UNIT-I

1. What are called network support layers?

   The physical, data link, and network layers are the network support layers

2. What are called User support layers?

   The session, presentation, and application layers are the user support layers

3. Why we need Transport layer?

   The transport layer links the network support layers and the user support layers.

4. What is the purpose of Physical layer?

   The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

5. What is the use of Data link layer?

   The data link layer is responsible for delivering data units from one station to the next without errors.

6. What is the need for Network layer?

   The network layer is responsible for the source-to-destination delivery of a packet across multiple network links.

7. What is subnetting?

   Subnetting divides one large network into several smaller ones. Subnetting adds an intermediate level of hierarchy in IP addressing.

8. What is meant by masking ?

   Masking is a process that extracts the network address from an IP address. Subnet masking is a process that extracts the subnetwork address from an IP address. A network or subnet address is obtained from applying the bit-wise AND operation on the IP address and the mask.

9. What is supernetting?

   Supernetting combines several networks into one large one.

10. What is meant by connectionless protocol?

The IP protocol is a connectionless protocol. Every packet is independent and has no relationship to any other packet.

11. What is direct delivery?

The delivery of a packet is called direct if the deliverer (host or router) and the destination are on the same network.

12. What is indirect delivery?

The delivery of a packet is called indirect if the deliverer (host or router) and the destination are on different networks

13. What is the function of routing table?

Every host or router has a routing table to route IP packets. In next hop routing instead of a complete list of the stops the packet must make only the address of the next hop is listed in the routing table. In network specific routing all hosts on a network share one entry in the routing table. In host specific routing the full IP address of a host is given in the routing table. In default routing, a router is assigned to receive all packets with no match in the routing table.

14. What is static and dynamic routing?

A static routing table's entries are updated manually by an administrator. A dynamic routing table's entries are updated automatically by a routing protocol.

15. What are the fields included in routing table?

The routing table can consist of seven fields: a mask, a destination address, a next-hop address, flags, a reference count, a use, and an interface. The routing module applies the mask, row by row, to the received destination address until a match is found. Classless addressing requires hierarchical and geographical routing to prevent immense routing tables.

16. What is the maximum length of a datagram?

The maximum length of a datagram is 65,535 bytes.

17. What is Maximum Transfer Unit?

The MTU is the maximum number of bytes that a data link protocol can encapsulate. MTUs vary from protocol to protocol

18. What is Fragmentation?

Fragmentation is the division of a datagram into smaller units to accommodate the MTU of a data link protocol. The fields in the IP header that relate to fragmentation are the identification number, the fragmentation flags, and the fragmentation offset. The IP datagram header consists of a fixed, 20- byte section and a variable options section with a maximum of 40 bytes.

19. How the errors are detected in IP?

The error detection method used by IP is the checksum. The checksum uses one's complement arithmetic to add equal-size sections of the IP header. The complemented result is stored in the checksum field. The receiver also uses one's complement arithmetic to check the header.

20. What are the modules and tables in IP package?

An IP package can consist of the following: a header-adding module, a processing module, a routing module, a fragmentation module, a reassembly module, a routing table, an MTU table, and a reassembly table.

21. What is IP address?

The Internet address (or IP address) is 32 bits (for IPv4) that uniquely and universally defines a host or router on the Internet. The portion of the IP address that identifies the network is called the netid. The portion of the IP address that identifies the host or router on the network is called the hostid. An IP address defines a device's connection to a network.

22. What is Unicast, Multicast and Broad cast communication?

Unicast communication is one source sending a packet to one destination.

Multicast communication is one source sending a packet to multiple destinations. Hosts with the same multicast address can either be on the same network or on different networks. Multicast addresses are often used for information retrieval and conferencing purposes.

Broadcast communication is one source sending a packet to all hosts on its network.

23. List the components of IP package?

An IP package can consist of the following: a header-adding module, a processing module, a routing module, a fragmentation module, a reassembly module, a routing table, an MTU table, and a reassembly table.

24. What are the difference fields in Routing table?

The routing table can consist of seven fields: a mask, a destination address, a next-hop address, flags, a reference count, a use, and an interface.

25. What is class less addressing?

Classless addressing requires hierarchical and geographical routing to prevent immense routing tables.

26. What are the operations carried out in Checksum?

The checksum uses one's complement arithmetic to add equal-size sections of the IP header. The complemented result is stored in the checksum field. The receiver also uses one's complement arithmetic to check the header

27. What is the function of ARP?

The purpose of ARP is to map IP address of a host with MAC address.ARP finds the physical address of a host if its IP address is known.

28. Define Proxy ARP?

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware(physical) address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router.

29. How to represent a decimal dotted notation in binary form in IPv4?

IP address in binary and dotted-decimal notation.

