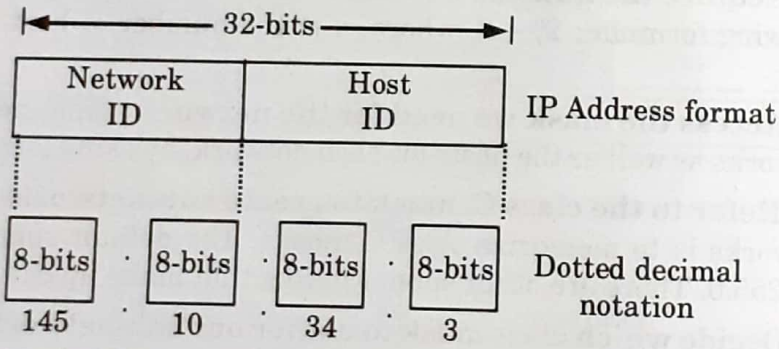


Fig. 3.21.2. IPv4 address format and dotted decimal format.

2. IPv6 (Internet Protocol Version 6) :

An IPv6 address is 128-bit long as shown in Fig. 3.21.3.

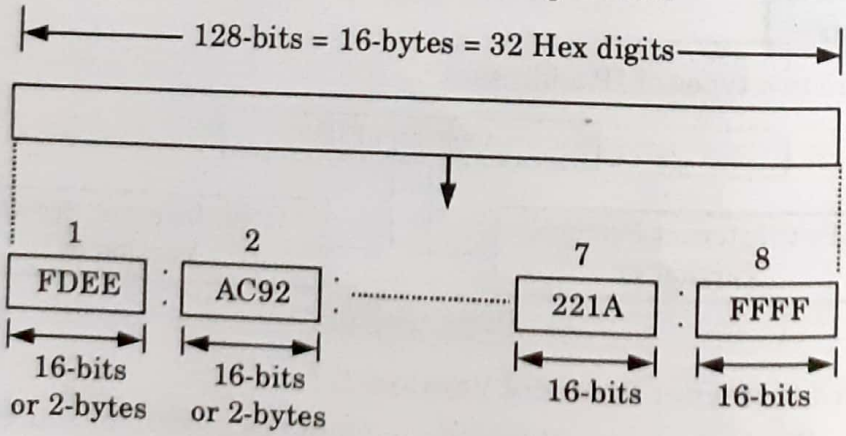


Fig. 3.21.3. IPv6 address.

Hexadecimal colon notation :

1. IPv6 uses a special notation called hexadecimal colon notation. In this, the total 128-bits are divided into 8 sections, each one 16-bits or 2-bytes long.
2. The 16-bits or 2-bytes in binary correspond to four hexadecimal digits of 4-bits each.
3. Hence, the 128-bits in hexadecimal form will have $8 \times 4 = 32$ hexadecimal digits. These are in groups of 4 digits and every group is separated by a colon as shown in Fig. 3.21.3.
4. In IPv6, about 15% of the address space is initially allocated, the remaining 85% being reserved for future use.

Que 3.22. Draw and explain the packet format of IPv4.

Answer

The IPv4 datagram format is shown in Fig. 3.22.1. The key fields in the IPv4 datagram are the following :

i. **Version number :** This 4-bits field is used to specify the IP protocol version of the datagram. By looking at the version number, the router can determine how to interpret the remainder of the IP datagram.

ii. **Header length :** In the IPv4 datagram header these 4-bits are needed to determine where in the IP datagram the data actually begins.

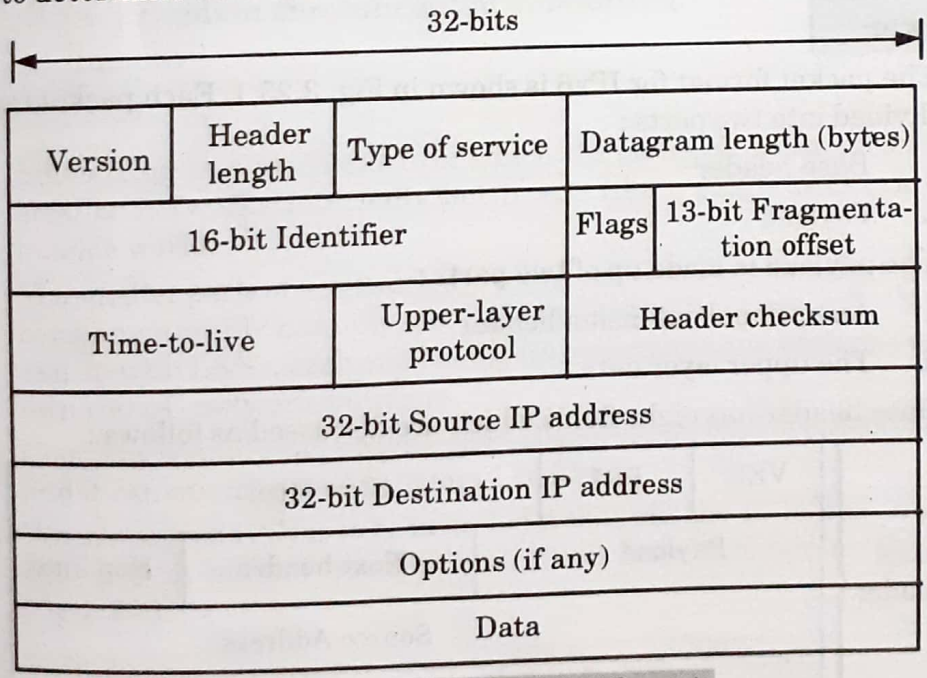


Fig. 3.22.1. IPv4 datagram format.

iii. **Type of service :** The type of service bits were included in the IPv4 header to allow different types of IP datagrams to be distinguished from each other.

iv. **Datagram length :** This is the total length of the IP datagram (header plus data) measured in bytes. This field is 16-bits long.

v. **Identifier, flags, fragmentation offset :** These three fields are used in IP fragmentation.

vi. **Time-to-live :** The time-to-live (TTL) field is included to ensure the datagrams do not circulate forever in the network. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, the datagram must be dropped.

vii. **Protocol :** This field is used only when an IP datagram reaches its final destination.

viii. **Header checksum :** The header checksum is used by router for detecting errors in the received IP datagram. The header checksum is computed by treating each 2-bytes in the header as a number and summing these numbers using 1's complement arithmetic.

ix. **Source and destination IP addresses :** Source IP address field contain IP of source which create IP datagram. Destination IP address field contain IP of receiver to which IP datagram is received. The length of both fields is 32-bit.

x. **Options :** The options field allows an IP header to be extended.

xi. **Data (payload) :** In most circumstances, the data field of the IP datagram contains the transport layer segment (TCP or UDP) to be delivered to the destination.

Que 3.23. Explain the packet format for IPv6.

Answer

1. The packet format for IPv6 is shown in Fig. 3.23.1. Each packet can be divided into two parts :
   i. Base header
   ii. Payload
2. The payload is made up of two parts :
   i. An optional extension header
   ii. The upper layer data
3. Base header has eight fields which are discussed as follows :

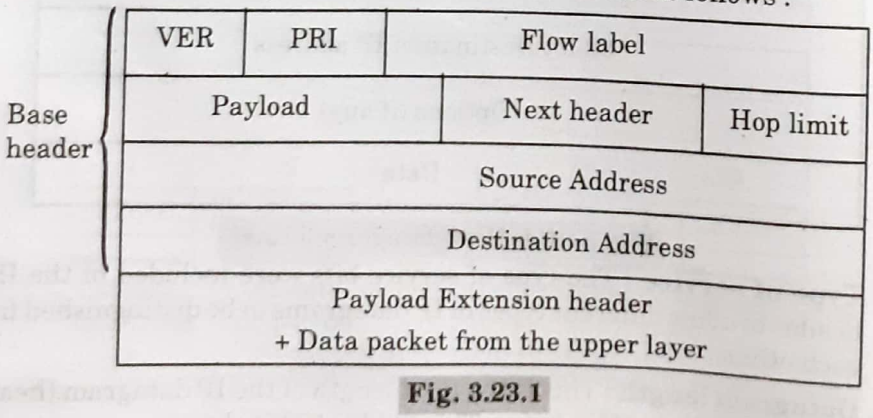


Fig. 3.23.1

i. **Version :** This is 4-bit field which defines the version number of IP. For IPv6, the value is 6.

ii. **Priority :** The 4-bit priority field defines the priority of the packet with respect to traffic congestion.

iii. **Flow label :** The flow label is a 3-byte field that is designed to provide special handling for a particular flow of data.

iv. **Payload length :** The 2-byte payload length field defines the total length of IP datagram excluding the base header.

v. **Next header :** The next header is an 8-bit field defines the header that follows the base header in the datagram.

vi. **Hop limit :** This 8-bit hop limit field serves the same purpose as TTL field in IPv4.

vii. **Source address :** The source address field is a 16-bytes internet address that identifies the original source of datagram.

viii. **Destination address :** The destination address field is a 16-byte internet address that usually identifies the final destination of the datagram.

ix. **Extension header :** Extension header field help in processing of data packets by appending different extension header. Each extension header has a length equal to multiple of 64-bits.

Que 3.24. Explain the concept of subnetting.

Answer

1. Subnetting is a mechanism in which the network splits into several smaller networks internally but it acts like a single network to the outside world.
2. The smaller parts of a network are called subnets. For example, a growing company initially has only one LAN but as the time passes by it might end up with LANs, each one having its own router and each one with its own class C network numbers.
3. Company should start up with class B address instead of class C address and it can number the host from 1 to 254.
4. When a second LAN is to be installed it can split the 16-bit host numbers into a 6-bit subnet number and 10-bit host number as shown in Fig. 3.24.1.

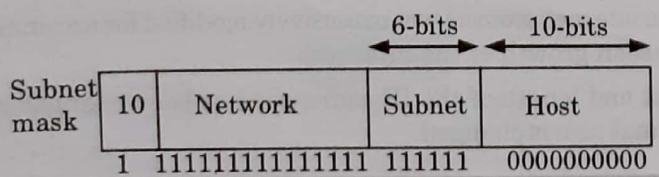


Fig. 3.24.1. One of the ways to subnet a class B network.

5. Due to this split it is possible to connect 62 LANs (0 and 1 are reserved) and each one can contain up to 1022 hosts.
6. The number of 1's in the subnet mask is more than the number of 1's in the corresponding default mask.
7. In a subnet mask, we change some of the leftmost 0's in the default mask to make it a subnet mask. Fig. 3.24.2 shows the difference between the class B default mask and subnet mask for the same block.
8. The number of subnets is determined by the number of extra 1's.
9. For three extra 1's, the number of subnets will be $2^3 = 8$. For n extra 1's, the number of subnets is 2^n.

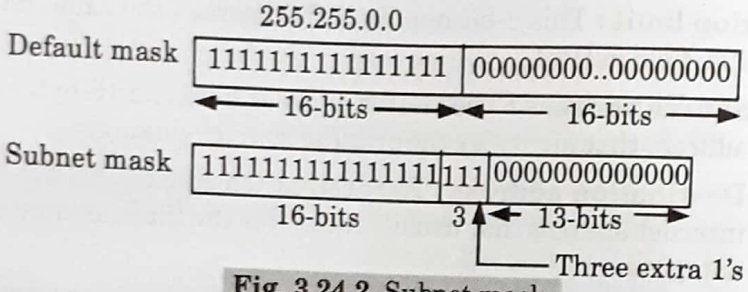


Fig. 3.24.2. Subnet mask.

Que 3.25. What are deficiencies of IPv4 ? How IPv6 was modified to overcome these deficiencies ?

Answer

1. The deficiency of IPv4 is its address field. IP relies on network layer addresses to identify end points on networks, and each networked device has a unique IP address.
2. Other identified deficiencies of the IPv4 protocol are :
   i. Complex host and router configuration
   ii. Non-hierarchical addressing
   iii. Large routing tables
   iv. Non-trivial implementations in providing security
   v. Multicasting

To overcome these deficiencies :

1. To overcome these problems/deficiencies the Internet Protocol Version 6 (IPv6) is used.
2. In IPv6, the internet protocol was extensively modified for accommodating the unforeseen growth of the internet.
3. The format and length of the IP addresses has been changed and the packet format also is changed.

Que 3.26. **Perform the subnetting of the following IP address 160.11.X.X. Original subnet mask 255.255.0.0 and number of subnet 6 (six).** **AKTU 2014-15, Marks 10**

Answer

Given : Network IP address = 160.11.X.X

Subnet mask = 255.255.0.0

Number of subnet = 6

Let us consider a network. First we divide the network into four subnet as shown in Fig. 3.26.1, by using two bits of hostid part as

160.11.□□----------

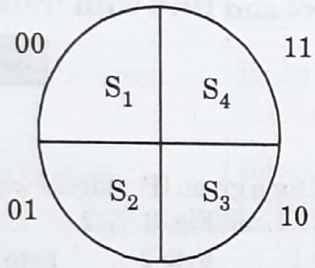


Fig. 3.26.1.

Range of subnet S_1 : 160. 11.0.0 – 160.11.63.0

Range of subnet S_2 : 160. 11.64.0 – 160.11.127.0

Range of subnet S_3 : 160. 11.128.0 – 160.11.191.0

Range of subnet S_4 : 160. 11.192.0 – 160.11.255.0

Now we divide the subnet S_3 into two more subnet as S_{31} and S_{32} as shown in Fig. 3.26.2 by using one bit from hostid part as

160.11.10□00000--------

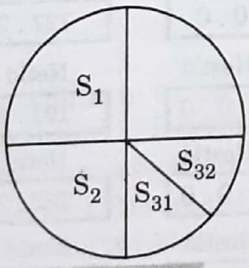


Fig. 3.26.2.

Range of subnet S_{31} : 160.11.128.0 – 160.11.159.0

Range of subnet S_{32} : 160.11.160.0 – 160.11.191.0

Again we divide subnet S_4 into two more subnet as S_{41} and S_{42} as shown in Fig. 3.26.3, by using one bit from hostid part as

160.11.11 0 00000.....

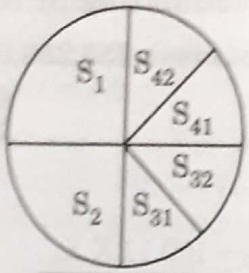


Fig. 3.26.3.

Range of subnet S_{41} :160.11.192.0 – 160.11.223.0
Range of subnet S_{42} :160.11.224.0 – 160.11.254.0
So, IP address 160.11.X.X has six subnets as $S_1, S_2, S_{31}, S_{32}, S_{41}, S_{42}$.

Que 3.27. Give an IP address, how will you extract its netid and hostid and compare IPv4 and IPv6 with frame format.

AKTU 2013-14, Marks 10

Answer

To extract netid and hostid for a given IP address we use internet class and its range as shown in Fig. 3.27.1 and Fig. 3.27.2.

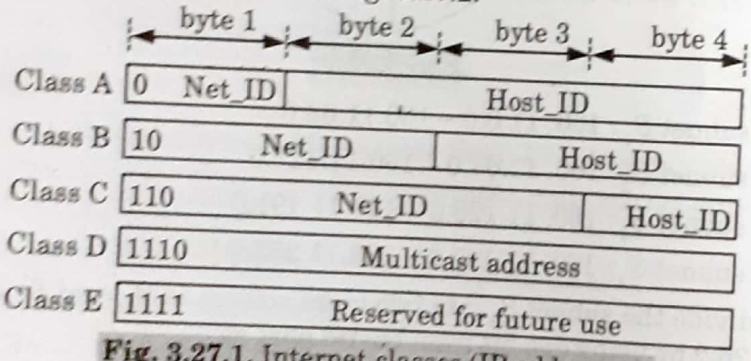


Fig. 3.27.1. Internet classes (IP addresses).

	From	To
Class A	0 . 0 . 0 . 0	127 . 255 . 255 . 255
	Netid Hostid	Netid Hostid
Class B	128 . 0 . 0 . 0	191 . 255 . 255 . 255
	Netid Hostid	Netid Hostid
Class C	192 . 0 . 0 . 0	233 . 255 . 255 . 255
	Netid Hostid	Netid Hostid
Class D	224 . 0 . 0 . 0	239 . 255 . 255 . 255
	Group address	Netid Hostid
Class E	240 . 0 . 0 . 0	255 . 255 . 255 . 255
	Undefined	Undefined

Fig. 3.27.2. Classes range of IP.

Comparison :

S. No.	IPv4	IPv6
1.	Source and destination addresses are 32-bits (4-bytes) in length.	Source and destination addresses are 128-bits (16-bytes) in length.
2.	IP Sec support is optional.	IP Sec support is required.
3.	No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the flow label field.
4.	Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
5.	Header includes a checksum.	Header does not include a checksum.
6.	Header includes options.	All optional data is moved to IPv6 extension headers.

IPv4 frame format : Refer Q. 3.22, Page 3–23A, Unit-3.
IPv6 frame format : Refer Q. 3.23, Page 3–24A, Unit-3.

Que 3.28. What is meant by fragmentation ? Is fragmentation needed in concatenated virtual circuit internets, or in any datagram system ? **AKTU 2013-14, Marks 10**

OR

Is fragmentation needed in concatenated virtual circuit internets or only in datagram systems ? Explain. **AKTU 2015-16, Marks 7.5**

Answer

1. Fragmentation is a technique in which the gateways break up large packets into smaller one called as fragments.
2. Then each fragment is sent as a separate internet packet.

Recombination of fragments : The recombination of fragments can be done by using one of the following two strategies :

Strategy - 1 for fragmentation (Transparent strategy) :

1. In this strategy, the fragmentation caused by a "small packet" network is made transparent to any subsequent network through which the packets will pass.
2. When a large packet arrives at a gateway G_1 in Fig. 3.28.1, it breaks the packet into fragments.

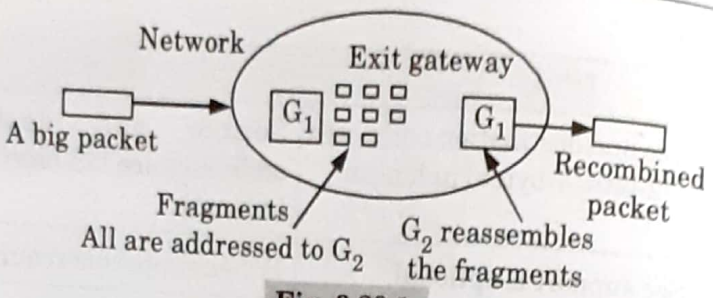


Fig. 3.28.1.

3. Each fragment is then addressed to the same exit gateway (G_2) that recombines all these fragments.

Strategy - 2 for fragmentation (Non-transparent strategy) :

1. In this strategy, the fragmented packets are not reassembled at any intermediate stage. That means the exit gateways will not reassemble the fragments.
2. Instead each fragment is treated as a separate original packet. All these packets are passed through the exit gateway or gateways and their recombination is carried out at the destination host as shown in Fig. 3.28.2.

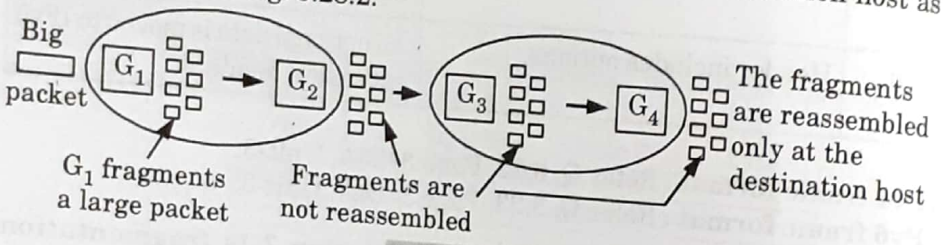


Fig. 3.28.2.

Need of fragmentation in internet :

Yes, fragmentation is needed in concatenated virtual circuit internet due to following reasons :

1. To break the packets into smallest maximum size Packet Data Unit (DDU).
2. To support the packet for different network.

