PUBLISHED BY : **Apram Singh**
Quantum Publications®
(A Unit of Quantum Page Pvt. Ltd.)
Plot No. 59/2/7, Site - 4, Industrial Area,
Sahibabad, Ghaziabad-201 010

Phone : 0120-4160479
Email : pagequantum@gmail.com **Website: www.quantumpage.co.in**
Delhi Office : 1/6590, East Rohtas Nagar, Shahdara, Delhi-110032

Computer Networks (CS/IT : Sem-6)
1st Edition : *2010-11*
2nd Edition : *2011-12*
3rd Edition : *2012-13*
4th Edition : *2013-14*
5th Edition : *2014-15*
6th Edition : *2015-16*
7th Edition : *2016-17*
8th Edition : *2017-18*
9th Edition : *2018-19*
10th Edition : *2019-20*
11th Edition : *2020-21 (Thoroughly Revised Edition)*

Price: Rs. 110/- only

Printed at : Mayank Enterprises, Delhi-110093.

CONTENTS

KCS 603 : Computer Networks

1 UNIT

Introductory Concepts

CONTENTS

PART-1

Goals and Application of Networks.

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. Networks 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 Uttar Pradesh 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 NOIDA.

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. To 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 includes credit history searches, foreign exchange and investment services and Electronic Fund Transfer (EFT).
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

Categories of Network.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Q 1.3. Describe different categories of network.

Answer

Following are the different categories of network :

1. **LAN (Local Area Network) :**
   i. Local Area Network is a group of computers connected to each other in a small area such as building, office.
   ii. LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
   iii. It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
   iv. The data is transferred at an extremely faster rate in Local Area Network.
   v. Local Area Network provides higher security.
2. **PAN (Personal Area Network) :**
   i. Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
   ii. Personal Area Network is used for connecting the computer devices of personal use.
3. **MAN (Metropolitan Area Network) :**
   i. A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
   ii. Government agencies use MAN to connect to the citizens and private industries.
   iii. In MAN, various LANs are connected to each other through a telephone exchange line.
4. **WAN (Wide Area Network) :**
   i. A Wide Area Network is a network that extends over a large geographical area such as states or countries.
   ii. A Wide Area Network is quite bigger network than the LAN.
   iii. A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.

PART-3

Organization of the Internet, ISP, Network Structure and Architecture (Layering Principles, Service Protocols and Standards)

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.4. Describe the organization of internet.

Answer

1. Internet is basically a hierarchy structure of networks that allows one internet connected device to connect to another internet connected device, both being at different geographical locations.
2. These networks must have access to use internet protocols and all networks must support TCP/IP.
3. Every computer that is connected to internet has a unique address. This address is called IP address where IP stands for internet protocol.
4. This address is in the form of nnn.nnn.nnn.nnn where nnn can be any number in the range from 0 to 225.
5. This IP address is provided to your computer if you are connected to LAN or an ISP (internet service provider).
6. Depending on what network your computer or device is connected, your IP address can be temporary or permanent.

Que 1.5. Write short note on ISP.

Answer

1. Internet Service Provider (ISP) is a company which provides internet connection to end user.
2. There are 3 levels of Internet Service Provider (ISP): Tier-1 ISP, Tier-2 ISP, and Tier-3 ISP.
   - **a. Tier-1 ISP :**
     - i. These ISPs are at the top of the hierarchy and they have a global reach. They do not pay for any internet traffic through their network instead lower-tier ISPs have to pay a cost for passing their traffic from one geolocation to another which is not under the reach of that ISPs.
     - ii. Generally, ISPs at the same level connect to each other and allow free traffic passes to each other. Such ISPs are called peers.
     - iii. Due to this cost is saved. They build infrastructure to provide traffic to all other Internet Service Providers, not to end users.

   - **b. Tier-2 ISP :**
     - i. These ISPs are service provider who makes connection between Tier-1 and Tier-3 ISPs.
     - ii. They have regional or country reach and they behave just like Tier-1 ISP for Tier-3 ISPs.
   - **c. Tier-3 ISP :**
     - i. These ISPs are closest to the end users and helps them to connect to the internet by charging some money.
     - ii. These ISPs work on purchasing model. These ISPs have to pay some cost to Tier-2 ISPs based on traffic generated.

Que 1.6. Explain network architecture.

Answer

The two types of network architectures are used :

1. **Peer-to-Peer network :**
   - i. Peer-to-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
   - ii. Peer-to-Peer network is useful for small environments, usually up to 10 computers.
   - iii. Peer-to-Peer network has no dedicated server.
   - iv. Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.
2. **Client/Server Network :**
   - i. Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as server.
   - ii. The central controller is known as a server while all other computers in the network are called clients.
   - iii. A server performs all the major operations such as security and network management.
   - iv. A server is responsible for managing all the resources such as files, directories, printer, etc.
   - v. All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

Que 1.7. What are the advantage and disadvantages of peer-to-peer and client/ server network ?

Answer

Advantages of peer-to-peer network :

1. It is less costly as it does not contain any dedicated server.
2. If one computer stops working other computers will not stop working.
3. It is easy to set up and maintain as each computer manages itself.

Disadvantages of peer-to-peer network :

1. It does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
2. It has a security issue as the device is managed itself.

Advantages of client/server network :

1. A Client/Server network contains the centralized system. Therefore we can back up the data easily.
2. A Client/Server network has a dedicated server that improves the overall performance of the whole system.
3. Security is better in Client/Server network as a single server administers the shared resources.
4. It also increases the speed of the sharing resources.

Disadvantages of client/cerver network :

1. Client/Server network is expensive as it requires the server with large memory.
2. A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
3. It requires a dedicated network administrator to manage all the resources.

Que 1.8. What is the need of layered architecture ? What do you understand by layering principles ?

Answer

Need of layered architecture :

1. A layered architecture allows us to discuss a well-defined, specific part of a large and complex system.
2. This simplification provides modularity, making it much easier to change the implementation of the service provided by the layer.

3. As long as the layer provides the same service to the layer above it, and uses the same services from the layer below it, the remainder of the system remains unchanged when a layer's implementation is changed.
4. For large and complex systems the ability to change the implementation of a service without affecting other components of the system is important advantage of layering.

Layering principles : Following are the two principles of protocol layering :

1. **First Principle :**
   - i. The first principle dictates that if we want bidirectional communication, each layer should be able to perform two opposite tasks, one in each direction.
   - ii. For example, the 3rd layer task is to listen (in one direction) and talk (in the other direction). The 2nd layer needs to be able to encrypt and decrypt. The 1st layer needs to send and receive mail.
2. **Second Principle :**
   - i. The second principle is that the two objects under each layer at both sites should be identical.
   - ii. For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a ciphertext letter. The object under layer 1 at both sites should be a piece of mail.

Que 1.9. 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 undergoes 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 1.10. What do you mean by service primitives ?

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.

Que 1.11. What do you understand by the terms protocols and standards in computer networks ?

Answer

Protocols :

1. In computer networks, communication occurs between entities in different systems.
2. An entity is anything capable of sending or receiving information.
3. But two entities cannot just send bit streams to each other and expect to be understood.
4. For communication to occur, the entities must agree on a protocol.
5. A protocol is a set of rules that govern data communication.

6. A protocol defines what is communicated, how it is communicated, and when it is communicated.
7. The key elements of a protocol are syntax, semantics, and timing.

Standards :

1. A standard provides a model for development that makes it possible for a product to work regardless of the individual manufacturer.
2. Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers.
3. They guarantee national and international interoperability of data and telecommunications technology and processes.
4. They provide guidelines to manufacturers, vendors, government agencies, and other service providers.
5. Data communication standards fall into two categories :
   i. **De jure (by law) standards :** De jure standards are those that have been legislated by an officially recognized body.
   ii. **De facto (by fact) standards :** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards.

PART-4

The OSI Reference Model.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.12. Describe OSI reference model in detail.

OR

Discuss the services of each layer of OSI reference model.

AKTU 2014-15, Marks 05

OR

What is OSI Model ? Explain the functions; protocols and services of each layer.

AKTU 2017-18, Marks 10

OR

What is OSI Model ? Explain the functions, protocols and services of each layer.

AKTU 2018-19, Marks 10

Answer

OSI model :

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.

Following are the different layers with its function :

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.

Functions and services of Physical layer :

i. The physical layer performs bit-by-bit data delivery over a physical transmission medium.

ii. It provides a standardized interface to the transmission medium, including a mechanical specification of electrical connectors and cables.

iii. The physical layer is responsible for electromagnetic compatibility.

Protocols of Physical layer : RS – 232, RS – 449, Ethernet (IEEE 802.3), and others.

2. Data link layer :

i. The data link layer transforms the physical layer 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).

Functions and services of Data-Link layer :

i. The important and essential function of Data Link Layer is to provide an interface to network layer.

ii. The main aim of Data Link Layer is to transmit data frames they have received to destination machine so that these data frames can be handed over to network layer of destination machine.

Protocols of Data-Link layer : HDLC, SDLC, IEEE 802.2, X.25 protocols.

3. Network layer :

i. The network layer is responsible for the source to destination delivery of a packet.

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.

Functions and services of Network layer :

Functions of the network layer include :

a. Connectionless communication

b. Host addressing

c. Message forwarding

Protocols of Network layer : IPv4, IPv6, ARP, ICMP.

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.

Functions and services of Transport layer :

i. It divides the message received from the session layer into segments and numbers them to make a sequence.

ii. Transport layer makes sure that the message is delivered to the correct process on the destination machine.

iii. It also makes sure that the entire message arrives without any error else it should be retransmitted.

Protocols of Transport layer : TCP, UDP, SCTP.

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.

Functions and services of Session layer :

i. It establishes, maintains, and ends a session.

ii. Session layer enables two systems to enter into a dialog.

iii. It also allows a process to add a checkpoint to stream of data.

Protocols of Session layer : PSAP, SSAP

6. Presentation layer :

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

Functions and services of Presentation layer :

i. Character code translation from ASCII to EBCDIC.

ii. **Data compression :** Allows to reduce the number of bits that needs to be transmitted on the network.

iii. **Data encryption :** Helps to encrypt data for security purposes.

iv. It provides a user interface and support for services like email and file transfer.

Protocols of Presentation layer : LLC, MAC.

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.

Functions and services of Application layer :

i. Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.

ii. It allows users to log on to a remote host.

iii. This layer provides various e-mail services.

iv. This layer offers distributed database sources and access for global information about various objects and services.

Protocols of Application layer : TELNET, FTP, SMPTP, DNS HTTP, NNTP.

Que 1.13. Explain functionalities of every layer in OSI reference model with neat block diagram. **AKTU 2016-17, Marks 10**

Answer

Functionality of every layer :

1. The **physical layer** coordinates the functions required to transmit a bit stream over a physical medium.
2. The **data link layer** is responsible for delivering data units from one station to the next without errors.
3. The **network layer** is responsible for the source-to-destination delivery of a packet across multiple network links.
4. The **transport layer** is responsible for the source-to-destination delivery of the entire message.
5. The **session layer** establishes, maintains, and synchronizes the interactions between communicating devices.

6. The **presentation layer** ensures interoperability between communicating devices through transformation of data into a mutually agreed-upon format.
7. The **application layer** enables the users to access the network.

Block diagram of OSI reference model :

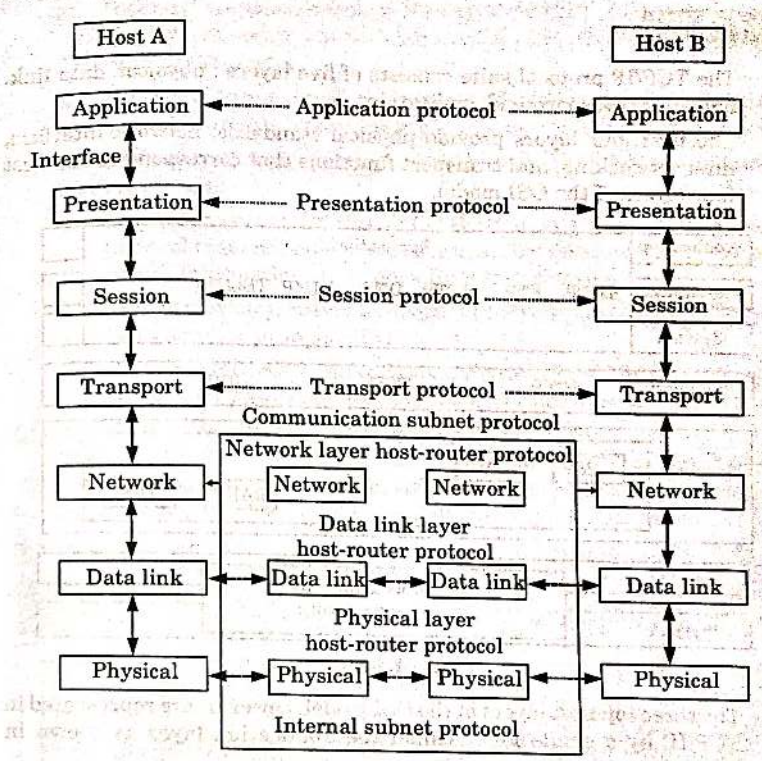


Fig. 1.13.1.

PART-5

TCP/IP Protocol Suite.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.14. **List the layers in the TCP/IP model.**

OR

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

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.

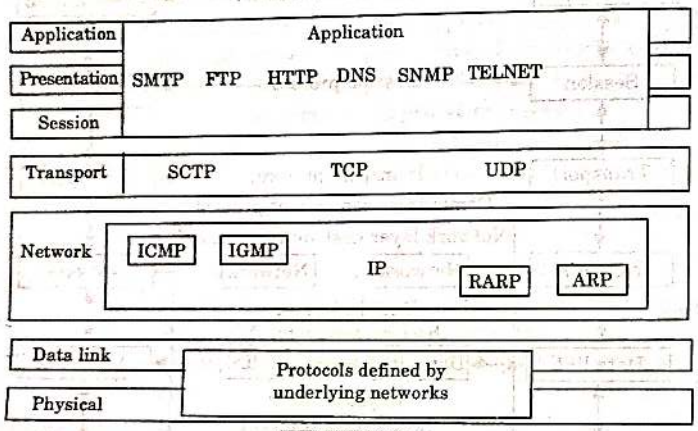


Fig. 1.14.1.

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. 1.14.1.

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.

PART-6

Network Device and Components.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.15. **Describe different network devices.**

OR

What are the components of network ?

Answer

1. **Repeater :**
   i. A repeater operates at the physical layer.

ii. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

iii. Repeaters do not amplify the signal.

iv. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.

v. It is a 2 port device.

2. **Hub :**

i. A hub is basically a multiport repeater.

ii. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.

iii. Hubs cannot filter data, so data packets are sent to all connected devices.

3. **Bridge :**

i. A bridge operates at data link layer.

ii. A bridge is a repeater, with add on the functionality of filtering the content by reading MAC addresses of source and destination.

iii. It is also used for interconnecting two LANs working on the same protocol.

iv. It has a single input and single output port, thus making it a 2 port device.

4. **Switch :**

i. A switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance.

ii. A switch is a data link layer device.

iii. The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

5. **Routers :**

i. A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device.

ii. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

iii. Router divide broadcast domains of hosts connected through it.

6. **Gateway :**

i. A gateway is a passage to connect two networks together that may work upon different networking models.

ii. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

iii. Gateways are also called protocol converters and can operate at any network layer.

iv. Gateways are generally more complex than switch or router.

PART-7

Physical Layer, Network Topology Design, Types of Connection.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.16. Write short note on physical layer.

Answer

1. Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another.
2. This layer deals with the setup of physical connection to the network and with transmission and reception of signals.
3. Physical layer defines electrical and physical specifications for devices.
4. The physical layer defines the relationship between a device and a transmission medium, such as a copper or optical cable.
5. The physical layer (also known as layer 1) deals with bit-level transmission between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.
6. The primary concern of this layer is transmission of individual bits from one node to another over a physical medium.

Que 1.17. 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 2018-19, Marks 10**

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.

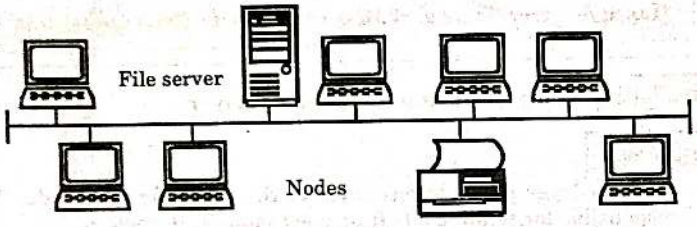


Fig. 1.17.1.

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 down the bus.

Advantages of bus topology :

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 :

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. 1.17.2.

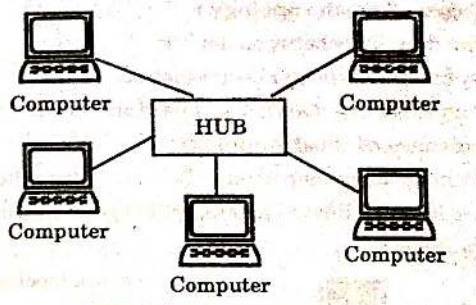


Fig. 1.17.2. Star topology.

Advantages of star topology :

i. Easy to install and wire.

ii. It can accommodate different wiring.

Disadvantages of star topology :

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 non-redundant links cannot be added to mesh network.

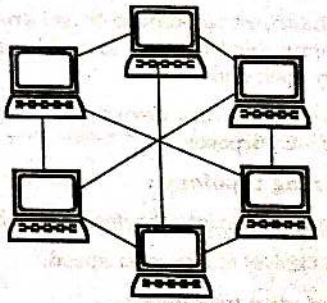


Fig. 1.17.3.

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

Advantages of mesh topology :

i. Redundant links between devices.

ii. Easy fault identification and isolation.

iii. An unusable link does not incapacitate the entire system.

Disadvantages of mesh topology :

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 :**

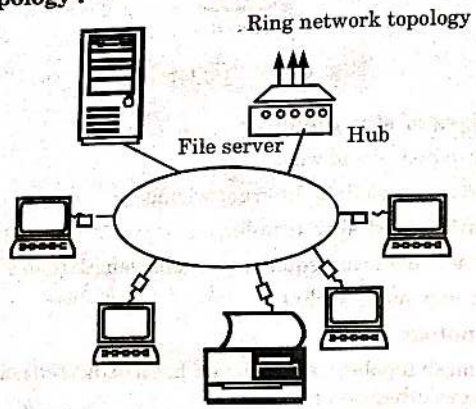


Fig. 1.17.4.

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.

Advantages of ring topology :

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

ii. Data packets travel at a greater speed.

