`

Chettinad College of Engineering & Technology
Approved by AICTE-New Delhi and Affiliated to Anna University-Chennai

Department of Computer Science Engineering

CS3591-Computer Network QUESTION BANK

Unit I Introduction and Application Layer

PART-A

1)Define a data Communication? List out the five components?

These are sender, receiver, communication medium, the message to be communicated, and certain rules called protocols to be followed during communication. The communication media is also called transmission media.

2)Define the term Protocal?

The most common meaning of protocol is “a system of rules that explain the correct conduct and procedures to be followed in formal situations,” as in these example sentences: The soldier's actions constituted a breach of military protocol. They did not follow the proper diplomatic protocols.

3)Define a layer?

Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer. The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software

4)What are the four main properties of http?

It is the protocol that allows web servers and browsers to exchange data over the web. It is a request response protocol. It uses the reliable TCP connections by default on TCP port 80. It is stateless means each request is considered as the new request.

5)Write the use of HTTP?

Hypertext Transfer Protocol (HTTP) is a method for encoding and transporting information between a client (such as a web browser) and a web server. HTTP is the primary protocol for transmission of information across the Internet.

6)What are the transmission modes of FTP?

Stream mode: The default mode, where data is transferred from FTP to TCP in stream bytes

Block mode: Data is transferred from FTP to TCP in the form of blocks, each block followed by a 3-byte header

Compressed mode: Used to transfer big files

7)Compare the HTTP and FTP?

HTTP is used to transfer web pages between a client and a server while FTP is used to transmit files among different hosts. HTTP does not require authentication while FTP requires authentication to transfer files from one host to another. HTTP is a stateless protocol while FTP can maintain states.

8)Mention the applications of FTP?

FTP is used for file transfers between one system and another, and it has several common use cases, including the following: Backup. FTP can be used by backup services or individual users to backup data from one location to a secured backup server running FTP services.

9)Short note on SNMP?

Simple Network Management Protocol (SNMP) is an internet standard protocol used to monitor and manage network devices connected over an IP. SNMP is used for communication between routers, switches, firewalls, load balancers, servers, CCTV cameras, and wireless devices.

10)Strength of SNMP?

Standardized device monitoring, eliminating the need for complex monitoring configurations.

Vendorless monitoring (meaning devices from any manufacturer are recognized)
Automatic parameter monitoring.
Real-time status updates.

11)Classification of Internet Standard Management Framework?

The framework consists of four parts: definitions of network management objects known as MIB objects. In the Internet network management framework, management information is represented a collection of managed objects that together form a virtual information store, known as the Management Information Base (MIB).

12)Classify the areas of Network management?

Performance Management.
Fault Management.
Configuration Management.
Accounting Management. Security Management.

13)Uses of network management?

Improved productivity.
Improved network security.
Holistic view of network performance.
Network administration.
Network operations.
Network maintenance.
Network provisioning.

14)Define DDNS?

Dynamic DNS (DDNS) is a service that can automatically update DNS records when an IP address changes. Domain names convert network IP addresses to human-readable names for recognition and ease of use.

15)What are the different network topologies to organize computer network?

Ring network topology
Mesh network topology
Star network topology
Tree network topology
Hybrid network topology

Part- B/C

1)Explain briefly about Data Communication?(Refer pg no: 1-2)

The term “Data Communication” comprises two words: Data and Communication. Data can be any text, image, audio, video, and multimedia files. Communication is an act of sending or receiving data. Thus, data communication refers to the exchange of data between two or more networked or connected devices.

2) Explain briefly about Networks? (Refer pg no: 1-4)

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

3)Explain briefly about Network Types? (Refer pg no: 1-6)

Two basic network types are local-area networks (LANs) and wide-area networks (WANs). LANs connect computers and peripheral devices in a limited physical area, such as a business office, laboratory, or college campus, by means of links (wires, Ethernet cables, fibre optics, Wi-Fi) that transmit data rapidly.

4)Explain briefly about OSI Model? (Refer pg no: 1-21)

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.

5)Explain briefly about Application layer protocols? (Refer pg no: 1-29)

Application layer protocols define the language that network applications speak to fulfill user requests. For example, an application layer protocol defines what message a web browser sends to a remote server to retrieve a web page.