30. Define TTL.

Time To Live Under the Internet Protocol, is an 8-bit field. In the IPv4 header, TTL is the 9th octet of 20. In the IPv6 header, it is the 8th octet of 40. The maximum TTL value is 255, the maximum value of a single octet.

The time-to-live value can be thought of as an upper bound on the time that an IP datagram can exist in an Internet system. The TTL field is set by the sender of the datagram, and reduced by every router on the route to its destination. If the TTL field reaches zero before the datagram arrives at its destination, then the datagram is discarded and an ICMP error datagram (11 - Time Exceeded) is sent back to the sender. The purpose of the TTL field is to avoid a situation in which an undeliverable datagram keeps circulating on an Internet system, and such a system eventually becoming swamped by such “immortals".

UNIT-II

1. List the components of IP package?

An IP package can consist of the following: a header-adding module, a processing module, a routing module, a fragmentation module, a reassembly module, a routing table, an MTU table, and a reassembly table.

2. What are the difference fields in Routing table?

The routing table can consist of seven fields: a mask, a destination address, a next-hop address, flags, a reference count, a use, and an interface.

3. What is class less addressing?

Classless addressing requires hierarchical and geographical routing to prevent immense routing tables.

4. What are the fields Option Header contains?

The options header contains the following information: a code field that identifies the option, option length, and the specific data.

5. What are the operations carried out in Checksum?

The checksum uses one's complement arithmetic to add equal-size sections of the IP header. The complemented result is stored in the checksum field. The receiver also uses one's complement arithmetic to check the header.

6. What is the size of MTU?

The MTU is the maximum number of bytes that a data link protocol can encapsulate. MTUs vary from protocol to protocol.

7. What is ICANN?

The Internet Corporation for Assigned Names and Numbers (ICANN), formerly known as IANA, is responsible for the management of Internet domain names and addresses.

8. List the various timers used in TCP.

Retransmission, Persistence, Keep alive and Time-waited.

9. Define closed loop congestion control.

Closed loop congestion control mechanisms try to alleviate congestion after it happens.

Back pressure – When a router is congested. It can inform the previous upstream router to reduce the rate of outgoing packets.

Choke points – Is a packet sent by a router to the source to inform it of congestion, same as ICMP's source quench packet.

Implicit signaling – The source can detect an implicit signal warning of congestion and slow down its sending rate.

10. What is the format of UDP packet? Explain.

Header and data. Header contains: Source port number, Destination port number, Total length, Checksum.

11. Describe the various fields in IP Header format.

The fields in the IP header that relate to fragmentation are the identification number, the fragmentation flags, and the fragmentation offset.

12. What are the modules and tables are in IP package?

An IP package can consist of the following: a header-adding module, a processing module, a routing module, a fragmentation module, a reassembly module, a routing table, an MTU table, and reassembly table.

13. What is BOOTP?

BOOTSTRAP Protocol is a client/server protocol designed to provide the following four information for a diskless computer or a computer that is booted for the first time. IP address, Subnet mask, IP address of a router, IP address of a name server.

14. What is DHCP?

The Dynamic Host Configuration Protocol has been derived to provide dynamic configuration. DHCP is also needed when a host moves from network to network or is connected and disconnected from a network.

15. What is Protocol?

A protocol is a set of rules that governs data communication; the key elements of a protocol are syntax, semantics, and timing.

16. What is Standards? What are the organizations involved in standard creation committee?

Standards are necessary to ensure that products from different manufacturers can work together as expected. The ISO, ITU-T, ANSI, IEEE, and EIA are some of the organizations involved in standards creation.

17. What is process-to-process communication?

The IP is responsible for communication at the computer level(host-to-host). As a network layer protocol, IP can deliver the message only to the destination computer. However, this is an incomplete delivery. The message still needs to be handed to the correct process. This is where a transport layer protocol such as UDP takes over. UDP is responsible for delivery of the message to the appropriate process.

18. What is Multiplexing and De-multiplexing?

In the TCP/IP protocol suite, there is one TCP but there are several application programs that may want to use its services. To handle this situation TCP does multiplexing and de-multiplexing.

19. Explain buffering?

TCP creates sending and receiving buffers for each connection. TCP uses a buffer to store the stream of data coming from the sending application program. The receiving TCP also buffer data when they arrive and deliver them to the application program.

20. What is connection establishment?

TCP transmit data in full-duplex mode, when two TCP's in two machines are connected they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data transfer is called connection establishment.

21. What is connection termination?

Any of the two parties involved in exchanging data can close the connection. When connection in one direction is terminated, the other party can continue sending data in the other direction. Therefore both machines are needed to close the connection in both direction.

22. Define open loop congestion control.?

In open loop congestion control, policies are applied to prevent congestion before it happens.