Disadvantage of ring topology :

i. Expensive topology.

Que 1.18. What are the number of cable links required for n devices connected in mesh, ring, bus and star topology ?

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 1.19. What are the types of connection in computer network ?

Answer

1. Point-to-point connections allow one device to communicate with one other device. For example, two phones may pair with each other to exchange contact information or pictures.
2. Broadcast/multicast connections allow a device to send one message out to the network and have copies of that message delivered to multiple recipients.
3. Multipoint connections allow one device to connect and deliver messages to multiple devices in parallel.

PART-8

Transmission Media.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.20. 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

OR

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

1. Transmission media is a pathway that carries the information from sender to receiver.
2. Signals travel from transmitter to receiver via a path known as medium. This medium can be guided or unguided.
3. A guided medium is contained within physical boundaries, while an unguided medium is boundless.

A. Wired or guided media or bound transmission media : The most popular types of guided media are :

1. Twisted-pair cable :

i. Twisted-pair cable consists of two insulated copper wires twisted together.

ii. Twisting allows each wire to have approximately the same noise environment.

iii. Twisted-pair cable transmits data in the form of an electric current.

Fig. 1.20.1. Twisted pair cable.

2. Coaxial cable :

i. Coaxial cable consists of the following layers (starting from the center) :

a. A metallic rod-shaped inner conductor.

b. An insulator covering the rod.

c. A metallic outer conductor (shield).

d. An insulator covering the shield.

e. A plastic cover.

ii. Coaxial cable transmits data in the form of an electric current.

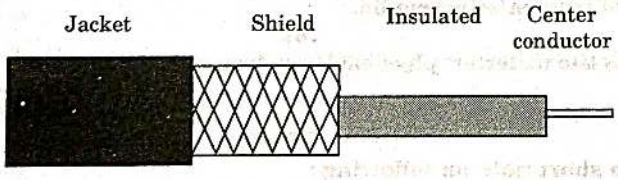


Fig. 1.20.2. Co-axial cable.

3. Optical fiber :

i. Fiber-optic cables are composed of a glass or plastic inner core surrounded by cladding.

ii. Fiber-optic cables carry data signals in the form of light. The signal is propagated along the inner core by reflection.

iii. Fiber-optic transmission has noise resistance, low attenuation, and high bandwidth capabilities,

iv. In fiber optics, signal propagation can be multimode or single mode.

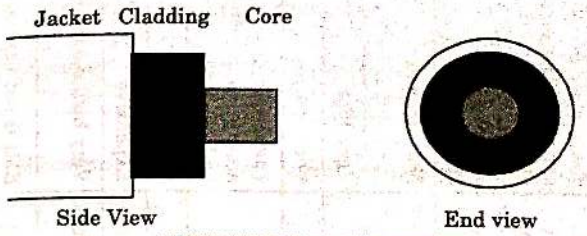


Fig. 1.20.3. Optical fiber cable.

B. Wireless or unguided media or unbound transmission media :

1. Radio waves can be used to transmit data. These waves use unguided media and are usually propagated through the air.
2. Radio wave propagation is dependent on frequency. There are five propagation types :

i. Surface propagation : VLF and LF waves use surface propagation. These waves follow the contour of the earth.

ii. Tropospheric propagation : MF waves are propagated in the troposphere, either through direct line-of-sight propagation or through reflection.

iii. Ionospheric propagation : HF waves travel to the ionosphere, where they are reflected back to a receiver in the troposphere.

iv. Line-of-sight propagation : VHF and UHF waves use line-of-sight propagation.

v. Space propagation : VHF, UHF, SHF, and EHF waves can be propagated into space and received by satellites.

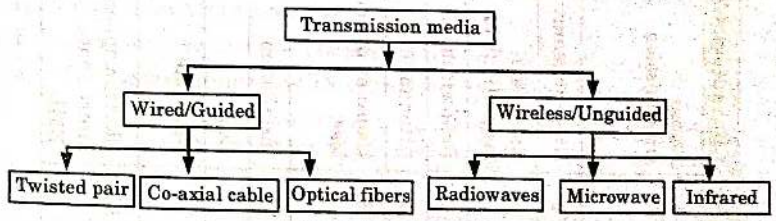


Fig. 1.20.4.

Que 1.21. **Compare twisted pair, co-axial and fiber optic cable.**

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-9

Signal Transmission and Encoding.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.22. **What do you mean by signal transmission ? How can we transmit a digital signal ?**

Answer

1. The physical layer moves data in the form of electromagnetic signals across a transmission medium.
2. Generally, the data are not in a form that can be transmitted over a network.
3. So the data must first be changed to a form that transmission media can accept.
4. For transmission, data needs to be changed to signals.
5. When this signal is transmitted over the transmission medium it is known as signal transmission.

Transmission of digital signal : We can transmit a digital signal by using one of two approaches: baseband transmission or broadband transmission.

A. Baseband Transmission :

1. Baseband transmission means sending a digital signal over a channel without changing it to an analog signal.
2. Baseband transmission needs a low-pass channel i.e., a channel having a bandwidth that starts from zero.
3. This is possible if we have a dedicated medium with a bandwidth constituting only one channel.
4. Following are two cases of a baseband communication :

   a. Low-pass channel with wide bandwidth :

   i. If we want to preserve the exact form of a non-periodic digital signal we need to send the entire spectrum between zero and infinity.

   ii. This is possible if we have a dedicated medium with an infinite bandwidth.

   iii. But we cannot have such a channel in real life.

iv. However, the amplitudes of the frequencies at the border of the bandwidth are so small that they can be ignored.

v. This means that if we have a medium with a very wide bandwidth (such as fiber optic cable) two stations can communicate with good accuracy.

b. Low-pass channel with limited bandwidth :

i. In a low-pass channel with limited bandwidth, we approximate the digital signal with an analog signal.

ii. The level of approximation depends on the bandwidth available.

B. Broadband Transmission :

1. Broadband transmission or modulation means changing the digital signal to an analog signal for transmission.
2. Modulation allows us to use a bandpass channel *i.e.*, a channel whose bandwidth does not start from zero.
3. This type of channel is more available than a low-pass channel.
4. In a bandpass channel we need to convert the digital signal to an analog signal before transmission.

Que 1.23. Write a short note on digital encoding.

OR

List the various line coding schemes.

Answer

Mechanisms for digital-to-digital encoding fall into following categories :

A. Unipolar :

1. Unipolar encoding is very simple and primitive.
2. Unipolar encoding uses only one polarity.
3. In unipolar encoding, all the signal levels are on one side of the time axis, either above or below.

a. NRZ (Non-Return-to-Zero) :

i. In a non-return-to-zero (NRZ) scheme the positive voltage defines bit 1 and the zero voltage defines bit 0.

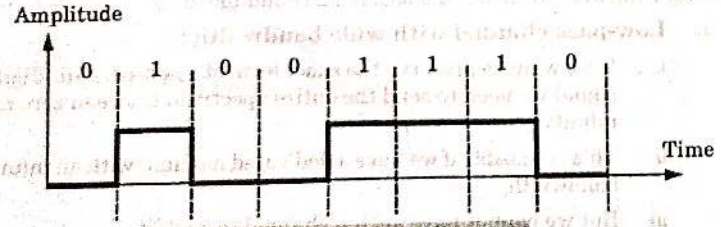


Fig. 1.23.1. Unipolar encoding.

ii. Since the signal does not return to zero at the middle of the bit it is called NRZ.

B. Polar :

1. Polar encoding uses two voltage levels: one positive and one negative.
2. By using both levels, in most polar encoding methods the average voltage level on the line is reduced.
3. NRZ encoding includes two methods: nonreturn to zero, level (NRZ-L), and nonreturn to zero, invert (NRZ-I).

a. NRZ-L :

i. In NRZ-L encoding, the level of the signal depends on the type of bit it represents.

ii. A positive voltage usually means the bit is a 0, and a negative voltage means the bit is a 1 (or vice versa).

iii. Thus, the level of the signal is dependent upon the state of the bit.

b. NRZ-I :

i. In NRZ-I, an inversion of the voltage level represents a 1 bit.

ii. It is the transition between a positive and a negative voltage that represents a 1 bit.

iii. A 0 bit is represented by no change.

iv. NRZ-I is superior to NRZ-L due to the synchronization provided by the signal change each time a 1 bit is encountered.

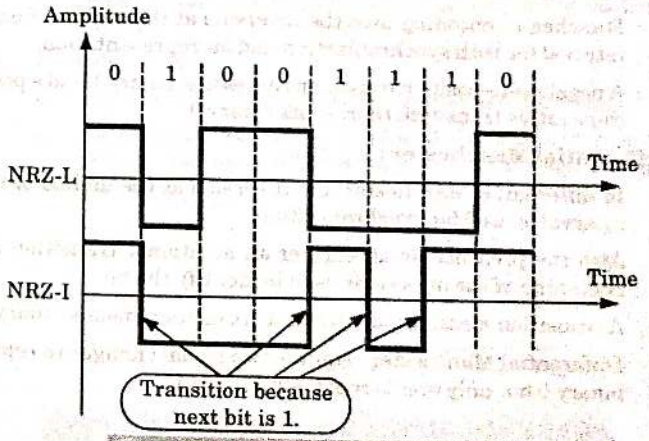


Fig. 1.23.2. NRZ-L and NRZ-I encoding.

c. Return to Zero (RZ) :

i. In NRZ encoding problem occurs when the sender and receiver clocks are not synchronized.

ii. The receiver does not know when one bit has ended and the next bit is starting.

iii. The solution to this problem is return-to-zero (RZ) scheme.

iv. RZ scheme uses three values: positive, negative, and zero.

v. In RZ, the signal changes not between bits but during the bit.

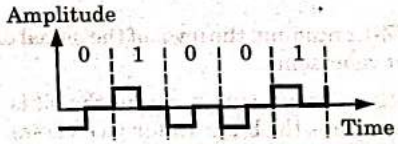


Fig. 1.23.3. Polar RZ scheme.

d. Biphase :

i. In biphase encoding, the signal changes at the middle of the bit interval but does not return to zero.

ii. Instead, it continues to the opposite pole.

iii. These midinterval transitions allow for synchronization.

iv. There are two types of biphase encoding : Manchester and differential Manchester.

1. Manchester :

i. Manchester encoding uses the inversion at the middle of each bit interval for both synchronization and bit representation.

ii. A negative-to-positive transition represents binary 1 and a positive-to-negative transition represents binary 0.

2. Differential Manchester :

i. In differential Manchester, the inversion at the middle of the bit interval is used for synchronization.

ii. Also the presence or absence of an additional transition at the beginning of the interval is used to identify the bit.

iii. A transition means binary 0 and no transition means binary 1.

iv. Differential Manchester requires two signal changes to represent binary 0 but only one to represent binary 1.

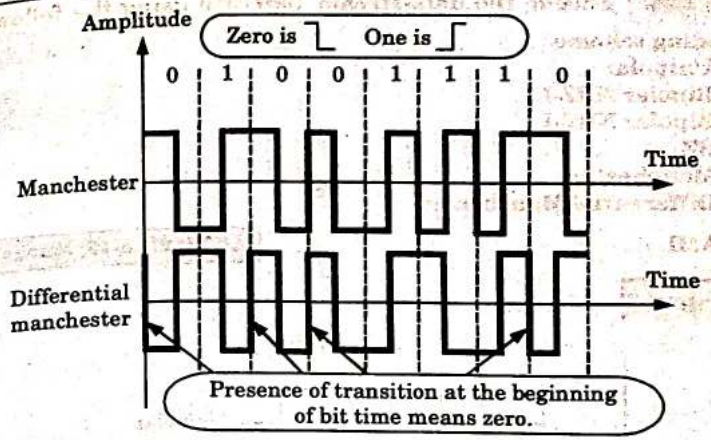


Fig. 1.23.4. Manchester and differential manchester encoding.

C. Bipolar :

1. In bipolar encoding, we use three levels: positive, zero, and negative.
2. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.
3. There are two variations of bipolar encoding: AMI and pseudoternary.

a. Alternate Mark Inversion (AMI) :

i. In AMI the word 'mark' means 1. So AMI means alternate 1 inversion.

ii. A neutral zero voltage represents binary 0.

iii. Binary 1s are represented by alternating positive and negative voltages.

b. Pseudoternary :

i. A variation of AMI encoding is called pseudoternary.

ii. In pseudoternary the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negative voltages.

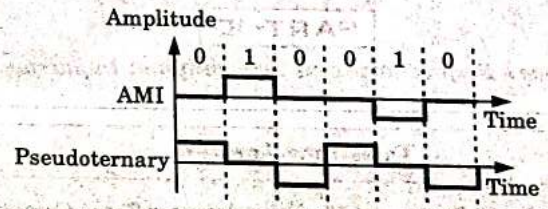


Fig. 1.23.5. Bipolar schemes : AMI and pseudoternary.

Que 1.24. **Encode the data-stream 10011010 using the following encoding scheme :**

i. Unipolar
ii. Bipolar NRZ-L
iii. Bipolar NRZ-I
iv. RZ
v. Manchester
vi. Differential Manchester
vii. AMI

AKTU 2018-19, Marks 10

Answer

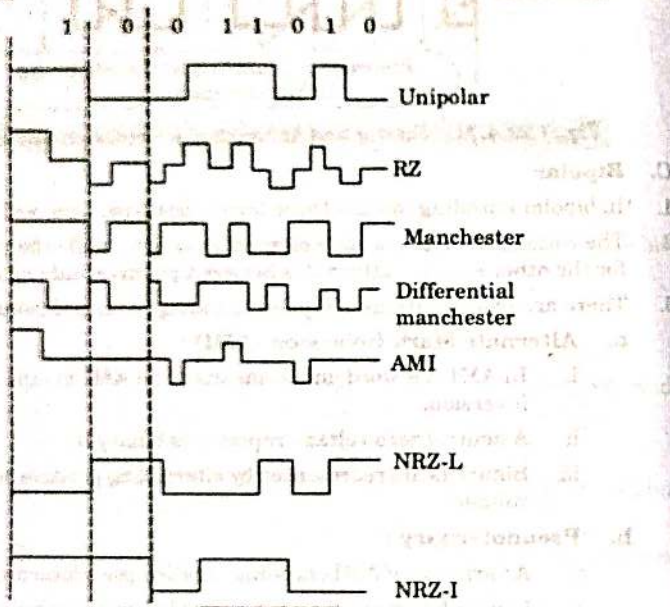


Fig. 1.24.1.

PART-10

Network Performance and Transmission Impairment.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.25. **Write a short note on network performance.**

Answer

1. Performance of a network pertains to the measure of service quality of a network as perceived by the user.
2. Performance can be measured using transit time and response time.
3. Transit time is the amount of time required for a message to travel from one device to another.
4. Response time is the elapsed time between an inquiry and a response.
5. The performance of a network depends on following factors :

A. Number of users :

i. The design of a network is based on an assessment of the average number of users that will be communicating at any one time.

ii. However during peak load periods the actual number of users can exceed the average and thereby decrease performance.

iii. How a network responds to peak load is measure of its performance.

B. Type of transmission medium :

i. The medium defines the speed at which data can travel through a connection.

ii. Today's networks are using faster transmission media like optical fiber.

iii. However, the speed of light imposes an upper bound on the data rate.

C. Hardware :

i. The types of hardware used in a network affect the speed and capacity of transmission.

ii. A higher-speed computer with greater storage capacity provides better performance.

D. Software :

i. The software used to process data also affects network performance.

ii. Moving a message from node to node requires processing to transform the raw data into transmittable signals.

iii. The software that provides this service affects both the speed and the reliability of a network link.

iv. Well-designed software can speed the process and make transmission more effective and efficient.

6. Performance of a network can also be evaluated by two networking metrics: throughput and delay.

7. More throughput and less delay is desirable.

Que 1.26. What do you understand by transmission impairment?

Answer

1. Signals travels through imperfect transmission media.
2. The imperfection of transmission media causes signal impairment.
3. This means that the signal at the transmitter is not same as the signal at the receiver of the medium.
4. There are three causes of impairment: attenuation, distortion, and noise.

A. Attenuation :

1. Attenuation means a loss of energy.
2. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium.
3. Some of the electrical energy in the signal is converted to heat.
4. To compensate for this loss, amplifiers are used to amplify the signal.

B. Distortion :

1. Distortion means that there is change in signal form or shape.
2. Distortion can occur in a composite signal made of different frequencies.
3. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination.
4. Differences in delay may create a difference in phase.
5. Therefore signal components at the receiver have phases different from what they had at the sender.
6. Hence the shape of the composite signal is not the same.

C. Noise :

1. Noise is another cause of impairment.
2. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

PART-11

Switching Techniques and Multiplexing.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 1.27. Explain the types of switching.

OR

Explain the various types of switching methods with suitable examples.

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. 1.27.1.

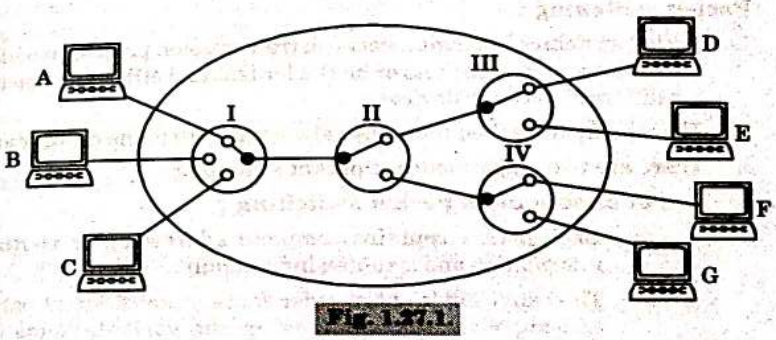


Fig. 1.27.1

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. 1.27.2.

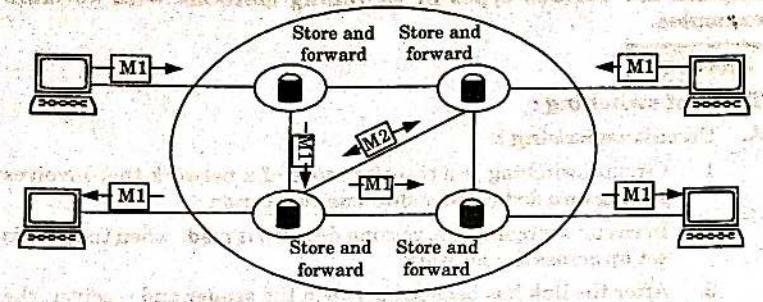


Fig. 1.27.2.

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.

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.

Que 1.28. Write short note on multiplexing.