Que 3.29. **What is the transmission time of a packet sent by a station if the length of the packet is 2 million bytes and the bandwidth of the channel is 300 kbps.** **AKTU 2014-15, Marks 10**

Answer

Given :

$B = 300$ kbps

Size of packet = 2000000 byte

$$T = \frac{\text{Data size}}{\text{Bandwidth}} = \frac{2000000 \times 8}{300 \times 1000} = 53.33 \text{ sec}$$

Que 3.30.

i. Find the class of each address

a. 140.213.10.80 b. 52.15.150.11

ii. **What is the type of the following address ?**

a. 4F::A234:2 b. 52F::1234:2222

Answer

AKTU 2015-16, Marks 10

i. a. **Given address :** 140. 213. 10. 80

The binary equivalent of 140 will be,

2	140	
2	70	0
2	35	0
2	17	1
2	8	1
2	4	0
2	2	0
	1	0

$(140)_2 = \underline{10}001100$

10 belongs to the class B.

b. **Given address :** 52.15.150.11

Binary equivalent of 52 will be

2	52	
2	26	0
2	13	0
2	6	1
2	3	0
	1	1

$(52)_2 = \underline{110}100$

110 belongs to class C.

ii. a. **Given address :** 4F : : A234 : 2

It could be expanded as follows :

004F : 0 : 0 : 0 : 0 : 0 : A234 : 2

Now, consider the leftmost byte *i.e.*, 4F

004F Hex = $\underbrace{0000\ \ 0000}_{\text{Type prefix}}$ 0100 1111

Leftmost 8-bits correspond to type prefix. All 8 zeros correspond to reserved address.

Thus, the type of 4F : : A234 : 2 is a reserved address.

b. **Given address :** 52F : : 1234 : 2222

It could be expanded as follows :

052F : 0 : 0 : 0 : 0 : 0 : 1234 : 2

Now, consider the leftmost byte *i.e.*, 52F

052F Hex = $\underbrace{0000\ \ 0101}_{\text{Type prefix}}$ 0010 1111

Thus, the type of 52F : : 1234 : 2222 is a network address.

Que 3.31. What is an interconnecting device in the internet ? Explain various interconnecting device used in the internet with suitable example.

Answer

Interconnecting devices are those devices which are used for sharing data over the network.

Different types of interconnecting devices are :

1. **Repeaters :**
   a. A repeater is a connecting device which can operate only in the physical layer.
   b. Repeater amplifies signals to ensure data transmission.
   c. A repeater receives a signal and before it get attenuated or corrupted, regenerates the original signal.

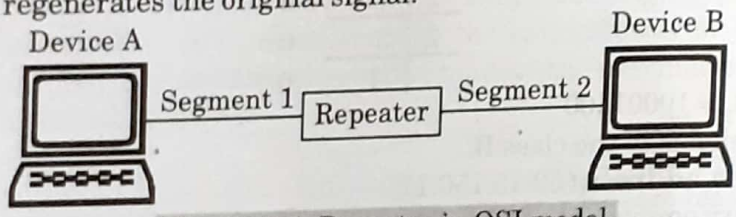


Fig. 3.31.1. Repeater in OSI model.

2. **Hubs :**
   a. Hub is a central location to connect various segments of media coming from various nodes.
   b. It is normally used for connecting stations in a physical star topology.
   c. A hub organizes the cables and relays signal to the other media segments as shown in Fig. 3.31.1.

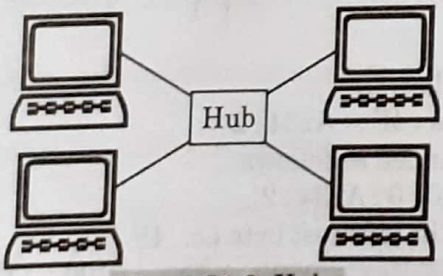


Fig. 3.31.2. Hub.

3. **Bridges :**
   a. A bridge can operate the physical as well as in the data link layer of the OSI model.
   b. It can regenerate the signal that it receives and it can check the physical (MAC) addresses of source and destination mentioned in the header of a frame.
4. **Routers :**
   a. Routers are devices that connect two or more networks as by using IP addresses.
   b. Various types of network can be interconnected through routers as shown in Fig. 3.31.3.

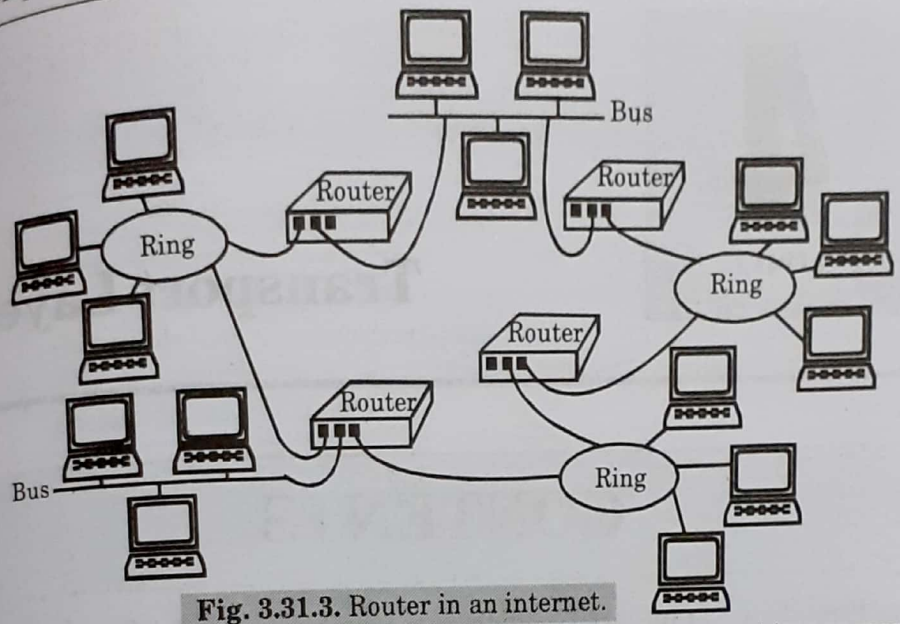


Fig. 3.31.3. Router in an internet.

c. Routers use logical and physical addressing to connect two or more logically separate networks.

5. Gateways :

a. A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks as shown in Fig. 3.31.4.

b. Gateway comprise of software, dedicated hardware or a combination of both.

c. Gateway operates through all the seven layers of the OSI model and all five layers of the internet model.

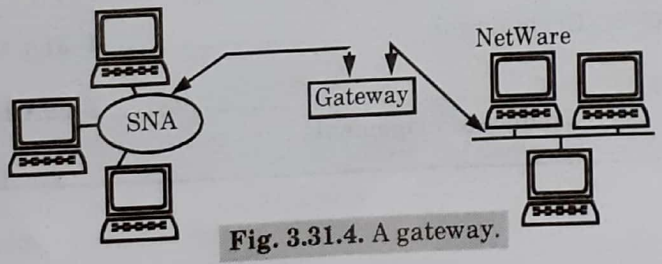


Fig. 3.31.4. A gateway.

6. Switches :

a. A switch is a device which provides bridging functionality with greater efficiency.

b. A switch acts as a multiport bridge to connect devices or segments in a LAN.

c. The switch acts as a buffer for each link to which it is connected.

d. When it receives a packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link.

e. If the outgoing link is free, the switch sends the frame to that particular link.

☺☺☺

4 UNIT

Transport Layer

CONTENTS

Part-1	:	Transport Layer-Design Issues	**4–2A to 4–5A**
Part-2	:	Connection Management	**4–5A to 4–12A**
Part-3	:	Session Layer-Design Issues ..... Remote Procedure Call	**4–12A to 4–15A**
Part-4	:	Presentation Layer : ..... Design Issues	**4–15A to 4–16A**
Part-5	:	Data Compression Techniques	**4–16A to 4–21A**
Part-6	:	Cryptography	**4–21A to 4–28A**
Part-7	:	TCP ..... Window Management	**4–29A to 4–30A**

PART-1

Transport Layer-Design Issues.

CONCEPT OUTLINE

- UDP is a connectionless protocol which is suitable for application that needs fast, efficient transmission.
- TCP is a connection oriented protocol which rearranges data packets in the specified order.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.1. **Write a short note on process-to-process delivery.**

OR

How transport layer is meant for process-to-process delivery ?

Answer

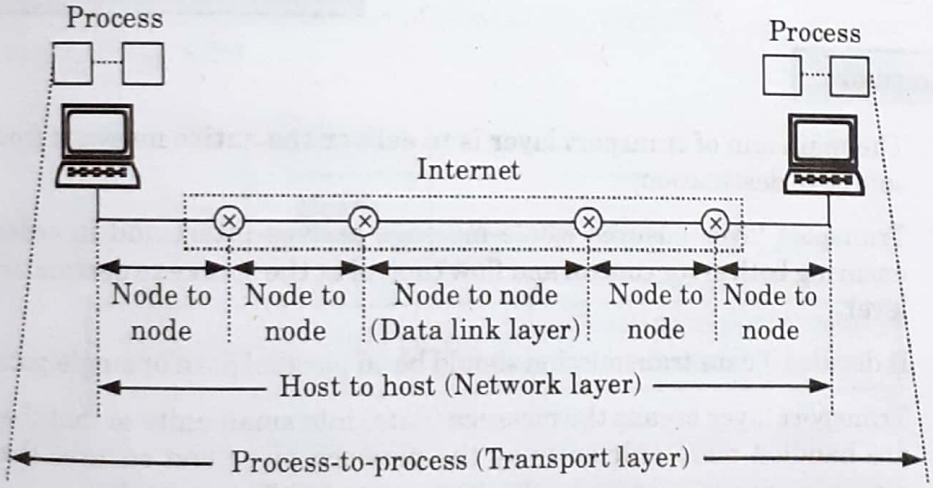


Fig. 4.1.1. Types of data deliveries.

1. The data link layer performs a node to node delivery. The network layer carries out the datagram delivery between two hosts (host to host delivery).
2. The real communication takes place between two process application programs for which we need the process-to-process delivery.
3. The transport layer takes care of the process-to-process delivery. In this a packet from one process is delivered to the other process.

4. The relationship between the communicating processes is the client-server relationship.

Que 4.2. **What are the design issues in transport layer ?**

Answer

Design issues with transport layer :

1. Accepting data from session layer, split it into segments and send to the network layer.
2. Ensure correct delivery of data with efficiency.
3. Error control and flow control.
4. End-to-end delivery of the packet.
5. Combining packets into message segment at receiver side.
6. Connection management.

Que 4.3. **Enumerate how the transport layer ensures that the complete message arrives at the destination and in the proper order.**

AKTU 2016-17, Marks 7.5

AKTU 2017-18, Marks 10

Answer

1. The main aim of transport layer is to deliver the entire message from source to destination.
2. Transport layer ensures whole message arrives intact and in order, ensuring both error control and flow control at the source to destination level.
3. It decides if data transmission should be on parallel path or single path.
4. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer and ensures that message arrives in order by checking error and flow control.
   a. **Flow control :** Flow control is performed end to end in this layer.
   b. **Error control :** Error control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error correction is done through retransmission.

Que 4.4. **Write a short note on User Datagram Protocol (UDP).**

Answer

1. User Datagram Protocol (UDP) provides a connectionless packet service that offers unreliable 'best effort' delivery.
2. Applications that do not require an acknowledgement of receipt of data, for example, audio or video broadcasting uses UDP.
3. UDP is also used by applications that typically transmit small amounts of data at one time, for example, the Simple Network Management Protocol (SNMP).
4. UDP provides a mechanism that application programs use to send data to other application programs.
5. UDP provides protocol port numbers to distinguish between multiple programs executing on a single device.
6. That is, an addition to the data sent, each UDP message contains both a destination port number and a source port number. This makes it possible for the UDP software at the destination to deliver the message to the correct application program, and for the application program to send a reply.
7. UDP packets are called as user datagram.

Que 4.5. Discuss the header format of UDP.

Answer

UDP have a fixed size header of 8-bytes. The format of user datagram is as shown in Fig. 4.5.1.

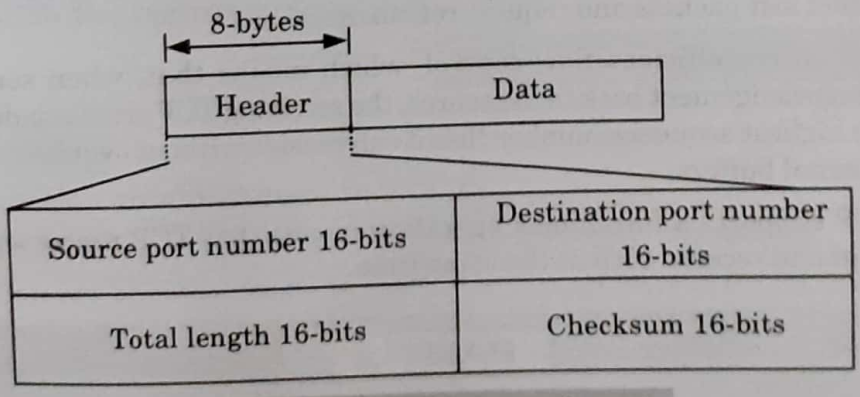


Fig. 4.5.1. User datagram format.

The UDP header is divided into the following four 16-bit fields :

1. **Source port :** Source port is an optional field, which indicates that port of the sending process and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.

2. **Destination port :** Destination port has a meaning within the context of a particular internet destination address.
3. **Length :** This is the size in bytes of the UDP packet, including the header and data. The minimum length of the header is 8-bytes.
4. **Checksum :** This is used to verify the integrity (*i.e.*, to detect errors) of the UDP header. The checksum is performed on a "pseudo header" consisting of information obtained from the IP header (source and destination address) as well as the UDP header.

Que 4.6. What do you mean by Transmission Control Protocol (TCP) ?

Answer

1. TCP (Transmission control protocol) is a connection-oriented protocol.
2. The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model.
3. Among the services, TCP provides stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.
4. With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers.
5. TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork.
6. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.
7. TCP offers efficient flow control, which means that, when sending acknowledgement back to the source, the receiving TCP process indicates the highest sequence number that it can receive without overflowing its internal buffers.
8. TCP supports a full-duplex operation means that TCP processes can send and receive both at the same time.

PART-2

Connection Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.7. **Differentiate between connection-oriented services with connectionless services.**

Answer

S. No.	Connection-oriented service	Connectionless service
1.	In connection-oriented service authentication is needed.	Connectionless service does not need any authentication.
2.	Connection-oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs.	Connectionless service protocol does not guarantee a delivery.
3.	Connection-oriented service is more reliable.	Connectionless service is less reliable.
4.	Connection-oriented service interface is stream based.	Connectionless service interface is message based.
5.	Packets travel sequentially.	Packets travel randomly.

Que 4.8. **Explain the three-way handshaking protocol to establish the transport level connection.**

AKTU 2016-17, 2017-18; Marks 10

Answer

Connection establishment in TCP :

1. To establish a connection, TCP uses a three-way handshake.
2. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections, this is called a passive open.
3. Once the passive open is established, a client may initiate an active open.
4. To establish a connection, the three-way (or 3-step) handshake occurs :
   a. **SYN :** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value *A*.
   b. **SYN-ACK :** In response, the server replies with a SYN-ACK. The acknowledgement number is set to one more than the received

sequence number $(A + 1)$, and the sequence number that the server chooses for the packet is another random number, B.

c. **ACK :** Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value *i.e.*, $A + 1$, and the acknowledgement number is set to one more than the received sequence number *i.e.*, $B + 1$.

5. At this point, both the client and server have received an acknowledgement of the connection.
6. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged.
7. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged.
8. With these, a full-duplex communication is established.

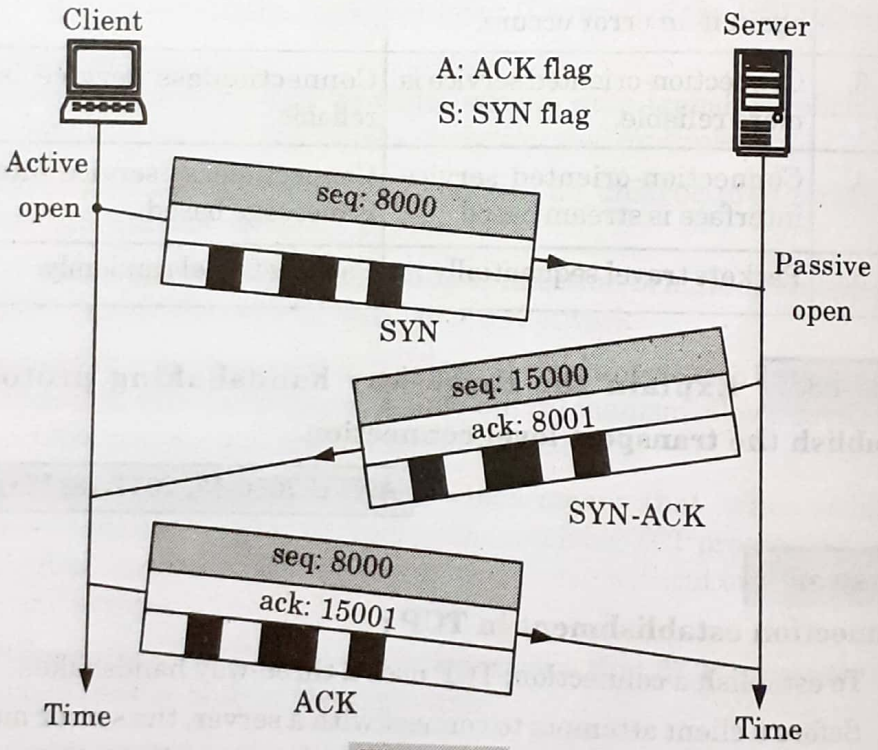


Fig. 4.8.1.

Que 4.9. Explain about the TCP header and working of TCP protocol and differentiate between TCP and UDP with frame format.

AKTU 2013-14, 2016-17, 2017-18; Marks 10

Answer

The segment consists of a 20 to 60 byte header, followed by data from the application program. The header is 20 bytes if there are no options and upto 60 bytes if it contains options.

1. **Source port :** A 16-bit number identifying the application that TCP segment originated from within the sending host.

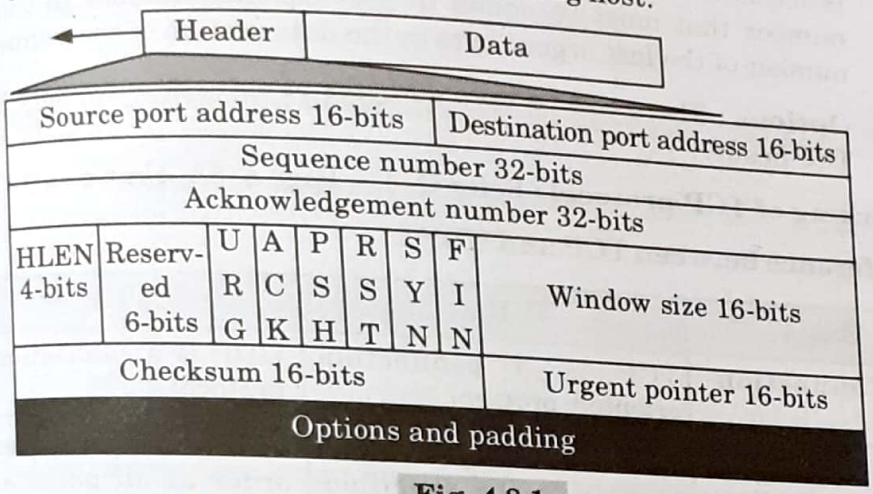


Fig. 4.8.1.

2. **Destination port :** A 16-bit number identifying the application that TCP segment is destined for on a receiving host.
3. **Sequence number :** A 32-bit number identifying the current position of the first data byte in the segment within the entire byte stream for the TCP connection.
4. **Acknowledgement number :** A 32-bit number identifying the next data byte that the sender expects from the receiver.
5. **Header length :** This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be in between 20 and 60.
6. **Reserved :** This is a 6-bit field reserved for future use.
7. **Control :** This field defines six different control bits or flags. One or more of these bits can be set at a time.
   i. **URG :** The value of urgent pointer field is valid.
   ii. **ACK :** The value of acknowledgement field is valid.
   iii. **PSH :** Push the data.
   iv. **RST :** Reset the data.
   v. **SYN :** Synchronize the sequence numbers during connection.
   vi. **FIN :** Terminate the connection.
8. **Window size :** This field defines the size of the window, in bytes, that the other party must maintain. The length of this field is 16-bits, which means that the maximum size of the window is 65,535 bytes.
9. **Checksum :** This 16-bit field contains the checksum. However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of the checksum for TCP is mandatory.

10. **Urgent pointer :** This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

11. **Options :** There can be upto 40-bytes of optional information in the TCP header.

