COMPUTER NETWORK- I
IMPORTANT QUESTION

Q1. Explain Nyquist Shanon sampling formula/ theorem.

A1.

- The Nyquist–Shannon sampling theorem, has been named after Harry Nyquist and Claude Shannon.
- It is a fundamental result in the field of information theory, in particular telecommunications and signal processing.
- The Nyquist Theorem, also known as the sampling theorem, is a principle that engineers follow in the digitization of analog signals (means conversion of analog signals to the digital signal).
- The theorem also leads to a formula for reconstruction of the original signal.
- Any analog signal consists of components at various frequencies. The simplest case is the sine wave, in which all the signal energy is concentrated at one frequency.
- In practice, analog signals usually have complex waveforms, with components at many frequencies.
- The highest frequency component in an analog signal determines the bandwidth of that signal. Suppose the highest frequency component, in hertz, for a given analog signal is f_{max}.
- According to the Nyquist Theorem, the sampling rate must be at least $2f_{max}$, or twice the highest analog frequency component.
- The sampling in an analog-to-digital converter is actuated by a pulse generator (clock). If the sampling rate is less than $2f_{max}$, some of the highest frequency components in the analog input signal will not be correctly represented in the digitized output.
- When such a digital signal is converted back to analog form by a digital-to-analog converter, false frequency components appear that were not in the original analog signal.
- This undesirable condition is a form of distortion called aliasing.

Q2. Explain CRC method for error detection.

A2.

- Cyclic redundancy checking is a method of checking for errors in data that has been transmitted on a communications link.
- A sending device applies a 16- or 32-bit polynomial to a block of data that is to be transmitted and appends the resulting cyclic redundancy code (CRC) to the block.
- The receiving end applies the same polynomial to the data and compares its result with the result appended by the sender.
- If they agree, the data has been received successfully. If not, the sender can be notified to resend the block of data.
- The ITU-TS (CCITT) has a standard for a 16-bit polynomial to be used to obtain the cyclic redundancy code (CRC) that is appended.
- IBM's Synchronous Data Link Control and other protocols use CRC-16, another 16-bit polynomial.
- A 16-bit cyclic redundancy code detects all single and double-bit errors and ensures detection of 99.998% of all possible errors.
- For larger transmissions, a 32-bit CRC is used. The Ethernet and token ring local area network protocols both used a 32-bit CRC.
- A less complicated but less capable error detection method is the checksum method.
- **(FOLLOW CLASS NOTES).**

Q3. Explain the concept of selective repeat ARQ.

A3.

- Selective Repeat ARQ / Selective Reject ARQ also known as a specific instance of the Automatic Repeat-Request (ARQ) protocol used to solve sequence number problem in communications.
- Selective Repeat is a connection oriented protocol in which both transmitter and receiver have a window of sequence numbers.

Q4. Explain the concept of Ethernet cabling.

A4. Ethernet cable is one of the most popular forms of network cable used on wired networks. Ethernet cables connect devices on local area networks such as PCs, routers and switches.

Proper Ethernet cables will have :

1. An 8-pin RJ45 connector on each end (not the 4 or 6 pin connectors often used on telephone cables)
2. Printed text along the cable indicating that it complies with the Ethernet standard.

In practice, the Ethernet standard has been around since the 1970's and has gone through many evolution cycles. Currently, 3 categories of Ethernet cable are in common use :

1. "**Cat 5**" : Now obsolete, ok for speeds up to 100Mbps.
2. "**Cat 5e**" : Good for speeds up to 1Gbps.
3. "**Cat 6**" : Good for speeds up to 1Gbps, and may support higher speeds as new Ethernet standards evolve.

CABLE MAKING PRACTICAL YOU HAVE DONE IN LAB…..EXPLAIN TYPES OF CABLING (i.e. straight cabling & cross over cabling)

Q5. Explain IPV6.

A5.