Answer

1. Multiplexing is a technique used to combine and send the multiple data streams over a single medium.
2. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.
3. Multiplexing is achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line.
4. Multiplexing follows many-to-one, *i.e.*, n input lines and one output line.

Que 1.29. Why we use multiplexing in computer network ?

Answer

1. The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
2. If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
3. When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
4. Transmission services are very expensive.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. What do you mean by service primitives ?
Ans: Refer Q. 1.10.

Q. 2. What is OSI Model ? Explain the functions, protocols and services of each layer.
Ans: Refer Q. 1.12.

Q. 3. Explain functionalities of every layer in OSI reference model with neat block diagram.
Ans: Refer Q. 1.13.

Q. 4. Discuss the TCP/IP protocol suite on the basis of protocol layering principle.

Ans: Refer Q. 1.14.

Q. 5. Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.

Ans: Refer Q. 1.17.

Q. 6. Discuss the different physical layer transmission media.

Ans: Refer Q. 1.20.

Q. 7. Compare twisted pair, co-axial and fiber optic cable.

Ans: Refer Q. 1.21.

Q. 8. Explain the various types of switching methods with suitable examples.

Ans: Refer Q. 1.27.

2 UNIT

Link Layer

CONTENTS

PART-1

Framing.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.1. Define framing. Why it is needed ?

Answer

1. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.
2. Data transmission means moving bits in the form of a signal.
3. During data transmission the physical layer provides bit synchronization.
4. The data-link layer packs bits into frames so that each frame is distinguishable from another.
5. Framing separates a message from one source to a destination by adding a sender address and a destination address.
6. The destination address defines where the packet is to go.
7. The sender address helps the recipient acknowledge the receipt.

Need of framing :

1. If a message is carried in one very large frame and a single-bit error occur it would require the retransmission of the whole frame.
2. Hence a message is divided into smaller frames, so that a single-bit error affects only that small frame.

Que 2.2. What are the different types of framing ?

Answer

Following are the types of framing :

1. **Fixed size :**
   i. The frame is of fixed size and there is no need to provide boundaries to the frame.
   ii. Length of the frame itself acts as delimiter.
2. **Variable size :**
   i. In this framing there is need to define end of frame as well as beginning of next frame to distinguish.

   ii. This can be done in two ways :

A. Character-Oriented Framing :

1. In character-oriented framing, data to be carried are 8-bit characters.
2. The header and the trailer are also multiples of 8 bits.
3. The header carries the source and destination addresses and other control information.
4. The trailer carries error detection redundant bits.
5. To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.
6. The flag is composed of protocol-dependent special characters. It signals the start or end of a frame.

B. Bit-Oriented Framing :

1. In bit-oriented framing, the data section of a frame is a sequence of bits.
2. In bit-oriented framing, we need a delimiter to separate one frame from the other.
3. Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame.

PART-2

Error Detection and Correction.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.3. 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 :

i. The term single bit error suggests that only one bit in the given data unit such as byte is in error.

ii. That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 2.3.1.

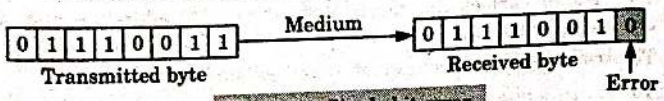


Fig. 2.3.1. Single bit error.

2. Burst errors :

i. 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.

ii. 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.

iii. Burst errors are illustrated in Fig. 2.3.2.

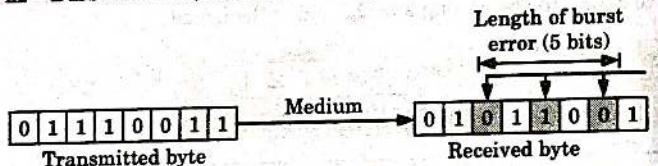


Fig. 2.3.2. Burst error.

Que 2.4. How 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.

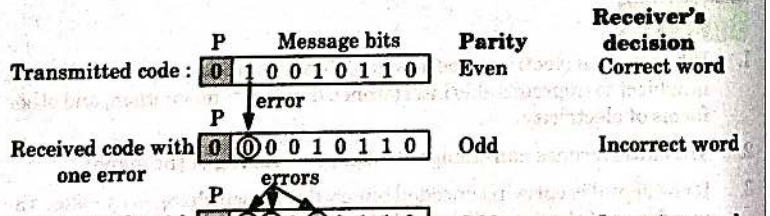


Fig. 2.4.1. The receiver detects the presence of error if the number of errors is odd *i.e.*, 1, 3, 5.

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 shown in Fig. 2.4.1.
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.
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 2.5. Explain the concept of checksum. How error is detected using the checksum byte ?

Answer

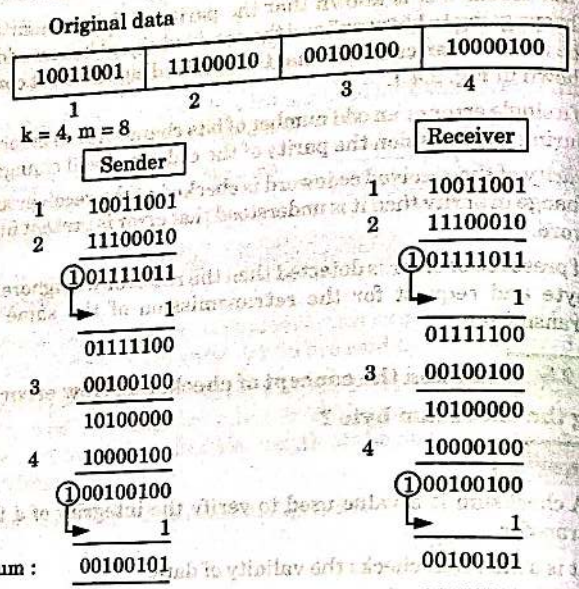
1. A checksum is a value used to verify the integrity of a file or a data transfer.
2. It is a sum that checks the validity of data.
3. A checksum is a simple type of redundancy check that is used to detect errors in data.
4. Checksums are typically used to compare two sets of data to make sure they 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.

Lets consider following data :

10011001111000100010010010000100



Que 2.6. 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 which 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. 2.6.1.

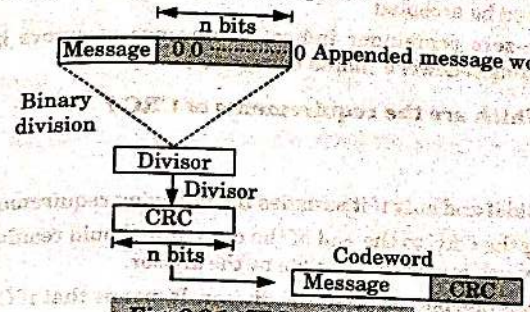


Fig. 2.6.1. CRC generator.

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. 2.6.1.

CRC checker :

1. Fig. 2.6.2 shows the CRC checker.

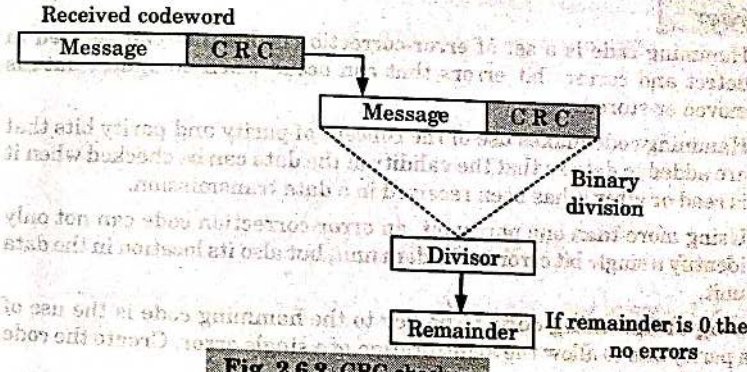


Fig. 2.6.2. CRC checker.

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 2.7. **Which are the requirements of CRC ?**

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 2.8. **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 can not 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.
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.

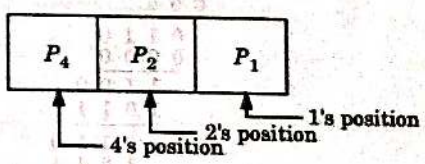
Hence put $P_2 = 0$ in the 2's position of the error word.

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

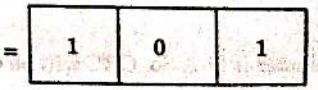
$\therefore$ $P_1 D_3 D_5 D_7 = 1\,0\,1\,1 \rightarrow$ Odd parity so error exists.

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

Step 4 : Write the error word :

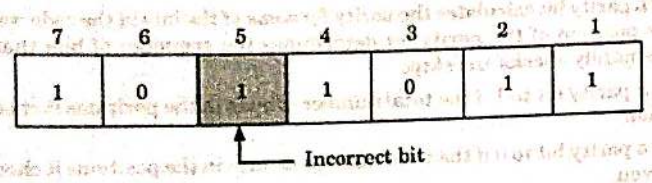


Substituting the values of P_4, P_2 and P_1 obtained in steps 1, 2 and 3 we get



$= (5)_{10}$

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



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 2.9. **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 2.10. **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. 2.8, Page 2–8B, 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.

PART-3

Flow Control (Elementary Data Link Protocol, Sliding Window Protocols).

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.11. 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 :**
   i. The data link layer act as a service interface to the network layer.
   ii. 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 :**
   i. The source machine sends data in the form of blocks called frames to the destination machine.
   ii. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.
3. **Flow control :**
   i. Flow control is done to prevent the flow of data frame at the receiver end.

   ii. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. **Error control :**
   i. Error control is done to prevent duplication of frames.
   ii. 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) :**
   i. This protocol is used to connect a workstation to the internet over a dial-up line using a modem.
   ii. It is connection-oriented protocol.
   iii. 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) :**
   i. This protocol is used by a lot of internet users to connect their home computers to the server of an Internet Service Provider (ISP).
   ii. Most of these users have a traditional modem and they are connected to the internet through a telephone line or a TV cable.
   iii. The PPP is used for controlling and managing the data transfer.
3. **High Level Data Link Control (HDLC) Protocol :**
   i. HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.
   ii. For the HDLC protocol the following three types of stations have been defined :
      a. **Primary station :** A primary station takes care of the data link management.
      b. **Secondary station :** A secondary station operates under the control of a primary station.
      c. **Combined station :** A combined station can act as both primary and secondary stations.
4. **Ethernet :**
   i. Ethernet supports nearly every protocol, and can operate with any networking equipment that adheres to the IEEE standard.
   ii. This openness, combined with the ease of use, has made Ethernet dominant in the local area network.
   iii. The Ethernet system consists of three basic elements :
      a. The physical medium used to carry Ethernet signals between computers.

b. A set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly access to the shared Ethernet channel.

c. An Ethernet frame that consists of a standardized set of bits used to carry data over the system.

Que 2.12. Explain sliding window protocol.

OR

Write short note on sliding window protocol.

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 $n-1$.
6. When the receiver sends an ACK, it includes the number of the next frame it expects to receive. For example, 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.

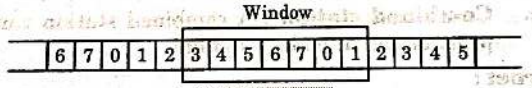


Fig. 2.12.1.

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.

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.

Que 2.13. 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. 2.13.1 illustrates the operation of the stop and wait protocol.

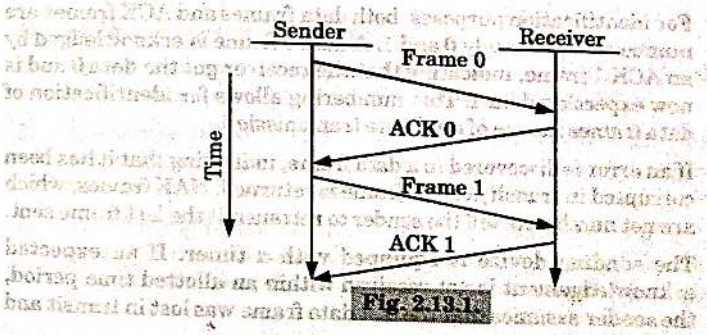


Fig. 2.13.1.

Que 2.14. State drawbacks of stop and wait protocols.

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 2.15. 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 :
   - i. The sending device keeps a copy of the last frame transmitted until it receives an acknowledgement for that frame.
   - ii. 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.
   - iii. 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.
   - iv. 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.

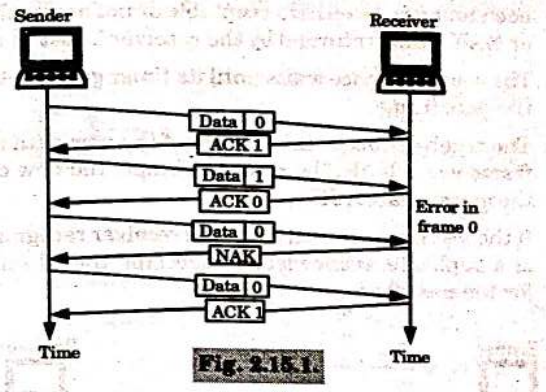


Fig. 2.15.1.

b. Operation in case of lost frame :

1. Any of the three frame types can be lost in transit. Fig. 2.20.2 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.

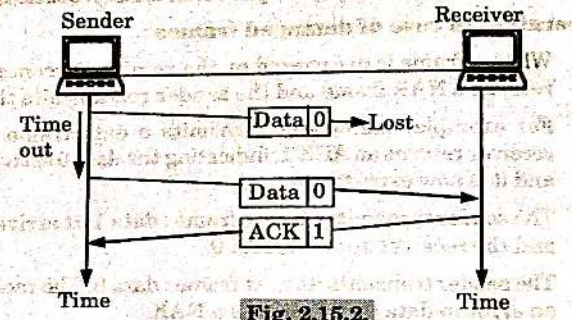


Fig. 2.15.2.

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.

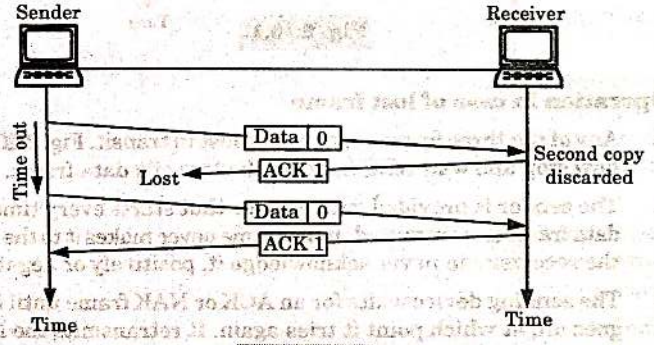


Fig. 2.15.3.

Que 2.16. Describe the Go-back-N ARQ protocol.

OR

Write a short note on Go-back-N ARQ. 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 :

i. The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back as shown in Fig. 2.16.1.

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

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

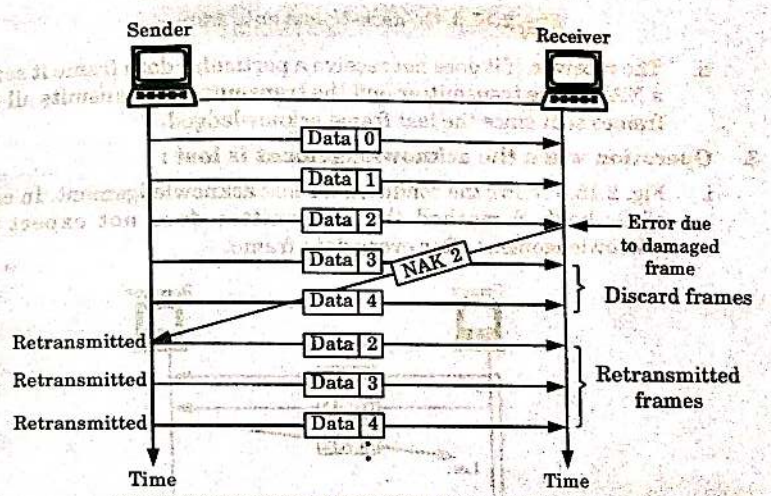


Fig. 2.16.1. Go-back-N, damaged data frame.

2. Operation when a frame is lost :

i. As shown in Fig. 2.16.2, the case of lost frame is also treated in the same manner as that of the damaged frame.

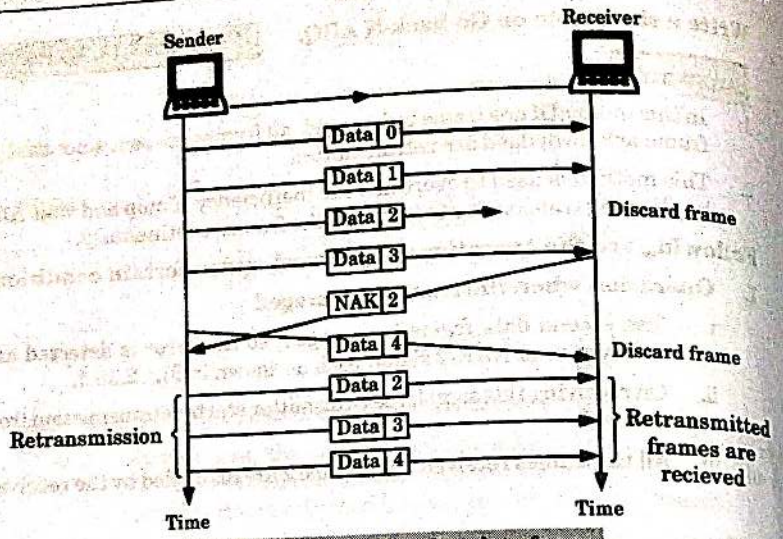


Fig. 2.16.2. Go-back-N, lost data frame.

ii. 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 :

i. Fig. 2.16.3 shows the condition for lost acknowledgement. In case of Go-back-N method the transmitter does not expect an acknowledgement after every data frame.

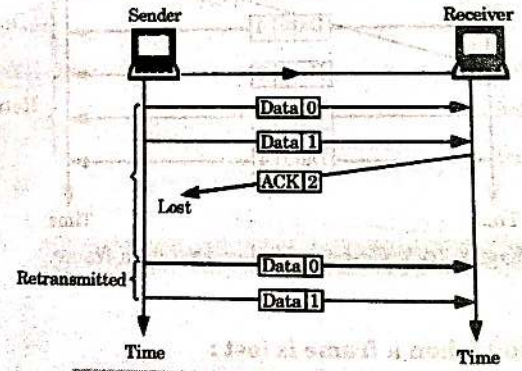


Fig. 2.16.3. Go-back-N, lost ACK frame.

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

iii. 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 2.17. 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 2.18. Write a short note on selective repeat ARQ.

OR

Explain ARQ error control technique, in brief.

AKTU 2015-16, Marks 07

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. 2.18.1.
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.

