KHWAJA MOINUDDIN CHISHTI LANGUAGE UNIVERSITY, LUCKNOW

2023-2024

Assignment

SUBMITTED BY:

Name: Ateeq Ahmad

Course: BCA

Semester: Vth

Roll No: 2104161010

Enrolment No: A-6179

Paper Name: Computer Networks

Paper code: BCA 502

SUBMITTED TO:

DR. Anmol Chand Jain

Department of Computer Science and Information Technology

UNIT - I

Question No. - 1:- Define Computer Networks it's components and features?

Answer:-

Computer Network:- A computer network is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows user to communicate more easily.

A computer network is a collection of two or more computer system that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

Computer Network Components:- It is the major parts which are needed to install the software. Some important network components are NIC, switch, cable, hub, router, and modem.

NIC:- NIC stands for Network Inter face Card, it is used to connect a computer to another computer on to a network.

Switch:- A switch is a hardware device that connects multiple devices on a computer network.

Cable:- Cable is a transmission media used for transmitting a signal.

Hub:- A Hub is a hardware device that devides the network connection among multiple devices.

Router:- A router is a hardware device which is used to connect a LAN with an internet connection

Modem:- A modem is a hardware device that allows the computer to the internet over the existing telephone line.

Features of computer Network:- A list of computer Network features is given bilow —

⇒ **Communication Speed**:- Network provides us to communicate over the network in a fast and efficient manner.

⇒ **File sharing**:- Computer network provides us to share the files with each other.

⇒ **Back up and Roll back is easy**:- Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the backup from the main server.

⇒ **Software and Hardware sharing**:- We can install the applications on the main server, therefor, the user can access the applications centrally.

⇒ **Security**:- Network allows the security by ensuring that the user has the right access the certain files and applications

⇒ **Scalability**. Scalability means that we can add the new components on the network.

⇒ **Reliability**:- Computer Network can use the alternative source for the data communication in case of any hardware failure.

Question No.-2:- Discuss topology. Explain computer architecture, type and application area of computer network.

Answer:- ~~Topology~~

Topology:- Topology defines the structure of the network of how all the components are interconnected to each other. There are five types of topology.

1- Bus Topology:- Every computer and network devices is connected to a single cable in a bus topology network.

2- Ring Topology:- The topology is named ring topology because one computer is connected to adjacent computer, with the final one being connected to the first.

3- Star Topology:- Each devices are directly connected with a central controller device, which is commonly reffered to as the HUB. And the sharing of data is only possible through HUB.

4- Mesh Topology:- In mesh topology each and every devices are directly connected with each other.

5- Tree Topology:- It has a root node which is connected to all other nodes, producing a hierarchy. Hierarchical topology is another name for it. The star topology is connected via bus topology called tree topology.

Computer Network Architecture!- It is defined as the physical and logical design of the software, hardware, protocals and media of the transmission of data. Symply we can say that how computers are organized and how task are allocated to the computer. There are two type of network architecture.

1- Peer-To-Peer Network!- Pear-To-Peer network is a network in which all the computers are linked together with equal privilage and responsibilities for processing the data. It is usefull for small environments, usually up to 10 computers. It has no directed server. Special permissions are assigned to each computer for sharing the resources.

2- Client/Server Network!- Client/Server Network is a network model designed for the end user called clients, to access the resources such as ~~song~~ songs, video etc. from a central computer known as server. while all the computers in the network are called clients. A server performs all the major operations such as security and network management. A server is responsible for managing all the resources such as files, directories, printer, etc.

Question No-3: Give Transmission modes and Explain OSI, TCP/IP.

Answer:

Transmission mode:- The way in which the data is transmitted from one device to another device is known as transmission mode. The transmission mode is also known as communication mode. Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
The transmission mode is defined in the physical layer.
Transmission mode is devided into three categories.—
Simplex mode, Half-duplex mode and Full-duplex mode.