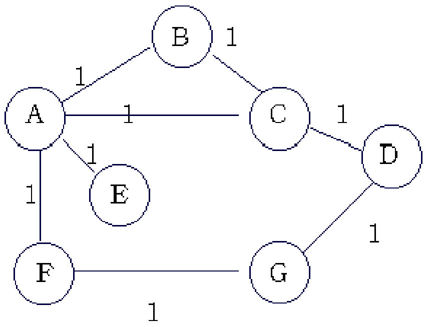
- Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP).
- It the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
- IPv6 was developed by the Internet Engineering Task Force (IETF).
- For practical purposes, IPv6 addresses are not human readable or memorable.
- Pv6 uses a 128-bit address, allowing 2^{128}.
- They have the form : x:x:x:x:x:x:x:x, where each ‘x’ is a value that can be between 0 and 4 hexadecimal digits long. For example: 2620:0:2ef0:7040:250:60ff:fe03:32b9
- The format and length of IPv6 addresses differs from one address to another.
- This complexity of the syntax will make it impossible to handle managing IP address space using a simple spreadsheet – it will simply not work.\
- IPv6 address boundaries are much more difficult to manage.

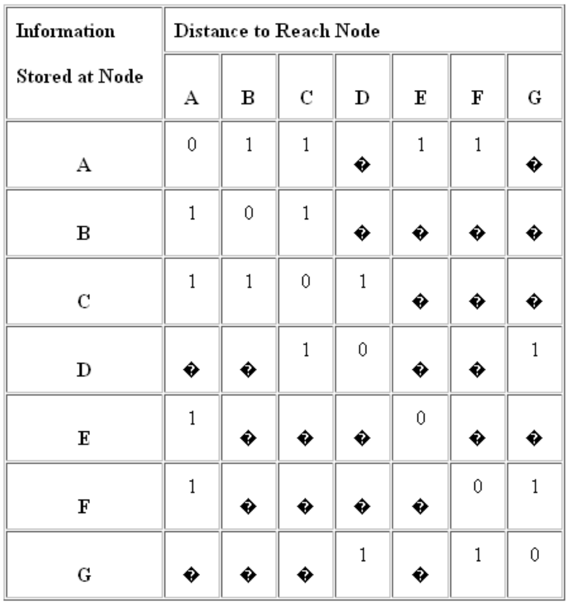
Q6. Explain distance vector routing.

A6.

- In distance vector routing each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.
- The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
- A link that is down is assigned an infinite cost.

Example





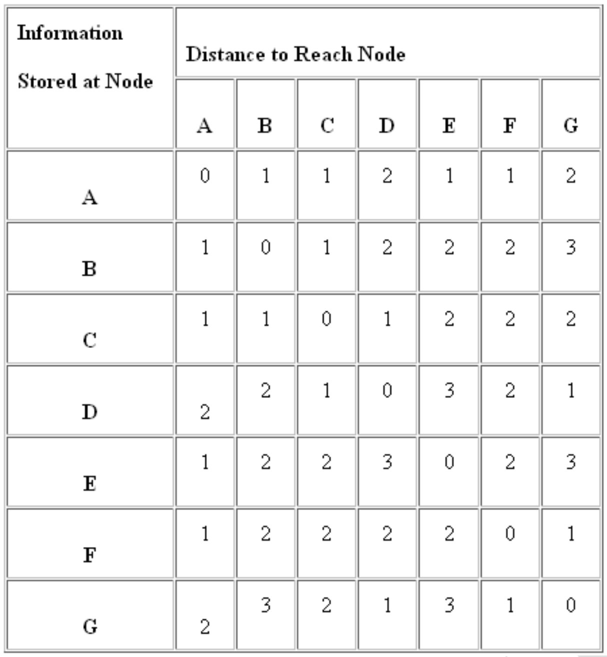
Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	�	1	1	�
B	1	0	1	�	�	�	�
C	1	1	0	1	�	�	�
D	�	�	1	0	�	�	1
E	1	�	�	�	0	�	�
F	1	�	�	�	�	0	1
G	�	�	�	1	�	1	0

Table 1. Initial distances stored at each node (global view).

