# DHANALAKSHMI SRINIVASAN INSTITUTE OF RESEARCH AND TECHNOLOGY-SIRUVACHUR
# CS6551-COMPUTER NETWORKS

## PART-A (2 MARKS)

### UNIT-I

**1. What are the three criteria necessary for an effective and efficient network?**

The most important criteria are performance, reliability and security.Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w.Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe.
Security issues include protecting data from unauthorized access and viruses.

**2. Group the OSI layers by function?**

The seven layers of the OSI model belonging to three subgroups.Physical, data link and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another.Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems.The transport layer ensures end-to-end reliable data transmission.

**3. What are header and trailers and how do they get added and removed?**

Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer are taken.

**4. What are the features provided by layering?**
Two nice features:

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

**5. Why are protocols needed?**

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

**6. What are the two interfaces provided by protocols?**

- Service interface
- Peer interface

Service interface- defines the operations that local objects can perform on the protocol.

Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

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

- Twisted pair(the wire that your phone connects to)
- Coaxial cable(the wire that your TV connects to)
- Optical fiber(the medium most commonly used for high-bandwidth, long-distance links)
- Space(the stuff that radio waves, microwaves and infra red beams propagate through)

**8. Define Signals?**

Signals are actually electromagnetic waves traveling at the speed of light. The speed of light is, however, medium dependent-electromagnetic waves traveling through copper and fiber do so at about two-thirds the speed of light in vacuum.

**9. What is wave's wavelength?**

The distance between a pair of adjacent maxima or minima of a wave, typically measured in meters, is called wave's wavelength.

**10. Define Modulation?**

Modulation -varying the frequency, amplitude or phase of the signal to effect the transmission of information. A simple example of modulation is to vary the power (amplitude) of a single wavelength.

**11. Explain the two types of duplex?**

- Full duplex-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
- Half duplex-it supports data flowing in only one direction at a time.

**12. What is CODEC?**
A device that encodes analog voice into a digital ISDN link is called a CODEC, for coder/decoder.

**13. What is spread spectrum and explain the two types of spread spectrum?**
Spread spectrum is to spread the signal over a wider frequency band than normal in such a way as to minimize the impact of interference from other devices.
- Frequency Hopping
- Direct sequence

**14. What are the different encoding techniques?**
- NRZ
- NRZI
- Manchester
- 4B/5B

**15.  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.

**16. 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.

**17. What are the ways to address the framing problem?**
- Byte-Oriented Protocols(PPP)
- Bit-Oriented Protocols(HDLC)
- Clock-Based Framing(SONET)

**18. Distinguish between peer-to-peer relationship and a primary-secondary relationship. peer -to- peer relationship?**

All the devices share the link equally.Primary-secondary relationship: One device controls traffic and the others must transmit through it.

## 19. Mention the types of errors and define the terms?
There are 2 types of errors

- Single-bit error.
- Burst-bit error.

Single bit error: The term single bit error means that only one bit of a given data unit (such as byte character/data unit or packet) is changed from 1 to 0 or from 0 to 1.

Burst error:  Means that 2 or more bits in the data unit have changed from 1 to 0 from 0 to 1.

## 20.  List out the available detection methods.
There are 4 types of redundancy checks are used in data communication.

- Vertical redundancy checks (VRC).
- Longitudinal redundancy checks (LRC).
- Cyclic redundancy checks (CRC).
- Checksum.

## 21. Write short notes on VRC.
The most common and least expensive mechanism for error detection is the vertical redundancy check (VRC) often called a parity check. In this technique a redundant bit called a parity bit, is appended to every data unit so, that the total number of 0's in the unit (including the parity bit) becomes even.

## 22. Write short notes on LRC.
In longitudinal redundancy check (LRC), a block of bits is divided into rows and a redundant row of bits is added to the whole block.

## 23. Write short notes on CRC.
The third and most powerful of the redundancy checking techniques is the cyclic redundancy checks (CRC) CRC is based on binary division. Here a sequence of redundant bits, called the CRC remainder is appended to the end of data unit.

## 24. Write short notes on CRC checker.
A CRC checker functions exactly like a generator. After receiving the data appended with the CRC it does the same modulo-2 division. If the remainder is all

0's the CRC is dropped and the data accepted. Otherwise, the received stream of bits is discarded and the dates are resent.

### 25. Define checksum.

The error detection method used by the higher layer protocol is called checksum. Checksum is based on the concept of redundancy.