OSI Model:- OSI stands for Open System Interconnection. It is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
OSI consists of seven layers, and each layer performs a particular task.
Each layer is self-contained, so that task assigned to each layer can be performed independently.
A list of seven layers are given below—

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

TCP/IP Model:- The TCP/IP model consists of five layers – application layer, transport layer, network layer, data link layer and physical layer.

The first four layers provide physical standards, network interface, internet working, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

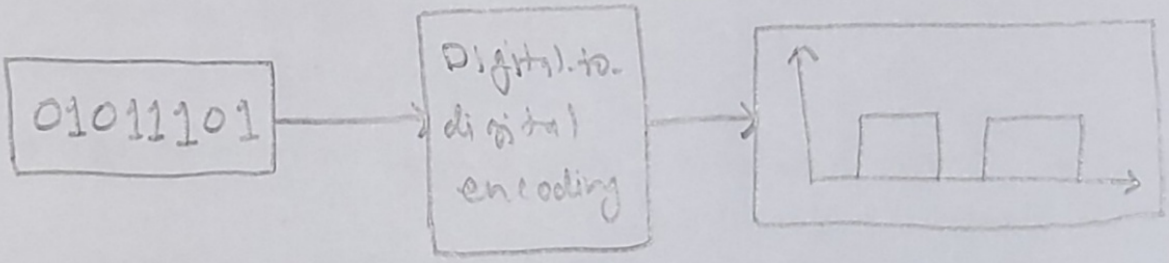
Question No 4: In Physical layer discuss digital and analog transmission paradiagram.

Answer:

Digital Transmission:- Data can be represented either in analog or digital form.

The computer used the digital form to store the information. Therefore, the data need to be converted in digital form so that it can be used by a computer.

Digital-To-Digital Conversion:- Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by a computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding.



Digital-to-digital encoding is devided into three categories.—

1- Unipolar Encoding.

2- Polar Encoding.

3- Bipolar Encoding.

Analog Transmission:- To send the digital data over an analog media, it needs to be converted into analog signal. There can be two cases according to data formatting.

When digital data is converted into bandpass analog signal, it is called digital-to-analog conversion.

When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion.

Digital-to-Analog Conversion:- When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

There are three kinds of digital-to-analog conversion.—

1- Amplitude Shift Keying
2- Frequency Shift Keying
3- Phase Shift Keying

Analog-to Analog Conversion:- Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog-to-Analog conversion can be done in three ways-

1- Amplitude Modulation.
2- Frequency Modulation.
3- Phase Modulation.

Question No. - 5:- Explain multiplexing. Discuss about switching techniques used in computer networks.

Answer:

Multiplexing:- 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.

Multiplexer is achieved by using a device called Multiplexer (MUX) that combine n input lines to generate a single output line.

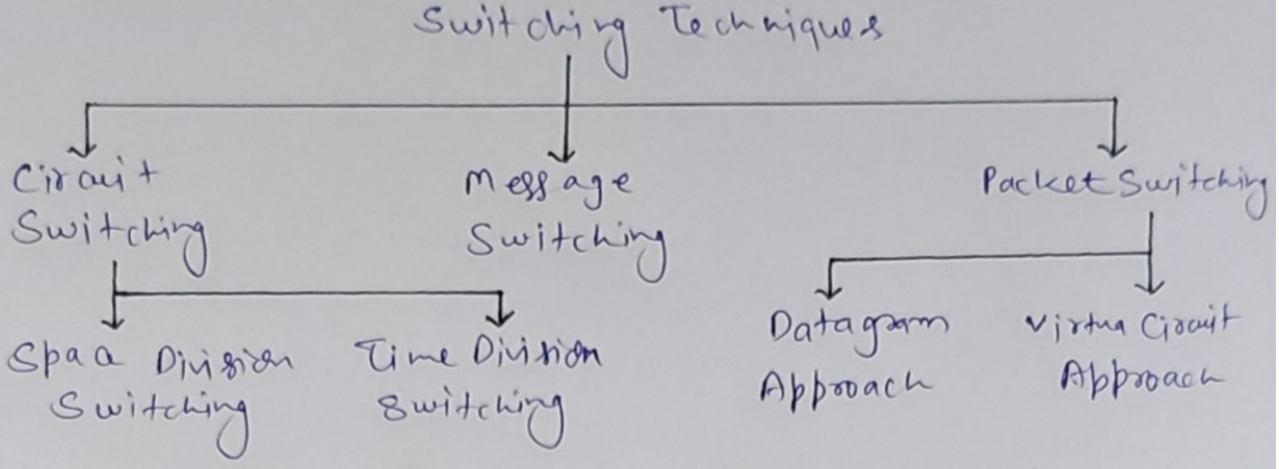
Demultiplexing is achieved by using a device called Demultiplexer (DEMUX), that separates a signal into its components signals (one input and n outputs).

