

# CS6551 – COMPUTER NETWORKS

## QUESTION BANK

### UNIT 1

#### PART A

1. What are the different types of connections (direct links) available?
2. What metrics are used to assess the performance of a network?
3. What is topology?
4. For n devices in a network, what is the number of cable links required for a mesh and ring topology?
5. Assume 6 devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?
6. Mention the different physical media?
7. What is the need for layering?
8. What is a protocol?
9. How does NRZ-L differ from NRZ-I?
10. What are the main features of Internet Architecture?
11. What are the responsibilities of data link layer?
12. What is framing?
13. What are the ways to address the framing problem?
14. If data is 011011111111100 what is the transmitted data and if received data is 01111110000111011111011111011001111110 what is the actual data in HDLC framing?
15. What are the issues in data link layer?
16. Define Bandwidth and Latency.
17. Define Error detection and correction.
18. What is redundancy?
19. List out the available detection methods.
20. Write short notes on CRC.
21. Define flow control?
22. Define ARQ.
23. Mention the categories of flow control?
24. Define HDLC.
25. What is piggy backing?
26. Define socket. How it is created?

#### PART B

1. Explain network architecture in detail
2. Explain different error detection and correction mechanisms with examples
3. Explain different flow control mechanisms used in brief.
4. What is framing? Explain different types of framing protocols with their format.
5. Explain how network software is implemented in networks.

**UNIT 1**  
**PART A ANSWERS**

**1. What are the different types of connections (direct links) available?**

Two types are

1. Point to point
2. Multipoint

**2. What metrics are used to assess the performance of a network?**

Network performance is measured in two fundamental ways:

1. bandwidth (also called throughput)
2. latency (also called delay).

**3. What is topology?**

Topology refers to the way in which network is laid out physically. Two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and the linking devices to one another.

The basic topologies are:

- Mesh
- Star
- Bus hybrid
- Ring

**4. For n devices in a network, what is the number of cable links required for a mesh and ring topology?**

- Mesh topology –  $n(n-1)/2$
- Ring topology –  $n$

**5. Assume 6 devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?**

Number of cables =  $n(n-1)/2 = 6(6-1)/2 = 15$  Number of  
ports per device =  $n-1 = 6-1 = 5$

**6. Mention the different physical media?**

1. Guided ( Bounded )
  - a. Twisted pair cable
    - i. Shielded
    - ii. Unshielded
  - b. Coaxial cable
    - i. Baseband
    - ii. Broadband
  - c. Fibre optic cable
2. Unguided (Unbounded)
  - a. Radio transmission
  - b. Microwave transmission

## **7. What is the need for layering?**

Layering provides two nice features.

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

## **8. What is a protocol?**

- A protocol is a set of rules that govern data communication.
- Protocol defines the interfaces between the layers in the same system and with the layers of peer system
- These are the Building blocks of a network architecture
- Two interfaces provided by protocols
  - Service interface
  - Peer interface

## **9. How does NRZ-L differ from NRZ-I?**

In the NRZ-L sequence, positive and negative voltages have specific meanings: positive for 0 and negative for 1. In the NRZ-I sequence, the voltages are meaningless.

Instead, the receiver looks for changes from one level to another as its basis for recognition of 1s.

## **10. What are the main features of Internet Architecture?**

1. Does not imply strict layering. The application is free to bypass the defined transport layers and to directly use IP or other underlying networks
2. An hour-glass shape – wide at the top, narrow in the middle and wide at the bottom. IP serves as the focal point for the architecture
3. In order for a new protocol to be officially included in the architecture, there needs to be both a protocol specification and at least one (and preferably two) representative implementations of the specification

## **11. What are the responsibilities of data link layer?**

Specific responsibilities of data link layer include the following.

- a) Framing
- b) Physical addressing
- c) Flow control
- d) Error control
- e) Access control.

## **12. What is framing?**

It divides the stream of bits received from the upper layer (network layer) into manageable data units called frames. It adds a header to the frame to define the physical address (source address & destination address).

Two types of framing are

1. Fixed-Size Framing
2. Variable –Size framing

**13. What are the ways to address the framing problem?**

1. Byte-Oriented Protocols – BYSYNC, PPP, DDCMP
2. Bit-Oriented Protocols - HDLC
3. Clock-Based Framing - SONET

**14. If data is 011011111111100 what is the transmitted data and if received data is 01111110000111011111011111011001111110 what is the actual data in HDLC framing?**

*transmitted data*

0111111001101111101111100001111110

actual data is \*000111011111-11111-110\*

**15. What are the issues in data link layer?**

The data link layer has a number of specific functions it can carry out. These functions include

- a) Providing a well-defined service interface to the network layer.
- b) Dealing with transmission errors.
- c) Regulating the flow of data so that slow receivers are not swamped by fast senders.