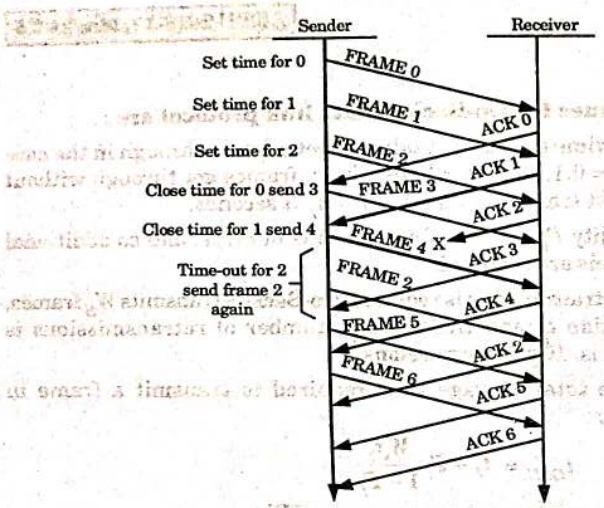


Fig. 2.18.1.

PART-4

Medium Access Control and Local Area Networs : Channel Allocation.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.19. Explain medium access control sublayer.

Answer

1. The MAC sublayer is very important in LANs because it is a broadcast network. Fig. 2.19.1, show the position of MAC sublayer.

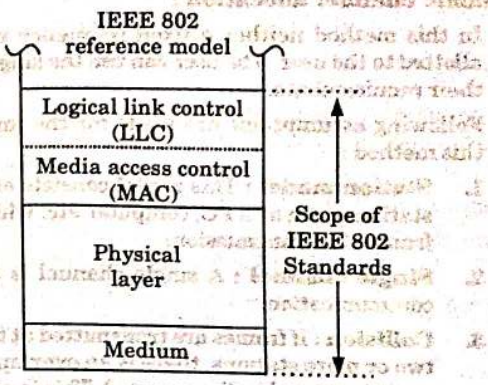


Fig. 2.19.1.

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 Link Control (LLC) sublayer :

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

Que 2.20. 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 2.21. 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 2.22. Describe CSMA/CA in brief.

OR

Write a short note on collision avoidance.

Answer

CSMA/CA :

1. Carrier Sense Multiple Access/Collision Avoidance is a network contention protocol used for carrier transmission in networks using the 802.11 standard.
2. CSMA/CA works to avoid collisions prior to their occurrence.
3. In CSMA/CA nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".
4. When the nodes do transmit, they transmit their packet data in its entirety.

CSMA/CA procedure :

1. Fig. 2.22.1 shows the flow chart explaining the principle of CSMA / CA.

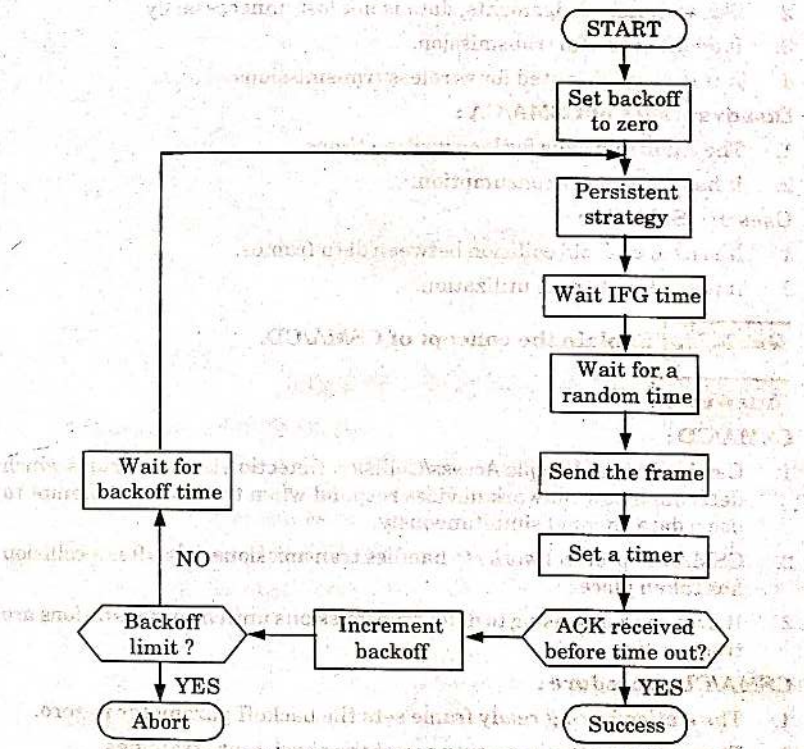


Fig. 2.22.1. CSMA / CA procedure.

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 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.

Advantages of CSMA/CA :

1. CMSA/CA prevents collision.
2. Due to acknowledgements, data is not lost unnecessarily.
3. It avoids wasteful transmission.
4. It is very much suited for wireless transmissions.

Disadvantages of CSMA/CA :

1. The algorithm calls for long waiting times.
2. It has high power consumption.

Uses of CSMA/CA :

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

Que 2.23. Explain the concept of CSMA/CD.

Answer

CSMA/CD :

1. *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.*
2. *CSMA/CD protocol works to handles transmissions only after a collision has taken place.*
3. *It uses carrier-sensing to defer transmissions until no other stations are transmitting.*

CSMA/CD procedure :

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.

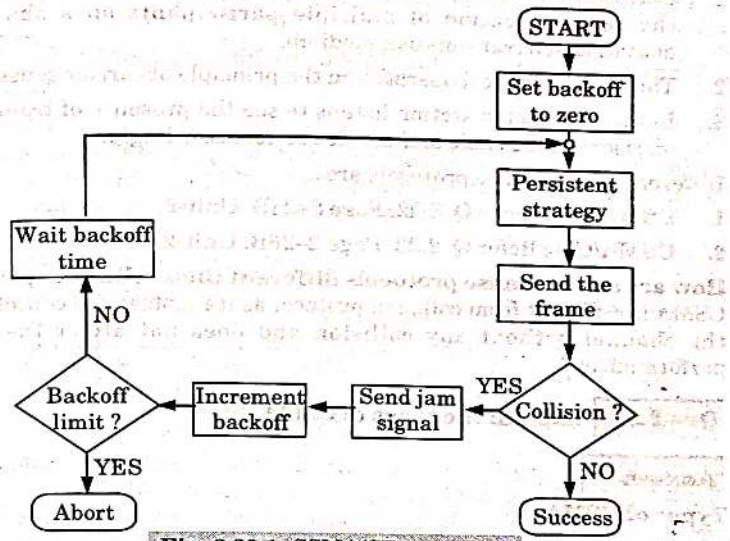


Fig. 2.23.1. CSMA/CD procedure.

Advantages of CSMA/CD :

1. It is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

Disadvantages of CSMA/CD :

1. Though this algorithm detects collisions, it does not reduce the number of collisions.
2. It is not appropriate for large networks.
3. Its performance degrades exponentially when more stations are added.

Uses of CSMA/CD :

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

Que 2.24. **Explain Carrier Sense Multiple Access (CSMA) protocol.**

OR

Discuss different carrier sense protocols. How are they different than collision protocols ? **AKTU 2017-18, Marks 10**

Answer

1. Carrier Sense Multiple Access (CSMA) is a basic method that controls the communication of multiple participants on a shared and decentralized transmission medium.
2. The CSMA protocol operates on the principle of carrier sensing.
3. 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 :** Refer Q. 2.22, Page 2–24B, Unit-2.
2. **CSMA/CD :** Refer Q. 2.23, Page 2–26B, Unit-2.

How are carrier sense protocols different then collisions protocols : CSMA is different from collision protocol as it resolves the contention for the channel without any collision and does not affect the system performance.

Que 2.25. **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-5

LAN Standard.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.26. **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. 2.26.1.

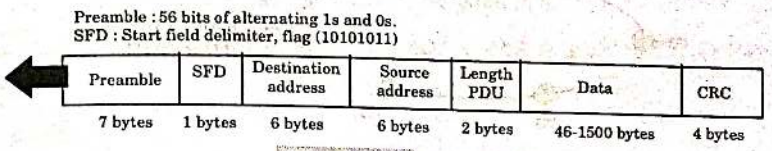


Fig. 2.26.1.

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 2.27. 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. 2.27.1. 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.

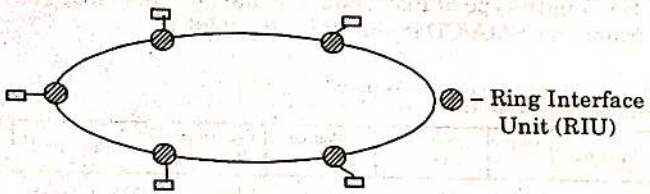


Fig. 2.27.1.

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 2.28. 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. 2.28.1. The physical topology is bus topology as shown in Fig. 2.28.1.

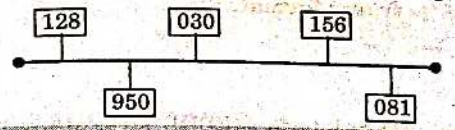


Fig. 2.28.1. Physical topology in token passing.

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 2.29. Differentiate between 802.3, 802.4, and 802.5 IEEE standards.

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

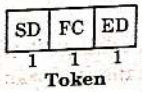
Que 2.30. Define Fiber Distributed Data Interface (FDDI) in detail with the help of its frame format.

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 :



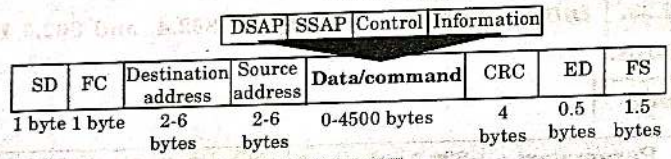


Fig. 2.30.1.

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 2.31. 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. 2.30, Page 2–32B, Unit-2.

PART-6

Link Layer Switches and Bridges (Learning Bridge and Spanning Tree Algorithm).

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.32. Write short note on link layer switches and bridges.

Answer

A. Switches :

1. A switched network consists of a series of interlinked nodes, called switches.
2. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
3. In a switched network, some of these nodes are connected to the end systems (computers or telephones).
4. Others are used only for routing.
5. Fig 2.32.1 shows a switched network.
6. The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V.

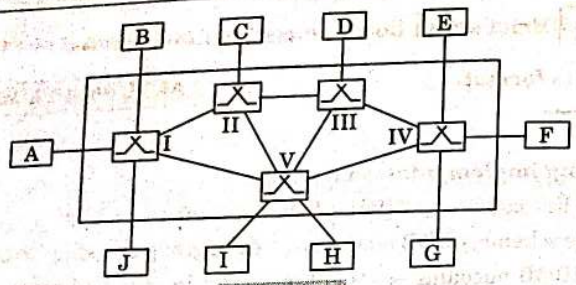


Fig. 2.32.1.

7. Each switch is connected to multiple links.

B. Bridges :

1. Bridges are a data link layer device which connects multiple LANs together to form a larger LAN.

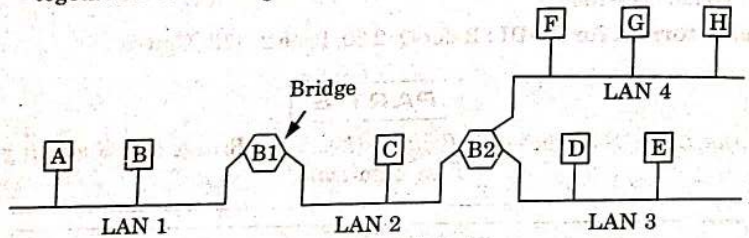


Fig. 2.32.2.

2. In Fig 2.32.2 there are four LAN's which are connected by two bridges.
3. It stores and forwards Ethernet frames, *i.e.*, it has to do with the MAC address rather than the IP address.
4. It also examines frame header and selectively forwards frames based on MAC destination address.
5. Bridges are transparent, *i.e.*, hosts are unaware of presence of bridges.
6. Bridges are plug-and-play and self-learning devices.
7. At the physical level the bridge boosts the signal strength like a repeater or completely regenerates the signal.

Que 2.33. Write a short note on learning bridge.

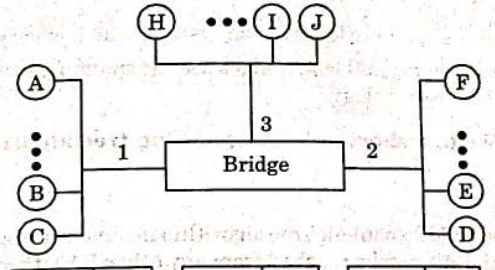
Answer

1. The earliest bridges had forwarding tables that were static.
2. Each table entry was manually entered during bridge setup.
3. A better solution to the static table is a dynamic table.
4. Dynamic table maps addresses to ports automatically.

5. To make a table dynamic, we need a bridge that gradually learns from the frame movements.
6. To do this, the bridge inspects both the destination and the source addresses.
7. The destination address is used for the forwarding decision (table lookup).
8. The source address is used for adding entries to the table and for updating purposes.

Example :

1. Suppose C sends frame to D and D replies back with frame to C.



Address	Port

a. Original

Address	Port
C	1

b. After C sends a frame to D

Address	Port
C	1
D	2

c. After D sends a frame to C

Fig. 2.33.1.

2. C sends frame to D.
3. The bridge has no entry for either C or D.
4. So the frame goes out from all three ports; the frame floods the network.
5. Bridge notes that C is on port 1. This means that frames destined for C, in the future, must be sent out through port 1.
6. The bridge adds this entry to its table. The table has its first entry now.
7. Frame is received by D.
8. D generates and sends frame to C.
9. Bridge sees frame from D.
10. Bridge notes that D is on port 2. This means that frames destined for D, in the future, must be sent out through port 2.
11. The bridge adds this entry to its table. The table has its second entry.
12. Now the bridge has an entry for C, so it forwards the frame only to port 1. There is no flooding.

13. The process of learning continues as the bridge forwards frames.

Que 2.34. Why spanning tree algorithm is required ?

Answer

1. As long as there are no redundant bridges in the system transparent bridges work fine.
2. However it is desirable to have redundant bridges to make the system more reliable.
3. If a bridge fails, another bridge takes over until the failed one is repaired or replaced.
4. Redundancy can create loops in the system, which is very undesirable.
5. To solve the looping problem, bridges use the spanning tree algorithm to create a loopless topology.

Que 2.35. Write a short note on spanning tree algorithm.

Answer

1. In a bridged LAN, spanning tree algorithm means creating a topology in which each LAN can be reached from any other LAN through one path only.
2. There is no loop present.
3. We cannot change the physical topology of the system because of physical connections between cables and bridges.
4. So we create a logical topology that overlay the physical one.
5. Both LANs and bridges are represented as nodes.
6. The connection of a LAN to a bridge and vice versa is represented by the connecting arcs.
7. To find the spanning tree, we need to assign a cost (metric) to each arc.
8. The process to find the spanning tree involves three steps :

   Step 1 : Every bridge has a built-in ID. Each bridge broadcasts this ID so that all bridges know which one has the smallest ID. The bridge with the smallest ID is selected as the root bridge (root of the tree).

   Step 2 : The algorithm tries to find the shortest path (a path with the shortest cost) from the root bridge to every other bridge or LAN. The shortest path can be found by examining the total cost from the root bridge to the destination. The combination of the shortest paths creates the shortest tree.

   Step 3 : Based on the spanning tree, we mark the ports that are part of the spanning tree, the forwarding ports, which forward a frame that the

bridge receives. We also mark those ports that are not part of the spanning tree, the blocking ports, which block the frames received by the bridge.

9. There is only one single path from any LAN to any other LAN in the spanning tree system. No loops are created.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. What is hamming code ? Explain its working with suitable example.
Ans. Refer Q. 2.8.

Q. 2. Discuss the issues in the data link layer and about its protocol on the basis of layering principle.
Ans. Refer Q. 2.11.

Q. 3. Write short note on sliding window protocol.
Ans. Refer Q. 2.12.

Q. 4. Write a short note on stop and wait ARQ.
Ans. Refer Q. 2.15.

Q. 5. Write a short note on Go-back-N ARQ.
Ans. Refer Q. 2.16.

Q. 6. Illustrate the performance issues for Go-Back-N data link protocol.
Ans. Refer Q. 2.17.

Q. 7. Discuss different carrier sense protocols. How are they different than collision protocols ?
Ans. Refer Q. 2.24.

Q. 8. Brief about how line coding implemented in FDDI and describe its format.
Ans. Refer Q. 2.31.

Q. 9. Write a short note on learning bridge.
Ans. Refer Q. 2.33.

☺☺☺

3 UNIT

Network Layer

CONTENTS

PART-1

Point-to-Point Networks, Logical Addressing.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.1. What is a point-to-point network ? Give the advantages and disadvantages of a point-to-point network.

Answer

1. A point-to-point network is a permanent link between two endpoints.
2. A point-to-point connection provides a dedicated link between two devices.
3. The dedicated link between two devices can be wire or cable, microwave or satellite link.
4. The entire capacity of the link is reserved for transmission between two devices.
5. A point-to-point network uses different types of topology (mesh or star) to connect two internet nodes.

Advantages of a point-to-point network :

1. **Speeds :** A point-to-point network usually use leased lines so the speeds are guaranteed.
2. **Control & Monitor :** By using the same connection, it becomes easier to monitor data usage across all sites.
3. **Prioritise :** Point-to-point leased lines allow you to prioritise certain types of data making your connection fast and reliable.
4. **Better Security :** With broadband your data is going through a public network, this increases the risk of it being intercepted. But with point to points it's your own private networks, so you can transfer data securely.

Disadvantages of a point-to-point network :

1. **Distance :** For geographically distant locations a point-to-point network becomes more expensive.
2. **Limited Connections :** With a point to point you can only connect two sites, which can be a disadvantage if you have multiple sites.
3. **Fragile :** If one node stops working within the point-to-point network then the whole system will stop working.

Que 3.2. What do you mean by logical addressing ?

Answer

1. Usually, computers communicate through the Internet.
2. The data transmitted by the sender computer passes through several LANs or WANs before reaching the destination computer.
3. For this level of communication, we need a global addressing scheme known as logical addressing.
4. An IP address is used globally to refer to the logical address in the network layer of the TCP/IP protocol.
5. The Internet addresses are 32 bits in length; this gives us a maximum of 232 addresses.
6. These addresses are referred to as IPv4 addresses or IP addresses.
7. An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device to the Internet.
8. One IPv4 address defines just one connection of the computer the internet.
9. There can never be more than one IPv4 address for two devices connected to the internet at the same time.
10. If a device is connected to the internet through n connections, it is supposed to have n logical addresses.