Working of TCP protocol : Refer Q. 4.8, Page 4–6A, Unit-4.

Difference between TCP and UDP :

Basis	TCP	UDP
Connection	TCP is a connection oriented protocol.	UDP is a connectionless protocol.
Ordering of data packets	TCP rearranges data packets in the specified order.	UDP has no inherent order as all packets are independent of each other.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header size	TCP header size is 20-bytes.	UDP header size is 8-bytes.
Error checking	TCP does error checking.	UDP does error checking, but has no recovery option.

Que 4.10. **Draw the diagram of TCP header and explain the use of the following :**

i. **Source and destination port addresses**
ii. **Sequence and acknowledgement numbers**
iii. **Control bits**
iv. **Window size**
v. **Urgent pointer**

Describe the role of checksum field and option pad bytes.

AKTU 2014-15, Marks 10

Answer

TCP header : Refer Q. 4.9, Page 4–7A, Unit-4.

Use :

i. **Use of source and destination port address :** This field is used to identify the source and destination address of the host.

ii. **Use of sequence number :** The sequence number field is used to set a number on each TCP packet so that the TCP stream can be properly sequenced .

Use of acknowledgment number : This field is used when we acknowledge a specific packet a host has received.

iii. **Use of control bit :** This field is used to relay information between TCP peers.

iv. **Use of window size :** This field is used to indicate to the sender the amount of data that it is able to accept.

v. **Use of urgent pointer :** This field is used when the segment contain urgent data.

Role of checksum : The role of TCP/IP checksum is to detect corruption of data over a TCP or IPv4 connection.

Role of option pad bytes : Role of option pad byte is to ensure that the data part of the packet begins on a 32-bit boundary, and no data is lost in the packet.

Que 4.11. Explain TCP congestion control algorithm in internet. What is TCP segment header ? Also, discuss TCP connection management. **AKTU 2015-16, Marks 10**

Answer

TCP congestion control algorithm in internet :

1. Initialization for a given connection sets cwnd (congestion window) to one segment and ssthresh (when a loss occurs, fast retransmit is sent, half of the current cwnd is saved as ssthresh) to 65535 bytes.
2. The TCP output routine never sends more than the lower value of cwnd or the receiver's advertised window.
3. When congestion occurs (timeout or duplicate ACK), one-half of the current window size is saved in ssthresh. Additionally, if the congestion is indicated by a timeout, cwnd is set to one segment.
4. When new data is acknowledged by the other end, increase cwnd, but the way it increases depends on whether TCP is performing slow start or congestion avoidance. If cwnd is less than or equal to ssthresh, TCP is in slow start; otherwise, TCP is performing congestion avoidance.

TCP segment header : Refer Q. 4.9, Page 4–7A, Unit-4.

TCP connection management :

1. Connections are established in TCP using the three-way handshake.
2. To establish a connection, one side, the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source or nobody in particular.
3. The other side, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (for example, a password).
4. The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit off and waits for a response.
5. When this segment arrives at the destination, the TCP entity checks to see if there is a process that has done a LISTEN on the port given in the destination port field. If not, it sends a reply with the RST bit on to reject the connection.

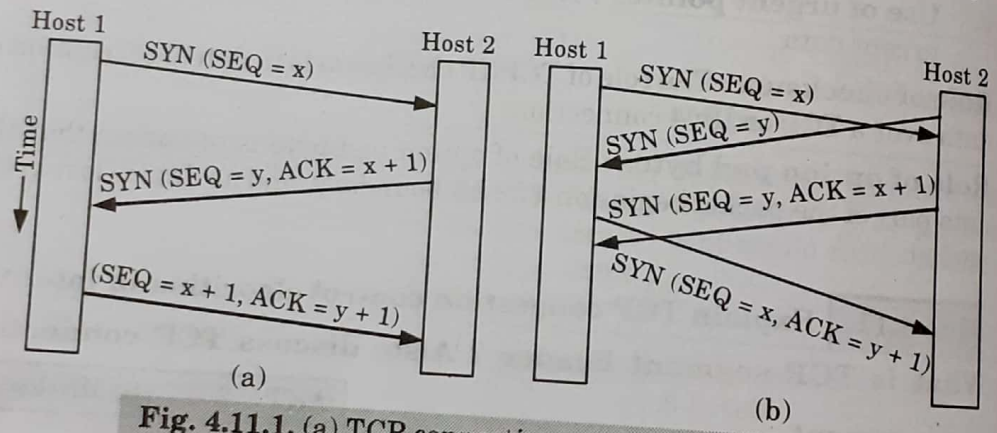


Fig. 4.11.1. (a) TCP connection establishment in the normal case. (b) call collision.

Que 4.12. Why TCP is preferred over UDP in some applications ? Explain the reasons and also mention those applications.

Answer

TCP is preferred over UDP in some application because of following reasons :

1. TCP ensures ordered delivery of a stream of bytes from user to server.
2. TCP is more reliable since it manages message acknowledgment and retransmissions in case of lost parts.
3. TCP transmissions are sent in a sequence and they are received in the same sequence.
4. TCP uses both error detection and error recovery.
5. TCP is a heavy weight connection requiring three packets for a socket connection and handles congestion control.

TCP are preferred over UDP in applications like multiplayer online games.

PART-3

Session Layer-Design Issues, Remote Procedure Call.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.13. Discuss the design issues of session layer. List the services provided by session layer.

Answer

Design issues with session layer :

1. To allow machines to establish sessions between them in a seamless fashion.
2. Provide enhanced services to the user.
3. To manage dialog control.
4. To provide services such as token management and synchronization.

List of session layer services :

1. **Authentication :**
   a. Authentication is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true.
   b. This involves confirming the identity of a person, the origins of an artifact, or assuring that a computer program is a trusted one.
2. **Permissions or access control :**
   a. Use of authentication and authorization is access control.
   b. Access is controlled by insisting on an authentication procedure to identity the user.
3. **Checkpoints :** Session layer is responsible for creating several checkpoints that are also treated as recovery points *i.e.*, in case of failure the system rollback to its previous checkpoint configuration or action.

Que 4.14. Write a short note on Remote Procedure Call (RPC).

Answer

1. When a process on machine-1 calls a procedure on machine-2, then the calling process on machine-1 is suspended and execution of the called

procedure takes place on machine-2 and no message passing is visible to the programmer. This technique is called as RPC (Remote Procedure Call).

2. The calling procedure is known as client and the called procedure is known as the server.
3. The principle behind RPC is to make a remote procedure call look like as a local call.
4. To call a remote procedure, the client program should be bound with a small library procedure called as client-stub which represents the server procedure in the client's address space.
5. Similarly a server is bound with a procedure called as the server-stub.
6. Fig. 4.14.1 shows the actual steps in making RPC.

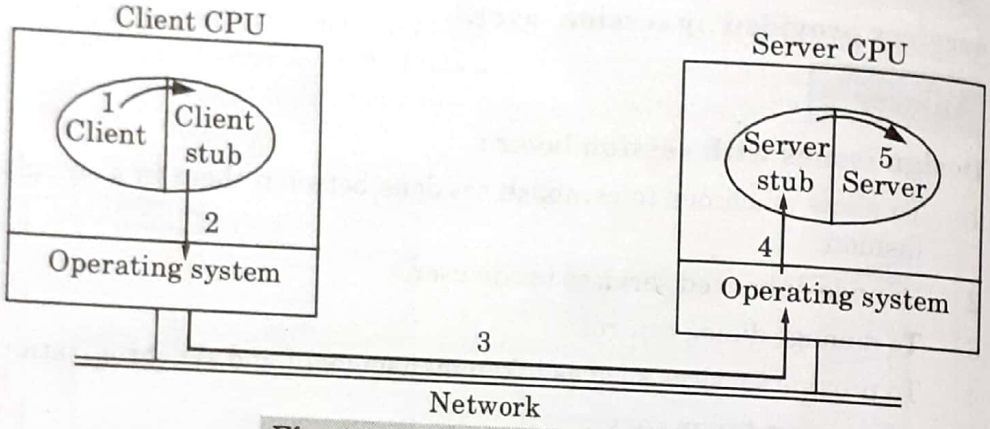


Fig. 4.14.1. Steps in making RPC.

Step 1 : Client calls the client-stub. This is a local procedure call with the parameters pushed on to the stack in the normal way.

Step 2 : Client-stub packs the parameters into a message and makes a system call to send the message. Packing the parameters is called as marshaling.

Step 3 : The message is sent from client machine to server machine.

Step 4 : The incoming packet is passed to the server-stub.

Step 5 : Server-stub calls the server procedure with the unmarshaled parameters.

7. The reply from server to client traces the same path in the opposite direction.

Que 4.15. Discuss the problem related to RPC.

Answer

Problems related to RPC :

1. It is not possible to pass pointers because client and server are in different address space.

2. It becomes impossible for the client-stub to marshal the parameters, the size of which is not known.
3. The problem is that it is not always possible to find out the types of the parameter, not even from a formal specification or code itself.
4. Generally the calling and called procedures can communicate by using global variables in addition to using parameters. But if the called procedure is moved to a remote machine, then the code will fail because the global variables are not being shared anymore.

Que 4.16. Discuss the RPC design and implementation issues.

AKTU 2014-15, Marks 05

Answer

Design and implementation issues in RPC :

1. **Structure :**
   i. A widely used organization for RPC mechanisms is based on the concept of stub procedures.
   ii. When a program (client) makes a remote procedure call, say $p(x, y)$ it actually makes a local call on a dummy procedure or a client-stub procedure corresponding to procedure P.
   iii. The client-stub procedure constructs a message containing the identity of the remote procedure and parameters, if any, to be passed.
   iv. It then sends the message to the remote server machine.
   v. When the remote procedure completes execution, the control returns to the server-stub procedure.
   vi. The server-stub procedure passes the results back to the client-stub procedure at the calling machine, which returns the results to the client.
2. **Binding :**
   i. Binding is a process that determines the remote procedure, and the machine on which it will be executed, upon a remote procedure invocation.
   ii. The binding process may also check the compatibility of the parameters passed and the procedure type called with what is expected from the remote procedure.
   iii. One approach for binding in the client-server model makes use of a binding server.
3. **Parameter and result passing :**
   i. To pass parameters or results to a remote procedure, a stub procedure has to convert the parameters and results into an appropriate representation first and then pack them into a buffer in a form suitable for transmission.

ii. After the message is received, the message must be unpacked.

iii. This approach requires the machine to know how to convert all the formats that can possibly be used. This approach also has poor portability because whenever a new representation is introduced into the system, existing software needs to be updated.

4. **Error handling, semantics and correctness :** A remote procedure call can fail for at least two reasons : computer failures and communication failures. Handling failures in distributed systems is difficult.

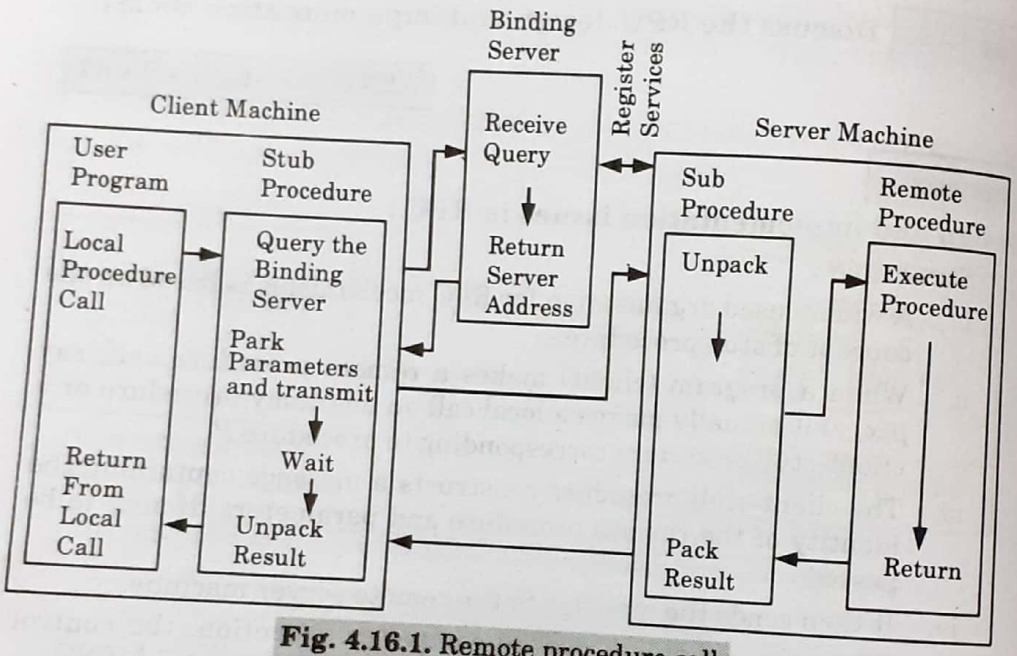


Fig. 4.16.1. Remote procedure call.

PART-4

Presentation Layer : Design Issues.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.17. **Discuss the design issues in presentation layer. Write the functions of presentation layer.**

Answer

Design issues in presentation layer :

1. To manage and maintain the syntax and semantics of the information transmitted.

2. Encoding data in a standard agreed upon way. For example : String, double, date, etc.
3. Perform standard encoding on wire.

Functions of presentation layer :

1. **Translation :** It translates data between the formats the network requires and the format the computer expects.
2. **Encryption :** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression :** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of data compression is to reduce the number of bits to be transmitted. It is important in transmitting multimedia such as audio, video, text etc.

The presentation layer has following issues :

1. **Data format :** Converting the complex data structures used by an application - strings, integers, structures, etc., into a byte stream transmitted across the network, representing information in such a way that communicating peers agree to the format of the data being exchanged.
2. Compressing data to reduce the amount of transmitted data (for example, to save money).
3. **Security and privacy issues :**
   - i. **Encryption :** Scrambling the data so that only authorized participants can unscramble the messages of a conversation.
   - ii. **Authentication :** Verifying that the remote party really is the party they claim to be rather than an impostor.

PART-5

Data Compression Techniques.

CONCEPT OUTLINE

- Data compression techniques :
  - i. Lossless compression
  - ii. Lossy compression

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.18. Describe data compression. What are the techniques/ types of data compression ?

Answer

Data compression :

1. Data compression is the way of downloading the compressed form of text, audio and video data using the computer.
2. Data compression is essential for efficient storage and transmission of different type of data.
3. A data compression system consists of an encoder and a decoder.
4. The encoder performs compression of the incoming data and decoder is used for decompression and reconstruction as shown in Fig. 4.18.1.

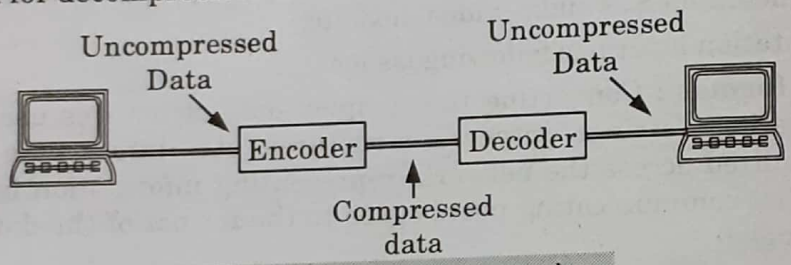


Fig. 4.18.1. Data compression.

Types of compression :

1. **Lossless compression (or data compaction) :**
   a. In lossless compression, the redundant information contained in the data is removed.
   b. In lossless compression, there is no loss of information.
   c. Lossless compression has lower compression ratio.
2. **Lossy compression :**
   a. In lossy compression, there is a loss of information in a controlled manner.
   b. The lossy compression is not completely reversible.
   c. The lossy compression has higher compression ratio.

Que 4.19. Write short notes on :

i. Digital audio
ii. Audio compression
iii. Streaming audio

AKTU 2013-14, Marks 10

Answer

i. Digital audio :

1. Digital audio is a technology that is used to record, store, manipulate, generate and reproduce sound using audio signals that have been encoded in digital form.

2. It also refers to the sequence of discrete samples that are taken from an analog audio waveform.
3. A digital audio signal may be stored or transmitted.
4. Digital audio can be stored on a CD, a digital audio player, a hard drive, a USB flash drive, or any other digital data storage device.
5. Digital audio can be carried over digital audio interfaces.
6. Digital audio can be carried over a network using audio over Ethernet, audio over IP or other streaming media standards and systems.

ii. Audio compression :

1. Before audio can be transmitted over a computer network, it must be digitized and compressed.
2. Audio compression is important because uncompressed audio consumes tremendous amount of storage and bandwidth.
3. Two techniques used for audio compression :

a. Predictive encoding :

i. In predictive encoding the difference between the samples are encoded instead of encoding all the sampled values.

ii. This type of compression is normally used for speech. Several standards have been defined such as GSM (13 Kbps), G.729 (8 Kbps) etc.

b. Perceptual encoding (MP3) :

i. The most common compression technique that is used to create CD-quality audio is based on the perceptual encoding technique.

ii. MP3 (MPEG audio layer 3) uses this technique.

iii. MP3 uses two phenomena, frequency and temporal masking, to compress audio signal.

iv. MP3 produces three data rates : 96 Kbps, 128 Kbps and 160 Kbps.

v. The rate is based on the range of the frequencies in the original analog audio.

iii. Streaming audio : To understand the concept of streaming audio we have following four approaches :

a. Using a web server :

i. A compressed audio file can be downloaded as a text file.

ii. The client (browser) can use the services of HTTP and send a GET message to download the file.

iii. The web server can send the compressed file to the browser.

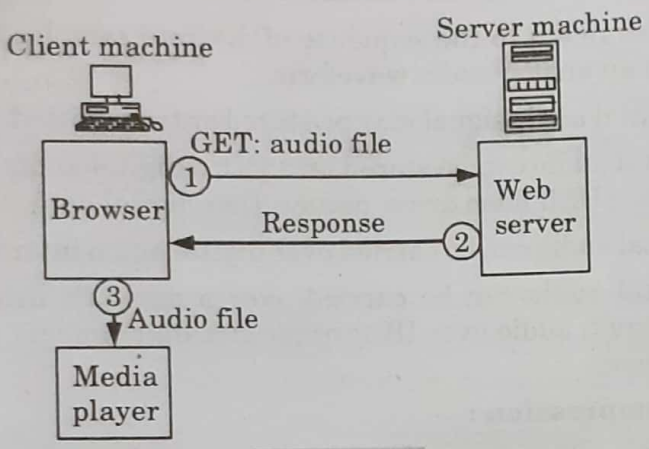


Fig. 4.19.1.

iv. The browser can then use a help application, normally called a media player, to play the file as shown in Fig. 4.19.1.

v. This approach is very simple and does not involve streaming.

b. Using a web server with a metafile :

i. In another approach, the media player is directly connected to the web server for downloading the audio file.

ii. The web server stores two files : the actual audio file and a metafile that holds information about the audio file. Fig. 4.19.2 shows the steps in this approach.

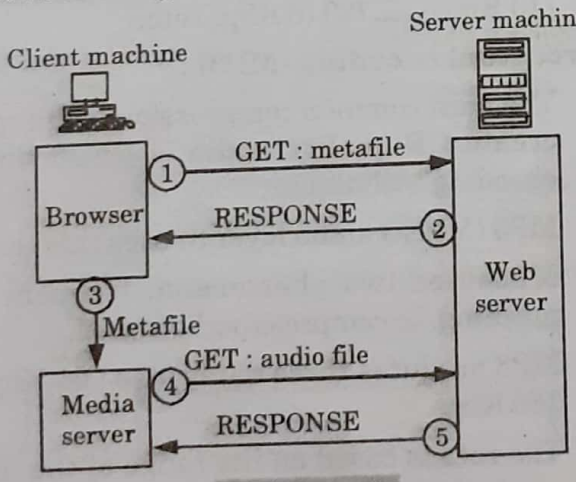


Fig. 4.19.2.

c. Using a media server :

i. The problem with the second approach is that the browser and the media player both use the services of HTTP. HTTP is designed to run over TCP.

ii. This is appropriate for retrieving the metafile, but not for retrieving the audio file.

iii. The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of streaming.

iv. We need to dismiss TCP and its error control; we need to use UDP.

v. However, HTTP, which accesses the web server, and the web server itself are designed for TCP; we need another server, a media server, as shown in Fig. 4.19.3.