6)Explain briefly about FTP? (Refer pg no: 1-39)

FTP (File Transfer Protocol) is a standard network protocol used for the transfer of files from one host to another over a TCP-based network, such as the Internet. FTP works by opening two connections that link the computers trying to communicate with each other.

7)Explain briefly about SNMP? (Refer pg no: 1-71)

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).

8)Explain briefly about Email and Email Protocol? (Refer pg no: 1-43)

Email protocols define how the email message has to be encoded, how it needs to be sent, received, rendered, and so on, and hence they are essential. While email protocols make the process behind emails a bit complex, the protocols ensure that email is a standard, reliable, and universal mode of communication.

9)Explain briefly about DNS? (Refer pg no: 1-56)

The Domain Name System (DNS) turns domain names into IP addresses, which browsers use to load internet pages. Every device connected to the internet has its own IP address, which is used by other devices to locate the device.

Unit II Transport Layer

PART-A

1) What are the services provided by Transport layer protocol ?

The services provided by Transport layer protocol are Reliable communication over an unreliable channel

It provides connection-oriented and connectionless services

It provides logical communication between processes running on hosts.

2) What is TCP ?

TCP provides a connection oriented, reliable, byte stream service. The term connection-oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.

3) What factors govern the rate at which TCP sends segments ?

1. The current window size specifies the amount of data that can be in transmission at any one time. Small windows imply little data; large windows imply a large amount of data.

2. If our retransmit timer is too short, TCP retransmits segments that have been delayed, but not lost, increasing congestion at a time when the network is probably already congested.

4) What value should TCP use for a retransmission timer ?

1. If our value is too short, we will retransmit prematurely, even though the original segment has not been lost.

2. If our value is too long, the connection will remain idle for a long period of time after a lost segment, while we wait for the timer to go off.

3. Ideally, we want out timer to be close to the true round trip (delay) time (RTT). Because the actual round trip time variés dynamically (unlike in the data link layer), using a fixed timer is inadequate.

5) The maximum payload of a TCP segment is 65,495 bytes. Why was such as a strange number is chosen ?

In IPv4, IP packet is 65535 bytes long because of the 16-bit field of total length. IPv4 header and TCP header are both at least 20 bytes, so TCP payload will be 65535-40 65495 bytes.

IPv6 "Payload Length" field is 16 bits so maximum IP packet is also 24= 65535 bytes. IP header is 40 bytes so maximum length of a TCP segment itself, not payload or "Application Data" field is of 65535-40 = 65395 bytes.

6) List the different phases used in TCP connection.

1) TCP connection establishment

2) TCP connection termination

3) TCP connection release

7) How do fast retransmit mechanism of TCP works ?

With fast retransmit, the sender retransmits the missing TCP segments before their retransmission timers expire. Because the retransmission timers did not expire for the missing TCP segments, missing segments are received at the destination and acknowledged by the receiver more quickly than they would have been without fast retransmit and the sender can more quickly send later segments to the receiver. This process is known as fast recovery.

8) Define congestion control.

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

9) Suppose TCP operates over a 1-Gbps link, utilizing the full bandwidth continuously. How long will it take for the sequence numbers to wrap around, completely 7 Suppose an added 32-bit timestamp field increments, 1000 times during this wrap around time, how long will it take for the, timestamp filed to wraparound?

TCP AdvertisedWindow is 16 bits, SequenceNum is 32 bits. At most there will be 2 bytes on the fly in this 1 Gbps link. The corresponding transmission time is 2x8/1 x 10-34.36 sec. So it will take 34.36 sec to wrap around the sequence number.

Each increment of timestamp 34.36 sec / 1000 = 34.36 ms, So the total time can be expressed by this timestamp = 34.36 x 10-3 x 233 sec -1.48 x 10 sec = 4.68 year

So, by adding this timestamp, it will take 4.68 year to wrap around the sequence number.

10) How does transport layer perform duplication control?

TCP uses a sequence number to identity each byte of data. It helps to avoid duplicate data and disordering during transmission.

11) What do you mean by slow start in TCP congestion ?

Slow-start is part of the congestion control strategy used by TCP, the data transmission protocol used by many Internet applications. Slow-start is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting, that is, to avoid causing network congestion.

12) Why does UDP exist? Would it not have been enough to just let user processes send raw IP packets ?