PART-2

Basics Internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP)

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.3. 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 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.

Que 3.4. What is IP addressing ? How it is classified ? How is subnet addressing is performed ? **AKTU 2015-16, 2017-18, Marks 10**

OR

Give the classification of different IP address.

Answer

IP addressing :

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.
3. Each TCP/IP host is identified by a logical IP address.

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 zero.
   iii. The next seven bits (completing the first octet) complete network ID. The remaining 24 bits (the last three octets) represent the host ID.
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 network ID. The remaining 16 bits (last two octets) represent the host ID.

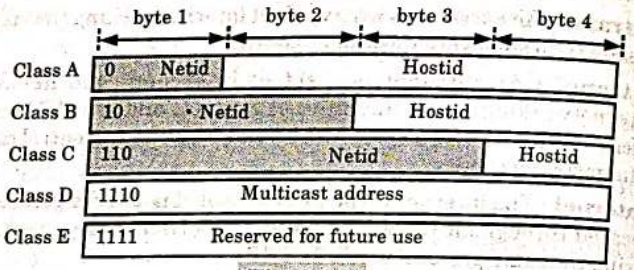


Fig. 3.4.1.

3. Class *C* :

i. Class *C* addresses are used for small networks.

ii. The three high-order bits in a class *C* addresses are always set to binary 110.

iii. The next 21 bits (completing the first three octets) complete the network ID. The remaining 8 bits (last octet) represent the host ID.

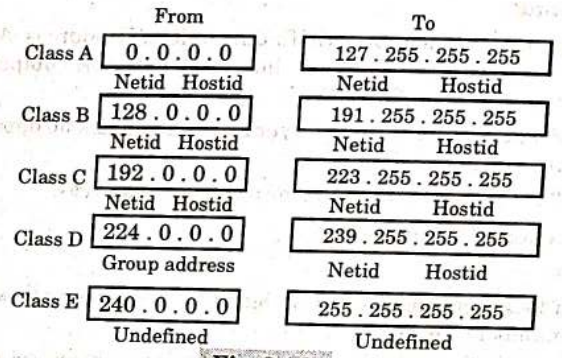


Fig. 3.4.2.

4. Class *D* :

i. Class *D* addresses are reserved for IP multicast addresses.

ii. The four high-order bits in a class *D* addresses 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 out what the broadcast address is.

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

Step 4 : Acquire the number of hosts : Find out the amount of hosts by using the formula : $2^n - 2$. The n component is the number of host bits in the mask.

Step 5 : Assess the mask you will 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 : The best way 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 3.5. 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.

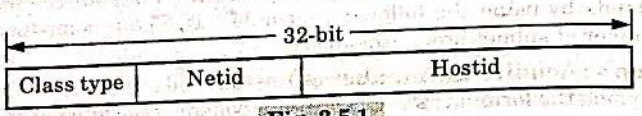


Fig. 3.5.1.

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 3.6. Write a short note on Classless Inter-Domain Routing (CIDR).

Answer

1. Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses and for IP routing.
2. The Internet Engineering Task Force introduced CIDR in 1993 to replace the previous classful network addressing architecture on the Internet.
3. Its goal was to slow the growth of routing tables on routers across the Internet, and to slow the rapid exhaustion of IPv4 addresses.
4. The objective of CIDR was to address scalability issues with classful IP addresses which are based on three classes - Class A, B, and C.
5. CIDR allows IP addresses to be variable and not bound by the size limitations of Classes A, B, and C.
6. Since it is not bound by Class, CIDR can organize IP addresses into subnetworks independent of the value of the addresses themselves.
7. This is referred to as supernetting.

Que 3.7. Write a short note on ARP. Also explain its working.

Answer

Address Resolution Protocol (ARP) :

1. The address resolution protocol (ARP) is a protocol used by 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 ARP, 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 to a server process.
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.

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. 3.7.1.

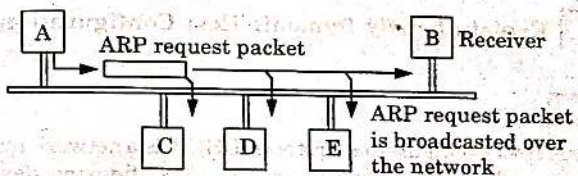


Fig. 3.7.1. ARP request is broadcast.

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*.

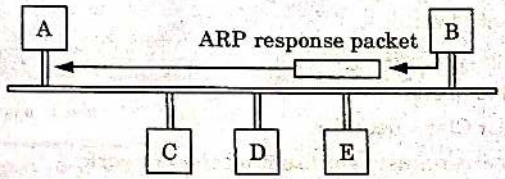


Fig. 3.7.2. ARP response unicast.

4. The ARP response packet has the IP and MAC addresses of the receiver *B* in it. This packet is delivered only to *A*. This is shown in Fig. 3.7.2. Thus host *A* has obtained the MAC address of *B* using ARP.

Que 3.8. Write a short note on Reverse Address Resolution Protocol (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 MAC address to corresponding 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.

Que 3.9. Explain briefly Dynamic Host Configuration Protocol (DHCP).

Answer

1. Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks.
2. DHCP is an enhancement of an older protocol called BOOTP.
3. Dynamic Host Configuration Protocol (DHCP) is an application layer protocol which is used to provide :
   a. Subnet Mask
   b. Router Address
   c. DNS Address
   d. Vendor Class Identifier
4. A DHCP server must be present on the network.
5. A device connected to the network requests an IP address from the DHCP server using the DHCP protocol.

6. The server assigns a unique address to the device, identifying it for TCP/IP communication, and supplies other network configuration parameters.
7. In the absence of a DHCP server, a device that needs an IP address must be manually assigned a static address.
8. DHCP can be implemented on home networks to large campus networks and regional ISP networks.
9. Any router or residential gateway can act as a DHCP server.

Que 3.10. What do you mean by Internet Control Message Protocol (ICMP) ?

Answer

1. The IP protocol has no error-reporting or error-correcting mechanism.
2. The IP protocol also lacks a mechanism for host and management queries.
3. The Internet Control Message Protocol (ICMP) has been designed to compensate for these deficiencies.
4. It is used for error handling in the network layer, and it is primarily used on network devices such as routers.
5. ICMP is a network layer protocol.
6. However, its messages are not passed directly to the data-link layer.
7. The messages are first enclosed inside IP datagram and then passed to the data-link layer.
8. ICMP messages are divided into two categories : error-reporting messages and query messages.

Que 3.11. Give the general format of ICMP messages.

Answer

1. ICMP messages are divided into two categories : error-reporting messages and query messages.
2. When a router or a host processes an IP packet it may encounter problems, the error-reporting messages report these problems.

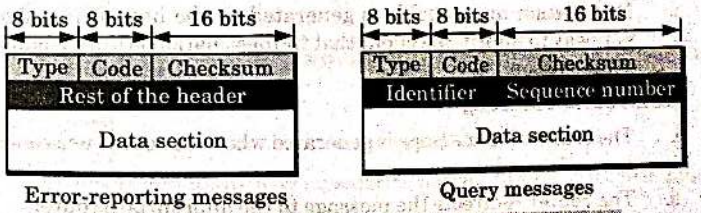


Fig. 3.11.1. General format of ICMP messages.

3. When a network manager wants specific information from a router the query message provide this information.
4. An ICMP message has an 8-byte header and a variable-size data section.
5. The general format of the header is different for each message type, but the first 4 bytes are common to all.
6. In Fig. 3.11.1 the ICMP type defines the type of the message.
7. The ICMP code field specifies the reason for the particular message type.
8. The checksum field is the 16-bit one's complement of the one's complement sum of the ICMP message starting with the ICMP type.
9. The rest of the header is specific for each message type.
10. The data section carries information for finding the original packet that had the error.
11. In query messages, the data section carries extra information based on the type of query.

Que 3.12. What are error reporting messages in ICMP ?

Answer

Following are various error reporting messages in ICMP :

1. **Source quench message :**
   i. When receiving host detects that rate of sending packets is too fast it sends the source quench message to the source to slow the pace down.
   ii. ICMP will take source IP from the discarded packet and informs to source by sending source quench message.
   iii. Then source will reduce the speed of transmission so that router will be free of congestion.
2. **Parameter Problem :**
   i. A parameter problem message can be sent when either there is a problem in the header of a datagram or some options are missing or cannot be interpreted.
3. **Destination un-reachable :**
   i. Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.
4. **Redirection Message :**
   i. The redirection message is generated when the source uses a wrong router to send its message.
   ii. The router redirects the message to the appropriate router.
   iii. Also it informs the source to change its default router in the future.

   iv. The IP address of the default router is sent in the message.
5. **Query Messages :**
   i. Query messages are used to test the liveliness of hosts or routers in the Internet.
   ii. It is use to find the one-way or the round-trip time for an IP datagram between two devices.
   iii. It is use to find out whether the clocks in two devices are synchronized.
   iv. Query messages come in pairs: request and reply.

PART-3

Routing, Forwarding and Delivery, Static and Dynamic Routing, Routing Algorithm and Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.13. What do you understand by routing ?

Answer

1. In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
2. The main job of the network layer is to provide the best route.
3. Routing provides this information.
4. Routing refers to the way routing tables are created to help in forwarding the packets.
5. The routing protocol is a routing algorithm that provides the best path from the source to the destination.
6. The best path is the path that is the "least-cost path" from source to the destination.

Que 3.14. What do you understand by delivery in context of network layer ?

Answer

1. Delivery refers to the way a packet is handled by the network layer.
2. The network layer supervises the handling of the packets by the underlying physical networks.

3. The delivery of a packet is accomplished by using direct and indirect methods of delivery.

A. Direct Delivery :

1. In a direct delivery the source and destination of the packet are located on the same physical network.
2. Also direct delivery occurs when the delivery is between the last router and the destination host.
3. To determine if the delivery is direct we extract the network address of the destination (using the mask).
4. Then we compare this address with the addresses of the networks to which it is connected.
5. If a match is found, the delivery is direct.

B. Indirect Delivery :

1. If the source and destination of the packet are not located on the same physical network, the packet is delivered indirectly.
2. In an indirect delivery, the packet goes from router to router until it reaches its final destination.
3. A delivery always involves one direct delivery but zero or more indirect deliveries.
4. The last delivery is always a direct delivery.

Que 3.15. What do you understand by forwarding ? Mention some of the forwarding techniques.

Answer

1. Forwarding refers to the way a packet is delivered to the next station.
2. Forwarding requires a router to have a routing table.
3. With the help of routing table a router find the route for the packet which is to be forwarded.
4. However, this simple solution is impractical due the large number of entries needed in the table which makes table lookups inefficient.

Forwarding techniques : Following are various forwarding techniques which can make the size of the routing table manageable :

A. Next-Hop Method :

1. One technique to simplify the routing table is called the next-hop method.
2. In this technique the routing table holds only the address of the next hop.
3. However, the entries of a routing table must be consistent with one another.

B. Network-Specific Method :

1. This technique helps to reduce the routing table and simplify the searching process.
2. Here, we have only one entry that defines the address of the destination network itself.
3. All hosts connected to the same network are treated as one single entity.

C. Default Method :

1. Another technique to simplify routing is called the default method.
2. In this technique instead of listing all networks in the entire Internet, host just has one entry called the default.
3. It is normally defined as network address 0.0.0.0.

Que 3.16. Explain static and dynamic routing.

Answer

A. Static routing :

1. Static routing is a process in which we have to manually add routes in routing table.
2. Static routes are manually configured by a network administrator by adding in entries into a routing table.
3. Static routes are fixed and do not change if the network is changed or reconfigured.
4. Static routing is used on a router to maximise routing efficiency and to provide backups in case dynamic routing information fails to be exchanged.
5. Static routing can also be used in stub networks, or to provide a gateway of last resort.
6. Static routing is also known as non-adaptive routing.

B. Dynamic routing :

1. In dynamic routing a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
2. If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.
3. Dynamic protocols are used to discover the new routes to reach the destination.
4. In dynamic routing all the routers must have the same dynamic routing protocol in order to exchange the routes.
5. If any route goes down, then the automatic adjustments are made to reach the destination.
6. Dynamic routing is also known as adaptive routing.

Que 3.17. **What are the advantages and disadvantages of static and dynamic routing ?**

Answer

A. Advantages of static routing :

1. **No Overhead :** It has no overhead on the CPU usage of the router. Hence cheaper router can be used to obtain static routing.
2. **Bandwidth :** It has not bandwidth usage between the routers.
3. **Security :** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

B. Disadvantages of static routing :

1. For a large network, it is very difficult to add each route manually to the routing table.
2. The system administrator should have a good knowledge of a topology as he has to add each route manually.

C. Advantages of dynamic routing :

1. It is easier to configure.
2. It is more effective in selecting the best route in response to the changes in the condition or topology.

D. Disadvantages of dynamic routing :

1. It is more expensive in terms of CPU and bandwidth usage.
2. It is less secure as compared to static routing.

Que 3.18. **Give difference between static and dynamic routing.**

Answer

S. No.	Static routing	Dynamic routing
1.	In static routing routes are user defined.	In dynamic routing routes are updated according to topology.
2.	Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
3.	Static routing provides more security.	Dynamic routing provides less security.
4.	Static routing is manual.	Dynamic routing is automated.
5.	Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
6.	Additional resources are not required.	Additional resources are required.
7.	Failure of link disrupts the rerouting.	Failure of link does not interrupt the rerouting.

Que 3.19. **What is unicast routing ? Discuss unicast routing protocols.**

AKTU 2018-19, Marks 07

AKTU 2017-18, Marks 10

AKTU 2015-16, Marks 05

OR

Explain path vector routing protocol.

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. 3.19.1.
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.

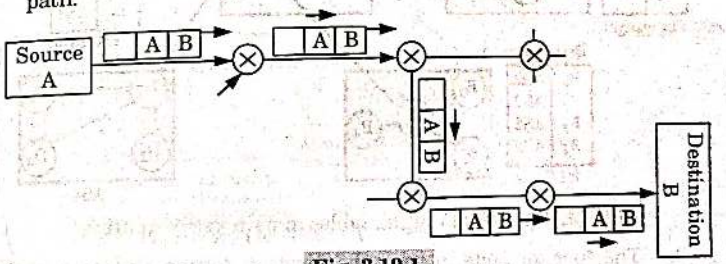


Fig. 3.19.1.

Following are the three unicast routing protocol :

i. Distance vector routing protocol :

1. In distance vector routing, each router maintains a routing table (each router knows the identity of every other router in the network).
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. Second part gives an estimate of the time or distance to that destination.

ii. Link state routing :

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.

iii. Path vector routing :

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. This single node is called the speaker node.

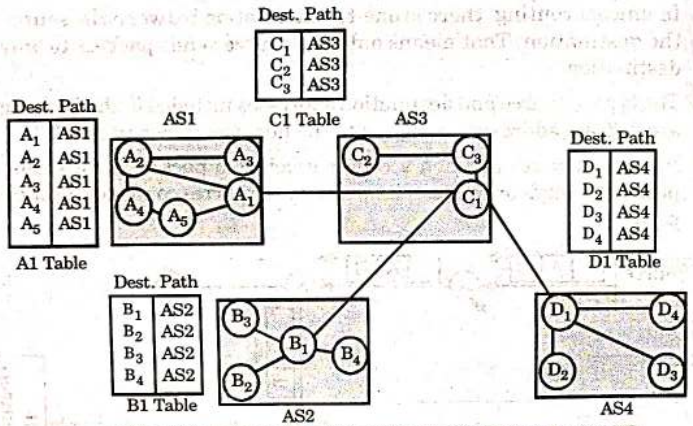


Fig. 3.19.2. Initial routing tables in path vector routing.

3. The speaker node in an authentication server creates a routing table and advertises it to speaker nodes in the neighbouring ASs.
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 3.20. Explain distance vector routing algorithm and how it updates the routing tables with the help of example.

Answer

Distance vector routing algorithm : Refer Q. 3.19, Page 3–16B, 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. 3.20.1 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. 3.16.1 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.

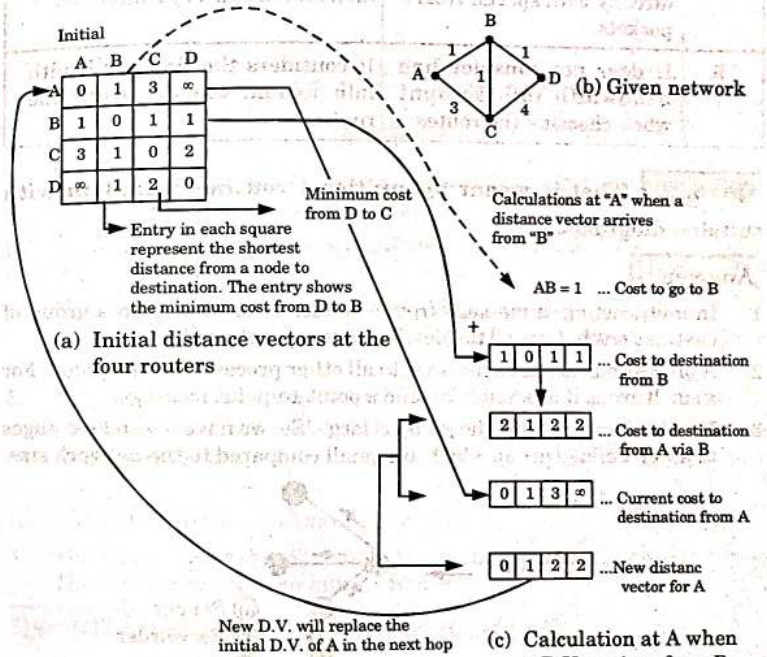


Fig. 3.20.1. Distance vector algorithm at router A.

Que 3.21. Discuss link state routing. Compare distance vector routing with link state routing.

Answer

Link state routing : Refer Q. 3.19, Page 3–16B, 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 3.22. What is meant by multicast routing ? Explain with suitable diagrams.

Answer

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.

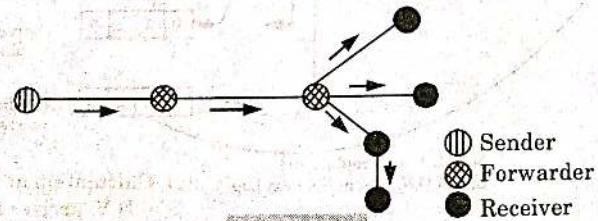


Fig. 3.22.1.

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. 3.22.1.

Que 3.23. 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. 3.23.1.

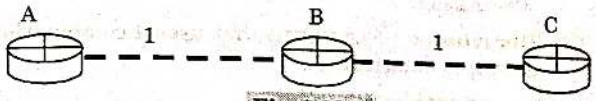


Fig. 3.23.1.