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Note that each node only knows the information in one row of the table.

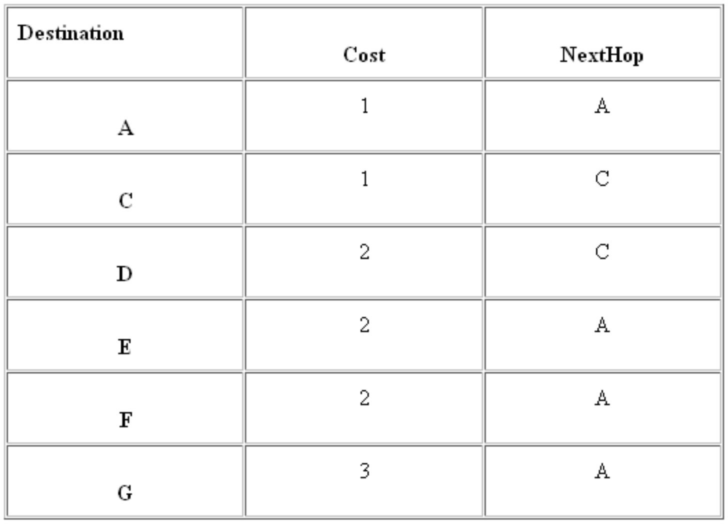
1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, **A** sends its information to its neighbors **B,C,E**, and **F**.)
2. If any of the recipients of the information from **A** find that **A** is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through **A**. (node **B** learns from **A** that node **E** can be reached at a cost of 1; **B** also knows it can reach **A** at a cost of 1, so it adds these to get the cost of reaching **E** by means of **A**. **B** records that it can reach **E** at a cost of 2 by going through **A**.)
3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, **B** knows that it was **A** who said " I can reach **E** in one hop" and so **B** puts an entry in its table that says " To reach **E**, use the link to **A**.)



Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Table 2. final distances stored at each node (global view).

In practice, each node's forwarding table consists of a set of triples of the form:
(Destination, Cost, NextHop).
For example, Table 3 shows the complete routing table maintained at node B for the network in figure1.



Destination	Cost	NextHop
A	1	A
C	1	C
D	2	C
E	2	A
F	2	A
G	3	A

Table 3. Routing table maintained at node B.

Q7. Explain Manchester encoding scheme.
A7.

- Manchester encoding is a synchronous clock encoding technique used by the physical layer to encode the clock and data of a synchronous bit stream.
- In this technique, the actual binary data to be transmitted over the cable are not sent as a sequence of logic 1's and 0's.
- Instead, the bits are translated into a slightly different format that has a number of advantages over using straight binary encoding.
- In the Manchester encoding shown, a logic 0 is indicated by a 0 to 1 transition at the centre of the bit and a logic 1 is indicated by a 1 to 0 transition at the centre of the bit.

- Note that signal transitions do not always occur at the 'bit boundaries' (the division between one bit and another), but that there is always a transition at the centre of each bit.
- The Manchester encoding rules are summarized below:

Original Data	Value Sent
Logic 0	0 to 1 (upward transition at bit centre)
Logic 1	1 to 0 (downward transition at bit centre)

Q8. Explain subnetting.
A8.

- A subnetwork, or subnet, is a logically visible subdivision of an IP network.
- The practice of dividing a network into two or more networks is called subnetting.
- Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security.
- The most common reason is to control network traffic.
- In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment.
- Applying a subnet mask to an IP address allows you to identify the network and node parts of the address.
- The network bits are represented by the 1s in the mask, and the node bits are represented by the 0s.
- Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address or Number.
- For example, using our test IP address and the default Class B subnet mask, we get:

```
10001100.10110011.11110000.11001000     140.179.240.200   Class B IP Address
11111111.11111111.00000000.00000000     255.255.000.000   Default Class B Subnet Mask
--------------------------------------------------------
10001100.10110011.00000000.00000000     140.179.000.000   Network Address
```

Default subnet masks:

- Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000
- Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000
- Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

Q9. Binary Exponential Backoff Algorithm
A9.