There are possibly many IP connections between two systems (identified by their IP addresses) for different applications on each end. UDP "Source Port" field identifies the associated application in the source system and "Destination Port" the associated application in the destination system.

13) Give some examples of applications where UDP is preferred over TCP.

1) In multicasting

2) Route update protocol in RIP

14) What are the types of QoS tools?

Classification these tools identify and (if desired) mark flows.

Congestion management these tools queue and service flows in different ways to provide preferential treatment to a certain flow(s)

Congestion avoidance this tool prevents a queue from filling, to allo high-priority traffic to enter the queue. This tool also provides for overcongestion avoidance in an internet/intranet.Shaping/policing these tools limit the bandwidth that flow(s) uses. Link efficiency these tools provide a method of mitigating del experienced on lower-speed links

15) List some of the quality of service parameters of transport layer.

ISO specifies eleven QoS parameters for transport layer.

1. Connection establishment delay
2. Connection establishment failure probability
3. Throughput
4. Transit delay
5. Residual error rate
6. Transfer failure probability
7. Connection release delay
8. Connection release failure probability
9. Protection
10. Resilience
11. Priority

PART-B/C

1)Explain Briefly about Transport Services (Refer pg no: 2-5)

- Address Mapping.
- Assignment of Network Connection.
- Multiplexing of Transport Connections.
- Splitting of Transport Connection.
- Establishment of Transport Connection.
- Data Transfer.
- Segmentation and Concatenation of TPDUs.
- Flow Control.

2)Explain Briefly about User Datagram Protocol (UDP) (Refer pg no: 2-19)

What is the User Datagram Protocol (UDP/IP)? The User Datagram Protocol, or UDP, is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred.

3)Explain Briefly about Transmission Control Protocol (TCP) (Refer pg no: 2-26)

Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

4)Explain Briefly about Adaptive Retransmission(Refer pg no: 2-43)

Thus, after the sender waits for a timeout period and does not receive the ACK, it considers that the transmitted data packet has been lost, and thereby retransmits the data packet. The sending and receiving process is the same as that of the first sending of the data packet.

5)Explain Briefly about Congestion Control(Refer pg no: 2-45)

Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding

congestive collapse. Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.

6)Explain Briefly about Congestion Avoidance(Refer pg no: 2-49)

A congestion control scheme helps the network to recover from the congestion state. A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput. Such schemes prevent a network from entering the congested state.

7)Explain Briefly about Stream Control Transmission Protocol (SCTP)(Refer pg no: 2-51)

Stream Control Transmission Protocol (SCTP) is an IP Transport Layer protocol. SCTP exists at an equivalent level with User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), which provides transport layer functions to many Internet applications.

8)Explain Briefly about Quality of Service (QoS) (Refer pg no: 2-60)

Quality of service (QoS) is the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity.

9) Explain Briefly about SCTP Pocket Format(Refer pg no: 2-54)

Each SCTP packet consists, in addition to the common header, of chunks. Each chunk has a common format, but the contents can vary. The green bytes in the diagram above signify one chunk. An 8-bit value predefined by the IETF to identify the contents of the chunk value field.

Unit III Network Layer

PART-A

1)What is the network address?

When an organization is given a block of addresses, the organization is free to allocate: The addresses to the devices that need to be connected to the Internet. The first address in the class is normally treated as a special address. The first address is called the network address and defines the organization network.

2)What is IP addressing ?

An IP address is a numerical label assigned to each device in a computer network that uses Internet protocol for communication.

Two important functions at IP address:

1) Host identification

2) Location addressing.

3) **Why is the IP header checksum recalculated at every router ?**

The IP header checksum is recalculated at every router because some of the IP header fields will change, such as the TTL and (if fragmentation occurs) total length, MF flag, and fragment offset.

4)Why are IP addresses hierarchical with netid and hostid?

IP address are hierarchical to reduce the size of routing tables. IP packets are routed only by netid until they reach their destination network where ARP is then used to resolve hostid to MAC address.

5) What is the time to live field in IP header ?

Time to live field is counter used to limit packet lifetimes. Counts in second and default value is 255 sec.

6) Identify the class and default subnet mask of the IP address 217.65.10.7 IP address

217.65 107 is from class C address and default subnet mask is 255.255.255.0.