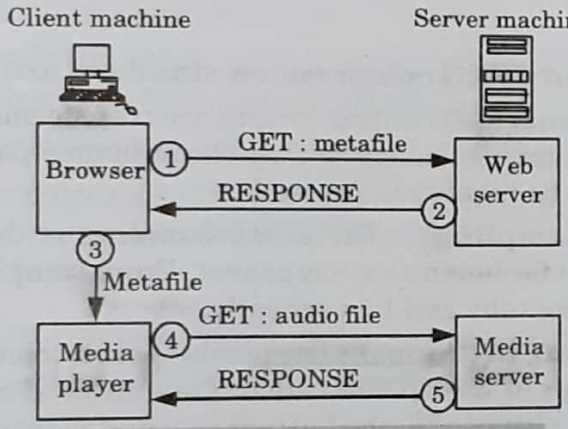


Fig. 4.19.3. Using a media server.

d. Using a media server and RTSP :

i. The Real Time Streaming Protocol (RTSP) is a control protocol designed to add more functionalities to the streaming process.

ii. Using RTSP, we can control the playing of audio.

iii. RTSP is an out-of-band control protocol that is similar to the second connection in FTP. Fig. 4.19.4 shows a media server and RTSP.

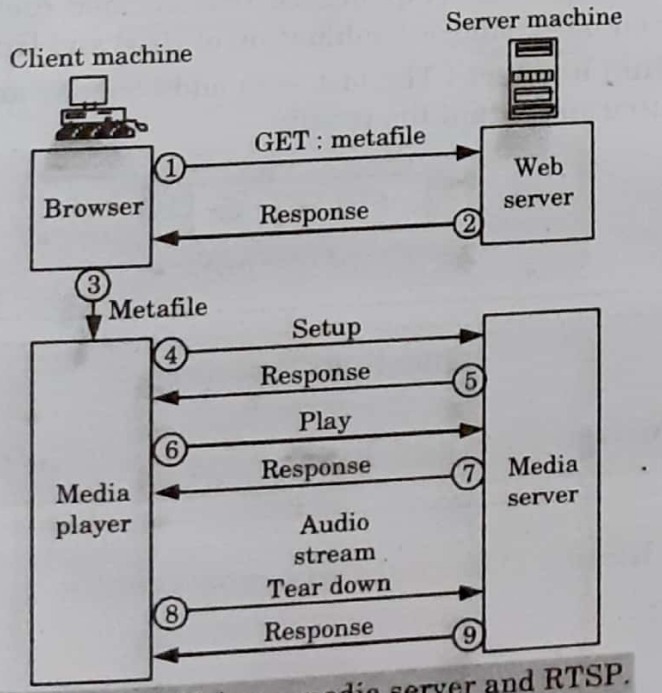


Fig. 4.19.4. Using a media server and RTSP.

Que 4.20. **Discuss the different steps of JPEG compression standard.** **AKTU 2014-15, Marks 05**

Answer

Different steps of JPEG compression standard are :

Step 1 (Transformation) : Colour images are transformed from RGB into a luminance/chrominance image so that chrominance part can lose much data and thus can be highly compressed.

Step 2 (Down sampling) : The down sampling is done for coloured component and not for luminance component. Down sampling is done either at a ratio 2:1 horizontally and 1:1 vertically.

Step 3 (Organizing in groups) : The pixels of each colour component are organized in groups of 8 × 2 pixels called "data units" if number of rows or column is not a multiple of 8, the bottom row and rightmost columns are duplicated.

Step 4 (Discrete Cosine Transform) : Discrete Cosine Transform (DCT) is then applied to each data unit to create 8×8 map of transformed components.DCT involves some loss of information due to the limited precision of computer arithmetic.

Step 5 (Quantization) : Each of the 64 transformed components in the data unit is divided by a separate number called its 'Quantization Coefficient (QC)' and then rounded to an integer.

Step 6 (Encoding) : The 64 quantized transformed coefficients of each data unit are encoded using a combination of RLE and Huffman coding.

Step 7 (Adding header) : The last step adds header and all the JPEG parameters used and output the result.

PART-6

Cryptography.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.21. **Write a short note on cryptography.**

Answer

1. Cryptography is the study of secret (crypto) writing (graphy).
2. It is concerned with developing algorithms that may be used to :

a. Conceal the context of some message from all except the sender and recipient (privacy or secrecy).

b. Verify the correctness of a message to the recipient (authentication).

3. It forms the basis of many technological solutions to computer and communications security problems.
4. Cryptography is the encoding of messages to render them unreadable by anyone other than their intended recipient(s).
5. Caesar cipher is one of the traditional cryptography techniques.
6. In modern cryptography it is essential to secure the computer network which is done using complex algorithms implemented on high speed computer systems.

Que 4.22. Define cryptography with the help of block diagram of symmetric and asymmetric key cryptography.

AKTU 2013-14, Marks 10

Answer

Cryptography : Refer Q. 4.21, Page 4–21A, Unit-4.

Symmetric key cryptography :

1. In symmetric key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

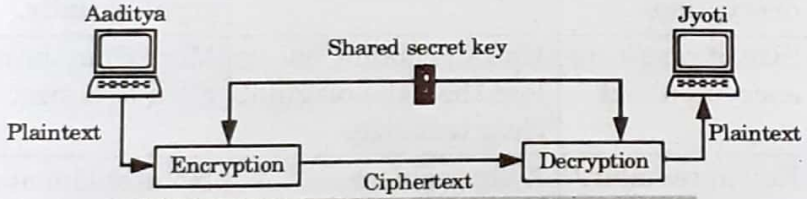


Fig. 4.22.1. Symmetric key cryptography.

2. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

Asymmetric key cryptography :

1. In asymmetric or public key cryptography, there are two keys : a private key and a public key.
2. The private key is kept by the receiver. The public key is announced to the public.
3. In Fig. 4.22.2 imagine Aaditya wants to send a message to Jyoti. Aaditya uses the public key to encrypt the message. When the message is received by Jyoti, the private key is used to decrypt the message.
4. In public key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption.

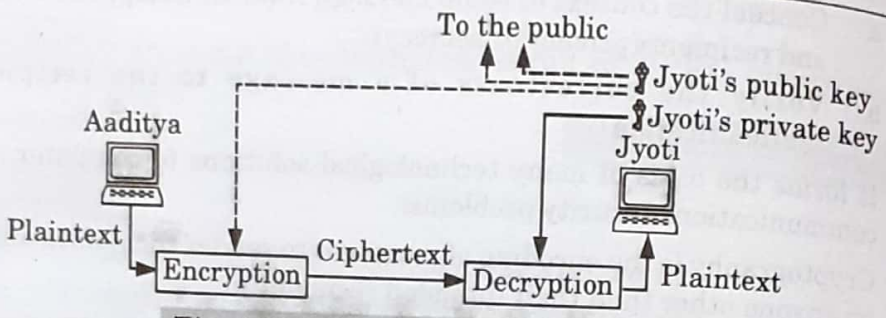


Fig. 4.22.2. Asymmetric key cryptography.

Que 4.23. Distinguish between symmetric and asymmetric key cryptography.

Answer

S. No.	Characteristic	Symmetric key cryptography	Asymmetric key cryptography
1.	Key used for encryption/ decryption	Same key is used for encryption and decryption.	One key used for encryption and another different key is used for decryption.
2.	Speed of encryption/ decryption	Very fast.	Fast, but less than symmetric key cryptography.
3.	Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
4.	Key agreement/ exchange	A big problem.	No problem at all.
5.	Number of key required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue.	Same as the number of participants, so scales up quite well.
6.	Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks).

Que 4.24. **Write a short note on RSA encryption algorithm.**

Answer

i. RSA is the most widely used public key algorithm.

ii. The principle of RSA is based on a fact that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back.

iii. The algorithm is as follows :

1. Take two very large prime numbers A and B of equal lengths and obtain their product (N).

$$\therefore \quad N = A \times B \qquad \ldots(4.24.1)$$

2. Subtract 1 from A as well as B and take the product T.

$$\therefore \quad T = (A - 1)(B - 1) \qquad \ldots(4.24.2)$$

3. Choose the public key (E) which is a randomly chosen number such that it has no common factors with T.

4. Obtain the private key (D) as follows :

$$D = E^{-1} \bmod T \qquad \ldots(4.24.3)$$

5. The rule (algorithm) for encryption of a block of plaintext M into ciphertext C is as follows :

$$C = M^E \bmod N \qquad \ldots(4.24.4)$$

That means the plaintext M is raised to the power of E (public key) and then divided by N. The mod term in equation (4.24.4) tells us that the remainder of this division is sent as the ciphertext C as shown in Fig. 4.24.1.

6. The received message C at the receiver is decrypted to obtain the plaintext back by using the following rule (algorithm).

$$M = C^D \bmod N \qquad \ldots(4.24.5)$$

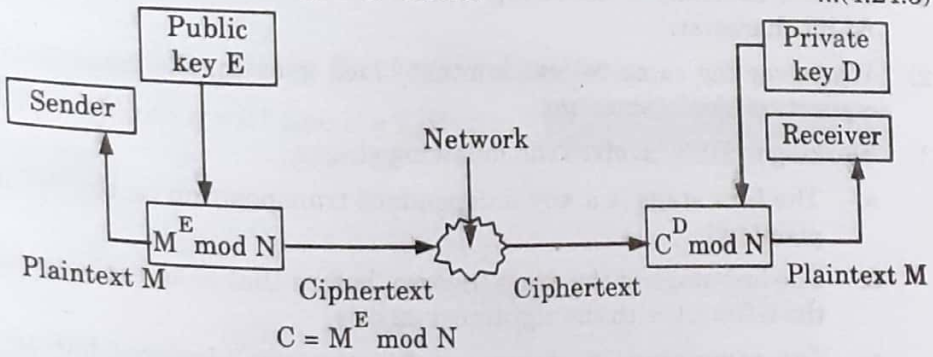


Fig. 4.24.1. Encryption and decryption in RSA.

Que 4.25. **Explain data encryption standard algorithm and its working in detail.**

Answer

1. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption.
2. DES is based on a symmetric key algorithm that uses a 56-bit key as shown in Fig. 4.25.1.

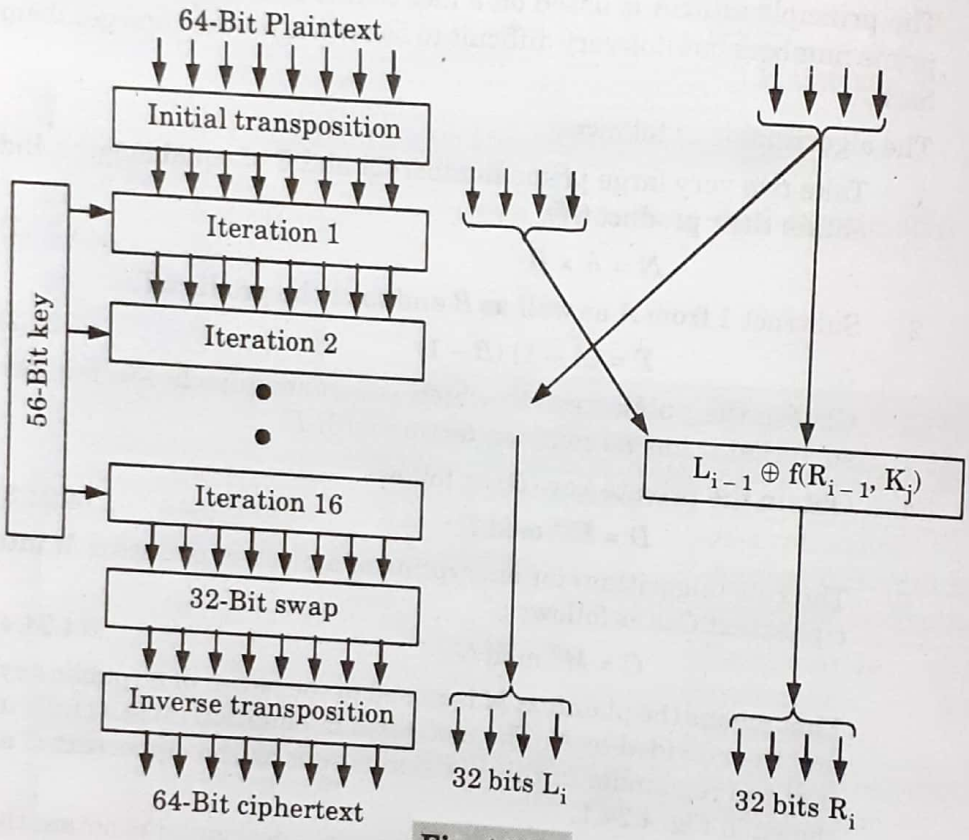


Fig. 4.25.1.

Working of DES :

1. DES is basically a mono-alphabetic substitution cipher using a 64-bit character.
2. Whenever the same 64-bit plaintext block goes in, the same 64-bit ciphertext block comes out.
3. Working of DES involves the following stages :
   a. The first stage is a key independent transposition on the 64-bit plaintext.
   b. The last stage is the exact inverse, before that is an exchange of the leftmost with the rightmost 32 bits.
   c. The remaining 16 stages are functionally identical but are parameterized by different functions of the key.
   d. The left output of an iteration stage is simply a copy of the right input. The right output is the exclusive OR of the left input and a

function of the right input and the key for this iteration. All the complexity lies in this functions which consists of four sequential steps.

Que 4.26. **Differentiate between the block cipher with transposition cipher.** **AKTU 2014-15, Marks 05**

Answer

S. No.	Block cipher	Transposition cipher
1.	A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.	Transposition cipher is the cipher in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
2.	Errors in transmitting one block generally do not affect other blocks.	Error in one letter will affect the whole ciphertext.
3.	Encryption process is slow.	Encryption process is fast.
4.	Security of block cipher depends on the design of encryption function.	Transposition cipher can be made more secure by performing more than one transposition.
5.	Algorithm breaks the plaintext into blocks and operates on each block independently.	Algorithm breaks the plaintext into letters and operates on each letter independently.

Que 4.27. **Using the RSA public key cryptosystem with $a = 1, b = 2$ etc.**

I. If $p = 7$ and $q = 11$, list five legal values for d.

II. If $p = 13$ and $q = 31$ and $d = 7$, find e. **AKTU 2014-15, Marks 05**

Answer

I.

$$p = 7 \qquad q = 11$$

$$n = p \times q = 7 \times 11 = 77$$

$$\phi(n) = (7 - 1) \times (11 - 1) = 6 \times 10 = 60$$

Choose a number relatively prime to $\phi(n)$ and satisfy the condition $1 < e < 60$ such that $gcd\,(\phi, e) = 1$

i.e., e = {13, 17, 19, 23, 29. 31, 37, 41, 43, 47, 53, 59}

Now, taking $e = 13$

$ed \bmod \phi(n) = 1$

$d = e^{-1} \bmod \phi(n)$

$d = 13^{-1} \bmod 60$

$d = 13^{\phi(77)-1} \bmod 60$

$d = 13^{59} \bmod 60$

$d = [[(13 \bmod 60)^4]^{13} ((13)^7 \bmod 60)] \bmod 60$

$d = 37 \bmod 60$

$d = 37$

Now, taking $e = 17$

$d = e^{-1} \bmod \phi(n)$

$d = 17^{-1} \bmod 60$

$d = 17^{59} \bmod 60$

$d = [[(17 \bmod 60)^3]^{17} ((17)^8 \bmod 60)] \bmod 60$

$d = (53 \times 1) \bmod 60$

$d = 53$

Taking $e = 19$

$d = e^{-1} \bmod \phi(n)$

$d = 19^{-1} \bmod 60$

$d = 19^{59} \bmod 60$

$d = [[(19 \bmod 60)^3]^{19} ((19)^2 \bmod 60)] \bmod 60$

$d = (19)^{19} \times 1 \bmod 60$

$d = [((19 \bmod 60)^1)^{18} \times 19 \times 1] \bmod 60$

$d = 1 \times 1 \times 19$

$d = 19$

Similarly by taking $e = 29$, we get $d = 29$

and $e = 37$, we get $d = 13$

Five legal value of d are 37, 53, 19, 29, 13.

II.

$p = 13 \quad q = 31 \quad d = 7$

$n = p \times q = 13 \times 31 = 403$

$\phi(n) = (13 - 1) \times (31 - 1) = 12 \times 30 = 360$

$ed \bmod \phi(n) = 1$

$e = d^{-1} \bmod \phi(n)$

$= 7^{-1} \bmod 360$

$= 7^{\phi(403)-1} \bmod 360$

$= 7^{359} \bmod 360$

$= [(7^{11} \bmod 360)^{32} \times (7^7 \bmod 360)] \bmod 360$

$= [(103)^{32} \bmod 360 \times 223] \bmod 360$

$= [(103^4 \bmod 360)^8 \times 223] \bmod 360$

$$= [(121^4 \bmod 360)^2 \times 223] \bmod 360$$
$$= [(121)^2 \bmod 360 \times 223] \bmod 360$$
$$= (241 \times 223) \bmod 360$$
$$= 103$$

Que 4.28. Write a short note on voice over IP.

AKTU 2015-16, 2017-18; Marks 05

Answer

1. Voice over Internet Protocol (VoIP) is a technology used for delivering different kinds of data from a source to a destination using IP (Internet Protocol).
2. The data may be in many forms, including files, voice communication, pictures, fax or multimedia messages. VoIP is most often used for telephone calls, which are almost free of charge.
3. VoIP uses codes to encapsulate audio into data packets, transmit the packets across an IP network and unencapsulate the packets back into audio at the other end of the connection.
4. By eliminating the use of circuit-switched networks for voice, VoIP reduces network infrastructure costs, enables providers to deliver voice services over their broadband and private networks, and allows enterprises to operate a single voice and data network

Que 4.29. What are the problems for full implementation of voice over IP ? Did you think we will stop using the telephone network very soon ?

AKTU 2014-15, Marks 05

Answer

Problem for full implementation of VoIP are :

1. The computer must always be available in on mode with the internet connected.
2. Even if any one of the entities *i.e.*, the computer or internet fails to work, the telephone system will also not work.
3. There may be some delay in the voice due to problems in the internet.
4. The connection may lose in the middle if the internet connection is disconnected.
5. It may be susceptible to attacks.
6. The susceptibility of phone service to power failures can also occur.
7. The nature of IP makes it difficult to locate network users geographically and hence emergency calls cannot be routed easily.

No, we will not stop using telephone network.

PART-7

TCP, Window Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.30. Compare and contrast TCP with RTP. Are both doing the same things ?

AKTU 2014-15, Marks 05

Answer

S. No.	TCP	RTP
1.	TCP stands for Transmission Control Protocol.	RTP stands for Real Time Transport Protocol.
2.	It is a lossless protocol.	RTP is a stateless protocol,
3.	It is a slow process.	It is a faster than TCP.
4.	It cannot tolerate packet loss.	It can tolerate packet loss.
5.	TCP is not generally used for "real-time" streaming.	RTP is used for "real-time" streaming.

No, they are not doing the same things.

Que 4.31. What is the total delay (latency) for a frame size of 10 million bits that is being set up on link with 15 routers, each having 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 2×10^8 m/sec. The link has bandwidth of 6 Mbps.

AKTU 2015-16, Marks 10

Answer

We have, Latency = processing time + queuing time + transmission time + propagation time

Processing time = $15 \times 1\ \mu s = 15\ \mu s = 0.000015$ s

Queuing time = $15 \times 2\ \mu s = 30\ \mu s = 0.000030$ s

Transmission time = $(10{,}000{,}000)/(6\ \text{Mbps}) = 1.67$ s

Propagation time = $(3000\ \text{km})/(2 \times 10^8\ \text{m/s}) = 0.015$ s

$\therefore$ Latency = $0.000015 + 0.000030 + 1.67 + 0.015 = 1.685045$ s

Que 4.32. **A rectangular wave-guide ($a = 2$ cm, $b = 1$ cm) filled with deionized water ($\mu = 1$, $\xi = 81$) operates at 3 GHz. Determine all propagating modes and corresponding cut-off frequencies.**

AKTU 2015-16, Marks 10

Answer

For a general transverse electric (TE) or transverse magnetic (TM) mode, the cut-off frequency is given as :

$$f_c = \frac{v_0}{2\sqrt{\mu\xi}}\sqrt{\left(\frac{m}{a}\right)^2 + \left(\frac{n}{b}\right)^2} = \frac{3\times10^8}{2\sqrt{1\times81}}\sqrt{\left(\frac{m}{0.02}\right)^2 + \left(\frac{n}{0.01}\right)^2}$$

$$= 1.667\sqrt{0.25m^2 + n^2} \text{ GHz}$$

The cut-off frequencies as calculated from the equation for different values of m and n are given in the Table 4.32.1.