2. Let the matrices (weight or cost) between the routers is the number of jumps to reach the neighbour router.
3. In the Fig. 3.23.1 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.

Que 3.24. 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 3.25. **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.

PART-4

Congestion Control Algorithm, IPv6.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 3.26. **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 3.27. 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 3.28. 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.

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. 3.26, Page 3–22A, 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.

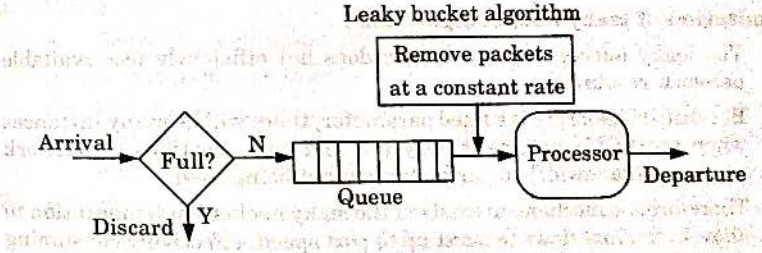


Fig. 3.28.1.

5. A simple leaky bucket implementation is shown in Fig. 3.28.1. 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.

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 3.29. **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 3.30. **What do you mean by congestion control and QoS ? What are the parameters of QoS ? Explain.**

Answer

Congestion control : Refer Q. 3.26, Page 3–22A, 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 :

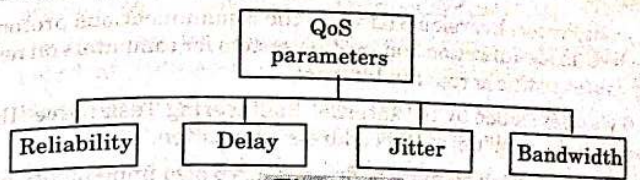


Fig. 3.30.1.

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 3.31. What is Internet Protocol version 6 (IPv6) ?

Answer

1. Internet Protocol version 6 (IPv6) is the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
2. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the problem of IPv4 address exhaustion.
3. In addition to offering more addresses, IPv6 also implements features not present in IPv4.
4. It simplifies aspects of address configuration, network renumbering, and router announcements when changing network connectivity providers.
5. It simplifies processing of packets in routers by placing the responsibility for packet fragmentation into the end points.
6. IPv6 addresses are represented as eight groups, separated by colons, of four hexadecimal digits. For example, 2001:db8::8a2e:370:7334.

Que 3.32. Explain the packet format for IPv6.

Answer

1. The packet format for IPv6 is shown in Fig. 3.32.1. 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 :
   i. **Version :** This is 4-bit field which defines the version number of IP. For IPv6, the value is 6.

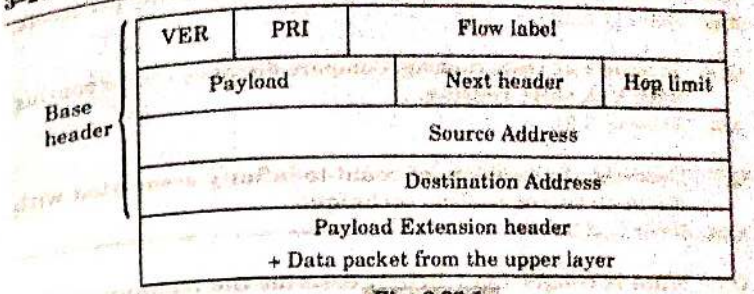


Fig. 3.32.1.

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.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. What is IP addressing ? How it is classified ? How is subnet addressing is performed ?

Ans. Refer Q. 3.4.

Q. 2. Write a short note on ARP. Also explain its working.

Ans. Refer Q. 3.7.

Q. 3. What is unicast routing ? Discuss unicast routing protocols.

Ans. Refer Q. 3.19.

Q. 4. Discuss link state routing. Compare distance vector routing with link state routing.

Ans. Refer Q. 3.21.

Q. 5. Describe the problem of count-to-infinity associated with distance vector routing technique.

Ans. Refer Q. 3.23.

Q. 6. What is congestion ? Briefly describe the techniques that prevent congestion.

Ans. Refer Q. 3.26.

Q. 7. Define traffic shaping. Elaborate leaky bucket algorithm used for congestion control.

Ans. Refer Q. 3.28.

Q. 8. Write a short note on token bucket algorithm. What are the limitations of leaky bucket algorithm ?

Ans. Refer Q. 3.29.

Transport Layer

CONTENTS

PART-1

Process to Process Delivery.

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

1. A process is an application program running on a host.
2. The data link layer performs a node to node delivery.
3. The network layer performs host to host delivery.
4. Process-to-process delivery of the entire message is the responsibility of transport layer.
5. The transport layer is responsible for the delivery of a packet, part of a message, from one process to another.
6. The most common way to achieve process-to-process communication is through the client/server paradigm.
7. A process on the local host, called a client, needs services from a process on the remote host, called a server.
8. Both processes (client and server) should have the same name.
9. For communication, we must define the following :
   - i. *Local host*
   - ii. *Local process*
   - iii. *Remote host*
   - iv. *Remote process*

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

Answer

Design issues with transport layer :

1. Accepting data from session layer, splitting it into segments and sending 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. Four aspects of reliable delivery and flow control at transport layer ensure whole message arrives at the destination intact and in order.
3. **Aspects of reliable delivery :**

A. Error Control :

- i. The primary goal of reliability is error control while transferring data.
- ii. Data must be delivered to its destination exactly as originated from the source.
- iii. While 100 percent error-free delivery is impossible, transport layer protocols are designed to come as close as possible.
- iv. Mechanisms for error handling at this layer are based on error detection and retransmission.

B. Sequence Control :

- i. On the sending end, the transport layer ensures that data units received from upper layers are usable by lower layers.
- ii. On the receiving end, it ensures that various pieces of a transmission are correctly reassembled.

C. Loss Control :

- i. The transport layer ensures that entire pieces of a transmission arrive at the destination.
- ii. When data have been segmented for delivery, some segments may be lost in transit.
- iii. Sequence numbers allow the receiver's transport layer protocol to identify any missing segments and request redelivery.

D. Duplication Control :

i. Transport layer guarantees that no piece of data is duplicated.

ii. Sequence numbers allow the receiver to identify and discard duplicate segments.

4. **Flow Control :** Flow control ensures whole message arrives at the destination intact and in order.

i. The transport layer is also responsible for flow control.

ii. Flow control at this layer is performed end-to-end.

iii. Transport layer flow control uses a sliding window protocol.

PART-2

Transport Layer Protocols (UDP and TCP).

Questions-Answers

Long Answer Type and Medium Answer Type Questions

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 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. 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.
7. UDP packets are known 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 shown in Fig. 4.5.1.

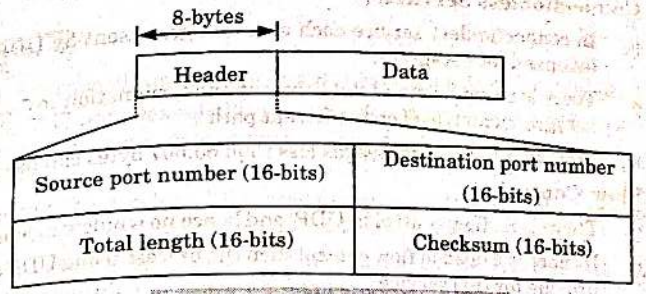


Fig. 4.5.1. User datagram format.

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

1. **Source port :**
   i. 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.
   ii. If not used, a value of zero is inserted.
2. **Destination port :**
   i. Destination port has a meaning within the context of a particular internet destination address.
3. **Length :**
   i. This is the size in bytes of the UDP packet, including the header and data.
   ii. The minimum length of the header is 8-bytes.
4. **Checksum :**
   i. This is used to verify the integrity (*i.e.*, to detect errors) of the UDP header.
   ii. 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 are the general services provided by UDP ?

Answer

Following are various general services provided by UDP :

A. Process-to-Process Communication :

i. Process-to-process communication is provided by UDP using :
   a. Socket addresses,
   b. Combination of IP addresses and port numbers.

B. Connectionless Services :

i. In connectionless service each user datagram sent by UDP is an independent datagram.
ii. There is no connection establishment and termination so each user datagram can travel on a different path.
iii. Processes sending messages less than 65,507 bytes can use UDP.

C. Flow Control :

i. There is no flow control in UDP, and hence no window mechanism.
ii. If there is a need of flow control then the process using UDP should provide for this service.

D. Error Control :

i. Except checksum, there is no error control mechanism in UDP.
ii. When the receiver detects an error through the checksum, the user datagram is discarded.
iii. If there is a need of error control then the process using UDP should provide for this service.

E. Checksum :

i. UDP checksum calculation includes :
   a. Pseudoheader,
   b. UDP header, and
   c. Data coming from the application layer.

Que 4.7. Mention some of the applications of UDP.

Answer

Following are the applications of UDP :

1. UDP is used in process requiring simple request-response communication and very little flow and error control.
2. UDP is used in process having its own internal flow- and error-control mechanisms.
3. UDP is used in transport protocol for multicasting.
4. UDP is used in SNMP.
5. UDP is used for some route updating protocols (example : RIP).
6. UDP is used for interactive real-time applications that cannot tolerate uneven delay between sections of a received message.

Que 4.8. 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.

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

AKTU 2016-17, 2017-18, 2018-19; Marks 10

Answer

TCP header : 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.
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.

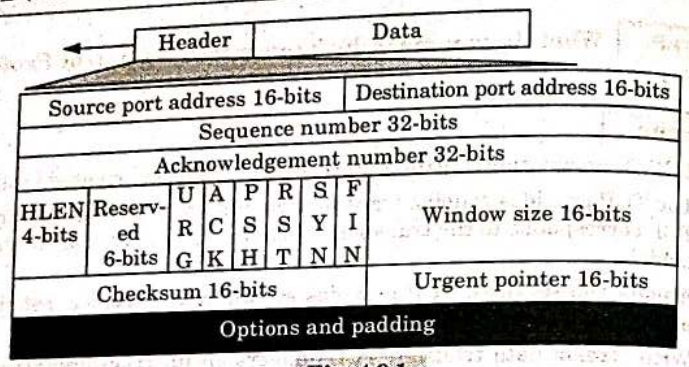


Fig. 4.9.1.

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 bytes.
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). The length of this field is 16-bits.
9. **Checksum :** This 16-bit field contains the checksum for error control. It is mandatory in TCP as opposed to UDP.
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.
11. **Options :** There can be upto 40-bytes of optional information in the TCP header.

Working of TCP protocol :

1. TCP/IP divides communication tasks into layers that keep the process standardized.
2. The data packets pass through four layers before they are received by the destination device, then TCP/IP goes through the layers in reverse order to put the message back into its original format.

3. TCP establishes and maintains a connection between applications or devices until they finish exchanging data.
4. It determines how the original message should be broken into packets, numbers and reassembles the packets, and sends them on to their destination.
5. TCP also sends and receives packets from the network layer, handles the transmission of any dropped packets, manages flow control, and ensures all packets reach their destination.
6. TCP/IP uses a three-way handshake to establish a connection between a device and a server.

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.

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

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

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

vi. **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. 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.

Que 4.12. 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.

PART-3

Multiplexing, Connection Management.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.13. Write a short note on multiplexing.

Answer

1. The transport layer uses multiplexing to improve the transmission efficiency.
2. In transport layer multiplexing occurs in two ways : upward or downward.

A. Upward Multiplexing :

1. In upward multiplexing multiple transport-layer connections use the same network connection.
2. The transport layer uses virtual circuits based on the services of the lower three layers.
3. The underlying networks charge for each virtual circuit connection.

4. An established circuit is used cost-effectively by sending several transmissions bound for the same destination along the same path by using upward multiplexing.

B. Downward Multiplexing :

1. In downward multiplexing one transport-layer connection uses multiple network connections.
2. To improve throughput (speed of delivery) a single connection is split among several different paths.
3. This option is used when the underlying networks have slow or low capacity.

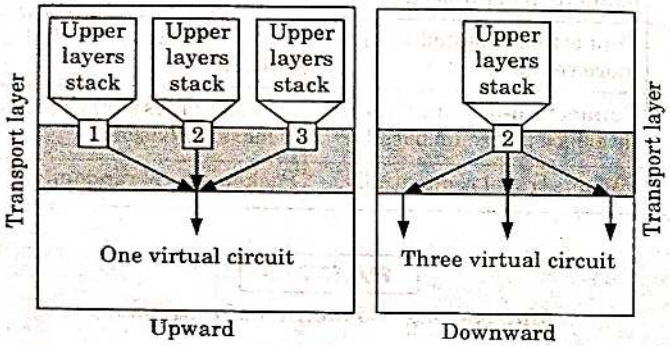


Fig. 4.13.1. Multiplexing.

Que 4.14. 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.

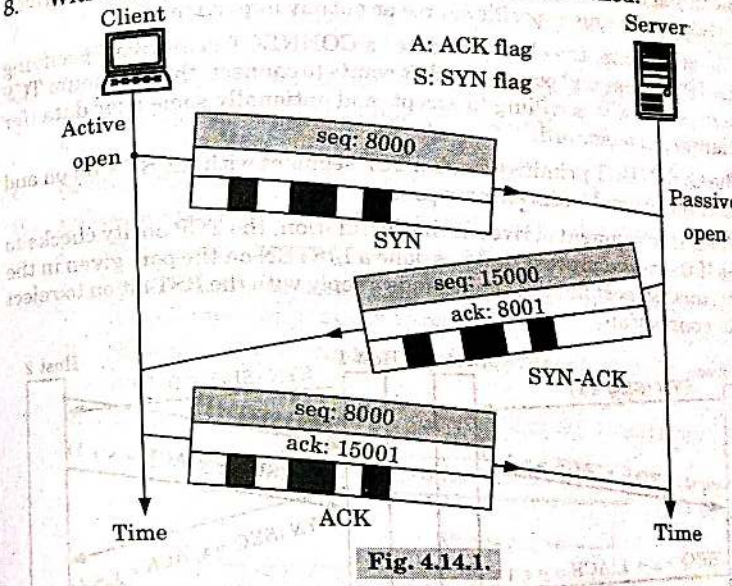


Fig. 4.14.1.

Que 4.15. 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.

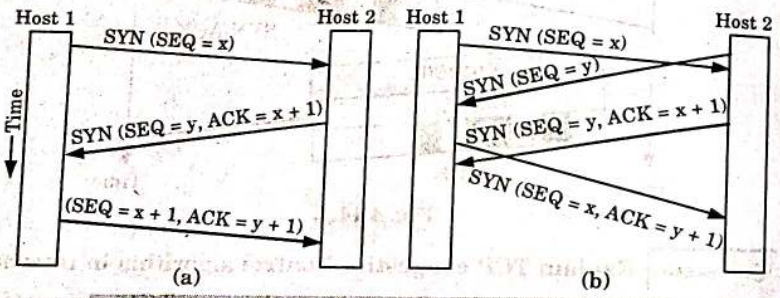


Fig. 4.15.1. (a) TCP connection establishment in the normal case. (b) call collision.

PART-4

Flow Control and Retransmission, Window Management, TCP Congestion Control, Quality of Services.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 4.16. Write a short note on flow control in transport layer.

Answer

1. The transport layer is responsible for flow control.
2. In transport layer flow control is performed end-to-end.
3. Flow control in transport layer uses a sliding window protocol.
4. This window can vary in size to accommodate buffer occupancy.
5. With a varying-size window, the actual amount of data the window can hold is flexible.
6. A sliding window makes data transmission more efficient.
7. It also helps to control the flow of data so that the receiver does not become overwhelmed.
8. Sliding windows used at the transport layer are byte oriented.
9. Following points are worth mentioning about sliding windows :
   i. The sender does not have to send a full window's worth of data.
   ii. Based on the sequence number of the acknowledged data segment an acknowledgment can expand the size of the window.
   iii. The size of the window can be increased or decreased by the receiver.
   iv. The receiver can send an acknowledgment at anytime.

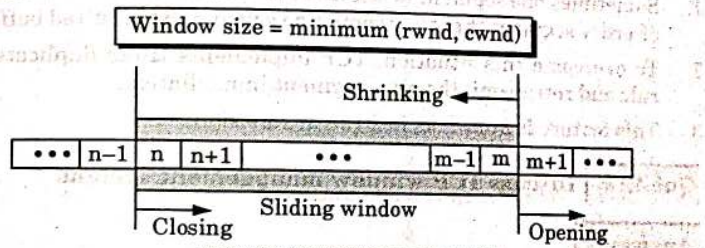


Fig. 4.16.1. Sliding window.

10. Fig 4.16.1 shows the sliding window.
11. The imaginary window has two walls: one left and one right.
12. The window is opened, closed, or shrunk. These activities are in the control of the receiver.

13. Opening a window means moving the right wall to the right.
14. This allows more new bytes in the buffer that are eligible for sending.
15. Closing the window means moving the left wall to the right.
16. This means that some bytes have been acknowledged.

Que 4.17. What is the need for retransmission of segments in transport layer ?

Answer

1. Error control mechanism in transport layer revolves around the concept of retransmission of segments.
2. When a segment is corrupted, lost, or delayed, it is retransmitted.
3. A segment is retransmitted when a retransmission timer expires or when the sender receives three duplicate ACKs.

A. Retransmission after timer expires :

1. TCP maintains one retransmission time-out (RTO) timer for all outstanding segments.
2. When the timer matures, the earliest outstanding segment is retransmitted.
3. The value of RTO is dynamic in TCP.
4. Value of RTO is updated based on the round-trip time (RTT) of segments.
5. An RTT is the time needed for a segment to reach a destination and for an acknowledgment to be received.
6. It uses a back-off strategy.

B. Retransmission after three duplicate ACK segments :

1. Sometimes one segment is lost and the receiver receives so many out-of-order segment that they cannot be saved due to limited buffer size.
2. To overcome this situation, TCP implements three-duplicate-ACKs rule and retransmit the miss segment immediately.
3. This feature is known as fast retransmission.

Que 4.18. Discuss TCP window management system.

Answer

1. Window management in TCP ensures reliability in packet delivery and reduction in wastage of time in waiting for the acknowledge after each packet.
2. TCP uses two buffers and one window, to control the flow of data coming from the sending application program.

3. The application program creates data and writes it to the buffer.
4. The sender imposes a window on this buffer and sends the segments as long as the size of the window is not zero.
5. The TCP receiver has buffer also.
6. It receives data, checks them, and stores them in buffer to be consumed by the receiving application program.
7. A sliding window is used to make transmission more efficient as well as to control the flow of data.