**16. Define Bandwidth and Latency.**

- Bandwidth
  - Width of the frequency band
  - Number of bits per second that can be transmitted over a communication link
- **latency** refers to a delay in packet delivery
- Latency = Propagation + transmit + queue

**17. Define Error detection and correction.**

**Error Detection:**

Data can be corrupted during transmission. It is called as an error. For reliable communication, the receiver must find out the errors occurred in the data which is called as error detection. Its achieved by redundancy.

Methods used are, Parity check, Cyclic redundancy Check, Checksum

**Error Correction:**

It is the mechanism to correct the errors and it can be handled in 2 ways.

- a) When an error is discovered, the receiver can have the sender retransmit the entire data unit.
- b) A receiver can use an error correcting coder, which automatically corrects certain error (hamming codes)

**18. What is redundancy?**

It is the error detecting mechanism, which means a shorter group of bits or extra bits may be appended at the destination of each unit.

### 19. List out the available detection methods.

There are 3 types of redundancy checks are used in data communication.

1. Parity check
  - *Simple parity check ( Vertical Redundancy Check)*
  - *Two dimensional Parity Check (Longitudinal Redundancy Check)*
2. Cyclic redundancy check
3. Checksum.

### 20. Write short notes on CRC.

**CRC** is based on binary division. In CRC, instead of adding bits to achieve the desired parity, a sequence of redundant bits, called the CRC or the CRC remainder, is appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

- At its destination, the incoming data unit is assumed to be intact and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

### 21. Define flow control?

Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment.

- This is accomplished using a combination of two fundamental mechanisms called acknowledgement and timeout.
- achieved through two different mechanisms
  1. Stop and Wait
  2. Sliding window

### 22. Define ARQ.

The general strategy of using *acknowledgements* and *timeouts* to implement reliable delivery is sometimes called Automatic Repeat reQuest (ARQ).

### 23. Mention the categories of flow control?

There are 2 methods have been developed to control flow of data across communication links.

- a) Stop and wait - send one from at a time.
- b) Sliding window - send several frames at a time.

### 24. Define HDLC.

High-Level Data Link Control is a bit-oriented data link protocol designed to support both half-duplex and full duplex communication over point to point and midpoint links. A bit oriented protocol is not concerned with byte boundaries—it simply views the frame as a collection of bits.

## 25. What is piggy backing?

Piggy backing means combining data to sent and acknowledgement of the frame received in one single frame.

Piggy backing can save bandwidth because the overhead from a data frame and an ACK frame can be combined into just one frame

## 26. Define socket. How it is created?

Socket is the end point in communication.

```
#include <sys/socket.h>
```

```
int socket (int family, int type, int protocol);
```

Returns: non-negative descriptor if OK, -1 on error

Where,

- family - specifies the protocol family  
( AF\_INET / AF\_INET6 / AF\_LOCAL)
- type - specifies the type of the socket  
( SOCK\_STREAM, SOCK\_DGRAM, SOCK\_RAW)
- protocol - specifies the protocol to be used for the socket.  
(IPPROTO\_protocol name)  
-protocol field is set to zero for TCP and UDP protocols.

**UNIT 2**  
**Question Bank**

**PART A**

1. What are the functions of MAC?
2. What is CSMA?. List the protocols used with CSMA
3. Define the term carrier sense in CSMA/CD?
4. What is the access method used by wireless LAN?
5. Define Ethernet
6. What is fast Ethernet and gigabit Ethernet?
7. What is the use of transceiver?
8. What is a hidden node and exposed node?
9. What is a Bluetooth?
10. What are the four prominent wireless technologies?
11. What are the four steps involves in scanning?
12. What is exponential back off?
13. What is the use of switches?
14. Differentiate circuit switching and packet switching
15. Compare datagram approach and virtual circuit approach.
16. What is a role of VCI?
17. What is a bridge? What are the functions of bridges?
18. What is a loop problem in bridges?
19. How does a given bridge learn whether it should forward a multicast frame over a given port?
20. What are the limitations of bridges?
21. In what way bridges differs from switches?
22. What are the advantages of datagram delivery model?
23. Define IP.
24. Find the class of the following addresses  
227.13.14.88  
227.13.14.88
25. Define subnetting
26. 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?
27. Define CIDR
28. What is ARP?
29. What is DHCP?
30. What is ICMP?