Table 4.32.1.

Cut-off frequency (in GHz) for TM modes				Cut-off frequency (in GHz) for TE modes				
	$n = 1$	$n = 2$	...		$n = 0$	$n = 1$	$n = 2$	
$m = 1$	1.863	3.436	...	$m = 0$	×	1.667	3.333	...
$m = 2$	2.357	3.727	...	$m = 1$	0.833	1.863	3.436	...
$m = 3$	3.005	⋱		$m = 2$	1.667	2.357	3.727	...
	⋮			$m = 3$	2.500	3.005	⋱	
				$m = 4$	3.333	⋮		
					⋮			

Since the operating frequency is 3 GHz, all the propagating modes and their cut-off frequencies are given in the Table 4.32.2.

Table 4.32.2.

Mode	Cut-off frequency (GHz)
TE_{10}	0.833
TE_{01}, TE_{20}	1.667
TE_{11}, TM_{11}	1.863
TE_{21}, TM_{21}	2.357
TE_{30}	2.500

☺☺☺

5

UNIT

Application Layer

CONTENTS

Part-1	:	Application Layer : File Transfer	**5–2A to 5–4A**
Part-2	:	Access and Management	**5–4A to 5–7A**
Part-3	:	Electronic Mail	**5–7A to 5–10A**
Part-4	:	Virtual Terminals ..... Other Applications	**5–10A to 5–18A**
Part-5	:	Example Network-Internet and Public Network	**5–18A to 5–21A**

PART-1

Application Layer : File Transfer.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.1. Explain application layer with its services.

Answer

Refer Q. 1.3, Page 1–4A, Unit-1.

Que 5.2. Write a short note on file transfer protocol.

AKTU 2013-14, Marks 2.5

AKTU 2015-16, 2017-18; Marks 05

Answer

1. FTP (File Transfer Protocol) is the simplest and most secure way to exchange files over the internet. The most common use for FTP is to download files from the internet.
2. FTP exists primarily for the transfer of data between two end points.
3. FTP creates both a control and a data connection in order to transfer files.
4. Within an active FTP session, the control connection is established from the client to the server, with the data connection established from the server to the client.

Que 5.3. How does FTP work ? Differentiate between passive and active FTP.

AKTU 2016-17, Marks 10

Answer

Working of FTP :

1. The client FTP application opens a control connection to the server on destination port 21, and specifies a source port as the source to which the FTP server should respond (using TCP).
2. The FTP server responds on port 21.
3. The FTP server and client negotiate the data transfer parameters.

4. The FTP server opens a second connection for data on port 20 to the original client.
5. The client responds on the data port, completing a TCP connection.
6. Data transfer begins.
7. The server indicates the end of the data transfer.
8. Client closes the connection once the data is received.
9. The data connection is closed.
10. The FTP connection is closed.

Difference between passive and active FTP :

S. No.	Passive FTP	Active FTP
1.	Passive FTP does not provide security to the FTP server.	Active FTP provides more security to the FTP server.
2.	Passive FTP does not have connection issues from firewalls.	Active FTP may cause problems because of firewalls.
3.	In passive FTP, the command channel and the data channel are established by the client.	In active FTP, client establishes the command channel and the server establishes the data channel.
4.	Passive mode is used as a default mode of a browser.	Active mode is not used as a default mode of a browser.

Que 5.4. **Write a short note on :**

i. **MIME**

ii. **TFTP**

AKTU 2013-14, Marks 05

Answer

i. **MIME :**

1. The Multipurpose Internet Mail Extension (MIME) protocol was developed to define a method of moving multimedia files through existing email gateways.
2. It offers a simple standardized way to represent and encode a wide variety of media types, including textual data in non-ASCII character sets, for transmission via internet mail.
3. MIME defines extensions to SMTP to support binary attachments of arbitrary format.

5. The original internet mail message protocol was designed with the text mail messages in mind.
6. MIME provides an extensible format for including multimedia components within a mail message.

ii. TFTP :

1. The TFTP stand for Trivial File Transfer Protocol.
2. It makes UDP (User Datagram Protocol) connections.
3. Its default port number is 69.
4. It is connectionless.
5. It is not reliable.
6. It has no acknowledgement policy.

PART-2

Access and Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.5. Write a short note on DNS in the internet.

AKTU 2013-14, 2015-16, 2017-18; Marks 05

Answer

1. The Domain Namespace (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the internet or a private network.
2. Domain Namespace is a system that can map a name to an address and conversely an address to a name.
3. To identify an entity, TCP/IP protocol uses the IP address, which uniquely identifies the connection of a host to the internet. However, people prefer to use names instead of addresses.
4. Therefore, in TCP/IP, this is the Domain Namespace (DNS).
5. DNS is a protocol that can be used in different platforms.
6. In the internet, the domain namespace (tree) is divided into three different sections : generic domains, country domains and inverse domain.

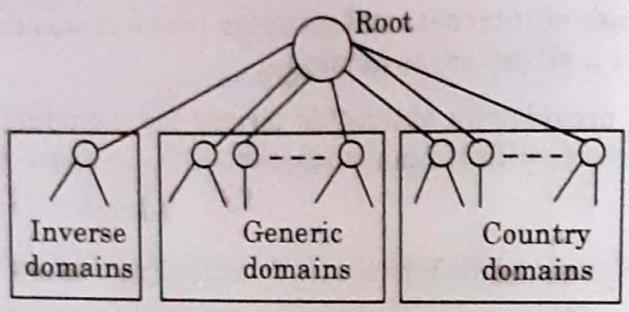


Fig. 5.5.1.

Que 5.6. **How does DNS perform data name resolution ? What are the different types of name servers ? Mention the DNS message format for query and reply messages.** **AKTU 2015-16, Marks 10**

OR

Discuss the message format of DNS.

Answer

DNS name resolution process : The process of mapping a name to an address or vice-versa is called as name address resolution.

Mapping names to addresses :

1. In this, the resolver gives a domain name to the server and requests for the corresponding IP address. The server checks the generic or country domains to get the corresponding address.
2. If the domain name is from the generic domain section the resolver receives a domain name such as xxx.yyy.zzz.edu.
3. The query is sent to the local DNS server for resolution by the resolver.
4. If the local server does not get the answer then, it will refer the resolver to other servers or asks them directly.
5. The same procedure is followed for a name country domain.

Mapping addresses to names :

1. In this, a client sends an IP address to a server and requests for its name. This type of query is called as PTR query.
2. To answer the PTR query, the DNS uses the inverse domain.
3. If the IP address is 142.36.48.118 then the resolver first inverts the address and adds two labels "in_addr" and "arpa" to it. So, the domain name sent is 118.48.36.142 in_addr.arpa.
4. This is received by the local DNS and resolved.

Different types of name server :

i. Primary server :

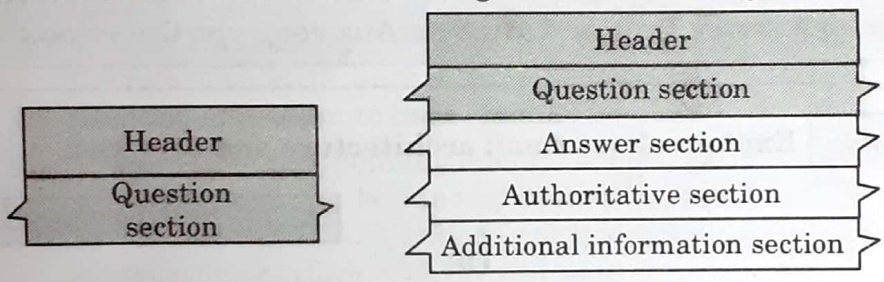
1. It is a server which stores a file about its zone.
2. It is authorized to create, maintain and update the zone file. It stores the zone file on a local disk.

ii. Secondary server :

1. This server transfers complete information about a zone from another server which may be primary or secondary server.
2. The secondary server is not authorized to create or update a zone file. If its zone file is to be updated, then it is to be done by the primary server.

DNS message format :

1. DNS has two types of messages and both of them have the same format.
   a. Query
   b. Response or reply
2. The formats of the two DNS messages are shown in Fig. 5.6.1.



(a) Query (b) Response or reply

Fig. 5.6.1.

3. Both query and reply messages have the same header format with some fields set to zero for query messages. The header is 12 byte long.
4. The header format for both the types of message is shown by shaded portions in Fig. 5.6.1.

Que 5.7. Define DNS and its requirement. Explain the specific features of it.

Answer

DNS : Refer Q. 5.5, Page 5–4A, Unit-5.

Requirements of DNS :

1. It should have unique name.
2. It should uniquely identify the corporate / company.

Features of DNS :

1. It associates various information with domain names assigned to each of the participating entities.

2. The Domain Namespace delegates the responsibility of assigning domain names and mapping those names to internet resources by designating authoritative name servers for each domain.
3. The Domain Namespace also specifies the technical functionality of the database service that is at its core.
4. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet Protocol Suite.
5. The Domain Namespace maintains the domain name hierarchy and provides translation services between it and the address spaces.

PART-3

Electronic Mail.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.8. Explain about email architecture and services.

AKTU 2013-14, Marks 10

OR

Write a short note on electronic mail. **AKTU 2015-16, Marks 05**

Answer

1. Electronic mail (or email) can be defined as the exchange of computer stored messages by telecommunications.
2. These messages, usually in text form, are sent from one computer to another via a telephone line. When we send a message, it is usually stored on a remote computer until the receiver goes online and checks the mail.
3. Email addresses often have three parts :
   i. The username
   ii. The host or domain name
   iii. The type of domain
4. **For example :** pagequantum@gmail.com, the first part, pagequantum is the username which identifies the recipient, next part gmail is the host or domain name of the mail server where the recipient's mailbox is located. The final part .com identifies the type of domain (For example,

: .com for commercial sites, .edu for educational institutions, .org for non-profit groups etc).

An email system consists of three subsystems :

1. **Mail transfer agent :** A Mail Transfer Agent (MTA) transfers email messages between hosts using SMTP.
   a. A message may involve several MTAs as it moves to its intended destination. Most users are totally unaware of the presence of MTA's, even though every email message is sent through at least one MTA.
   b. While the delivery of messages between machines may seem rather straightforward, the entire process of deciding if a particular MTA can or should accept a message for delivery is quite complicated.
2. **Mail delivery agent :** A Mail Delivery Agent (MDA) is utilized by the MTA to deliver email to a particular user's mailbox.
   a. In many cases, MDA is actually a Logical Delivery Agent (LDA), such as bin / mail or Procmail. However, sendmail can also play the role of an MDA, such as when it accepts a message for a local user and appends it to their email spool file.
   b. Any program that actually handles a message for delivery to the point where it can be read by Mail User Agent (MUA) can be considered as MDA. MDAs do not transport messages between systems or interface with the end user.
   c. Many users do not directly utilize MDAs, because only MTAs and MUAs are necessary to send and receive email. However, some MDAs may be used to sort messages before they are read by a user.
3. **Mail user agent :** A Mail User Agent (MUA) is a synonymous with an email client application.
   a. An MUA is a program that, at the very least, allows a user to read and compose email messages.
   b. Many MUAs are capable of retrieving messages via the POP or IMAP protocols, setting up mail boxes to store messages, and sending outbound messages to an MTA.

Que 5.9. What are the basic functions of email system ?

Answer

Email systems support five basic functions which are as follows :

1. **Composition :**
   a. The process of creating messages and to answer them is known as composition.

b. The system can also provide assistance with addressing and a number of header fields attached to each message.

2. **Transfer :**
   a. It is the process of moving messages from the sender to the recipient.
   b. This includes establishment of a connection from sender to destination or some intermediate machine, transferring the message, and breaking the connection.
3. **Reporting :** The reporting system is designed to tell the sender whether the message was delivered or rejected or lost.
4. **Displaying :**
   a. It is the process of displaying the incoming messages so that it can be read by the user.
   b. For this purpose simple conversions and formatting are required to be done.
5. **Disposition :**
   a. This is concerned with what the recipient does with the received message. Disposition is the final step in email system.
   b. Some of the possibilities are as follows :
      i. Throw after reading
      ii. Throw before reading
      iii. Save messages
      iv. Forward messages
      v. Process messages in some other way

Que 5.10. Explain the functioning of email gateway.

Answer

1. The email using SMTP can work properly if both the sender and the receiver are connected to the internet and can support TCP connections between them.
2. There can be many machines which are not on the internet but still want to send and receive email. This is made possible by using the application layer email gateways as shown in Fig. 5.10.1.
3. In Fig. 5.10.1, host *A* speaks only TCP/IP and RFC 822 whereas host *B* speaks only OSI TP4 and X.400. So, without the email gateway they cannot exchange email gateway. But email gateway allows them to exchange emails.
4. Host *A* first establishes a TCP connection to the gateway. Then it uses SMTP and transfer message (1) to the gateway message buffer.

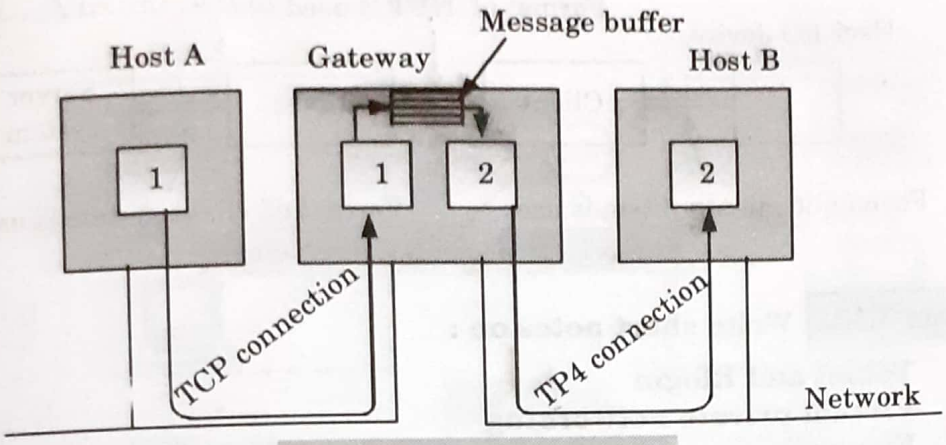


Fig. 5.10.1. Email gateway.

5. Then the gateway daemon establishes a TP4 connection (OSI equivalent of TCP) with the destination host *B*, and message (2) is transferred using the OSI equivalent of SMTP.
6. A gateway process is supposed to extract incoming messages from one queue and deposit them in the other.

PART-4

Virtual Terminals, Other Applications.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.11. Write a short note on virtual terminal.

Answer

1. NVT (Network Virtual Terminal) is a bi-directional device. It has a keyboard and a printer. The keyboard produces outgoing data and the printer responds to the incoming one. The outgoing data goes out over the Telnet connection.
2. NVT uses the client server architecture and it is treated as a half duplex device.
3. Fig. 5.11.1, illustrates the use of NVT by Telnet.
4. The character set for NVT is defined by the Telnet protocol. It is fairly easy to define the NVT format.
5. NVT uses the standard 7-bit ASCII representation for data. It includes 95 printable characters (letters, punctuation marks, digits etc.) and three control codes.

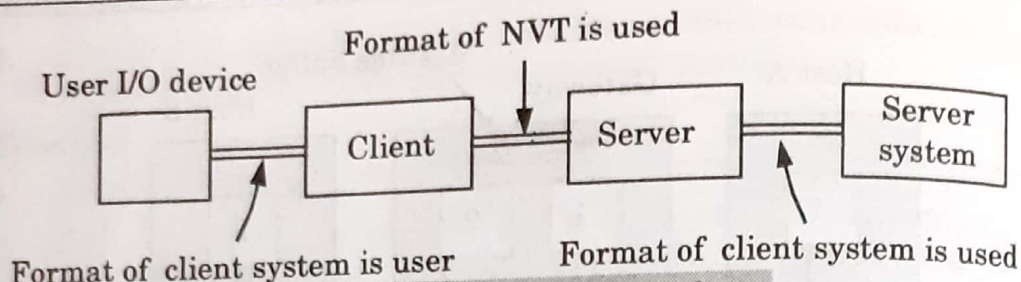


Fig. 5.11.1. Use of NVT by Telnet.

Que 5.12. Write short notes on :

i. Telnet and Rlogin
ii. Virtual private networking
iii. Firewall

Answer

i. Telnet and Rlogin :

1. Rlogin is an alternative remote login application program for host that runs the Unix operating system. Rlogin takes advantage of the fact that both the client and server run a similar operating system, and for this reason, is simpler then Telnet.
2. Telnet is a remote login protocol for executing command on a remote host. The Telnet protocol runs in a client-server mode and uses the TCP protocol for data transmission.

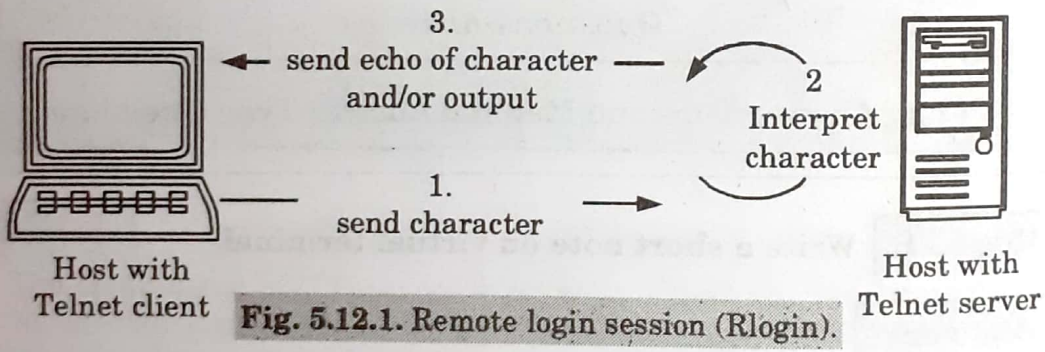


Fig. 5.12.1. Remote login session (Rlogin).

3. The mode of operation in a Telnet session is illustrated in Fig. 5.12.1. At the Telnet client, a character that is typed on the keyboard is not displayed on the monitor, but, instead, is encoded as an ASCII character and transmitted to a remote Telnet server.
4. At the server, the ASCII character is interpreted as if a user had typed the character on the keyboard of the remote machine. If the keystroke results in any output, this output is encoded as (ASCII) text and sent to the Telnet client, which displays it on its monitor.
5. The output can be just the (echo of the) typed character or it can be the output of a command that was executed at the remote Telnet server.

ii. Virtual private network :

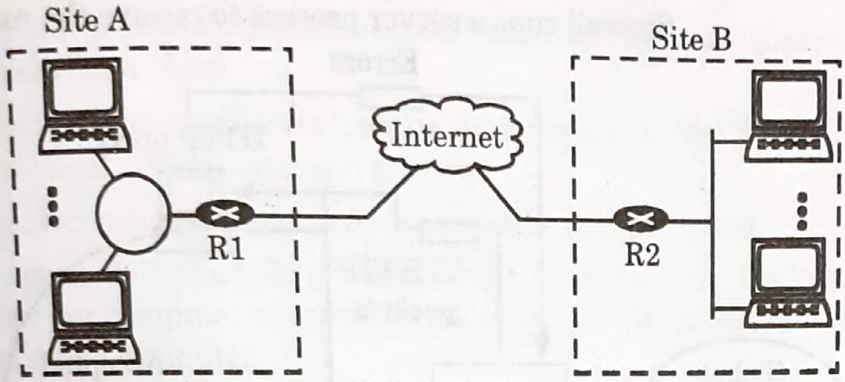


Fig. 5.12.2.

1. VPN creates a network that is private but virtual.
2. It is private because it guarantees privacy inside the organization.
3. It is virtual because it does not use real private WANs.
4. The network is physically public but virtually private.
5. Fig. 5.12.2 shows the idea of a virtual private network. Routers R1 and R2 use VPN technology to guarantee privacy for the organization.

iii. Firewall :

1. A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the internet.
2. It is designed to forward some packets and filter others.