7) Find the class of each address

a) 00000001 00001011 00001011 11101111

b) 14.23.120.B

a) The first bit is 0. This is a class A address.

b) The first byte is 14 (between 0 and 127). This is a class A address

8) What is the network address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0 7

25.34.12.56

255.255.0.0

25.34.0.0

Network address is 25.34.0.0

9) Give at least three reasons why NAT is widely used these days.

•No need to allocate IP range from ISP.

- Local network can be configured and changed as required. The changes must not be published.
- Changing the ISP is simplified.

•Local hosts are not visible to the outside world unless the router is configured to allow this.

10) What are the problems arising with NAT ? Name two of them.

The main problem is the violation of the end-to-end principle. Since the network address might change (due to NAT) some applications, especially P2P or VoIP ones, must take this into consideration. Furthermore, routers should not touch anything above layer 3.

11) Identify the class/speciality of the following IP addresses:

a) 110.34.56.45

b) 127.1.1.1

c) 212.208.63.23

d) 255.255.255.255

a) 110.34.56.45 Class A

b) 127.1.1.1 Loop back address

c) 212.208.63.23 - Class C

d) 255.255.255.255 Broadcast address.

12) Define subnetting

Subnetting is a technique that allows a network administrator to divide one physical network into smaller logical networks and thus, control the flow of traffic for security or efficiency reasons.

13) What are the new broadcast methods Included in IPv6 ?

Unicast, multicast and anycast.

14) Why is IPv4 to IPv6 transition is required ?

As publicly available IPv4 addresses have been exhausted. IPv4, the current internet protocol version has crossed 30 years of time period. The expanding user base and increased number of IP-enabled devices created a need for an upgraded version.From mobile apps to non-traditional computing devices populating the Internet of Things, businesses rely on ITs ability to deliver new services to both end users and customers. But these services and the infrastructure used to support them require ir addresses and that means an IPv6 migration.

15) Highlight the characteristics of datagram networks. Characteristics of datagram

networks are as follows:

i Host can send a packet anywhere at any time.

ii Each packet is forwarded independently.

PART-B&C

1) Netwok Layer Services? (Page no: 3-2)

The network Layer is the third layer in the OSI model of computer networks. Its main function is to transfer network packets from the source to the destination. It is involved both the source host and the destination host. At the source, it accepts a packet from the transport layer, encapsulates it in a datagram, and then delivers the packet to the data link layer so that it can further be sent to the receiver. At the destination, the datagram is decapsulated, and the packet is extracted and delivered to the corresponding transport layer.

2) Explain in detail DHCP.(Page no: 3-59)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

3) Explain the working of DHCP protocol with its header format.(Page no:3-62)

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cellphones, etc. is an application layer protocol that is used to provided.

4) Draw IPv6 packet header format. (Page no:3-30)

IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. Let's look at the header of IP version 6 and understand how it is different from the IPv4 header.

5) Explain about IPv6. Compare IPv4 and IPv6. (Page no:3-7 ,3-30)

The address through which any computer communicates with our computer is simply called an Internet Protocol Address or IP address. For example, If we want to load a web page or we want to download something, we require the address for delivery of that particular file or webpage. That address is called an IP Address.

6) Write note on: Internet protocol. (Page no:3-2)

What is the Internet Protocol (IP)? The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets.

7) Subnetting Network(Page no:3-17)

One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routes, increasing network speeds. Subnetting, the segmentation of a network address space, improves address allocation efficiency.

8) Explain in detail ICMP. (Page no:3-44)

ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.

9)Write note on Internet protocol.

What is the Internet Protocol (IP)? The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets.

Unit IV Routing

PART-A 1)

1)Define geographic routing.

To decrease the size of the routing table even further, it necessary to extend hierarchical routing to include geographical routing. It divides the entire address space into a few large blocks.

2) What is multicasting routing ?

Delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once. **3)**

3)What Is multicast ? What is the motivation for developing multicast ?

Multicasting means delivering the same packet simultaneously to a group of clients. Motivation for developing multicast is that there are applications that want to send a packet to more than one destination hosts.

4) Mention any four applications of multicasting.

• Broadcasts of Radio or Video

•Videoconferencing

•Shared Applications

•IGMP is used by multicast routers to keep track of membership in a multicast group.

5) Describe the difference between static and dynamic routing 7

Static routing is configured by the network administrator and is not capable of adjusting to changes in the network without network administrator intervention. Dynamic routing adjusts to changing network circumstances by analyzing incoming routing update messages without administrator intervention.