### 26. What are the steps followed in checksum generator?

The sender follows these steps a) the units are divided into k sections each of n bits. b) All sections are added together using 2's complement to get the sum. c) The sum is complemented and become the checksum. d) The checksum is sent with the data.

### 27. Mention the types of error correcting methods.

There are 2 error-correcting methods.

- Single bit error correction
- Burst error correction.

### 28. Write short notes on error correction?

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

- When an error is discovered, the receiver can have the sender retransmit the entire data unit.
- A receiver can use an error correcting coder, which automatically corrects certain errors.

### 29. What is the purpose of hamming code?

A hamming code can be designed to correct burst errors of certain lengths. So the simple strategy used by the hamming code to correct single bit errors must be redesigned to be applicable for multiple bit correction.

### 30. 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.

### 31. 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.

### 32. 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.

### 33. What is a buffer?

Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.

## UNIIT-II

### 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 are the functions of LLC?

The IEEE project 802 models take the structure of an HDLC frame and divides it into 2 sets of functions. One set contains the end user portion of the HDLC frame – the logical address, control information, and data. These functions are handled by the IEEE 802.2 logical link control (LLC) protocol.

### 3. What is Ethernet?

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

### 4. 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.

### 5. Define Repeater?

A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals. However, no more than four repeaters may be positioned between any pairs of hosts, meaning that an Ethernet has a total reach of only 2,500m.

### 6. Define collision detection?

In Ethernet, all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision detection.

**7. Why Ethernet is said to be a I-persistent protocol?**
An adaptor with a frame to send transmits with probability '1 'whenever a busy line goes idle.

**8. 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.

**9. What is token holding time (THT)?**
It defines that how much data a given node is allowed to transmit each time it possesses the token or equivalently, how long a given node is allowed to hold the token.

**10. What are the two classes of traffic in FDDI?**
- Synchronous
- Asynchronous

**11. What are the four prominent wireless technologies?**
- Bluetooth
- Wi-Fi(formally known as 802.11)
- WiMAX(802.16)
- Third generation or 3G cellular wireless.

**12. Define 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.

**13. 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.

## 14. Explain the term handoff?

If the phone is involved in a call at the time , the call must be transferred to the new base station in what is called a hand off.

## 15. Define satphones?

Satphones use communication satellites as base stations, communicating on frequency bands that have been reserved internationally for satellite use.

## 16. How to mediate access to a shared link?

Ethernet,token ring, and several wireless protocols. Ethernet and token ring media access protocols have no central arbitrator of access. Media access in wireless networks is made more complicated by the fact that some nodes may be hidden from each other due to range limitations of radio transmission.

## 17. Define Aggregation points?

It collects and processes the data they receive from neighboring nodes, and then transmit the processed data. By processing the data incrementally, instead of forwarding all the raw data to the base station, the amount of traffic in the network is reduced.

## 18. Define Beacons?

Beacon to determine their own absolute locations based on GPS or manual configuration. The majority of nodes can then derive their absolute location by combining an estimate of their position relative to the beacons with the absolute location information provided by the beacons.

## 19. What is the use of Switch?

It is used to forward the packets between shared media LANs such as Ethernet. Such switches are sometimes known by the obvious name of LAN switches.

## 20. Explain Bridge?

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.

## 21. What is Spanning tree?

It is for the bridges to select the ports over which they will forward frames.

**22. What are the three pieces of information in the configuration messages?**
      1. The ID for the bridge that is sending the message.
      2. The ID for what the sending bridge believes to the root bridge.
      3. The distance, measured in hops, from the sending bridge to the root bridge.

**23. What is broadcast?**
Broadcast is simple – each bridge forwards a frame with a destination broadcast address out on each active (selected) port other than the one on which the frame was received.

**24. What is multicast?**
It can be implemented with each host deciding for itself whether or not to accept the message.

**25. 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.

**26. What are the limitations of bridges?**
- scale
- heterogeneity

## UNIT-III

**1. Define packet switching?**
A packet switch is a device with several inputs and outputs leading to and from the hosts that the switch interconnects.

**2. What is a virtual circuit?**
A logical circuit made between the sending and receiving computers. The connection is made after both computers do handshaking. After the connection, all packets follow the same route and arrive in sequence.

**3. What are data grams?**
      In datagram approach, each packet is treated independently from all others. Even when one packet represents just a place of a multi packet transmission, the

network treats it although it existed alone. Packets in this technology are referred to as datagram.

**4. What is meant by switched virtual circuit?**

Switched virtual circuit format is comparable conceptually to dial-up line in circuit switching. In this method, a virtual circuit is created whenever it is needed and exits only for the duration of specific exchange.