## PART B

1. Discuss about physical properties of Ethernet 802.3 with necessary diagram of Ethernet transceiver, adapter and algorithm.
2. a) What is internetworking?. Explain its service model, global address and packet format.  
b) Explain the operations and packet format of ARP in detail
3. Explain the following
  - a. ICMP
  - b. DHCP
4. Explain the functioning of wireless LAN in detail
5. Explain bridges and switches in brief.
6. Explain CSMA and protocols with Collision detection and Avoidance
7. A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.



**UNIT 2**  
**Question Bank**

**PART A**

1. What are the functions of MAC?
2. What is CSMA?. List the protocols used with CSMA
3. Define the term carrier sense in CSMA/CD?
4. What is the access method used by wireless LAN?
5. Define Ethernet
6. What is fast Ethernet and gigabit Ethernet?
7. What is the use of transceiver?
8. What is a hidden node and exposed node?
9. What is a Bluetooth?
10. What are the four prominent wireless technologies?
11. What are the four steps involves in scanning?
12. What is exponential back off?
13. What is the use of switches?
14. Differentiate circuit switching and packet switching
15. Compare datagram approach and virtual circuit approach.
16. What is a role of VCI?
17. What is a bridge? What are the functions of bridges?
18. What is a loop problem in bridges?
19. How does a given bridge learn whether it should forward a multicast frame over a given port?
20. What are the limitations of bridges?
21. In what way bridges differs from switches?
22. What are the advantages of datagram delivery model?
23. Define IP.
24. Find the class of the following addresses  
227.13.14.88  
227.13.14.88
25. Define subnetting
26. 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?
27. Define CIDR
28. What is ARP?
29. What is DHCP?
30. What is ICMP?

## PART B

1. Discuss about physical properties of Ethernet 802.3 with necessary diagram of Ethernet transceiver, adapter and algorithm.
2. a) What is internetworking?. Explain its service model, global address and packet format.  
b) Explain the operations and packet format of ARP in detail
3. Explain the following
  - a. ICMP
  - b. DHCP
4. Explain the functioning of wireless LAN in detail
5. Explain bridges and switches in brief.
6. Explain CSMA and protocols with Collision detection and Avoidance
7. A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.

## UNIT 2

### PART A

#### **1. What are the functions of MAC?**

MAC sub layer resolves the contention for the shared media. It contains synchronization, flag, flow and error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.

#### **2. What is CSMA?. List the protocols used with CSMA**

CSMA (Carrier Sense Multiple Access)

CSMA is based on the principle "Sense Before Transmit or Listen Before Talk". Each station must listen before transmitting.

##### Types of CSMA Protocols

1. Non-Persistent CSMA
2. 1-Persistent CSMA
3. p-Persistent CSMA

#### **3. Define the term carrier sense in CSMA/CD?**

All the nodes can distinguish between idle and a busy-link and "collision detect" means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

CSMA/CD is Widely used for bus topology LANs (IEEE 802.3, Ethernet).

#### **4. What is the access method used by wireless LAN?**

CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) is the access method used by wireless LAN.

It is Used in a network where collision cannot be detected

#### **5. Define Ethernet**

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

- Uses CSMA/CD technology
- Uses Aloha (packet radio network) as the root protocol
- Ethernet can operate at
  - 100 Mbps (Fast Ethernet)
  - 1000 Mbps (Gigabit Ethernet)

Ethernet also used in full duplex, point-to-point configuration

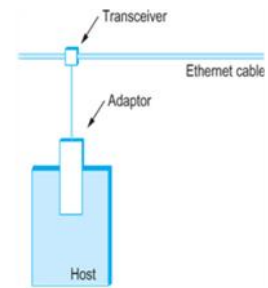
#### **6. What is fast Ethernet and gigabit Ethernet?**

100 Mbps Ethernet is called as Fast Ethernet

1000 Mbps Ethernet is called as Gigabit Ethernet

## 7. What is the use of transceiver?

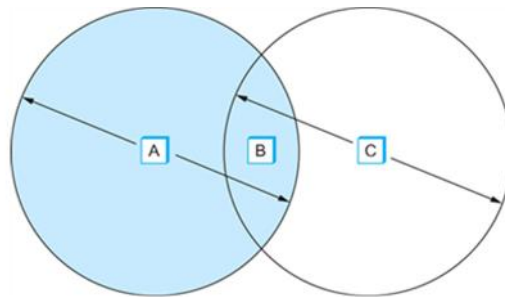
- A transceiver used in Ethernet (a small device directly attached to the tap) detects when the line is idle and drives signal when the host is transmitting.
- The transceiver also receives incoming signal.
- The transceiver is connected to an Ethernet adaptor which is plugged into the host.
- The protocol is implemented on the adaptor.