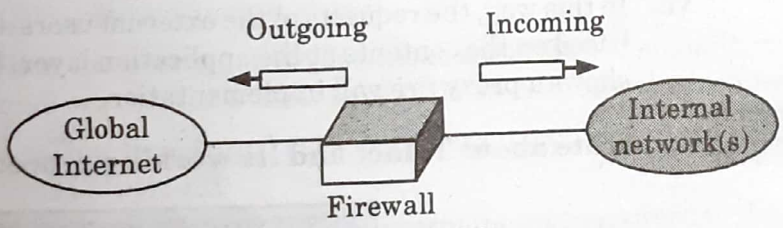


Fig. 5.12.3.

3. A firewall can be used to deny access to a specific host or a specific service in the organization.
4. A firewall is usually classified as a packet-filter or a proxy-based firewall.
   - **a. Packet-filter firewall :** A firewall can be used as a packet filter, it can forward or block packets based on the information in the network layer and transport layer headers : source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).
   - **b. Proxy-based firewall :**
     - i. Firewall stands between the customer (user client) computer and the corporation computer shown in Fig. 5.12.4.

ii. When the client process sends a message, the proxy firewall runs a server process to receive the request.

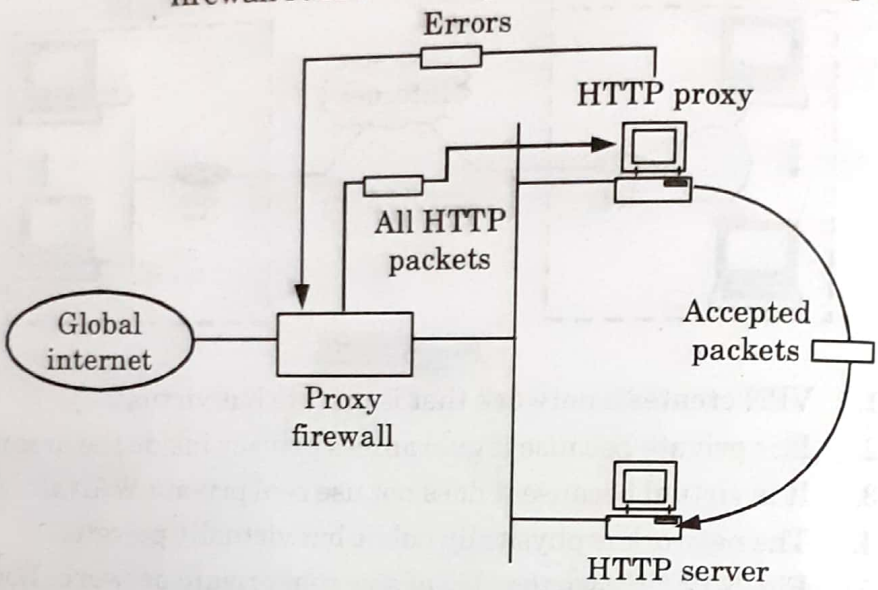


Fig. 5.12.4. Proxy firewall.

iii. The server opens the packet at the application level and finds out if the request is legitimate.

iv. If it is, the server acts as a client process and sends the message to the real server in the corporation.

v. If it is not, the message is dropped and an error message is sent to the external user.

vi. In this way, the requests of the external users are filtered based on the contents at the application layer. Fig. 5.12.4 shows a proxy firewall implementation.

Que 5.13. Elaborate about Telnet and its working procedure.

AKTU 2016-17, 2017-18; Marks 10

Answer

1. Telnet is a program to login into remote systems.
2. It uses TCP/IP protocol and underlying communication can take place through, satellites.
3. Telnet allows us to login in system for any operation and FTP is used only for file transfer use.
4. Telnet is an application used on the internet to connect to a remote computer, which enables an access to the computer and its resources.
5. Telnet is used for a number of activities such as telneting to a site, or checking email at another account, other online services.
6. Telnet is an example of cyberspace extension or cybertravel. The user can travel all across the internet to access machines or databases that may offer different services or information.

Working procedure :

1. Telnet uses software, installed on our computer, to create a connection with the remote host.
2. The Telnet client (software), will send a request to the Telnet server (remote host) when command is given.
3. The server will reply asking for a username and password.
4. If accepted, the Telnet client will establish a connection to the host, thus making our computer a virtual terminal and provide a complete access to the host's computer.
5. Telnet requires the use of a username and password, which means we need to have previously set up an account on the remote computer.

Que 5.14. Explain the two mail access protocols in brief :

i. POP3
ii. IMAP
iii. SMTP

AKTU 2013-14, Marks 10

Answer

i. POP3 :

1. The POP3 consists of client POP3 software and server POP3 software. Out of these, the client POP3 software is installed on the receiving computer whereas the mail server gets the server POP3 software installed on it.
2. When the user wants to download email from the mailbox on the email server, the events take place in the following sequence :
   a. The client (user) establishes a connection with the server on TCP port 110.
   b. The client then sends its username and password to the server in order to access the server mailbox.
   c. The user is then allowed to list and get the mail messages one by one.
   d. This is called as downloading.

ii. IMAP (Internet Message Access Protocol) :

1. IMAP was designed as a superset of POP3 and enhances both message retrieval and management.
2. IMAP protocol will not automatically download all emails, each time email program connects to email server.
3. The IMAP protocol allows us to see through email messages at the email server before we download them.
4. With IMAP we can choose to download our messages or just delete them.

5. IMAP is perfect if we need to connect to our email server from different locations, but only want to download our messages when we are back in office.
6. When using an IMAP mail server, email messages remain on the server where users can read or delete them.
7. IMAP also allows client applications to create, rename or delete mail directories on the server to organize and store email.
8. IMAP client applications are capable of caching copies of messages locally, so the user can browse previously read messages when not directly connected to the IMAP server.
9. IMAP is fully compatible with the important internet messaging standards, such as MIME, which allow for email attachments.
10. We can delete messages, search for text in messages, store messages in different folders, or even create and delete folders on the server system.

iii. SMTP (Simple Mail Transfer Protocol) :

1. The main function of text based SMTP protocol is to send emails.
2. It is used for sending message to a mail server for relaying.
3. It uses TCP (Transmission Control Protocol) to transfer message from client to server.
4. SMTP uses port 25 for message transmission.
5. SMTP messages are read by humans. These messages are first stored and then forwarded.

Que 5.15. Explain the SMTP can handle transfer of videos and images ? Also explain the advantages of IMAP4 over POP3 mail access protocols.

AKTU 2014-15, Marks 10

Answer

SMTP cannot handle transfer of videos and images.

Advantages of IMAP4 over POP3 :

1. In IMAP4, we can access our email from anywhere but in POP3 it is not possible.
2. In IMAP4 multiple users can connect to single mail box but POP3 can connect only single user to mail box.
3. In IMAP4 an email does not need to be deleted multiple times, which can be a problem in POP3.

Que 5.16. Write a short note on SNMP.

AKTU 2015-16, Marks 05

OR

Explain the SNMP protocols in detail.

AKTU 2016-17, Marks 15

AKTU 2017-18, Marks 10

Answer

1. The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite.
2. It provides a set of fundamental operations for monitoring and maintaining an internet. SNMP uses the concept of manager and agent.

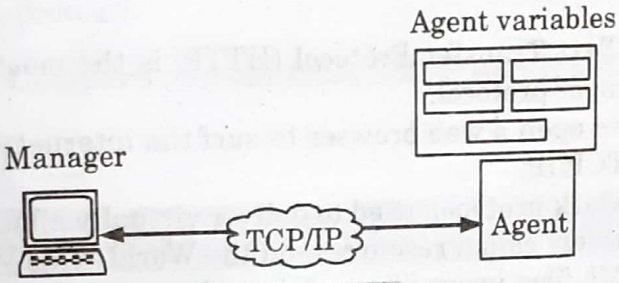


Fig. 5.16.1.

3. A manager is a host that controls and monitors a set of agents, usually routers.
4. The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
5. SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology.
6. It can be used in a heterogeneous internet made of different LANs and WANs connected by routers or gateways made by different manufacturers.

Que 5.17. What is the difference between an active web document and dynamic web page ? Also explain the role of CGI.

AKTU 2014-15, Marks 10

Answer

S. No.	Active web document	Dynamic web page
1.	An active web document is a document where the browser performs the logic instead of the server.	Dynamic web page is a page where server performs the logic instead of the browser.
2.	Active web document are downloaded in client environment and then run.	Dynamic web page runs on the server and then the result is sent to the user.
3.	It uses PHP as scripting language.	It uses AJAX with JavaScript.

Role of CGI :

1. It helps to create and handle dynamic document.
2. It provides sets of standards for web document.
3. It acts as a gateway for accessing other resources such as database.

Que 5.18. What do you mean by HTTP ?

Answer

1. The Hyper Text Transfer Protocol (HTTP) is the most widely used application layer protocol.
2. Each time we open a web browser to surf the internet, we are using HTTP over TCP/IP.
3. It is the network protocol, used to deliver virtually all files and other data (collectively called resources) on the World Wide Web, whether they are HTML files, image files, query results, or anything else. Usually, HTTP takes place through TCP/IP sockets.
4. A browser is an HTTP client because it sends requests to an HTTP server (web server), which then sends responses back to the client. The standard (and default) port for HTTP servers to listen on is 80, though they can use any port.
5. HTTP is used to transmit resources, not just files. A resource is some chunk of information that can be identified by a URL.
6. The most common kind of resource is a file, but a resource may also be a dynamically generated query result, the output of a CGI script, a document that is available in several languages, or something else.

Que 5.19. Explain the principle of HTTP operation. Why it is called stateless protocol.

Answer

1. The principle of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in the form of a letter with a MIME like format.
2. Fig. 5.19.1 shows the HTTP transactions between client and server.

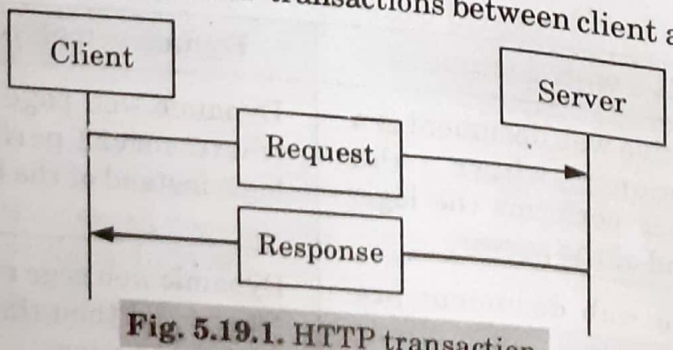


Fig. 5.19.1. HTTP transaction.

3. The client initializes the transaction by sending a request message and the server responds by sending a response.

Statelessness :

1. In HTTP, the server sends the files requested to the client without storing any state information about the client.
2. So, it may happen that the same client may ask the same information repeatedly to the server and the server would not even understand it. So, it will keep resending those files. As the HTTP server does not maintain any information about the state of client it is called as a stateless protocol.

Que 5.20. Compare and contrast SMTP and HTTP.

Answer

S. No.	SMTP	HTTP
1.	Message is transferred from client to server.	Message transfer is from client to server or the other way round.
2.	It uses TCP.	It uses TCP.
3.	It uses port 25 for transmission.	It uses port 80 for transmission.
4.	SMTP messages are to be read by humans.	HTTP messages are to be read and understood by the HTTP servers and HTTP clients.
5.	These messages are first stored and then forwarded.	These messages are immediately delivered.

PART-5

Example Networks-Internet and Public Network.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.21. Write a note on ARPANET.

Answer

1. ARPANET is a WAN which was designed to service in an event like nuclear attack.
2. ARPANET used the concept of packet switching network which is made of subnet and host computers.

3. The subnet was a datagram subnet and each subnet consists of minicomputers called IMPs (Interface Message Processors).
4. Each node of the network used to have an IMP and a host connected by a short wire as shown in Fig. 5.21.1.
5. The host could send messages of upto 8063 bits to its IMP. The IMP breaks them into packets and forwards them independently towards the destination.
6. The subnet was the first electronic store and forward type packet switched network. So, each packet was stored before it was forwarded by the IMP.
7. The original ARPANET design is as shown in Fig. 5.21.1.

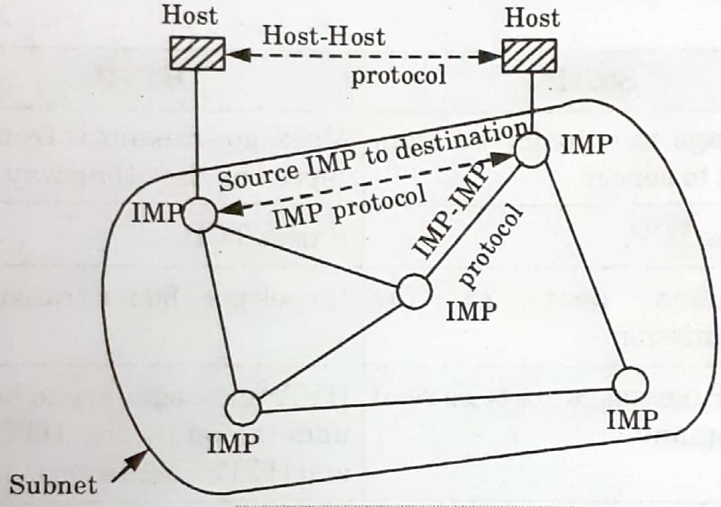


Fig. 5.21.1. ARPANET.

Que 5.22. Describe internet. What are the applications of internet ?

Answer

Internet :

1. The internet is a globally existing network of networks consisting of a huge number of computers located in all the parts of the world.
2. All the computers connected to the internet are part of this huge network.
3. Networking is interconnection of computers. Generally the networking topologies used for networking are star, bus, ring, loop etc.
4. When a limited number of computers are to be interconnected, the local area network (LAN) is used. But in the internet the interconnection is achieved even via satellites.

Applications of internet :

1. **Electronic mail (Email) :** Refer Q. 5.8, Page 5–7A, Unit-5.
2. **News :**
   a. Newsgroups are specialized forums in which users with a common interest can exchange messages.
   b. A large number of newsgroups can technical or non-technical topics.
3. **Remote login :** Refer Q. 5.12, Page 5–11A, Unit-5.
4. **File transfer :** Refer Q. 5.2, Page 5–2A, Unit-5.

5. World Wide Web (www) :

a. The www is analogous to a bulletin board or a notice board.

b. A "website" is a publically accessible notice board on the "server" or "host computer" connected to the internet.

c. Any user can view or read the contents of this area. The available information may be in the form of text, pictures, photographs, images or graphics. It can be on any subject or topic.

d. Each document on the "website" is called as "web page" or simply a "page". WWW has become the most popular application on the internet and the large amount of data that it contains is growing continuously.

Que 5.23. Write a note on public network. Discuss any one of its services.

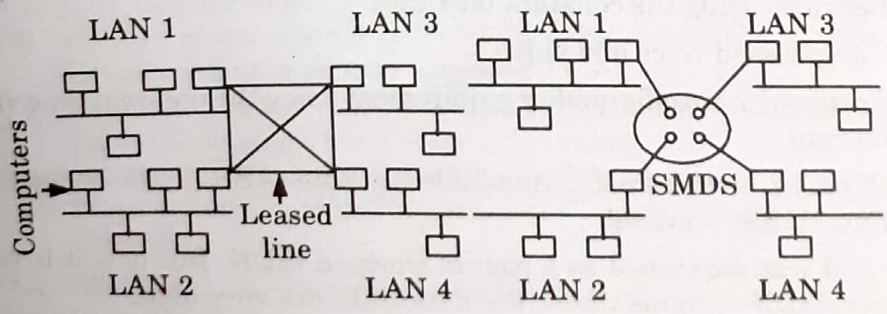
Answer

The telephone companies started offering networking services to the organizations which were interested in subscribing the services. Such systems are called as public network. Services provided by public network are :

i. SMDS
ii. Frame relay
iii. X.25
iv. ATM and broadband ISDN

SMDS-Switched Multimegabit Data Service :

1. The SMDS as shown in Fig. 5.23.1(b) is designed to connect the multiple LANs together. This is the first high speed broadband service offered to the public.
2. The SMDS network is in the telephone company's office. SMDS is designed to handle bursty service.
3. The type of traffic in interconnected LANs is not continuous but bursty type *i.e.*, once in a while a packet will be transferred from one LAN to other but otherwise there is no LAN to LAN traffic.
4. SMDS are supposed to be sufficiently fast. Standard speed is 45 Mbps.



(a) Four LANs interconnected using leased lines (b) Interconnection using SMDS

Fig. 5.23.1.

Que 5.24. **Differentiate between X.25 and frame relay.**

Answer

S. No.	X.25	Frame relay
1.	X.25 networks work at speed upto 64 kbps.	Frame relay operates at higher speed of 1.5 Mbps.
2.	Frames are delivered more reliably than frame relay.	Frames are delivered unreliably than X.25.
3.	Frames are delivered in order.	Frames delivered are not in proper order.
4.	Bad frames can be received back by sending acknowledgement signal.	Bad frames are discarded by frame relay.
5.	X.25 provides flow control.	Frame relay does not provide flow control.

Que 5.25. **Write a short note on ATM.**

Answer

1. ATM (Asynchronous Transfer Mode) is a streamlined packet transfer interface. ATM is a connection-oriented network.
2. ATM uses packets of fixed size for the communication of data. These packets are called as ATM cells.
3. ATM is used for efficient data transfer over high speed data networks.
4. ATM provides real time and non-real time services.

Services provided by ATM are :

1. Services using the constant bit rates.
2. Compressed voice and video.
3. Traffic with specific quality requirement using the non-real time variable bit rate.
4. IP based services using Available Bit Rate (ABR) and Unspecified Bit Rate (UBR) services.
5. ATM was developed as a part of work on ISDN. But now it is used in non-ISDN systems where the data rates are very high.

☺☺☺

1 UNIT

Introduction Concepts (2 Marks Questions)

1.1. What are the applications of computer networks ?

AKTU 2015-16, 2017-18; Marks 02

Ans. Applications of computer networks are :

1. Resource sharing
2. Personal communication
3. Connectivity and communication
4. Sharing of databases

1.2. List the advantages and disadvantages of ring topology.

AKTU 2017-18, Marks 02

Ans. Advantages of ring topology :

i. Fault tolerance builds into the design.
ii. Data packets travel at a greater speed.

Disadvantages of ring topology :

i. Expensive topology.
ii. Failure of one computer can impact other.

1.3. List the advantages and disadvantages of star topology.

AKTU 2016-17, Marks 02

Ans. Advantages of star topology :

i. Easy to install and wire.
ii. It can accommodate different wiring. It can be installed by twisted pair, coaxial cable or fiber optic cable.
iii. Failure of one node does not affect the rest of the network.

Disadvantages of star topology :

i. Depending on where the hubs are located, star networks can require more cable length than a linear topology.
ii. If the central hub fails, the whole network fails to operate.
iii. More expensive than linear bus topologies because of the cost of the hub.

1.4. Write about user access in ISDN.

AKTU 2016-17, Marks 02

Ans. A user can have access to the ISDN by means of a local interface to a digital pipe of certain bit rate. Such digital pipes of various sizes are available to satisfy different needs.

For example, a residential user will require a less capacity digital pipe then the capacity required for an office that would require a much higher capacity pipe.

1.5. What are the advantages and disadvantages of computer network ?

Ans. **Advantages of computer network :**

i. Increased speed
ii. Improved security
iii. Improved reliability
iv. Reduced cost
v. Flexible access

Disadvantages of computer network :

i. Equipment and support can be costly.
ii. Level of maintenance continues to grow.

1.6. Why do we need layering in network ?

Ans. Two reasons for using layered protocol are :

1. It breaks up the design problem into smaller and more manageable pieces.
2. Protocols can be changed easily without affecting higher or lower layers.

1.7. What is the role of data link layer ?

Ans. The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery. It makes the physical layer appear error free to the upper layer.

1.8. What are the criteria used to evaluate the transmission medium ?

Ans. Following are three criteria used to evaluate the transmission media :

1. **Throughput :** The throughput is the measurement of how fast data can pass through a point.
2. **Propagation speed :** Propagation speed measures the distance a signal or a bit can travel through a medium in one second.
3. **Propagation time :** Propagation time measures the time required for a signal to travel from one point of transmission medium to another.

1.9. Discuss quality of service.

Ans. Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. It also involves controlling and managing network resources by setting priorities of specific type of data.

1.10. Define UTP.

Ans.

i. A twisted pair consists of two insulated conductor twisted together in the shape of a spiral. It can be shielded or unshielded.
ii. The unshielded twisted pair cables are very cheap and easy to install. But they are badly affected by the electromagnetic noise interference.