**5. What is meant by Permanent virtual circuit?**

Permanent virtual circuits are comparable to leased lines in circuit switching. In this method, the same virtual circuit is provided between two uses on a continuous basis. The circuit is dedicated to the specific uses.

**6. What are the properties in star topology?**

- Even though a switch has a fixed number of inputs and outputs, which limits the number of hosts that can be connected to a single switch , large networks can be built by interconnecting a number of switches.
- We can connect switches to each other and to hosts using point-to point links, which typically means that we can build networks of large geographic scope.

**7. What is VCI?**

A Virtual Circuit Identifier that uniquely identifies the connection at this switch, and which will be carried inside the header of the packets that belongs to this connection.

**8. What is hop-by-hop flow control?**

Each node is ensured of having the buffers it needs to queue the packets that arrive on that circuit. This basic strategy is usually called hop-by-hop flow control.

**9. Explain the term best-effort?**

If something goes wrong and the packet gets lost, corrupted, misdelivered, or in any way fails to reach its intended destination, the network does nothing.

**10. What is maximum transmission unit?**

MTU- which is the largest IP datagram that it can carry in a frame .

**11. Define Routing?**

It is the process of building up the tables that allow thwe collect output for a packet to be determined.

**12. Define ICMP?**
Internet Control Message Protocol is 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

**13. Write the keys for understanding the distance vector routing?**
The three keys for understanding the algorithm are,
- Knowledge about the whole networks
- Routing only to neighbors
- Information sharing at regular intervals

**14. Write the keys for understanding the link state routing?**
The three keys for understanding the algorithm are,
- Knowledge about the neighborhood.
- Routing to all neighbors.
- Information sharing when there is a range.

**15. How the packet cost referred in distance vector and link state routing?**
In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

**16. Define Reliable flooding?**
It is the process of making sure that all the nodes participating in the routing protocol get a copy of the link state information from all the other nodes.

**17. What are the features in OSPF?**
- Authentication of routing messages.
- Additional hierarchy.
- Load balancing.

**18. 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 address with that network to several physical networks, which are now referred to as subnets.

**19. What are the different types of AS?**

- Stub AS
- Multi homed AS
- Transit AS

## 20. What is an Area?

An Area is a set of routers that are administratively configured to exchange link-state information with each other. There is one special area- the backbone area, also known as area 0.

## 21. What is Source Specific Multicast?

SSM , a receiving host specifies both a multicast group and a specific host .the receiving host would then receive multicast addressed to the specified group, but only if they are from the special sender.

## 22. What is meant by congestion?

Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources.

## 23. Why the congestion occurs in network?

Congestion occurs because the switches in a network have a limited buffer size to store arrived packets.

## 24. What are the rules of non boundary-level masking?

- The bytes in the IP address that corresponds to 255 in the mask will be repeated in the sub network address
- The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address
- For other bytes, use the bit-wise AND operator.

## 25. What is LSP?

In link state routing, a small packet containing routing information sent by a router to all other router by a packet called link state packet.

## UNIT-IV

## 1. Explain the main idea of UDP?

The basic idea is for a source process to send a message to a port and for the destination process to receive the message from a port.

**2. What are the different fields in pseudo header?**
- Protocol number
- Source IP address
- Destination IP addresses.

**3. Define TCP?**

TCP guarantees the reliable, in order delivery of a stream of bytes. It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.

**4. Define Congestion Control?**

It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

**5. State the two kinds of events trigger a state transition?**
- A segment arrives from the peer.
- The local application process invokes an operation on TCP.

**6. What is meant by segment?**

At the sending and receiving end of the transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment.

**7.  What is meant by segmentation?**

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.

**8. What is meant by Concatenation?**

The size of the data unit belonging to single sessions are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combining process is called concatenation.

**9. What is rate based design?**

Rate- based design, in which the receiver tells the sender the rate-expressed in either bytes or packets per second – at which it is willing to accept incoming data.

**10. Define Gateway.**
A device used to connect two separate networks that use different communication protocols.

**11. What is meant by quality of service?**
The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

**12. What are the two categories of QoS attributes?**
The two main categories are,
- User Oriented
- Network Oriented

**13. List out the user related attributes?**
User related attributes are SCR – Sustainable Cell Rate PCR – Peak Cell Rate MCR- Minimum Cell Rate CVDT – Cell Variation Delay Tolerance.

**14. What are the networks related attributes?**
The network related attributes are, Cell loss ratio (CLR) Cell transfer delay (CTD) Cell delay variation (CDV) Cell error ratio (CER).