Ethernet transceiver and adaptor

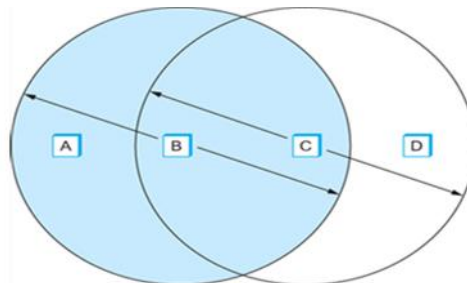
## 8. What is a hidden node and exposed node?

In wireless networking, the **hidden node problem** or **hidden terminal problem** occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP. This leads to difficulties in media access control.



The "Hidden Node" Problem. Although A and C are hidden from each other, their signals can collide at B. (B's reach is not shown.)

In wireless networks, the **exposed node problem** occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter.



C->D progress  
If B->A not possible  
Since C is exposed to B

Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D. (A and D's reaches are not shown.)

## 9. What is a Bluetooth?

Bluetooth fills the niche of very short-range communication between mobile phones, PDAs, notebook computers, and other personal or peripheral devices. For example, Bluetooth can be used to connect mobile phones to a headset, or a notebook computer to a printer.

**10. What are the four prominent wireless technologies?**

- Bluetooth
- Wi-Fi(formally known as 802.11)
- WiMAX(802.16)
- Third generation or 3G cellular wireless.

**11. What are the four steps involves in scanning?**

1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points, and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

**12. What is exponential back off?**

Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again. This strategy of doubling the delay interval between each transmission attempt is a general technique known as exponential back off.

**13. What is the use of switches?**

Such switches are sometimes known by the obvious name of LAN switches

- A mechanism that allows us to interconnect links to form a large network is called switches.
- Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- A multi-input, multi-output device which transfers packets from an input to one or more outputs

**14. Differentiate circuit switching and packet switching**

<b>Circuit switching</b>	<b>Packet switching</b>
The connection between two station is a dedicated path using physical links	Virtual connection is established between two station
Physical layer is responsible	Network layer is responsible
Messages are not packetized and there is a continuous flow of messages	Messages are divided into packets of fixed or variable size
Used in telephone companies	Used in switched WANs such as frame relay and ATM networks

**15. Compare datagram approach and virtual circuit approach.**

<b><i>Datagram approach</i></b>	<b><i>Virtual circuit switching</i></b>
<b><i>Connectionless approach</i></b>	<b><i>Connection-oriented approach</i></b>
Every packet contain enough information ie destination address that enable any switch to decide where the packet has to go.	Uses the concept of <i>virtual circuit</i> (VC). It establishes a VC before transfer begins.
To decide how to forward a packet, a switch consults a <i>forwarding table</i> (sometimes called a <i>routing table</i> )	Refers the VCI to forward the packet
A host can send a packet anywhere at any time,	First set up a virtual connection from the source host to the destination host and then send the data
Each packet is forwarded independently of previous packets that might have been sent to the same destination.	Packets are dependent as it travels through the same path
Any network component failure might not have any serious effect on communication if it is possible to find an alternate route around the failure and update the forwarding table accordingly	Network components failures cause serious effect on communication.
Host to host address is always needed in sending the datagram (Embedded in the datagram itself)	Host to host address is needed in link setup only
Error checking is required by host to resemble the packet and find out the missing packets.	Errors is handled by subnetwork. Host will receive the packets in correct sequence.
messages may be out of order in the communication sub-network	Messages passed in order to the network.