- Exponential backoff is an algorithm that uses feedback to multiplicatively decrease the rate of some process, in order to gradually find an acceptable rate.
- In a single channel contention based medium access control (MAC) protocols, whenever more than one station or node tries to access the medium at the same instant of time, it leads to packet collisions.
- If the collided stations tries to access the channel again, the packets will collide as the nodes are synchrozied in time.
- So the nodes need to be displaced in time. To displace them temporally, a backoff algorithm is used (example binary exponential backoff (BEB)).
- For example, in BEB algorithm, whenever a node's transmission is involved in a collision with another node's transmission, both nodes will choose a random waiting time and wait for this amount of time before attempting again.

- If they are not successful in this attempt, they double their contention window and choose a random waiting time before transmitting again.
- This process will be repeated for certain number of attempts.
- If the nodes are not successful in their transmission after this limit, the packets will be dropped from their queue.

Q10. What are data link protocols for noiseless and noisy channels?
A10.

NOISELESS CHANNELS

Let us first assume we have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel. The first is a protocol that does not use flow control; the second is the one that does. Of course, neither has error control because we have assumed that the channel is a perfect noiseless channel.

i) Simplest Protocol

Our first protocol, which we call the Simplest Protocol for lack of any other name, is one that has no flow or error control. Like other protocols we will discuss in this chapter, it is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver. We assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately. In other words, the receiver can never be overwhelmed with incoming frames.

ii) Stop-and-Wait Protocol

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming overwhelmed with frames,we somehow need to tell the sender to slow down. There must be feedback from the receiver to the sender. The protocol we discuss now is called the Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame. We still have unidirectional communication for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction. We add flow control to our previous protocol.

NOISY CHANNELS

Although the Stop-and-Wait Protocol gives us an idea of how to add flow control to its predecessor, noiseless channels are nonexistent. We can ignore the error (as we sometimes do), or we need to add error control to our protocols. We discuss three protocols in this section that use error control.

i) Stop-and-Wait Automatic Repeat Request

Stop-and-Wait Automatic Repeat Request (Stop-and Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol. To detect and correct corrupted frames, we need to add redundancy bits to our data frame . When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver. Lost frames are more difficult to handle than corrupted ones. In previous protocols, there was no way to identify a frame. The received frame could be the correct one, or a duplicate, or a frame out of order. The solution is to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated. The comlpted and lost frames need to be resent in this protocol. The sender keeps a copy of the sent frame. At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted. Since the protocol uses the stop-and-wait mechanism, there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.

ii) Go-Back-N Automatic Repeat Request

To improve the efficiency of transmission (filling the pipe), multiple frames must be in transition while waiting for acknowledgment. In other words, we need to let more than one frame be outstanding to keep the channel busy while the sender is waiting for acknowledgment. In this section, we discuss one protocol that can achieve this goal; in the next section, we discuss a second. The first is called Go-Back-N Automatic Repeat Request (the rationale for the name will become clear later). In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Q11. Explain CSMA & its protocols
A11.

- CSMA stands for Carrier Sensed Multiple Access (CSMA)
- CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting.
- MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.
- CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance.
- CSMA protocol is based on the principle of 'carrier sense'.
- The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.
- Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time.
- On large networks, the transmission time between one end of the cable and another is enough that one station may access the cable even though another has already just accessed it.
- The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.
- There Are Three Different Type of CSMA Protocols
  (i) I-persistent CSMA
  (ii) Non- Persistent CSMA
  (iii) p-persistent CSMA

(i) I-persistent CSMA

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start allover again.