**15. What is RED?**
Random Early Detection in each router is programmed to monitor its own queue length and when it detects that congestion is imminent, to notify the source to adjust its congestion window.

**16. What are the three events involved in the connection?**
For security, the transport layer may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:
- Connection establishment
- Data transfer
- Connection release

**17.What is Silly Window Syndrome?**
If the sender or the receiver application program processes slowly and can send only 1 byte of data at a time, then the overhead is high.This is because to send

one byte of data, 20 bytes of TCP header and 20 bytes of IP header are sent. This is called as silly window syndrome.

## UNIT-V

**1. What is the function of SMTP?**

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based
on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

**2. What is the difference between a user agent (UA) and a mail transfer agent (MTA)?**

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.
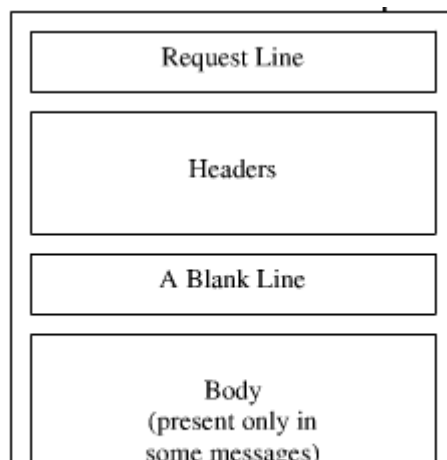
**3. How does MIME enhance SMTP?**

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and deliverers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

4. **Why is an application such as POP needed for electronic messaging?**

Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol, version 3(POP3). Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

5. Give                        the format of HTTP request message?

| |
|---|
| Request Line |
| Headers |
| A Blank Line |
| Body (present only in some messages) |

**6**. **What is the purpose of Domain Name System?**

Domain Name System can map a name to an address and conversely an address to name.

**7. Discuss the three main division of the domain name space**.

Domain name space is divided into three different sections: generic domains, country domains & inverse domain.
Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.
Country domain: Uses two characters to identify a country as the last suffix.
Inverse domain: Finds the domain name given the IP address.

**8. Discuss the TCP connections needed in FTP.**

FTP establishes two connections between the hosts. One connection is used for data transfer, the other for control information. The control connection uses very simple rules of communication. The data connection needs more complex rules due to the variety of data types transferred.

**9. Discuss the basic model of FTP.**

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

**10. Name four factors needed for a secure network?**

Privacy: The sender and the receiver expect confidentiality.
Authentication: The receiver is sure of the sender's identity and that an imposter has not sent the message.
Integrity: The data must arrive at the receiver exactly as it was sent.
Non-Reputation: The receiver must able to prove that a received message came from a specific sender.

**11. How is a secret key different from public key?**

In secret key, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In public key, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

## 12. What is a digital signature?

Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank. In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

## 13. What are the advantages & disadvantages of public key encryption?

Advantages:

a) Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.

b) The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantage:

If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

## 14. What are the advantages & disadvantages of secret key encryption?

Advantage:

Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages:

a) Each pair of users must have a secret key. If N people in world want to use this method, there needs to be N (N-1)/2 secret keys. For one million people to communicate, a half-billion secret keys are needed.

b) The distribution of the keys between two parties can be difficult.

## 15. Define permutation.

Permutation is transposition in bit level.

Straight permutation: The no. of bits in the input and output are preserved.

Compressed permutation: The no. of bits is reduced (some of the bits are dropped).

Expanded permutation: The no. of bits is increased (some bits are repeated).

## 16. Define substitution & transposition encryption?

.       Substitution: A character level encryption in which each character is replaced by another character in the set.

Transposition: A Character level encryption in which the characters retain their plaintext but the position of the character changes.

## 17. Define CGI?

.       CGI is a standard for communication between HTTP servers and executable programs. It is used in crating dynamic documents.

## 18. What are the requests messages support SNMP and explain it?

- GET
- SET

The former is used to retrieve a piece of state from some node and the latter is used to store a new piece of state in some node.
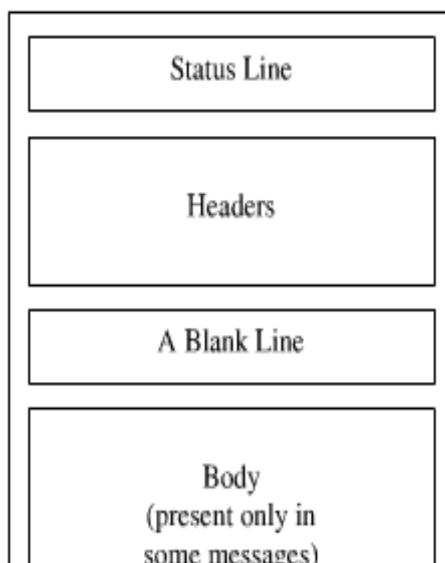
## 19. Define PGP?