6) What are adaptive routing algorithms ?

Adaptive routing algorithms change their routing decisions to reflect changes in the topology and usually the traffic as well. Distance vector and link state are example of this.

7) Define source routing.

All the information about the network topology is required to switch a packet across the network is provided by the source host. For switching that uses neither virtual circuits nor conventional datagrams is known as source routing.

8) How routers do differentiates the Incoming unicast, multicast or broadcast IP packets ?

The Ethernet network uses two hardware addresses which identify the source and destination of each frame sent by the Ethernet. The MAC destination address (all 1 s) is used to identify a broadcast packet (sent to all connected computers in a broadcast domain) or a multicast packet (lsb of 1" byte-1) (received by a selected group of computers).

Routers are operating at layer 3. Router use IP addresses to make forwarding decisions. Each port on a router is a member of a different network. When a router receives traffic from one network, it uses the destination IP address to determine which port to forward.

9) Differentiate between forwarding table and routing table.

Routing means finding a suitable path for a packet from sender to destination and Forwarding is the process of sending the packet toward the destination based on routing information.

10) What are the benefits of Open Shortest Path First (OSPF) protocol ?

Benefits:

1. Low traffic overhead
2. Support for complex address structures
3. Fast convergence
4. Good security. OSPF supports interface-based plaintext and MD5 authentication
5. Area based topology. Large OSPF networks are organized as a set of areas linked by a backbone.

11) Types of Routing ○ Static Routing ○ Default Routing ○ Dynamic Routing

12) **Advantages Of Static Routing** ○ **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing. ○ **Bandwidth:** It has not bandwidth usage between the routers.

- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

13) **Disadvantages of Static Routing** ○ For a large network, it becomes a very difficult task to add each route manually to the routing table. ○ The system administrator should have a good knowledge of a topology as he has to add each route manually.

14)Advantages of Dynamic Routing ○
It is easier to configure. ○ It is more effective in selecting the best route in response to the changes in the condition or topology.

15)Disadvantages of Dynamic Routing ○ It is more expensive in terms of CPU and bandwidth usage.

- It is less secure as compared to default and static routing.

Part-B&C

1)Explain Routing (Page no: 4-2)

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths.

2) Explain Routing Design Goals(Page no: 4-5)

The main goals of routing are:
Correctness: The routing should be done properly and correctly so that the packets may reach their proper destination.

- Simplicity: The routing should be done in a simple manner so that the overhead is as low as possible.

3 Explain Unicast Routing Protocol(Page no: 4-7)

Introduction. Unicast routing is the process of forwarding unicasted traffic from a source to a destination on an internetwork. Unicasted traffic is destined for a unique address.

4) Explain Distance Vector Routing(Page no: 4-9)

Distance-vector routing protocols measure the distance by the number of routers a packet has to pass; one router counts as one hop. Some distance-vector protocols also take into account network latency and other factors that influence traffic on a given route. **5) Explain Link State Routing(Page no: 4-20)**

The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network.

6) Explain Global Internet(Page no: 4-30)

The entire Internet connecting all countries. The global Internet term came about as countries such as China closed access to Internet sites outside its borders. See Internet.

7) Explain Hierarchical Routing(Page no: 4-35)

Hierarchical routing is the procedure of arranging routers in a hierarchical manner. A good example would be to consider a corporate intranet. Most corporate intranets consist of a high speed backbone network. Connected to this backbone are routers which are in turn connected to a particular workgroup.

8) Explain Multicasting Basic(Page no: 4-37)

Multicasting is a method of moving media streams from a single source to multiple destinations

within the same network. Multicasting networks are typically over-the-air television broadcast stations, cable system hubs, satellite transponders and internet protocol-based systems.

9) Explain Multicast Routing(Page no: 4-38)

Multicast routing is a networking method for efficient distribution of one-to-many traffic. A multicast source, such as a live video conference, sends traffic in one stream to a multicast group. The multicast group contains receivers such as computers, devices, and IP phones.

Unit-V

Data Link and Physical Layers

PART – A

What are the types of frame available in high level data link control ?

It defines three types of frames:

Information frames

Supervisory frames

Unnumbered frames

Define flow control and error control.