Que 4.19. What do you understand by silly window syndrome ? Also give solution of silly window syndrome.

Answer

1. Silly window syndrome is a problem that can degrade the TCP performance.
2. This problem occurs when the sender transmits data in large blocks, but an interactive application on the receiver side reads data 1 byte at a time.
3. This situation is shown in Fig. 4.19.1 :
   i. Initially the receiver's buffer is full so it sends a window size 0 to block the sender.
   ii. But the interactive application reads one byte from the buffer, so one byte space becomes empty.

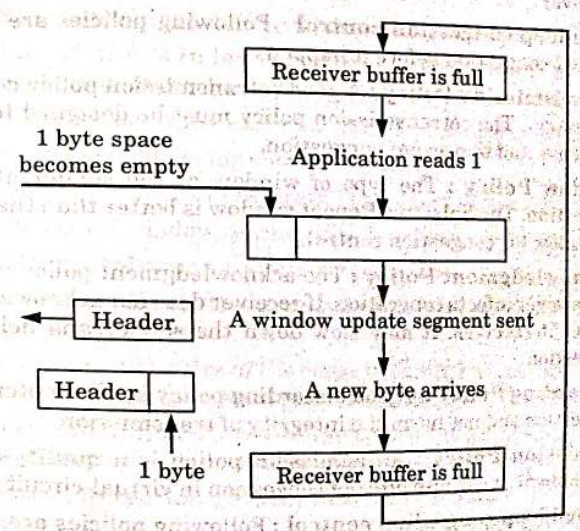


Fig. 4.19.1. Silly window syndrome.

iii. The receiving TCP sends a window update to the sender informing that it can send 1 byte.

iv. The sender sends 1-new byte.

v. The buffer is full again and the window size is 0. The behavior can continue forever.

Solution to silly window syndrome :

1. It was suggested that the receiver should not send a window update for 1 byte.
2. Instead it must wait until it has a substantial amount of buffer space available and then sends the window update.
3. The receiver should not send a window update until it can handle the maximum window size or its buffer is half empty, whichever is smaller.
4. The sender should not send tiny segments instead it must wait and send a full segment or at least one containing half of the receivers buffers size.

Que 4.20. Discuss congestion control in transport layer.

Answer

1. Congestion control refers to techniques and mechanisms that can either prevent congestion or remove congestion.
2. Congestion control mechanisms are divided into two categories : open-loop congestion control (prevention) and closed-loop congestion control (removal).

A. Open-loop congestion control : Following policies are applied to prevent congestion before it happens :

1. **Retransmission Policy :** A good retransmission policy can prevent congestion. The retransmission policy must be designed to optimize efficiency and to prevent congestion.
2. **Window Policy :** The type of window at the sender also affects congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.
3. **Acknowledgment Policy :** The acknowledgment policy imposed by the receiver affects congestion. If receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.
4. **Discarding Policy :** A good discarding policy by the routers prevent congestion and not harm the integrity of transmission.
5. **Admission Policy :** An admission policy is a quality-of-service mechanism. It can also prevent congestion in virtual-circuit networks.

B. Closed-loop congestion control : Following policies are applied to alleviate congestion after it happens :

1. **Backpressure :** In this congestion control mechanism a congested node stops receiving data from the immediate upstream node. The backpressure technique can be applied only to virtual circuit networks.
2. **Choke Packet :** A choke packet is a packet sent by a node to the source to inform it of congestion. In this method the router which has encountered congestion warns the source station directly.
3. **Implicit Signaling :** There is no communication between the congested node and the source. Using other symptoms the source guesses that there is congestion in the network.
4. **Explicit Signaling :** In explicit signaling the node experiencing congestion can explicitly send a signal to the source or destination.

Que 4.21. Show how TCP uses congestion control to avoid congestion ?

Answer

TCP's general policy for handling congestion is based on following three phases :

A. Slow start : Exponential Increase

1. TCP congestion control uses an algorithm called slow start.
2. The idea behind this algorithm is that the size of the congestion window (cwnd) starts with one maximum segment size (MSS).
3. The MSS is determined during connection establishment.
4. The size of the window increases one MSS each time an acknowledgment is received.
5. As the name implies, the window starts slowly, but grows exponentially.
6. There is a threshold to stop slow start phase.
7. The sender keeps track of ssthresh (slow-start threshold).
8. When the size of window reaches this threshold, slow start stops.

B. Congestion avoidance : Additive Increase

1. In congestion avoidance the algorithm undergoes an additive increase instead of an exponential one.
2. In TCP as soon as the size of the congestion window reaches the slow-start threshold, the slow-start phase stops and additive phase begins.
3. In this algorithm, after the whole window of segments is acknowledged, the size of the congestion window is increased by 1.

C. Congestion detection : Multiplicative Decrease

1. If congestion occurs, the congestion window size must be decreased.
2. When a segment is retransmitted the sender knows that congestion has occurred.

3. This retransmission occurs when a timer times out or when three ACKs are received.
4. In both cases the size of the threshold is cut to one-half (multiplicative decrease).
5. Most TCP implementations have following two reactions :
   a. If a time-out occurs there is a stronger possibility of congestion.
   b. If three ACKs are received there is a weaker possibility of congestion.

Que 4.22. What do you understand by Quality of service (QoS) ? Mention the techniques to improve QoS.

OR

What do you understand by quality of service parameters ? List various quality of service parameters. **AKTU 2018-19, Marks 07**

Answer

1. A stream o f packet, from a source to a destination is called a flow.
2. Quality of service is define as something a flow seeks to attain.
3. The need of each flow can be characterized by four primary QoS parameters :
   i. **Reliability :** It is the ability of a system to perform and maintain its functions under normal and unexpected conditions.
   ii. **Delay :** It is defined as the time interval elapsed between the departures of data from the source to its arrival at the destination.
   iii. **Jitter :** Jitter refers to the variation in time between packets arriving at the destination.
   iv. **Bandwidth :** It refers to the data rate supported by a network connection or interface.

Techniques for improving QoS :

1. **Over Provisioning :** In this technique the solution is to provide so much router capacity, buffer space and bandwidth that the packets just fly through.
2. **Buffering :**
   i. Flows can be buffered on the receiving side before being delivered.
   ii. Buffering does not affected the reliability of bandwidth.
   iii. Buffering does not increases the delay.
   iv. Buffering smoothes out the jitter.
3. **Scheduling :**
   i. Packets from different flows arrive at a switch or router for processing. A good scheduling technique treats the different flows in a fair and appropriate manner.
   ii. Following are some scheduling techniques to improve QoS :

A. **FIFO Queuing :**
   i. In FIFO queuing packets wait in a buffer (Queue) until the node is ready to process them.
   ii. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded.

B. **Priority Queuing :**
   i. In this packets are first assigned to priority class.
   ii. Each priority class has its own queue.
   iii. The packets in the highest priority queue are processed first.

C. **Weighted Fair Queuing :**
   i. In this method, the packets are assigned to different classes and admitted to different queues.
   ii. The queues are weighted based on the priority of the queues.
   iii. Higher priority means a higher weight.
   iv. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight.

4. **Traffic Shaping :** It is a mechanism to control the amount and the rate of the traffic sent to the network. Following techniques help shape the traffic :
   i. Leaky bucket
   ii. Token bucket

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. Enumerate how the transport layer ensures that the complete message arrives at the destination and in the proper order.

Ans. Refer Q. 4.3.

Q. 2. Write a short note on User Datagram Protocol (UDP).

Ans. Refer Q. 4.4.

Q. 3. Discuss the header format of UDP.

Ans. Refer Q. 4.5.

Q. 4. Explain about the TCP header and working of TCP protocol and differentiate between TCP and UDP with frame format.

Ans: Refer Q. 4.9.

Q. 5. 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.

Q. 6. Explain the three-way handshaking protocol to establish the transport level connection.

Ans: Refer Q. 4.14.

Q. 7. Explain TCP congestion control algorithm in internet. What is TCP segment header ? Also, discuss TCP connection management.

Ans: Refer Q. 4.15.

Q. 8. What do you understand by Quality of service (QoS) ? Mention the techniques to improve QoS.

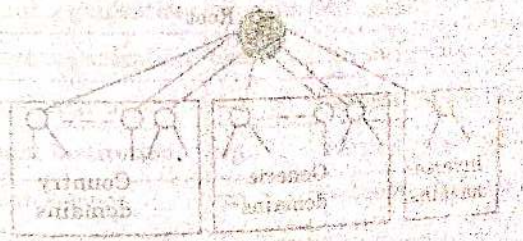
Ans: Refer Q. 4.22.

☺☺☺

5 UNIT

Application Layer

CONTENTS



PART-1

Domain Name System.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.1. **Write a short note on DNS in the internet.**

AKTU 2015-16, 2017-18; Marks 05

Answer

1. Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the internet.
2. DNS is a client-server application that provides name service for other applications.
3. DNS can map a name to an address and conversely an address to a name.
4. TCP/IP protocols use IP address to identify the connection of a host to the Internet.
5. However, for a person it is convenient to use names instead of addresses.
6. Hence we need a system that can map a name to an address and vice versa.
7. In TCP/IP we use Domain Name System (DNS) for this purpose.
8. In the Internet, the domain name space (tree) is divided into three sections: generic, country, and inverse domain.

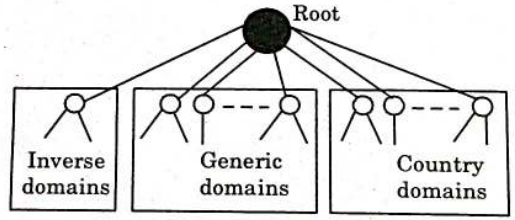


Fig. 5.1.1.

Que 5.2. **Write a short note on : generic domains, country domains, and inverse domain.**

Answer

A. Generic domains :

1. In generic domain the registered hosts are define according to their generic behavior.
2. Each node in the tree defines a domain, which is an index to the domain name space database.

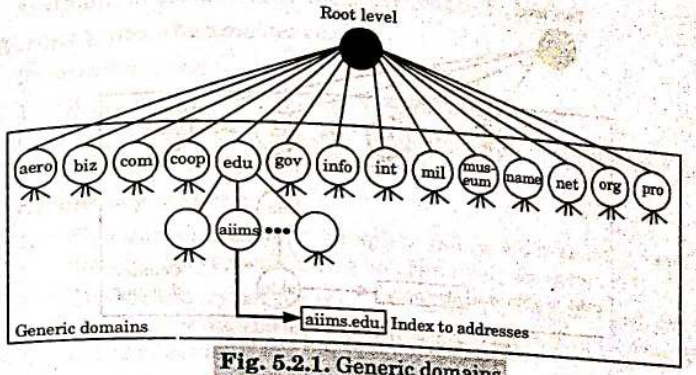


Fig. 5.2.1. Generic domains

3. The first level in the generic domain section allows fourteen possible labels.
4. Various organization types are described by these labels (Table 5.2.1).

Table 5.2.1. Generic domain levels.

Label	Description	Label	Description
aero	Airlines and aerospace	int	International organizations
biz	Businesses or firms	mil	Military groups
com	Commercial organizations	museum	Museums
coop	Cooperative organizations	name	Personal names (individuals)
edu	Educational institutions	net	Network support centers
gov	Government institutions	org	Nonprofit organizations
info	Information service providers	pro	Professional organizations

B. Country domains :

1. The country domain section follows the same format as the generic domains but uses two-character country abbreviations (e.g., "in" for India).

2. Second-level labels can be organizational, or they can be more specific, national designations.
3. For example, ac.in : This domain name is used for academic institutes in India, it represents academic institution website in India.
4. Fig 5.2.2 shows the country domain section. The address aktu.ac.in can be translated to Dr. A.P.J. Abdul Kalam Technical University in India.

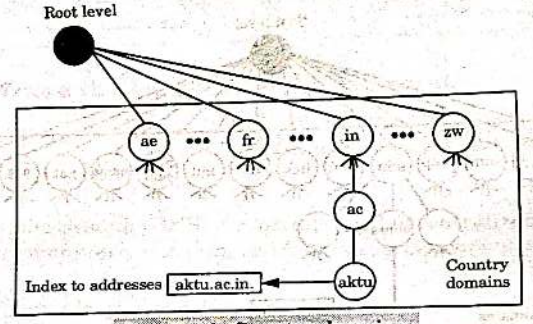


Fig. 5.2.2. Country domains.

C. Inverse domain :

1. The inverse domain is used to map an address to a name.
2. Inverse domain can be used to find the name of a host when given the IP address.
3. However due to rapid growth of the internet it is very difficult to keep track of inverse domain.
4. The inverse domains are now deprecated.

Que 5.3. 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 :

1. The process of mapping a name to an address or vice-versa is called name address resolution.
2. To map an address to a name or a name to an address we use a DNS client known as resolver.

3. The resolver approaches the nearest DNS server with a mapping request.
4. If the server has the information it provides the resolver with the information.
5. If the server does not have the information it either refers the resolver to other servers or asks other servers to provide the information.
6. After the resolver receives the mapping it interprets the response and delivers the result to the process that requested it.
7. A resolution can be either recursive or iterative.

Different types of name server :

i. Primary server :

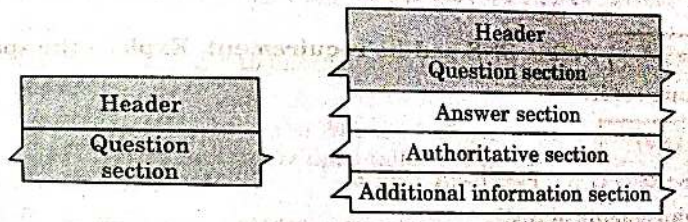
1. It is a server which stores a file about its zone.
2. It is authorized to create, maintain and update the zone file. It stores the zone file on a local disk.

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. 5.3.1.
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.



(a) Query (b) Response or reply

Fig. 5.3.1.

4. The header format for both the types of message is shown by shaded portions in Fig. 5.3.1.

Que 5.4. What are different types of resolution ?

Answer

A resolution can be either recursive or iterative.

A. Recursive Resolution :

1. The resolver can request for a recursive answer from a name server.
2. This means that the server is expected to supply the final answer.
3. If the server is the authority for the domain name, it responds.
4. If it is not the authority, it sends the request to another server (parent) and waits for the response.
5. If the parent is the authority, it responds; otherwise, it sends the query to another server.
6. When the query is finally resolved, the response travels back to the requesting client.
7. This is called recursive resolution.

B. Iterative Resolution :

1. Mapping can be done iteratively if the client does not ask for a recursive answer.
2. If the server is an authority for the name, it responds.
3. If it is not, it returns (client) the IP address of the server.
4. The client is responsible for repeating the query to this second server.
5. If the newly addressed serve can resolve the problem, it answers the query with the IP address.
6. If it cannot resolve the problem, it returns the IP address of a new server to the client.
7. Now the client again repeats the same query to this new server.
8. Since the client repeats the same query to multiple servers this process is known as iterative resolution.

Que 5.5. Define DNS and its requirement. Explain the specific features of it.

Answer

DNS : Refer Q. 5.1, Page 5–2A, 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-2

World Wide Web and Hyper Text Transfer Protocol.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.6. Write short note on World Wide Web.

Answer

1. World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet.
2. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc.
3. The WWW, along with internet, enables the retrieval and display of text and media.
4. The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or "hyperlinks" and accessed by HTTP.
5. These links are electronic connections that link related pieces of information so that users can access the desired information quickly.
6. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.

Que 5.7. What are the three types of Web documents ?

Answer

Following are the three types of Web documents :

A. Static Documents :

1. They are fixed-content documents that are created and stored in a server.
2. The user cannot change the contents in the server.
3. The user can get only a copy of the document.
4. When a user accesses the document, a copy of the document is sent.
5. The user can then use a browsing program to display the document.
6. Hypertext Markup Language (HTML) is a language used for creating static documents.

B. Dynamic Documents :

1. Whenever a browser requests a document, dynamic document is created by Web server.
2. The Web server runs an application program or a script that creates the dynamic document whenever requested.
3. The server returns the output of the program or script as a response to the browser request.
4. The contents of a dynamic document vary from one request to another because a fresh document is created for every request.
5. An example of a dynamic document is the retrieval of the time and date from a server.
6. The dynamic documents are created using Common Gateway Interface (CGI) technology.

C. Active Documents :

1. Active documents are programs or scripts that run at the client site.
2. For example, suppose we want to run a program that interacts with the user.
3. This program needs to run at the client site where the interaction takes place.
4. When a browser requests an active document, the server sends a copy of the document.
5. The document is then run at the client site.
6. The active documents are created using Java applets and JavaScript.

Que 5.8. What do you mean by HTTP ?

OR

Write short note on HTTP. **AKTU 2018-19, Marks 3.5**

Answer

1. The Hyper Text Transfer Protocol (HTTP) is the most widely used application layer protocol.

2. The HTTP is used to access data on the World Wide Web.
3. It is the network protocol used to deliver virtually all files and other data on the World Wide Web.
4. HTTP takes place through TCP/IP sockets.
5. The standard and default port for HTTP servers is 80.
5. HTTP functions as a combination of FTP and SMTP.
6. It is similar to FTP because it transfers files and uses the services of TCP.
7. HTTP is like SMTP because the data transferred between the client and the server look like SMTP messages.

Que 5.9. 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. 5.9.1 shows the HTTP transactions between client and server.

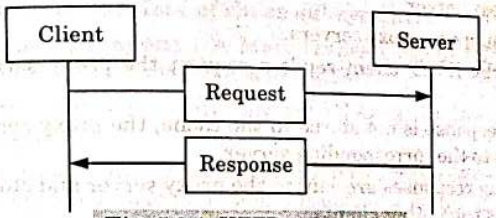


Fig. 5.9.1. HTTP transaction.

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. 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.
3. As the HTTP server does not maintain any information about the state of client it is called as a stateless protocol.

Que 5.10. 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.

Que 5.11. What is a proxy server and how it is related to HTTP ?

Answer

1. A computer that keeps copies of responses to recent requests is known as a proxy server.
2. HTTP supports proxy servers.
3. When the HTTP client sends a request the proxy server checks its cache.
4. If the response is not stored in the cache, the proxy server sends the request to the corresponding server.
5. Incoming responses are sent to the proxy server and stored for future requests from other clients.
6. The proxy server helps in reducing the load of the original server.
7. It decreases traffic and improves latency.
8. To use the proxy server the client must be configured to access the proxy server.

PART-3

Electronic Mail, File Transfer Protocol.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.12. Explain about email architecture and services.

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. 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 mailbox is located. The final part .com identifies the type of domain. For example, .com for commercial sites.