Pretty Good Privacy is used to provide security for electronic mail. It provides authentication, confidentiality, data integrity, and non repudiation.

## 20. Define SSH?

Secure Shell is used to provide a remote login, and used to remotely execute commands and transfer files and also provide strong client/server authentication / message integrity.

## 21. Give the format of HTTP response message?

| |
|---|
| Status Line |
| Headers |
| A Blank Line |
| Body (present only in some messages) |

**22. What is the difference between service point address, logical address and physical address? Service point addressing Logical addressing Physical addressing**

| Service point addressing | Logical addressing | Physical addressing |
|---|---|---|
| The transport layer header includes a type of address called a service point address or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer. | If a packet passes the network boundary we need another addressing to differentiate the source and destination systems. The network layer adds a header, which indicate the logical address of the sender and receiver. | If the frames are to be distributed to different systems on the network, the data link layer adds the header, which defines the source machine' s address and the destination Machine' s address. |

**21. Discuss the basic model of FTP.**

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

## 22.What is a digital signature?

Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank. In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

## 23.Draw the diagram foe explain security
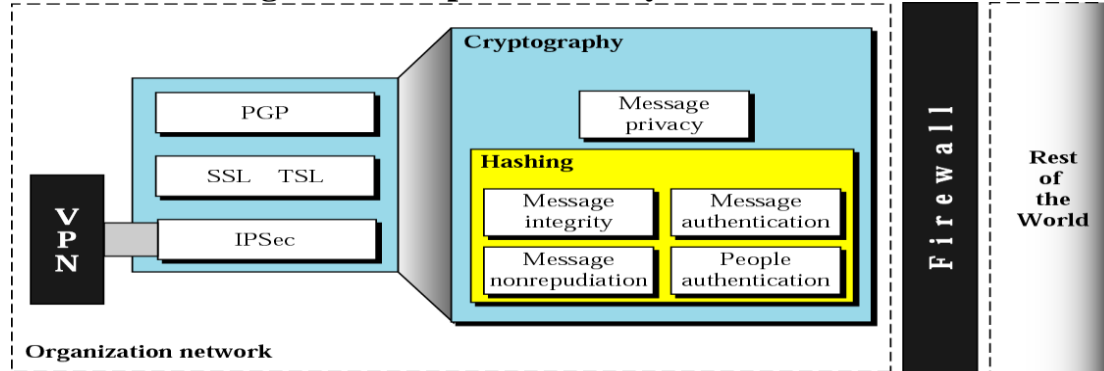


## 24. Define Cryptography
- Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks.

- Original message before being transformed is called **plaintext**.

- After the message is transformed, is called **ciphertext**.

- An encryption algorithm transforms the plaintext to ciphertext; a decryption algorithm transforms the ciphertext back to plaintext.

- The term cipher is used to refer to encryption and decryption algorithms.

## 25. What are the types of DNS Message
- Two types of messages

Query: header and question records

■ Response: Header, question records, answer records, authoritative records, and additional records.

## 26. What is TELNET PROTOCOL?

A TELNET connection is a Transmission Control Protocol (TCP)    connection used to transmit data with interspersed TELNET control information.

The TELNET Protocol is built upon three main ideas:  first, the    concept of a "Network Virtual Terminal"; second, the principle of    negotiated options; and third, a symmetric view of terminals and    processes.

## 27. What is PGP?

Pretty Good Privacy. A program using public key encryption popularly used with email

A high security RSA public-key encryption application for MS-DOS, Unix, VAX/VMS, and other computers. It was written by Philip R. Zimmermann  of Phil's Pretty Good(tm) Software and later augmented by a cast of thousands, especially including Hal Finney, Branko Lankester, and Peter Gutmann.

## 28. What is POP3?

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet.

## 29. What is IMAP.

IMAP (Internet Message Access Protocol) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP Version 4) is a client/server protocol in which e-mail is received and held for you by your Internet server.

IMAP can be thought of as a remote file server. POP3 can be thought of as a "store-and-forward" service.

## 30. What is SSH?

(**S**ecure **Sh**ell) A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs. Also serving as a secure client/server connection for applications such as database access and e-mail SSH supports a variety of authentication methods.