Retransmission policy – a good retransmission policy can prevent congestion, timers must be designed to optimize efficiency

Acknowledgment policy – the acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and helps prevent congestion.

Discard policy – Routers may prevent congestion and at the same time will not harm the integrity of the transmission.

UNIT – III

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. 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.

6. 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.

7. What are the two possible transport services?

Two basic types of transport services are Connection service Connectionless services

8. The transport layer creates the connection between source and destination. 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.

9. 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.

10. Why the congestion occurs in network?

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

11. What is Sliding Window?

The sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, he sender and receiver need to deal with only part of the possible sequence numbers.

12. What is Piggy Backing?

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

13. What is usage of Sequence Number in Reliable Transmission?

The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame. Since we want to minimize the frame size, the smallest range that provides unambiguous communication. The sequence numbers can wrap around.

14. What is Flow Control?

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

15. What is Error Control?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission.

16. Define Retransmission:

Retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

17 Compare Error Detection and Error Correction:

The correction of errors is more difficult than the detection. In error detection, checks only any error has occurred. In error correction, the exact number of bits that are corrupted and location in the message are known. The number of the errors and the size of the message are important factors.

18. Define ephemeral ports

The client program defines itself with a port number, called the ephemeral port number. The word ephemeral means short lived and is used because the life of a client is normally short. An ephemeral port number is recommended to be greater than 1023 for some client/server programs to work properly.

19. Define well known ports.

The server process must also define itself with a port number. This port number, however, cannot be chosen randomly. If the computer at the server site runs a server process, the process

at the client site that wants to access that server and use its services will not know the port number. Of course one solution would be to send a special packet and request the port number of a specific server, but this creates more overhead. So TCP has decided to use universal port numbers for server; these are called well-known port numbers.

20. Use of UDP.

UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FTP.

UDP is a suitable transport protocol for multicasting.

UDP is used for management processes such as SNMP.

UDP is used for some route updating protocols such as Routing Information protocol (RIP).

UDP is suitable for trivial file transfer protocol process includes little flow and error control.

21. Define Pushing data.

TCP buffer will create transmission delay. Some situation an application program that communicates interactively with another application program on the other end. The application program at the sending site can request a push operation; this means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. For set the push bit (PSH) can intimate receiving TCP must be delivered to the receiving application program.

22. Define Urgent data.

TCP as a stream of bytes. Each byte of data has a position in the stream. Some occasion's application program needs to send urgent bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program. So set URG bit, the sending application program tells the sending TCP that the piece of data is urgent.

23.List connection reset.

Denying a connection

Aborting a connection

Terminating an idle connection.

24. Define Half close.

In TCP, one end can stop sending data while still receiving data. This is called a half close.

25. Define simultaneous open.

In a simultaneous open, both applications issue active opens

26. Define simultaneous close.

In the situation, both ends issue an active close.

UNIT – IV&V

1. Define Transmission control block

   TCP coordinates the activities of transmission, reception, and retransmission for each TCP connection through a data structure shared by all processes. The data structure is known as a transmission control block or TCB. The TCB contains all information about the TCP connection includes address, port number, rtt time estimate, data has been sent or received, acknowledgement.

2. What is sequence space.

   The set of all possible sequence integers is known as the TCP sequence space.

3. Write note about finite state machine.

   The finite state machine specifies how TCP makes macroscopic state transitions in response to input or user commands; an implementation contains a separate mechanism that makes microscopic state transitions to control output and retransmission.

4. How to implement TCP finite state machine?

   Table driven – uses a two dimensional array in which each row corresponds to one state. Colum corresponds to one possible input event or operation that causes transition.

   Procedure-driven approach – uses one procedure for each input state. When an event occurs, TCP uses the current state to choose the correct procedure. It processes the input event and updates the state variable.

5. Define closed state processing.

   The closed state represents a TCB that has been allocated but not used in any way. The application program

6. Define Graceful shutdown.

   TCP uses a modified 3 way handshake to shutdown connections. One side calls it close operation (A). TCP on side A sends a FIN segment and moves to the FIN-WAIT-1 state. When it receives the FIN, the other side, calls it B, sends an ACK, moves to the CLOSE-WAIT state, and waits for the application to close connection. Back at side A, receipt of the ACK causes TCP to move to the FIN-WAIT-2 state.

   When the application on side B executes a close operation. TCP sends a FIN and moves to the LAST-ACK state. Side A receives the FIN, moves to the TIME-WAIT state, sends the final ACK, and shutdown the connection. When the last ACK arrives on side B, that side shutdown as well.

7. List TCP output messages.

1	SEND	send data and/or ACK
2	PERSIST	Send probe to test receiver's Zero Window
3	RETRANSMIT	Retransmit data segment
4	DELETE	Delete a TCB that has expired.