(ii) Non-persistent CSMA

- 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.
- After this time, it again checks the status of the channel and if the channel is free it will transmit.
- A station that has a frame to send senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

iii) p-persistent CSMA

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- Whenever a station becomes ready to send, it senses the channel.
- If channel is busy, station waits until next slot.
- If channel is idle, it transmits with a probability p.
- With the probability q=l-p, the station then waits for the beginning of the next time slot.
- If the next slot is also idle, it either transmits or waits again with probabilities p and q.
- This process is repeated till either frame has been transmitted or another station has begun transmitting.
- In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

GO THROUGH FOLLOWING PROTOCOLS

PPP- Point to point protocol

- PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.
- For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.
- PPP uses the Internet protocol (IP) (and is designed to handle others).
- It is sometimes considered a member of the TCP/IP suite of protocols.
- Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service.
- Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.
- PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission.
- It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.
- PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication.
- PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

SMTP- Simple Mail Transfer protocol

- SMTP stands for Simple Mail Transfer Protocol.

- It's a set of communication guidelines that allow software to transmit email over the Internet.
- Most email software is designed to use SMTP for communication purposes when sending email, and it only works for outgoing messages.
- When people set up their email programs, they will typically have to give the address of their Internet service provider's SMTP server for outgoing mail.
- There are two other protocols - POP3 and IMAP - that are used for retrieving and storing email.
- SMTP provides a set of codes that simplify the communication of email messages between servers.
- The other purpose of SMTP is to set up communication rules between servers.
- There are also ways to handle errors, including common things like incorrect email addresses.
- In a typical SMTP transaction, a server will identify itself, and announce the kind of operation it is trying to perform.
- The other server will authorize the operation, and the message will be sent
- SMTP was created in the early 1980's and it was built around basic concepts of server communication that go back to the 1970's.
- The greatest strengths of SMTP are reliability and simplicity. It's easy to set up software that uses the SMTP communication rules.
- Messages either get to a recipient, or there is an error message that explains why that wasn't possible.
- Most servers these days actually us a slightly updated version of the SMTP protocol called ESMTP (Extended Simple Mail Transfer Protocol).
- This was created to allow transmission of multimedia through email.
- When **someone sends** a picture or music file through their email program, ESMTP communication codes are used to identify the kind of data being transferred.

FTP- File Transfer Protocol

- File transfer protocol is used for exchanging files over the Internet.
- FTP works in the same way as HTTP for transferring Web pages from a server to a user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies.
- FTP uses the Internet's TCP/IP protocols to enable data transfer.
- FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (e.g., uploading a Web page file to a server).

Do Yourself-
IP, DHCL, POP3, TCP, UDP, HTTP, HDLC, SLIP

Q. Difference between TCP & UDP

A.

S. NO.	TRANSMISSION CONTROL PROTOCOL	USER DATAGRAM PROTOCOL
1	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
2	**In this** a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based .
3	TCP is suited for applications that require high reliability, and less transmission time.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.

4	Examples of TCP are HTTP, HTTPs, FTP, SMTP, Telnet	Examples of UDP are DNS, DHCP, TFTP, SNMP, RIP, VOIP.
5	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
6	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
7	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.
8	TCP header size is 20 bytes	UDP Header size is 8 bytes.
9	TCP is heavy-weight. TCP handles reliability and congestion control.	UDP is lightweight. It is a small transport layer designed on top of IP.
10	TCP requires three packets to set up a socket connection, before any user data can be sent.	There is no ordering of messages, no tracking connections, etc.
11	TCP does Flow Control. TCP handles reliability and congestion control.	UDP does not have an option for flow control
12	TCP does error checking	UDP does error checking, but no recovery options.
13	Hanshaking method is followed SYN, SYN-ACK, ACK	No handshake (connectionless protocol)
14	Acknowledgement segments are there	No Acknowledgement segments are there

Some more important questions….

Q. Explain link state routing.
Q. Explain static & dynamic channel allocation.
Q. What are the principles of congestion control.
Q. What are the various congestion control policies followed?

ALL THE BEST