Flow control: Flow control is a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

Error control: Error control is mechanism of retransmission of data by automatic repeat request (ARO). Error control involves both error detection and correction.

3. **List the services provided by data link layer ?**

Services provided by DLL:

1) Unacknowledged connectionless service.

2) Acknowledged connectionless service.

3) Acknowledged connection service.

4. **What Is HDLC?**

HDLC is a protocol that implements ARQ mechanisms. It supports communication over point-to-point or point-to-multipoint Links.

5. **State phases Involved In the operation of HDLC.** 1) Initialization 2) Data transfer 3) Disconnect.

6. **What is CSMA/CD ?**

Carrier senses multiple access with collision detection protocol sense the channel. If the channel is currently idle, transmit now. If channel is busy, wait until the channel is idle, then transmit. While transmitting, if collision is detected, stop transmitting data.

7. **Define the term medium access control mechanism ?**

The protocol that determines who can transmit on a broadcast channel are called Medium Access Control (MAC) protocol. The MAC protocols are implemented in the MAC sublayer which is the lower sublayer of the data link layer.

8. **Define throughput.**

The throughput S is defined as average successful traffic transmitted between stations per unit time.

9. **Define channel capacity.**

It is the maximum achievable throughput for a particular type of access scheme is called capacity of the channel.

10. **Define collision.**

When two or more stations transmits message on channel, the signals will superimpose on each other and is garbled beyond the decoding ability of receiving station, this is called as collisions.

11. Define baseband.

A signal transmission technology for transferring digital signal across a communication medium. Baseband signals are made up of varifying voltage levels to indicate binary 1's and 0's.

12. What do you mean by switching ?

Switching is mechanism for moving information between different networks and network segments.

13. What is meant by circuit switching ?

In circuit-switching, this path is decided upon before the data transmission starts. The system decides on which route to follow, based on a resource-optimizing algorithm.

14. Write the parameters used to measure network performance.

Network performance parameters:

1) Bandwidth

2) Throughput

3) Latency

4) Bandwidth-Delay product

5) Jitter

15. Define the terms: Bandwidth and Latency.

Bandwidth is also defined as the amount of data that can be transmitted in a fixed amount of time.

Latency is the amount of time it takes a data packet to travel from point A to point B.

PART – B & C

1. Explain in detail about the Data Link Layer ? (Page no: 5-2)

The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. The data link layer is Layer 2 in the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols.

2. Explain in detail about the HDLC. (Page no: 5-6)

HDLC (High-level Data Link Control) is a group of protocols or rules for transmitting data between network points (sometimes called nodes). In more technical terms, HDLC is a bit-oriented, synchronous data link layer protocol created by the International Organization for Standardization (ISO).

3. Explain about Point-to-point Protocol (Page no: 5-12)

Point-to-Point Protocol (PPP) is a TCP/IP protocol that is used to connect one computer system to another. Computers use PPP to communicate over the telephone network or the Internet.

4. Explain in detail about the Random Access and Controlled Access of the Media control Algorithm (Page no: 5-17, 5-34)

A controlled access protocol is a protocol in which a node has to wait for permission to send data. In contrast, random access protocols allow nodes in the network can send data at will. In random access protocols, two nodes may collide if they send data simultaneously, which hampers efficiency.

5. Explain the physical properties of ethernet 802.3 with necessary diagram of ethernet transceiver and adoptor. (Page no: 5-37)

The Ethernet is developed in the mid-1970 by researches at the Xerox Palo Alto Research Center (PARC); the Ethernet is a working example of the more general carrier sense, multiple accesses with collision detect (CSMA/CD) local area network technology.

6. Explain in detail about the Virtual LAN With neat diagram. (Page no: 5-44)

A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group

Explain in detail about the Wireless LAN (802.11) With neat diagram.

(Page no:5-51)

IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication.

Explain in detail about the Transmission Media and classification. (Page no: 5-76)

Transmission media acts a physical interface for communication in networks. There are two types of transmission media, namely guided and unguided. Guided transmission media are cables like twisted pair cables, coaxial cables, and fiber optic cables

Explain in detail about the Switching and its types with the neat diagram.

(Page no: 5-91)

There are three types of switching methods:

Switching.

Circuit Switching.

- Packet Switching. Datagram Packet Switching. Virtual Circuit Packet Switching.