**16. What is a role of VCI?**

- A virtual circuit identifier (VCI) that uniquely identifies the connection at this switch and that will be carried inside the header of the packets that belong to this connection
- An incoming interface on which packets for this VC arrive at the switch
- An outgoing interface in which packets for this VC leave the switch

### 17. What is a bridge? What are the functions of bridges?

It is a collection of LANs connected by one or more bridges is usually said to form an extended LAN. In their simplest variants, bridges simply accept LAN frames on their inputs and forward them out on all other outputs.

#### Functions of bridges (three criteria)

1. Frame filtering or forwarding
2. Learning
3. Avoidance of loops in system

### 18. What is a loop problem in bridges?

Loop Problem Transparent bridges work fine as long as there are no redundant bridges in the system. Systems administrators, however, like to have redundant bridges (more than one bridge between a pair of LANs) to make the system more reliable.

If a bridge fails, another bridge takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable

### 19. How does a given bridge learn whether it should forward a multicast frame over a given port?

It learns exactly the same way that a bridge learns whether it should forward a unicast frame over a particular port- by observing the source addresses that it receives over that port.

### 20. What are the limitations of bridges?

- scale
- heterogeneity

### 21. In what way bridges differs from switches?

Bridge	Switch
Bridges are generally used to connect two LANs( Local Area Networks)	switch is a network device that selects a path or circuit for sending a unit of data to its next destination.
Bridges usually have 2 to 16 ports	Switches are multi port network devices
bridges perform forwarding it in software	Switches perform forwarding in hardware
we need to have router over the Bridge to route the packets to desired destination	A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to.



Bridge is rarely used	Switches are frequently used
Bridge is a device that connects two LANs and controls data flow between them.	Switch is a networking device that learns which machine is connected to its port by using the device's IP address.

**22. What are the advantages of datagram delivery model?**

- ✓ Best-effort, connectionless service
- ✓ simplest service model
- ✓ asking for a reliable packet delivery service may need to include a lot of extra functionality into the router.
- ✓ It enables IP to “run over anything” ie today IP can run over many network technologies
- ✓ Higher level protocols such as TCP that run over IP is aware of all failure modes.

**23. Define IP.**

- IP stands for Internet Protocol
- Key tool used today to build scalable, heterogeneous internetworks
- It runs on all the nodes in a collection of networks and defines the infrastructure that allows these nodes and networks to function as a single logical internetwork
- Has two versions IPv4 and IPv6

**24. Find the class of the following addresses**

- 227.13.14.88.1.1.1 – class B
- 227.13.14.88.1.1.1 – class D

**25. Define subnetting**

Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned.

The idea is to take a single IP network number and allocate the IP addresses with that network number to several physical networks, which are now referred to as subnets.

**26. 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?**

AND operation with IP address and subnet masks gives 25.34.0.0



## 27. Define CIDR

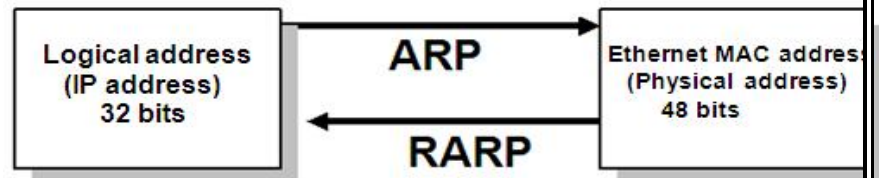
- Classless Inter-Domain Routing (CIDR)
- Do not use classes to determine network ID
- Assign any range of addresses to network
  - Use common part of address as network number
  - E.g., addresses 192.4.16 - 192.4.31 have the first 20 bits in common. Thus, we use these 20 bits as the network number
  - netmask is /20, /xx is valid for almost any xx
- Enables more efficient usage of address space (and router tables)

## 28. What is ARP?

- The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address.
- ARP is used to find the physical address of the node when its Internet address is known.

### ARP operation

1. ARP request
2. ARP reply



## 29. What is DHCP?

- Dynamic Host Configuration Protocol
- DHCP server is responsible for providing configuration information to hosts. There is at least one DHCP server for an administrative domain
- DHCP server maintains a pool of available addresses
- DHCP is a protocol that dynamically assigns IP addresses to host.
- DHCP relies on the existence of a DHCP server which is responsible for providing configuration information to host.
- The use of DHCP avoids the network administrator from assigning addresses to individual host.

## 30. What is ICMP?

- ICMP – Internet Control Message Protocol
- ICMP is used for error and control information
- Defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully
- ICMP always reports error messages to the original source.

ICMP messages are divided into two broad categories:

1. error-reporting messages
2. query messages.