8. Two basic design of TCP timer management.

Items on the timer delta list can store commands that the timer process interprets when the event occurs, or items on the list can store messages that the timer process delivers when the event occurs.

9. List five principle of tuning adaptive transmission.

Retransmission timer and backoff

Window-based flow control

Maximum segment size computation

Congestion avoidance and control

Round trip estimation

10. Use of Window based flow control

TCP uses window advertisement to control the flow of data across a connection.

11. What is Push data.?

TCP buffer will create transmission delay. Some situation an application program that communicates interactively with another application program on the other end. The application program at the sending site can request a push operation; this means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. For set the push bit (PSH) can intimate receiving TCP must be delivered to the receiving application program.

12.Write a note about Urgent data.

TCP as a stream of bytes. Each byte of data has a position in the stream. Some occasion's application program needs to send urgent bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program. So set URG bit, the sending application program tells the sending TCP that the piece of data is urgent.

13. What is sliding Window?

The window spans a portion of the buffer containing bytes.That a host can send before worrying about the acknowledgement from the other host. The window is called a sliding window because it can slide over the buffer as data and acknowledgements are sent and received.

14. . What is a difference between packets, datagram and frames?

A datagram is a basic transfer unit associated with a packet-switched network in which the delivery, arrival time and order are not guaranteed. The source and destination addresses as well as a type field are found in the header of a datagram. A packet consists of two kinds of data: control information and user data (also known as payload).

The control information provides data the network needs to deliver the user data, for example: source and destination addresses, error detection codes like checksums, and sequencing information. Typically, control information is found in packet headers and trailers, with user data in between. In computer networking and telecommunication, a frame is a digital data transmission unit or data packet that includes frame synchronization, i.e. a sequence of bits or symbols making it possible for the receiver to detect the beginning and end of the packet in the stream of symbols or bits.

15. Read the TCP specification to find out the exact conditions under which TCP can make the transition from FIN_WAIT-1 to TIME_WAIT.

When the application issues a close TCP enters the FIN_WAIT-1 state and When the TCPconnection has been closed down, the connection enters the TIME_WAIT state

16. . How Karn’s algorithm works?

[Karn and Partridge 1987] specify that when a timeout and retransmission occur, we cannot update the RTT estimators when the acknowledgment for the retransmitted data finally arrives. This is because we don't know to which transmission the ACK corresponds.

Karn's Algorithm is part of TCP and consists of 2 rules: Rule 1: Ignore RTT for retransmitted packets Rule 2: RTO (retransmission time-out) must be doubled after retransmission. This keeps TCP from using previous RTO forever.

17. . What is AIMD (Slow start)?

The additive increase/multiplicative-decrease (AIMD) algorithm is a feedback control algorithm used in TCP Congestion Avoidance. AIMD combines linear growth of the congestion window with an exponential reduction when a congestion takes place.

18. What is 2MSL?

The TIME_WAIT state is also called the 2MSL wait state. Every implementation must choose a value for the maximum segment lifetime (MSL). It is the maximum amount of time any segment can exist in the network before being discarded. We know this time limit is bounded, since TCP segments are transmitted as IP datagrams, and the IP datagram has the TTL field that limits its lifetime.

19. Persistent timer:

When the sender receives an ACK with window size zero, it immediately stops transmission and turns on the persistence timer and waits for the receiver to respond that the window size become nonzero value.

If the receiver does not respond till the timer expires, the sender will send a segment with 1 byte of data called a probe segment.When the receiver receives a probe segment, the receiver responds with the window size either zero or non zero. If it zero, the sender again restarts the persistence timer and waits on.

20. Keep alive timer

The keepalive concept is very simple: when you set up a TCP connection, you associate a set of timers. Some of these timers deal with the keepalive procedure. When the keepalive timer reaches zero, you send your peer a keepalive probe packet with no data in it and the ACK flag turned on. You can do this because of the TCP/IP specifications, as a sort of duplicate ACK, and the remote endpoint will have no arguments, as TCP is a stream-oriented protocol. On the other hand, you will receive a reply from the remote host (which doesn't need to support keepalive at all, just TCP/IP), with no data and the ACK set.

21. purposes: sliding window serves

(1) it guarantees the reliable delivery of data

(2) it ensures that the data is delivered in order,

(3) it enforces flow control between the sender and the receiver.

22. How RTT value estimated in TCP?

Round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. The RTT was originally estimated in TCP by: RTT = (α * Old_RTT) + ((1-α) * New_Round_Trip_Sample) Where α is constant weighting factor($0 \leq \alpha < 1$). Choosing a value α close to 1 makes the weighted average immune to changes that last a short time (e.g., a single segment that encounters long delay).