1.11. Define STP.

Ans.

1. STP cable has a metal foil or braided mesh included in order to cover each pair of twisted insulating conductors.
2. This known as the metal shield which is normally connected to ground so as to reduce the interference of the noise. But this makes the cable bulky and expensive.

1.12. What are the services provided by ISDN ?

Ans. ISDN provides the following services :

1. Existing voice applications
2. Data applications
3. Facsimile (FAX)
4. Teletext services
5. Videotext services

1.13. What are the advantages of ISDN ?

Ans.

i. The major benefits to the user can be expressed in terms of cost savings and flexibility.

ii. The integration of voice and different type of data on a single system reduces cost to a great extent.

iii. The requirements of various users can differ greatly in a number of ways but the ISDN has no much of flexibility that it can cater for the need of every user.

1.14. The filters used in telephony end offices limit high frequency components on telephone lines. What is its cut-off frequency when ADSL modems are used on customer lines ?

AKTU 2015-16, Marks 02

Ans. ADSL divides the bandwidth of a twisted pair cable of 1 MHz into three bands.

i. The first band is between 0 and 25 kHz. It is used for regular telephone.

ii. The second band is between 50 kHz and 200 kHz. It is used for upstream communication.

iii. The third band is between 250 kHz and 1 MHz. It is used for downstream communication.

Therefore, cut-off frequency will be 25 kHz.

1.15. If a binary signal is sent over a 3KHZ channel. Whose signal to noise ratio is 20db. What is the maximum achievable data rate ?

AKTU 2017-18, Marks 02

Ans. Maximum achievable data rate = Bandwidth $\times \log_2\left(1 + \frac{S}{N}\right)$

$= 3000 \times \log_2(1 + 10)$

$= 3000 \times \log_2(21) = 3966.65$

2 UNIT

Medium Access Sub Layer (2 Marks Questions)

2.1. What are the types of channel allocation ?

Ans. **Two types of channel allocation are :**

i. Static channel allocation
ii. Dynamic channel allocation

2.2. State the assumptions to be made in dynamic channel allocation.

Ans. **The assumptions made in dynamic channel allocation are :**

i. Single channel assumption
ii. Continuous time
iii. Slotted time
iv. Carrier sense
v. No carrier sense

2.3. Compare ALOHA with slotted ALOHA.

AKTU 2016-17, Marks 02

Ans.

S. No.	ALOHA	Slotted ALOHA
1.	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
2.	In pure ALOHA, the time is continuous.	In slotted ALOHA, the time is discrete.
3.	The time is not globally synchronized.	The time is globally synchronized.

2.4. Measurement of slotted ALOHA channel with infinite number of users show that the 10 percent of slots are idle.

i. What is the channel load ?
ii. What is the throughput ?

AKTU 2015-16, 2017-18; Marks 02

Ans.

i. $Pr[0]$ is the probability of a slot that does not contain frame, *i.e.*, idle frame slot.

$$Pr[0] = 0.1$$
$$Pr[0] = G^0 e^{-G}/0!$$
$$= 1 * e^{-G} = 0.1 \ln (e^{-G}) = \ln (0.1) * -G = -2.30259$$
$$G = -2.30259$$

The channel load is 2.30259.

ii. $$S = Ge^{-G}$$
$$= 2.30259 * e^{-2.30259}$$
$$= 0.230258$$

The throughput is 23.0258 %, below the optimal 36.8 %.

2.5. What are different types of CSMA protocol ?

Ans. Different types of CSMA protocol are :

i. Persistent CSMA
ii. Non-persistent CSMA
iii. P-persistent CSMA

2.6. What is piggybacking ?

AKTU 2016-17, 2017-18; Marks 02

Ans. Piggybacking is a technique of temporarily delaying outgoing acknowledgements so that they can be hooked into the next outgoing data frame.

2.7. How many layers are there in X.25 protocol ? Enlist the layers.

AKTU 2015-16, Marks 02

Ans. The X.25 protocol specifies three layers : the physical layer, the frame layer, and the packet layer. These layers define functions at the physical, data link and network layers of the OSI model.

2.8. Write down the drawbacks of stop and wait protocols.

Ans. Major drawbacks of stop and wait protocol are :

i. Only one frame is sent at a time.
ii. No pipelining.
iii. Timer should be set for each individual frame.

2.9. What is single bit error ?

Ans. The term single bit error means that only one bit of a given data unit (such as a byte, character, data unit) is changed from 1 to 0 or from 0 to 1.

2.10. Describe briefly burst error.

Ans. The term burst error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1. The first corrupted bit to the last corrupted bit.

2.11. What are different ways of error correction ?

Ans. **Different ways of error correction are :**

i. When an error is discovered the receiver can have the sender retransmit the entire data unit.

ii. A receiver can use an error-correcting code, which automatically corrects certain errors.

2.12. Describe briefly 1-persistent CSMA.

Ans. In this scheme, the station which wants to transmit continuously monitors the channel until it is idle and then transmits immediately.

2.13. Describe briefly Non-persistent CSMA.

Ans. In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.

2.14. State the requirements of CRC. **AKTU 2016-17, Marks 02**

Ans. A CRC will be valid if and only if it satisfies the following requirements :

1. It should have exactly one bit less than divisor.
2. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.

3 UNIT

Network Layer (2 Marks Questions)

3.1. List down the basic design issues of network layer.

Ans. **Basic design issues of network layer are :**

i. Routing of packets
ii. Congestion control
iii. Internetworking

3.2. Give the types of routing algorithms.

Ans. **Two types of routing algorithm are :**

i. Non-adaptive algorithms
ii. Adaptive algorithms

3.3. What is count-to-infinity problem ?

AKTU 2015-16, 2017-18; Marks 02

Ans. Count-to-infinity or routing loop problem is an issue in distance vector routing. This problem occurs when an interface goes down or when two routers send updates to each other at the same time.

3.4. Give the IP address 180.25.21.172 and the subnet mask 255.255.192.0, what is the subnet address ?

AKTU 2015-16, 2017-18; Marks 02

Ans. IP address = 180.25.21.172
Subnet mask = 255.255.192.0

	180	25	21	172
IP address	10110100 •	00011001 •	00010101 •	10101100
subnet mask	11111111 •	11111111 •	10000000 •	00000000
	255	255	192	0

ANDING

subnet address	10110100 •	00011001 •	00000000 •	00000000
	180 •	25 •	0 •	0

3.5. Provide few reasons for congestion in a network.

AKTU 2016-17, 2017-18; Marks 02

Ans. **Few reasons for congestion in a network are :**

1. Too many hosts in broadcast domain
2. Broadcast storm
3. Low bandwidth
4. Adding retransmitting hubs
5. Multicasting
6. Outdated hardware
7. Bad configuration management

3.6. With the given IP address, how will you extract its Net_ID and Host_ID ?

AKTU 2016-17, Marks 02

Ans. To extract Net_ID and Host_ID for a given IP address we use internet class and its range as shown in Fig. 1 and Fig. 2.

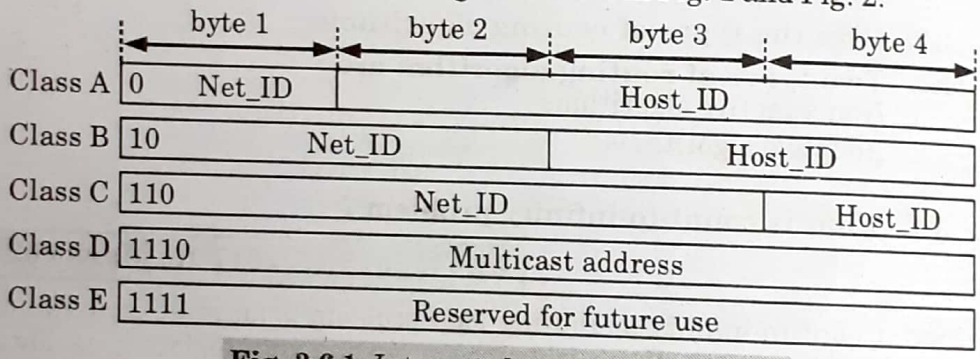


Fig. 3.6.1. Internet classes (IP addresses).

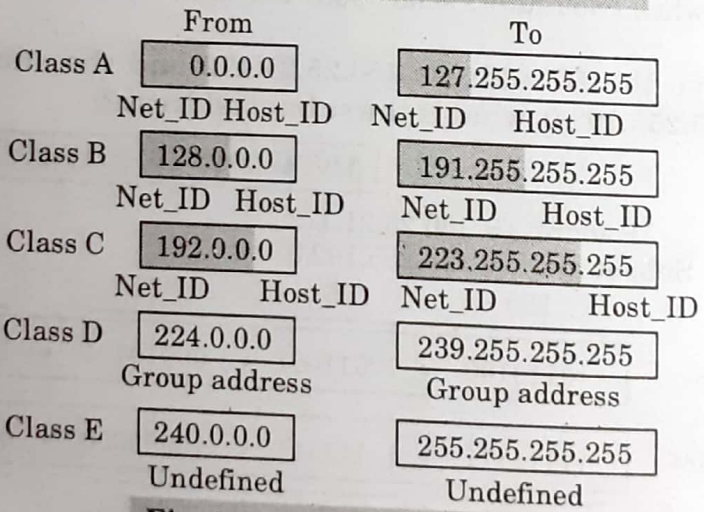


Fig. 3.6.2. Classes range of IP.

3.7. What is the net mask of the gateway interface in a subnetwork where maximum of 25 hosts exist and IP address of one of the hosts is 192.168.1.1 ?

AKTU 2015-16, Marks 02

Ans. Standard net mask for class C = 255.255.255.0
Number of host given = 25
IP address of one host = 192.168.1.1
∴ Net mask = 255.255.255.229

3.8. A typical socket-server application responds user requests using TCP over a specified port. What is the typical sequence in terms of socket functions on server side ?

AKTU 2015-16, Marks 02

Ans. Sequence of socket functions on server side are as follows :

1. Create a socket with the socket() function.
2. Bind the socket to an address using the bind() function.
3. Listen for connections with the listen() function.
4. Accept a connection with the accept() function system call. This call typically blocks until a client connects with the server.
5. Send and receive data by means of send() and receive().
6. Close the connection by means of the close() function.

3.9. Define routing. In what way it is different from switching ?

AKTU 2015-16, Marks 02

Ans. Routing is the process of selecting a path for traffic in a network or between or across multiple networks.
Routing is a process which is done between two networks using IP addresses while in switching, packets are transferred from source to destination using MAC address.

3.10. What are the main requirements of any routing protocol ?

Ans. Main requirements of any routing protocol are :

i. Ensuring that tables at different routers are consistent.
ii. Minimizing the size of the routing table.
iii. Minimizing control messages.
iv. Robustness

3.11. What are the function of router ?

Ans. Functions of a router are :

1. Restrict broadcasts to the LAN.
2. Act as the default gateway.
3. Perform protocol translation (Wired ethernet to wireless/WiFi, or ethernet to CATV).
4. Move (route) data between networks.
5. Learn and advertise loop free paths.
6. Calculate 'best paths' to reach network destinations.

3.12. What do you mean by repeater ?

Ans. A repeater (or regenerator) is an electronic device that operates on only the physical layer of the OSI model. A repeater installed on a link receives the signal before it becomes too weak or corrupted, regenerates the original bit pattern and puts the refreshed copy back onto the link.

3.13. Give the four types of ARP messages that may be sent by the ARP protocol.

Ans. **Four types of ARP messages are :**

i. ARP request
ii. ARP reply
iii. RARP request
iv. RARP reply

3.14. What are the goals of routing algorithms ?

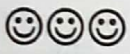
Ans. **Goals of routing algorithms are :**

i. Optimality
ii. Simplicity
iii. Robustness
iv. Rapid convergence
v. Flexibility

3.15. Give an example of packet meta-data.

AKTU 2015-16, Marks 02

Ans. An example of packet meta-data is the destination and source addresses contained in a packet's header fields. For bridges and switches, these addresses are the MAC or physical layer addresses.



4 UNIT

Transport Layer (2 Marks Questions)

4.1. List down the functions of the transport layer.

Ans. The functions of the transport layer are :

i. It allows multiple applications to communicate over a network at the same time.
ii. Process level addressing.
iii. Multiplexing and demultiplexing.
iv. Segmentation, packaging and reassembly.

4.2. Write down a brief description of session layer.

Ans. Session layer is concerned mainly with software application issues and not with the details of network and internet implementation. This layer is designed to allow devices to establish and manage sessions.

4.3. List down the phases of establishing a connection using session layer.

Ans. Phases of establishing a connection using session layer are :

i. Connection establishment
ii. Data transfer
iii. Connection release

4.4. What are the services provided by session layer ?

Ans. Services provided by session layer are :

i. Dialog management
ii. Synchronization
iii. Activity management
iv. Exception handling

4.5. Write down the main functions of presentation layer.

Ans. The main functions of presentation layer are :

i. Translation
ii. Compression
iii. Encryption

4.6. What are the quality of service parameters along with the flow characteristics ?

Ans. Quality of Service (QoS) parameters include attribute like jitter, minimum arrival time, average arrival time, execution time, blocking time. Four types of characteristics of QoS are : reliability, delay, jitter and bandwidth.

4.7. How does transport layer perform duplication control ?

AKTU 2016-17, 2017-18; Marks 02

Ans. Transport layer perform duplication control by avoiding duplicate transport connections or messages. To avoid these duplicates, transport protocol require the network layer to bound the Maximum Segment Lifetime (MSL) such that no segment remains in the network for longer than MSL seconds. Transport protocol entities must be able to safely distinguish between a duplicate CR segment and new CR segment.

4.8. Describe briefly the concept of cryptography.

Ans. Cryptography is the study of secret writing. It is concerned with developing algorithms that may be used to conceal the context of some message from all, except the sender and recipient.

4.9. What are the types of cryptography ?

Ans. **Types of cryptography are :**

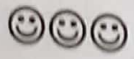
i. Symmetric key cryptography
ii. Asymmetric key cryptography

4.10. Describe the transposition cipher.

Ans. A transposition cipher is a method of encryption by which the positions held by units of plain text are shifted according to a regular system so that the cipher text constitutes a permutation of the plain text.

4.11. What is block cipher ?

Ans. A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text.



5 UNIT

Application Layer (2 Marks Questions)

5.1. What do you understand by File Transfer Protocol (FTP) ?

Ans. FTP is the simplest and most secure way to exchange files between a client and server on a computer network. FTP is used to download files from the internet.

5.2. Write down the disadvantages of FTP.

Ans. **Disadvantages of FTP are :**

i. Passwords and file contents are sent in clear text, which can be intercepted by eavesdroppers.

ii. Multiple TCP/IP connections are used, one for the control connection and one for each download, upload or directory listing.

5.3. Write short note on Virtual Private Network (VPN).

Ans. VPN is a technology that uses the global internet for intra and inter organization communication but require privacy in their internal communications. VPN allows organization to use the global internet for both private and public communications.

5.4. What are the types of firewall ?

Ans. **Types of firewall are :**

i. Packet filter firewall

ii. Proxy firewall

5.5. Mention the use of HTTP.

AKTU 2016-17, 2017-18; Marks 02

Ans. **Use of HTTP are :**

1. HTTP is used to retrieve interlinked resources.
2. HTTP is used to deliver data (HTML files, image files, query results, etc.) on the WWW.

5.6. Give the services offered by email.

Ans. **Services offered by email are :**

i. Communicate with people who have email accounts.

ii. Interact with people all over the world.

iii. Subscribe to electronic services.

iv. Participate in electronic conferences and discussions on an unlimited range of topics.

5.7. List out few email gateways. **AKTU 2016-17, Marks 02**

Ans. **Few email gateways are :**

1. Clearswift secure email gateway
2. McAfee security for email servers
3. Proofpoint email protection
4. Symantec messaging gateway

5.8. List down the different types of email programs.

Ans. **Different types of email programs are :**

i. Mail transfer agent
ii. Mail delivery agent
iii. Mail user agent

5.9. What is the difference between IMAP and POP3 ?

Ans.

S. No.	Parameter	IMAP	POP3
1.	TCP port used	143	110
2.	Email is stored at	Server	User's PC
3.	Email is read	Online	Offline
4.	Who backs up mailboxes	ISP	User

5.10. Write short note on SNMP.

Ans. Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.

5.11. Give the messages defined by SNMP.

Ans. SNMP defines five messages :

i. Get Request
ii. Get Next Request
iii. Get Response
iv. Set Request
v. Trap

5.12. What do you understand by MIME ?

Ans. Multipurpose Internet Mail Extension (MIME) protocol was developed to define a method of moving multimedia files through

existing email gateways. MIME defines extensions to SMTP to support binary attachments of arbitrary format.

5.13. What are the advantages and disadvantages of X.25 ?

Ans. Advantages of X.25 are :

1. Frame delivery is more reliable.
2. Frames are delivered in order.
3. Retransmission of frames is possible.
4. Flow control is provided.
5. X.25 supports the switched virtual circuits and permanent circuits.

Disadvantages of X.25 are :

1. X.25 is much slower than frame relay.

5.14. Describe the features of frame relay.

Ans. Features of frame relay are :

1. It delivers packets sequentially or inorder
2. No error control
3. No flow control

5.15. What are the advantages of frame relay ?

Ans. Advantages of frame relay are :

1. Streamlined communication process
2. The number of functions of a protocol at the user network interface is reduced.
3. Lower delay
4. Higher throughput
5. High access speed

B.Tech.

(SEM. VI) EVEN SEMESTER THEORY EXAMINATION, 2013-14
COMPUTER NETWORK

Time : 3 Hours **Max. Marks : 100**

Note : (1) Attempt **all** questions.
(2) All questions carry equal marks.

1. Attempt any **four** parts of the following : **(5 × 4 = 20)**

a. Discuss the TCP/IP protocol suite on the basis of protocol layering principle.

Ans. Refer Q. 1.5, Page 1–10A, Unit-1.

b. Define topology and explain the advantage and disadvantage of bus, star and ring topologies.

Ans. Refer Q. 1.9, Page 1–14A, Unit-1.

c. Explain briefly the bus backbone and star backbone.

Ans. Refer Q. 1.12, Page 1–19A, Unit-1.

d. Explain the user access in ISDN.

Ans. Refer Q. 1.19, Page 1–31A, Unit-1.

e. Compare twisted pair, co-axial and fiber optic cable.

Ans. Refer Q. 1.16, Page 1–25A, Unit-1.

f. Explain the various types of switching methods with suitable examples.

Ans. Refer Q. 1.17, Page 1–27A, Unit-1.

2. Attempt any **four** parts of the following : **(5 × 4 = 20)**

a. State drawbacks of stop and wait protocols.

Ans. Refer Q. 2.23, Page 2–19A, Unit-2.

b. What is piggybacking ?

Ans. Refer Q. 2.30, Page 2–26A, Unit-2.

c. Which are the requirements of CRC ?

Ans. Refer Q. 2.35, Page 2–32A, Unit-2.

d. How can you compare pure ALOHA and slotted ALOHA ?

Ans. Refer Q. 2.11, Page 2–10A, Unit-2.

e. Explain about CSMA/CD and CSMA/CA and its uses.

Ans. Refer Q. 2.7, Page 2–7A, Unit-2.

f. Differentiate between 802.3, 802.4, and 802.5 IEEE standards.

Ans. Refer Q. 2.17, Page 2–13A, Unit-2.

3. Attempt any **two** parts of the following : **(10 × 2 = 20)**

a. What is meant by fragmentation ? Is fragmentation needed in concentrated virtual circuit internets, or in any datagram system.

Ans. Refer Q. 3.28, Page 3–29A, Unit-3.

b. Give an IP address, how will you extract its net-id and host-id and compare IPv4 and IPv6 with frame format.

Ans. Refer Q. 3.27, Page 3–28A, Unit-3.

c. i. What is meant by unicast and multicast routing with suitable diagrams ?

Ans. Refer Q. 3.5, Page 3–5A, Unit-3.

ii. Write a short note on leaky bucket algorithm.

Ans. Refer Q. 3.13, Page 3–12A, Unit-3.

4. Attempt any **two** parts of the following : **(10 × 2 = 20)**

a. Explain about the TCP header and working of TCP protocol and differentiate between TCP and UDP with frame format.

Ans. Refer Q. 4.9, Page 4–7A, Unit-4.

b. Define cryptography with the help of block diagram of symmetric and asymmetric key cryptography.