Switching:- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.

Switching Techniques:- In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-two-one communication.

Classification of Switching Techniques——



Circuit Switching:- Circuit Switching is a switching technique that establishes a dedicated path between sender and receiver.
In this technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.

Message Switching:- Message switching is switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.

Packet Switching:- The packet switching is a switching technique in which the message is sent in one go, but it is devided into smaller pieces, and they are sent individually. The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.

UNIT-II

Question No-1:- What are the data link services? Explain all services offered by the link layer.

Answer:-

Data Link Layer:- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.

The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to destination, the datagram must be moved across an individual link.

The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.

The Data Link layer protocal defines the format of the packet exchanged across the nodes well as the actions such as error dedection, retransmission, flow control, and random access.

Following services are provided by the DataLink Layer—

1. Framing & Link Access
2. Reliable Delivery
3. Flow control
4. Error Dedection
5. Error Correction
6. Half-Duplex & Full-Duplex

1- **Framing & Link Access:-** Data Link Layer protocols encapsulate each network frame within a Link Layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted a number of data fields.

2- **Reliable Delivery:-** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is complished with transmission and acknowledgements.

3- **Flow control:-** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost.

4- **Error Detection:-** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a machanism to detect one or more errors.

5- **Error Correction:-** Error correction is similar to the error detection, except the receiving node not only detect the errors but also determine where the errors have occurred in the frame.

6- **Half-Duplex & Full-Duplex:-** In a Full-Duplex mode, both the nodes can transmit the data the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Question No. 2:- Discuss error detection and error correction.

Answer:

Error Detection:- When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An error is a situation when the message received at the receiver end is not identical to the message transmitted.

Errors can be classified into two categories——

1. Single-Bit Error.
2. Burst Error.

1- Single-Bit Error:- The only one bit of given data unit is changed from 1 to 0 or from 0 to 1.

Single-Bit Error does not appear more likely in serial data transmission.

Single-Bit Error mainly occurs in Parallel Data Transmission.

2- Burst Error:- The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.

The duration of noise is more than the duration of noise in Single-Bit.

Burst Errors are more likely to occur in serial data transmission.

Error Correction:- Error correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver. A single addition bit can detect the error, but cannot correct it. For correction the errors, one has to know the exact position of the error.

Error correction can be handled in two ways —

1. Backward error correction.
2. Forward error correction.

1. **Backward error correction**:- Once the error is discovered, the receiver requests the sender to retransmits the entire data unit.

2. **Forward error correction**:- In this case the receiver uses the error-correction code which automatically corrects the errors.

Question No-3:- What do you understand by flow control? Discuss stop and wait, sliding window.

Answer:

Flow control:- It is a set of procedures that tells the sender how much data it can transmit before the overwhelms the receiver.

The receiving data has limited and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.

There are two methods to control the flow of data.

1- Stop-and-wait:- In the stop-and-wait method, the sender wait for the acknowledgement after every every fame it sends.
when acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

2- Sliding Window:- The sliding window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
In this method, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently. Sliding window refers to imaginary boxes at both the sender and receiver end.
frames can be acknowledged even when the window is not completely filled.