An email system consists of three subsystems :

1. **Mail transfer agent :** A Mail Transfer Agent (MTA) transfers email messages between hosts using SMTP.
   i. A message may involve several MTAs as it moves to its intended destination.
   ii. 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.
   i. In many cases, MDA is actually a Logical Delivery Agent (LDA), such as bin / mail or Procmail. However, sendmail can also be used as an MDA.
   ii. 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.
   iii. MDAs do not transport messages between systems or interface with the end user.
   iv. Many users do not directly utilize MDAs, because only MTAs and MUAs are necessary to send and receive email.
3. **Mail user agent :** A Mail User Agent (MUA) is a synonymous with an email client application.

i. An MUA is a program that allows a user to read and compose email messages.

ii. 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 5.13. What are the basic functions of email system ?

Answer

Email systems support five basic functions which are as follows :

1. **Composition :**
   i. The process of creating messages and to answer them is known as composition.
   ii. The system can also provide assistance with addressing and a number of header fields attached to each message.
2. **Transfer :**
   i. It is the process of moving messages from the sender to the recipient.
   ii. 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 :**
   i. It is the process of displaying the incoming messages so that it can be read by the user.
   ii. For this purpose simple conversions and formatting are required to be done.
5. **Disposition :**
   i. This is concerned with what the recipient does with the received message. Disposition is the final step in email system.
   ii. Some of the possibilities are as follows :
      a. Throw after reading
      b. Throw before reading
      c. Save messages
      d. Forward messages
      e. Process messages in some other way

Que 5.14. Write a short note on following message access protocols :
a. Post Office Protocol, version 3 (POP3),
b. Internet Mail Access Protocol, version 4 (IMAP4).

Answer

A. Post Office Protocol, version 3 (POP3) :

1. POP3 is a simple and limited functionality message access protocol.
2. The client and server both have POP3 software installed on their respective computers.
3. Mail access starts when the client needs to download e-mail from the mailbox.
4. The client opens a connection to the server on TCP port 110.
5. It then sends its user name and password to access the mailbox.
6. The user can then list and retrieve the mail messages.
7. POP3 has two modes: delete and keep mode.
8. In delete mode, mail is deleted from the mailbox after each retrieval.
9. The delete mode is used when the user is working at her permanent computer.
10. In keep mode, mail remains in the mailbox after retrieval.
11. The keep mode is used when the user accesses her mail away from her primary computer.
12. The mail is read but kept in the system for later retrieval and organizing.

B. Internet Mail Access Protocol, version 4 (IMAP4) :

1. IMAP4 is similar to POP3, but it has more features.
2. IMAP4 is more powerful and more complex.
3. POP3 is deficient in several ways. IMAP4 provides the following extra functions :
   i. Prior to downloading a user can check the e-mail header.
   ii. Prior to downloading a user can search the contents of the e-mail for a specific string of characters.
   iii. A user can partially download e-mail. This is especially useful in limited bandwidth scenario.
   iv. A user can create, delete, or rename mailboxes on the mail server.
   v. Hierarchy of mailboxes can be created in a folder for e-mail storage.

Que 5.15. Write a short note on :
i. MIME
ii. TFTP

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.

Que 5.16. Write a short note on file transfer protocol.

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 5.17. 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.

PART-4

Remote Login, Network Management

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.18. **What is remote login ? Describe Telnet and its working procedure.**

OR

Elaborate about Telnet and its working procedure.

AKTU 2016-17, 2017-18; Marks 10

OR

Write short note on : Telnet. **AKTU 2018-19, Marks 3.5**

Answer

Remote login :

1. It is a process in which user can login into remote computer (site) and use services that are available on the remote computer.
2. It is implemented using Telnet.

Telnet :

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.

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 5.19. **Describe the working procedure of remote login.**

Answer

Procedure of Remote Login :

1. When the user types something on local computer, then local operating system accepts character.

2. Local computer does not interpret the characters; it will send them to Telnet client.
3. Telnet client transforms these characters to Network Virtual Terminal (NVT) characters and then pass them to the local TCP/IP protocol stack.
4. Commands or text in the form of NVT travelling through Internet arrives at the TCP/IP stack of remote computer.
5. Characters are then delivered to operating system and later to Telnet server.
6. Then Telnet server changes those characters to characters which can be understandable by remote computer.
7. However the remote operating system is not designed to receive characters from a Telnet server.
8. Therefore the characters cannot be passed directly to the operating system.
9. To overcome this problem we use pseudoterminal driver software.
10. Operating system then passes characters to the appropriate application program.

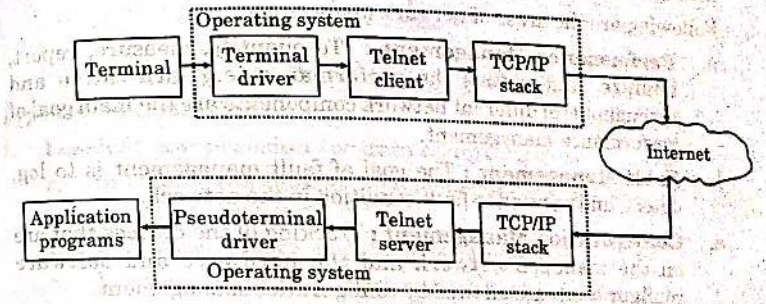


Fig. 5.19.1.

Que 5.20. **Write a short note on Network Virtual Terminal (NVT).**

Answer

1. The access mechanism of a remote computer is complex.
2. This is so because we are dealing with heterogeneous systems.
3. Every computer along with its operating system accepts a special combination of characters as tokens.
4. If we want to access a remote computer, we must know what type of computer we will be connected to, and install the specific terminal emulator used by that computer.

5. Using network virtual terminal (NVT) character set Telnet solves this problem.
6. Using this interface, the client Telnet translates characters from the local terminal into NVT form and delivers them to the network.
7. The server Telnet translates these characters from NVT form into the form acceptable by the remote computer.

Que 5.21. Write short note on network management.

Answer

1. Network management is the process of administering, managing, and operating a data network, using a network management system.
2. Modern network management systems use software and hardware to constantly collect and analyze data and push out configuration changes for improving performance, reliability, and security.
3. Network management is providing functions to control, plan, allocate, deploy, coordinate, and monitor network resources. Network management is part of most or all of the network devices.
4. Following are the areas of network management :
   a. **Performance Management :** To quantify, measure, report, analyze, and control the performance (e.g, utilization and throughput) of different network components are the main goal of performance management.
   b. **Fault Management :** The goal of fault management is to log, detect, and respond to fault condition in the network.
   c. **Configuration Management :** Tracking of the devices that are on the managed network and the hardware and software configurations are allowed by configuration management.
   d. **Accounting Management :** To specify, log, and control user and device access to network resources are allowed by accounting management.
   e. **Security Management :** It is responsible for controlling access to the network based on the predefined policy.

PART-5

Data Compression.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.22. 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. 5.22.1.

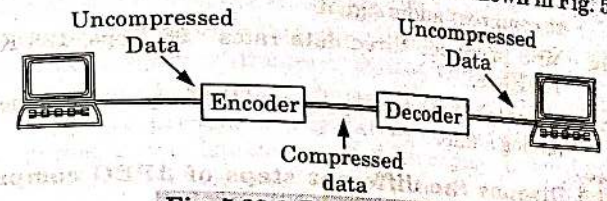


Fig. 5.22.1. Data compression.

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 5.23. Write short notes on : Audio compression.

Answer

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.

Que 5.24. Discuss the different steps of JPEG compression standard.

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.

Que 5.25. Write a short note on video compression.

Answer

1. The Moving Picture Experts Group (MPEG) method is used to compress video.
2. While compressing video we spatially compress each frame and temporally compress a set of frames.

A. Spatial Compression :

1. The spatial compression of each frame is done with JPEG.
2. Each frame can be independently compressed.

B. Temporal Compression :

1. In temporal compression, redundant frames are removed.
2. To temporally compress data, the MPEG method first divides frames into three categories: I-frames, P-frames, and B-frames.

i. **I-frames :** An intracoded frame (I-frame) is an independent frame. They are present at regular intervals. An I-frame appears periodically to handle some sudden change in the frame that the previous and following frames cannot show.

ii. **P-frames :** A predicted frame (P-frame) is related to the preceding I-frame or P-frame. Each P-frame contains only the changes from the preceding frame.

iii. **B-frames :** A bidirectional frame (B-frame) is related to the preceding and following I-frame or P-frame. B-frame is never related to another B-frame.

PART-6

Cryptography-Basic Concepts.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 5.26. 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 :

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

ii. 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 5.27. Define cryptography with the help of block diagram of symmetric and asymmetric key cryptography.

Answer

Cryptography : Refer Q. 5.26, Page 5–21B, Unit-5.

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.

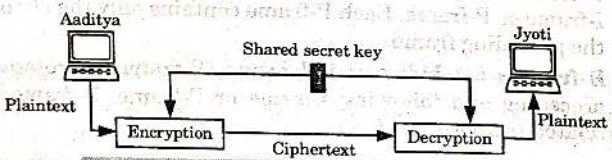


Fig. 5.27.1. Symmetric key cryptography.

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. 5.27.2 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.

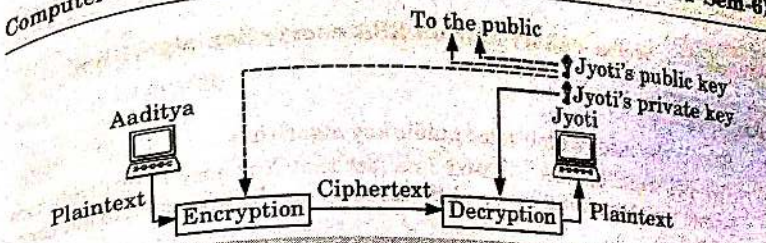


Fig. 5.27.2. Asymmetric key cryptography.

Que 5.28. 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 5.29. 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).

$$\therefore \quad N = A \times B \qquad ...(5.29.1)$$

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

$$\therefore \quad T = (A - 1)(B - 1) \qquad ...(5.29.2)$$

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 :

$$D = E^{-1} \bmod T \qquad ...(5.29.3)$$

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

$$C = M^E \bmod N \qquad ...(5.29.4)$$

That means the plaintext M is raised to the power of E (public key) and then divided by N. The mod term in equation (5.29.4) tells us that the remainder of this division is sent as the ciphertext C as shown in Fig. 5.29.1.

6. The received message C at the receiver is decrypted to obtain the plaintext back by using the following rule (algorithm).

$$M = C^D \bmod N \qquad ...(5.29.5)$$

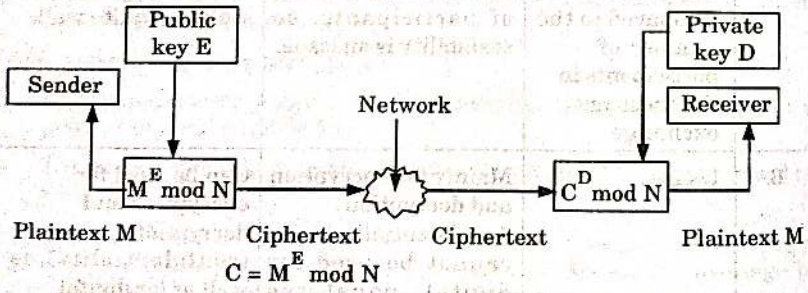


Fig. 5.29.1. Encryption and decryption in RSA.

Que 5.30. 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. 5.30.1.

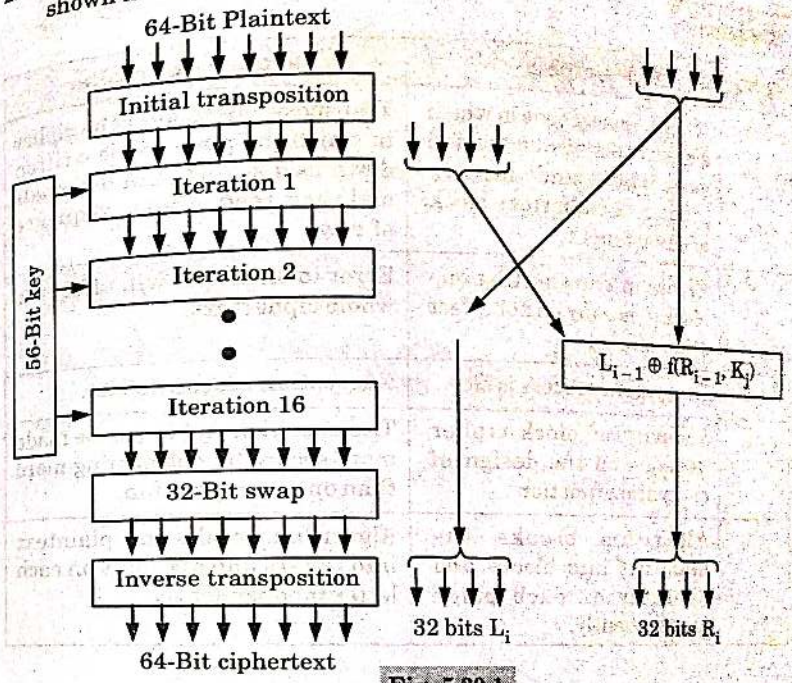


Fig. 5.30.1.

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 5.31. Differentiate between the block cipher with transposition cipher.

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.

VERY IMPORTANT QUESTIONS

Following questions are very important. These questions may be asked in your SESSIONALS as well as UNIVERSITY EXAMINATION.

Q. 1. Write a short note on DNS in the internet.
Ans. Refer Q. 5.1.

Q. 2. 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. 5.3.

Q. 3. Write a short note on electronic mail.
Ans. Refer Q. 5.12.

Q. 4. Write a short note on file transfer protocol.
Ans. Refer Q. 5.16.

Q. 5. How does FTP work ? Differentiate between passive and active FTP.
Ans. Refer Q. 5.17.

Q. 6. Elaborate about Telnet and its working procedure.
Ans. Refer Q. 5.18.

Q. 7. Write short notes on : Audio compression.
Ans. Refer Q. 5.23.

Q. 8. Define cryptography with the help of block diagram of symmetric and asymmetric key cryptography.
Ans. Refer Q. 5.27.

☺☺☺

1 UNIT

Introductory 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. 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.

1.5. 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.

1.6. 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.

1.7. What are different categories of network ?

Ans: Following are the different categories of network :

1. LAN (Local Area Network)
2. PAN (Personal Area Network)
3. MAN (Metropolitan Area Network)
4. WAN (Wide Area Network)

1.8. Define ISP.

Ans: Internet Service Provider (ISP) is a company which provides internet connection to end user, but there are basically three levels of ISP.

1.9. What are the advantages of peer-to-peer network ?

Ans: Advantages of peer-to-peer network :

1. It is less costly as it does not contain any dedicated server.
2. If one computer stops working but, other computers will not stop working.
3. It is easy to set up and maintain as each computer manages itself.

1.10. What are the disadvantages of peer-to-peer network ?

Ans. **Disadvantages of peer-to-peer network :**

1. In the case of peer-to-peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
2. It has a security issue as the device is managed itself.

1.11. What are the advantages of client/server network ?

Ans. **Advantages of client/server network :**

1. A Client/Server network contains the centralized system. Therefore we can back up the data easily.
2. A Client/Server network has a dedicated server that improves the overall performance of the whole system.

1.12. What are the disadvantages of client/server network ?

Ans. **Disadvantages of client/server network :**

1. Client/Server network is expensive as it requires the server with large memory.
2. It requires a dedicated network administrator to manage all the resources.

1.13 What are the components of network ?

Ans. Following are the components of network :

1. Repeater
2. Hub
3. Bridge
4. Switch

1.14. Define physical layer.

Ans. Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another.

1.15. What are the types of connection in computer network ?

Ans.

1. Point-to-point connections
2. Broadcast/multicast connections
3. Multipoint connections

1.16. Define multiplexing.

Ans. Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

☺☺☺

UNIT 2

Link Layer (2 Marks Questions)

2.1. Define framing.

Ans. Frames are the units of digital transmission particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in case of light energy.

2.2. What are the problems of framing ?

Ans. **Problems in Framing :**

1. Detecting start of the frame
2. How does station detect a frame
3. Detecting end of frame.

2.3. What are the types of framing ?

Ans. **Following are the types of framing :**

1. Fixed size
2. Variable size
   a. Length field
   b. End Delimeter (ED)

2.4. What are the types of channel allocation ?

Ans. **Two types of channel allocation are :**

i. Static channel allocation
ii. Dynamic channel allocation

2.5. 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

2.6. 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.

2.7. 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 %.

2.8. 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

2.9. 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.

2.10. 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.

2.11. 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.

2.12. 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.

2.13. 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.

2.14. 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.

2.15. 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, 2018-19; 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.

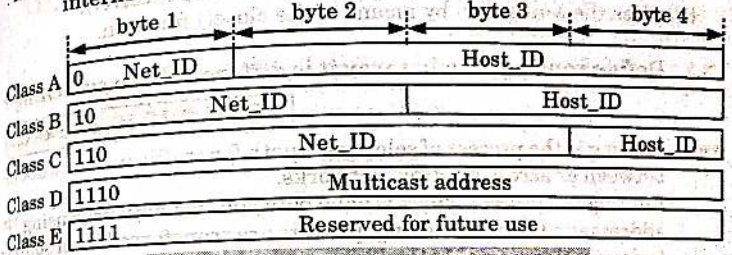


Fig. 3.6.1. Internet classes (IP addresses).

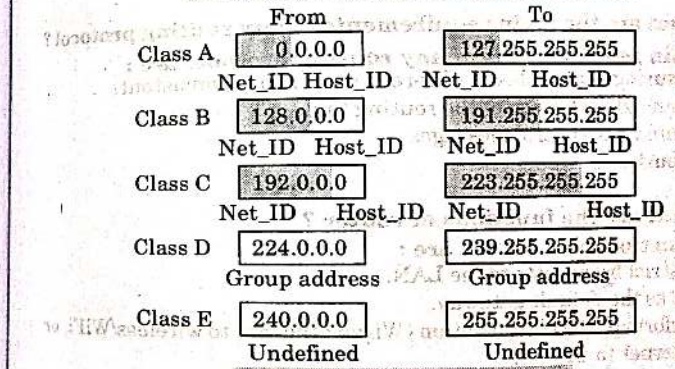


Fig. 3.6.2. Classes range of IP.

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 is 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 functions 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.

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 uses of HTTP.

AKTU 2016-17, 2017-18; Marks 02

Ans. **Uses 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. Mention 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. 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.

5.10. What are the types of cryptography ?

Ans. **Types of cryptography are :**

i. Symmetric key cryptography

ii. Asymmetric key cryptography

5.11. 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.

5.12. 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.

☺☺☺