Ans. Refer Q. 4.22, Page 4–22A, Unit-4.

c. Write short notes on :

i. Digital audio

ii. Audio compression

iii. Streaming audio

Ans. Refer Q. 4.19, Page 4–17A, Unit-4.

5. Attempt any **two** parts of the following : **(10 × 2 = 20)**

a. Explain the two mail access protocols in brief :

i. POP3 ii. IMAP iii. SMTP

Ans. Refer Q. 5.14, Page 5–14A, Unit-5.

b. Write a short notes on :

i. FTP

ii. DNS

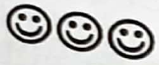
iii. MIME
iv. TFTP

Ans.

i. Refer Q. 5.2, Page 5–2A, Unit-5.
ii. Refer Q. 5.5, Page 5–4A, Unit-5.
iii. Refer Q. 5.4, Page 5–3A, Unit-5.
iv. Refer Q. 5.4, Page 5–3A, Unit-5.

c. Explain about email architecture and services.

Ans. Refer Q. 5.8, Page 5–7A, Unit-5.



B. Tech.
(SEM. VI) EVEN SEMESTER THEORY EXAMINATION, 2014-15
COMPUTER NETWORKS

Time : 3 Hours **Max. Marks : 100**

Note : Attempt **all** questions.

1. Attempt any **four** parts of the following : **(5 × 4 = 20)**

a. Differentiate between bit rate and baud rate. A modem constellation diagram has data point at coordinates : (1, 1), (1, –1), (–1, 1) and (–1, –1). How many bps can a modem with these parameters achieve at 1200 baud ? State two reason for using layered protocols.

Ans. Refer Q. 1.21, Page 1–32A, Unit-1.

b. What are the number of cable links required for *n* devices connected in mesh, ring, bus and star topology ?

Ans. Refer Q. 1.10, Page 1–17A, Unit-1.

c. Calculate the required bandwidth, if in a communication channel the signal power is 10W, and the information transmission rate is 10 kbps.

Ans. Refer Q. 1.22, Page 1–33A, Unit-1.

d. It is required to transmit a data at a rate of 64 kbps over a 3 kHz telephone channel. What is the minimum SNR required to accomplish this ?

Ans. Refer Q. 1.23, Page 1–33A, Unit-1.

e. What do you mean by service primitives ?

Ans. Refer Q. 1.8, Page 1–13A, Unit-1.

f. Discuss the services of each layer of OSI reference model.

Ans. Refer Q. 1.3, Page 1–4A, Unit-1.

2. Attempt any **four** parts of the following : **(5 × 4 = 20)**

a. Given a 10-bit sequence 1010011110 and a divisor of 1011. Find the CRC. Check your answer.

Ans. Refer Q. 2.37, Page 2–34A, Unit-2.

b. Answer the following :

i. A pure ALOHA network transmits 200 bit frames on shared channel of 200 kbps. What is the throughput if the system (all station together) produces 250 frames per second ?

Ans. Refer Q. 2.12, Page 2–10A, Unit-2.

ii. How can you compare pure ALOHA and slotted ALOHA ?

Ans. Refer Q. 2.11, Page 2–10A, Unit-2.

c. Discriminate between the send window and receive window for link and how are they related with.

i. A selective repeat retransmission scheme

ii. A Go-Back-N control scheme

Ans.

i. Refer Q. 2.27, Page 2–25A, Unit-2.

ii. Refer Q. 2.25, Page 2–22A, Unit-2.

d. Discuss different carrier sense protocols. How are they different than collision protocols ?

Ans. Refer Q. 2.4, Page 2–4A, Unit-2.

e. Sketch the Manchester and differential Manchester encoding for the bit stream : 0001110101.

Ans. Refer Q. 2.38, Page 2–35A, Unit-2.

f. Discuss the different physical layer transmission media.

Ans. Refer Q. 1.14, Page 1–22A, Unit-1.

3. Attempt any **two** parts of the following : **(10 × 2 = 20)**

a. Write short notes on following :

i. Stop and wait ARQ

ii. Sliding window protocol

iii. Go-Back-N ARQ

iv. Collision avoidance

Ans.

i. Refer Q. 2.24, Page 2–20A, Unit-2.

ii. Refer Q. 2.21, Page 2–17A, Unit-2.

iii. Refer Q. 2.25, Page 2–22A, Unit-2.

iv. Refer Q. 2.6, Page 2–5A, Unit-2.

b. Perform the subnetting of the following IP address 160.11.X.X. Original subnet mask 255.255.0.0 and number of subnet 6 (six).

Ans. Refer Q. 3.26, Page 3–27A, Unit-3.

c. What is the transmission time of a packet sent by a station if the length of the packet is 2 million bytes and the bandwidth of the channel is 300 kbps ?

Ans. Refer Q. 3.29, Page 3–30A, Unit-3.

4. Attempt any **two** parts of the following : **(10 × 2 = 20)**

a. Draw the diagram of TCP header and explain the use of the following :

i. Source and destination port addresses

ii. Sequence and acknowledgement numbers

iii. Control bits

iv. **Window size**

v. **Urgent pointer**

Describe the role of checksum field and option pad bytes.

Ans. Refer Q. 4.10, Page 4–9A, Unit-4.

b. **Answer the following :**

i. **Differentiate between the block cipher with transposition cipher.**

ii. **Using the RSA public key cryptosystem with $a = 1, b = 2$ etc.**

I. **If $p = 7$ and $q = 11$, list five legal values for d.**

II. **If $p = 13$ and $q = 31$ and $d = 7$, find e.**

Ans.

i. Refer Q. 4.26, Page 4–26A, Unit-4.

ii. Refer Q. 4.27, Page 4–26A, Unit-4.

c. **Discuss :**

i. **Different steps of JPEG compression standard.**

ii. **The RPC design and implementation issues.**

Ans.

i. Refer Q. 4.20, Page 4–21A, Unit-4.

ii. Refer Q. 4.16, Page 4–14A, Unit-4.

5. Attempt any **two** parts of the following : **(10 × 2 = 20)**

a. **Explain the SMTP can handle transfer of videos and images ? Also explain the advantages of IMAP4 over POP3 mail access protocols.**

Ans. Refer Q. 5.15, Page 5–15A, Unit-5.

b. **What is the difference between an active web document and dynamic web page ? Also explain the role of CGI.**

Ans. Refer Q. 5.17, Page 5–16A, Unit-5.

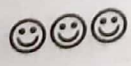
c. i. **Compare and contrast TCP with RTP. Are both doing the same things ?**

ii. **What are the problems for full implementation of voice over IP ? Did you think we will stop using the telephone network very soon ?**

Ans.

i. Refer Q. 4.30, Page 4–29A, Unit-4.

ii. Refer Q. 4.29, Page 4–28A, Unit-4.



B. Tech.
(SEM. VI) EVEN SEMESTER THEORY EXAMINATION, 2015-16
COMPUTER NETWORKS

Time : 3 Hours **Max. Marks : 100**

Note : Attempt questions from **all** sections as per directions.

SECTION-A

1. Attempt **all** parts of this section. Answer in brief. **(2 × 10 = 20)**

a. Given the IP address 180.25.21.172 and the subnet mask 255.255.192.0. What is the subnet address ?

Ans. Refer Q. 3.4, Page SQ–7A, Unit-3, Two Marks Questions.

b. What is count-to-infinity problem ?

Ans. Refer Q. 3.3, Page SQ–7A, Unit-3, Two Marks Questions.

c. The filters used in telephony end offices limit high frequency components on telephone lines. What is its cut-off frequency when ADSL modems are used on customer lines ?

Ans. Refer Q. 1.14, Page SQ–3A, Unit-1, Two Marks Questions.

d. Measurement of slotted ALOHA channel with infinite number of users show that the 10 percent of slots are idle.

i. What is the channel load ?

ii. What is the throughput ?

Ans. Refer Q. 2.4, Page SQ–4A, Unit-2, Two Marks Questions.

e. What is the net mask of the gateway interface in a subnetwork where maximum of 25 hosts exist and IP address of one of the hosts is 192.168.1.1 ?

Ans. Refer Q. 3.7, Page SQ–8A, Unit-3, Two Marks Questions.

f. A typical socket-server application responds user requests using TCP over a specified port. What is the typical sequence in terms of socket functions on server side ?

Ans. Refer Q. 3.8, Page SQ–9A, Unit-3, Two Marks Questions.

g. How many layers are there in X.25 protocol ? Enlist the layers.

Ans. Refer Q. 2.7, Page SQ–5A, Unit-2, Two Marks Questions.

h. Define routing. In what way it is different from switching ?

Ans. Refer Q. 3.9, Page SQ–9A, Unit-3, Two Marks Questions.

i. What are the applications of computer networks ?

Ans. Refer Q. 1.1, Page SQ–1A, Unit-1, Two Marks Questions.

j. Give an example of packet metadata.

Ans. Refer Q. 3.15, Page SQ–10A, Unit-3, Two Marks Questions.

SECTION-B

2. Attempt any **five** questions from this section. **(10 × 5 = 50)**

a. A rectangular wave-guide (a = 2 cm, b = 1 cm) filled with deionized water ($\mu = 1, \xi = 81$) operates at 3 GHz. Determine all propagating modes and corresponding cut-off frequencies.

Ans. Refer Q. 4.32, Page 4–30A, Unit-4.

b. i. An ALOHA network uses 19.2 Kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput for pure ALOHA network.

Ans. Refer Q. 2.13, Page 2–10A, Unit-2.

ii. What is unicast routing ? Discuss unicast routing protocols.

Ans. Refer Q. 3.6, Page 3–6A, Unit-3.

c. How does DNS perform data name resolution ? What are the different types of name servers ? Mention the DNS message format for query and reply messages.

Ans. Refer Q. 5.6, Page 5–5A, Unit-5.

d. Explain TCP congestion control algorithm in internet. What is TCP segment header ? Also, discuss TCP connection management.

Ans. Refer Q. 4.11, Page 4–10A, Unit-4.

e. What is the total delay (latency) for a frame size of 10 million bits that is being set up on link with 15 routers, each having 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 2×10^8 m/sec. The link has bandwidth of 6 Mbps.

Ans. Refer Q. 4.31, Page 4–29A, Unit-4.

f. What is OSI model ? Explain the functions and protocols and services of each layer.

Ans. Refer Q. 1.4, Page 1–10A, Unit-1.

g. What is IP addressing ? How it is classified ? How subnet addressing is performed ?

Ans. Refer Q. 3.20, Page 3–19A, Unit-3.

SECTION-C

Attempt any **two** questions from this section. **(15 × 2 = 30)**

3. i. Is fragmentation needed in concatenated virtual circuit internets or only in datagram systems ? Explain.

Ans. Refer Q. 3.28, Page 3–29A, Unit-3.

ii. What is hamming code ? Explain its working with suitable example.

Ans. Refer Q. 2.36, Page 2–32A, Unit-2.

4. Answer each questions :

i. Find the class of each address

a. 140.213.10.80

b. 52.15.150.11

ii. What is the type of the following address ?

a. 4F::A234:2

b. 52F::1234:2222

Ans. Refer Q. 3.30, Page 3–30A, Unit-3.

iii. What is congestion ? Name the techniques that prevent congestion.

Ans. Refer Q. 3.11, Page 3–11A, Unit-3.

5. Write short notes on any three of the following :

i. DNS in the internet

ii. Voice over IP

iii. SNMP

iv. Electronic mail

v. File Transfer Protocol

Ans.

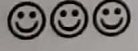
i. Refer Q. 5.5, Page 5–4A, Unit-5.

ii. Refer Q. 4.28, Page 4–28A, Unit-4.

iii. Refer Q. 5.16, Page 5–15A, Unit-5.

iv. Refer Q. 5.8, Page 5–7A, Unit-5.

v. Refer Q. 5.2, Page 5–2A, Unit-5.



B. Tech.

(SEM. VI) EVEN SEMESTER THEORY EXAMINATION, 2016-17

COMPUTER NETWORK

Time : 3 Hours **Max. Marks : 100**

Section-A

1. Attempt **all** parts : **(2 × 10 = 20)**

a. Write about user access in ISDN.

Ans. Refer Q. 1.4, Page SQ–1A, Unit-1, Two Marks Questions.

b. List the advantages and disadvantages of star topology.

Ans. Refer Q. 1.3, Page SQ–1A, Unit-1, Two Marks Questions.

c. Compare ALOHA with slotted ALOHA.

Ans. Refer Q. 2.3, Page SQ–4A, Unit-2, Two Marks Questions.

d. State the requirements of CRC.

Ans. Refer Q. 2.14, Page SQ–6A, Unit-2, Two Marks Questions.

e. Provide few reasons for congestion in a network.

Ans. Refer Q. 3.5, Page SQ–8A, Unit-3, Two Marks Questions.

f. With the given IP address, how will you extract its net-id and host-id ?

Ans. Refer Q. 3.6, Page SQ–8A, Unit-3, Two Marks Questions.

g. What is piggybacking ?

Ans. Refer Q. 2.6, Page SQ–5A, Unit-2, Two Marks Questions.

h. How does transport layer perform duplication control ?

Ans. Refer Q. 4.7, Page SQ–12A, Unit-4, Two Marks Questions.

i. Mention the use of HTTP.

Ans. Refer Q. 5.5, Page SQ–13A, Unit-5, Two Marks Questions.

j. List out few email gateways.

Ans. Refer Q. 5.7, Page SQ–14A, Unit-5, Two Marks Questions.

Section-B

2. Attempt any **five** of the following : **(10 × 5 = 50)**

a. Discuss the issues in the data link layer and about its protocol on the basis of layering principle.

Ans. Refer Q. 2.20, Page 2–15A, Unit-2.

b. Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.

Ans. Refer Q. 1.9, Page 1–14A, Unit-1.

c. Consider the use of 10 K-bit size frames on a 10 Mbps satellite channel with 270 ms delay. What is the link utilization for stop-and-wait ARQ technique assuming $P = 10^{-3}$?

Ans. Refer Q. 2.29, Page 2–26A, Unit-2.

d. Brief about how line coding implemented in FDDI and describe its format.

Ans. Refer Q. 2.19, Page 2–15A, Unit-2.

e. Explain about the TCP header and working of TCP and differentiate TCP and UDP with frame format.

Ans. Refer Q. 4.9, Page 4–7A, Unit-4.

f. Explain the three-way handshaking protocol to establish the transport level connection.

Ans. Refer Q. 4.8, Page 4–6A, Unit-4.

g. Elaborate about Telnet and its working procedure.

Ans. Refer Q. 5.13, Page 5–13A, Unit-5.

h. How does FTP work ? Differentiate between passive and active FTP.

Ans. Refer Q. 5.3, Page 5–2A, Unit-5.

Section-C

Attempt any **two** of the following : **(15 × 2 = 30)**

3. i. Explain functionalities of every layer in OSI reference model with neat block diagram.

Ans. Refer Q. 1.3, Page 1–4A, Unit-1.

ii. Illustrate the performance issues for Go-Back-N data link protocol.

Ans. Refer Q. 2.26, Page 2–24A, Unit-2.

4. i. Describe the problem of count-to-infinity associated with distance vector routing technique.

Ans. Refer Q. 3.10, Page 3–10A, Unit-3.

ii. Enumerate how the transport layer ensures that the complete message arrives at the destination and in the proper order.

Ans. Refer Q. 4.3, Page 4–3A, Unit-4.

5. Explain the SNMP protocols in detail.

Ans. Refer Q. 5.16, Page 5–15A, Unit-5.

B. Tech.

(SEM. VI) EVEN SEMESTER THEORY EXAMINATION, 2017-18

COMPUTER NETWORK

Time : 3 Hours **Max. Marks : 100**

Note : 1.Attempt all sections. If require any missing data; then choose suitably.

Section-A

1. Attempt all question in brief : **(2 × 10 = 20)**

a. What are the applications of computer networks ?

Ans. Refer Q. 1.1, Page SQ–1A, Unit-1, Two Marks Questions.

b. List the advantages and disadvantages of ring topology.

Ans. Refer Q. 1.2, Page SQ–1A, Unit-1, Two Marks Questions.

What is count-to-infinity problem ?

Refer Q. 3.3, Page SQ–7A, Unit-3, Two Marks Questions.

d. Give the IP address 180.25.21.172 and the subnet mask 255.255.192.0, what is the subnet address ?

Ans. Refer Q. 3.4, Page SQ–7A, Unit-3, Two Marks Questions.

e. What is piggybacking ?

Ans. Refer Q. 2.6, Page SQ–5A, Unit-2, Two Marks Questions.

f. Measurement of slotted ALOHA channel with infinite number of users show that the 10 percent of slots are idle.

(i) What is the channel load ?

(ii) What is the throughput ?

Ans. Refer Q. 2.4, Page SQ–4A, Unit-2, Two Marks Questions.

g. Provide few reasons for congestion in a network.

Ans. Refer Q. 3.5, Page SQ–8A, Unit-3, Two Marks Questions.

h. How does transport layer perform duplication control ?

Ans. Refer Q. 4.7, Page SQ–12A, Unit-4, Two Marks Questions.

i. If a binary signal is sent over a 3KHZ channel. Whose signal to noise ratio is 20db. What is the maximum achievable data rate ?

Ans. Refer Q. 1.15, Page SQ–3A, Unit-1, Two Marks Questions.

j. **Mention the use of HTTP.**

Ans. Refer Q. 5.5, Page SQ–13A, Unit-5, Two Marks Questions.

Section-B

2. Attempt any **three** of the following : **(10 × 3 = 30)**

a. **Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.**

Ans. Refer Q. 1.9, Page 1–14A, Unit-1.

b. **Discuss the issues in the data link layer and about its protocol on the basis of layering principle.**

Ans. Refer Q. 2.20, Page 2–15A, Unit-2.

c. **What is congestion ? Briefly describe the techniques that prevent congestion.**

Ans. Refer Q. 3.11, Page 3–11A, Unit-3.

d. **Explain about the TCP header and working of TCP and differentiate TCP and UDP with frame format.**

Ans. Refer Q. 4.9, Page 4–7A, Unit-4.

e. **Elaborate about Telnet and its working procedure.**

Ans. Refer Q. 5.13, Page 5–13A, Unit-5.

Section-C

3. Attempt any **one** of the following : **(10 × 1 = 10)**

a. **What is OSI model ? Explain the functions; protocols and services of each layer.**

Ans. Refer Q. 1.4, Page 1–10A, Unit-1.

b. **Discuss the different physical layer transmission media.**

Ans. Refer Q. 1.14, Page 1–22A, Unit-1.

4. Attempt any **one** of the following : **(10 × 1 = 10)**

a. **Discuss different carrier sense protocols. How are they different then collisions protocols ?**

Ans. Refer Q. 2.4, Page 2–4A, Unit-2.

b. **Write short notes on following :**

i. **Stop and Wait ARQ**
ii. **Sliding window protocol**
iii. **Go-Back-N ARQ**

Ans.
i. Refer Q. 2.24, Page 2–20A, Unit-2.
ii. Refer Q. 2.21, Page 2–17A, Unit-2.
iii. Refer Q. 2.25, Page 2–22A, Unit-2.

5. Attempt any **one** of the following : **(10 × 1 = 10)**

a. What is IP addressing ? How it is classified ? How subnet addressing is performed ?

Ans. Refer Q. 3.20, Page 3–19A, Unit-3.

b. What is unicast routing ? Discuss unicast routing protocols.

Ans. Refer Q. 3.6, Page 3–6A, Unit-3.

6. Attempt any **one** of the following : **(10 × 1 = 10)**

a. Enumerate how the transport layer ensures that the complete message arrives at the destination and in the proper order.

Ans. Refer Q. 4.3, Page 4–3A, Unit-4.

b. Explain the three-way handshaking protocols to establish the transport level connection.

Ans. Refer Q. 4.8, Page 4–6A, Unit-4.

7. Attempt any **one** of the following : **(10 × 1 = 10)**

a. Write short notes on any two of the following :
i. DNS in the internet
ii. Voice Over IP
iii. File Transfer Protocol

Ans.
i. Refer Q. 5.5, Page 5–4A, Unit-5.
ii. Refer Q. 4.28, Page 4–28A, Unit-4.
iii. Refer Q. 5.2, Page 5–2A, Unit-5.

b. Explain the SNMP protocols in detail.

Ans. Refer Q. 5.16, Page 5–15A, Unit-5.