Question No. 4: In Error control discuss (Stop-and-wait ARQ) and (Sliding window ARQ).

Answer:- Error control is a technique of error detection and transmission.

There are two types of Error control technique —

1- Stop-and-wait ARQ:- Stop-and-wait ARQ is a technique used to transmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receive the acknowledgement of the last transmitted frame. If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. It works with the timer, If the acknowledgement is not received within the alloted time, then the sender assumes that the frames is lost during the transmission, so it will retransmit the frame.

2- Sliding window ARQ:- Sliding window ARQ is a technique used for continuous transmission error control.

In this case, the sender keeps the copies of all transmitted frames until they have bee acknowledge.

The receiver can send either NAK or ACK depending on the conditions.

The sliding window ARQ is equipped with the timer to handle the lost acknowledgement.

UNIT - III

Question No-1: Explain the function of network layer.

Answer:

Network Layer:- The Network Layer is the third layer of the OSI model.

It handle the service requests from the transport layer and further forwards the service request to the data link layer. The network layer translates the logical address into physical address.

The main role of the network layer is to move the packets from sending host to the receiving host.

There are some functions performed by network layer—

Routing:- When a packet reaches the router's input link, the router will move the packets to the router's output link.

Logical Addressing:- The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to the distinguish b/w source and destination system.

Internetworking:- This is the main role of network layer that it provide the logical connection b/w different types of network.

Fragmentation:- The fragmentation is a process of breaking a packets into the smallest individual data units that travel through different networks.

Question No-21- Explain network addressing (IPv4 & IPv6). Difference b/w IPv4 & IPv6.

Answer:-

Network Addressing:- Network addressing is one of the major responsibilities of the network layer.
Network addresses are always logical, i.e., software-based address.

IPv4:- IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.
Ex:- 66.94.29.13

IPv6:- IPv6 is the next generation of IP address.
The main difference b/w IPv4 and IPv6 is the address size of IP address. IPv6 is a 128-bit hexa decimal address made up of 8 sets of 16 bit each, and these 8 sets are separated by a colon.
In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time. This hexadecimal address contains both number and alphabets.
IPv6 is capable of producing over 340 undecillion ($3.4 * 1038$) address.

Question No. 3:- Discuss Routing, Static, Dynamic and Default.

Answer:-

Routing:- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as router.
A router works at the network layer in the OSI model and internet layer in TCP/IP model.
Router can be classified into three categories.

1- Static Routing:- Static Routing is also known as Nonadaptive Routing. It is a technique in which the administrator manually adds the routes in a routing table. In this technique, routing decisions are not made based on the condition or topology of the networks.

2- Dynamic Routing:- It is also useful when the bulk of transmission networks have to transmit the data to the same hop device.
When a specific route is mentioned in the routing table, the route will choose the specific route rather than the default. It is also known as adaptive route.

3- Default Routing:- Default routing is a technique in which a router configured to send all the packets to the same hop device, and it does not matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in ~~default~~ default routing.
Default routing is used when networks deal with the single exit point.

Question No 4: Discuss about Network Layer Protocols (ARP, RARP, ICMP, IGMP, and IP).

Answer:-

ARP:- ARP stands for Address Resolution Protocol. It is used to associate an IP address with the MAC address.
Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily.

RARP:- RARP stands for Reverse Address Resolution Protocol. The protocol which is used to obtain the IP address from one server is known as RARP.
The message format of the RARP is similar to the ARP.

ICMP:- ICMP stands for Internet Control Message Protocol. The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender. ICMP uses echo test/reply to check whether the destination is reachable and responding. ICMP messages are transmitted within IP datagrams.

IGMP:- IGMP stands for Internet Group Message Protocol. The IGMP protocol is used by hosts and router to support multicasting.
The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the member of a group.

Question No-5:- Discuss Adaptive and Non-adaptive routing.

Answer:

Adaptive Routing Algorithm:- An adaptive routing algorithm is also known as dynamic routing algorithm
This algorithm makes the routing decisions based on the topology and network traffic.
The main parameters related to this algorithm are hop count, distance and estimated transit time.

Non-Adaptive Routing Algorithm:- Non-adaptive routing algorithm is also known as a static routing algorithm
When booting up the network, the routing information stores to the routers.
Non-adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

UNIT-IV

Question No-1:- Discuss Transport Layer Protocol (TCP & UDP).

Answer

Transport Layer Protocol:- The transport layer is represented by two protocols— TCP & UDP.

TCP:- TCP stands for Transmission control Protocol. It provides full transport layer services to applications.

It is a connection-oriented means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission

UDP:- UDP stands for user datagram protocol.

UDP is a simple protocol and it provides nonsequenced transport functionality. UDP is a connectionless protocol.

This type of protocol is used when reliability and security are less important than speed and size.

The paket produced by the UDP protocol is known as the user datagram.

Question No. 2:- Discuss Application Layer Protocols (DNS, FTP, Telnet, SMTP, HTTP, SNMP).

Answer:

Application Layer Protocol:- An application layer protocol defines how the application processes running on different system, pass the messages to each other.

DNS:- DNS stands for Domain Name System. DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address. DNS is required for the function of the internet. Each node in a tree has a domain name and a full domain name is a sequence of symbols specified by dots.

FTP:- FTP stands for file transfer protocol. It is a standard network protocol provided by the TCP/IP used for transmitting the files from on host to another. It is also used for downloading the files to computer from other servers. It provides the sharing of files.

Telnet:- A popular client-server program Talent is used to meet such demands. Telnet is an abbreviation for terminal network.
Telnet provides a connection to the ~~network~~ remote computer in such a way that the local terminal appears to be at the remote side.

SMTP:- SMTP stands for Simpal Mail Transfer Protocol.

SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called SMTP.

It is a program used for sending messages to other computer users based on e-mail addresses.

It provides a mail exchange between users on the same or different computer.

SNMP:- SNMP stands for Simple Network Management Protocol.

SNMP is a framework used for managing devices on the internet.

It provides a set of operations for monitoring and managing the internet.

SNMP has two components Manager and agent.

The manager is a host that control and monitors a set of agents such as routers.

HTTP:- HTTP stands for HyperText Transfer Protocol.

It is a protocol used to access the data on the World wide Web (www).

The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

This protocol is known as HyperText Transfer protocol because of the efficiency that allow us to use in a hypertext environment where there are rapid jumps from one document to another document.

Question No.3:- Explain Network Application Architecture.

Answer:-

Network Application Architecture:- Application architecture is different from the network architecture. The network architecture is fixed and provides a set of services to applications. The application on the other hand is designed by the application developer and defines how the application should be structured over the various end system. Application architecture is of two types—

1- Client-Server Architecture:- An application program running on the local machine sends a request to another application program is know as client, and a program that ~~serves~~ serves a request is known as a server.

2- P2P (Peer-to-Peer) Architecture:- It has no dedicated server in a data center. The peer are the computers which are not owned by the service provider. Most of the peer reside in the homes, offices, schools and universities. The peers communicate with each other without passing the information through a dedicated server, this architecture is known as peer-to-pee architecture.

Question No. 4:- Discuss Network Security (IP Sec & Firewalls).

Answer:-

Computer Network Security:- Computer Network Security consists of measures taken by business or some organization to monitor and prevent unauthorized access from the outsider attackers.

IP security (IP Sec):- IP Sec is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocol needed for security key exchange and key management are defined in it.

Firewalls:- A firewall is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and bassed on a defined set of security rules it accepts, rejects or drops that specific traffic

Accept: allow the traffic.

Reject: block the traffic but reply with an "unreachable error"

Drop: block the traffic with no reply.

A firewall establishes a barrier b/w secured internal networks and outside untrusted network, such as the internet.

References

⇒ https://www.geeksforgeeks.com.

⇒ https://www.javapoint.com.

⇒ https://www.tutorialpoint.com.