1. **List out the transport layer service primitives and their meaning.**

**A service is specified by a set of primitives. A primitive means operation. To access the service a user process can access these primitives. These primitives are different for connection oriented service and connectionless service.**

**There are five types of service primitives:**

1. **LISTEN : When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.**
2. **CONNECT : It connects the server by establishing a connection. Response is awaited.**
3. **RECEIVE: Then the RECEIVED call blocks the server.**
4. **SEND : Then the client executes SEND primitive to transmit its request followed by the execution of RECEIVE to get the reply. Send the message.**
5. **DISCONNECT : This primitive is used for terminating the connection. After this primitive one can’t send any message. When the client sends a DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by the client then the process is terminated.**

**Connection Oriented Service Primitives**

* **There are 4 types of primitives for Connection Oriented Service :**

| **CONNECT** | **This primitive makes a connection** |
| --- | --- |
| **DATA, DATA-ACKNOWLEDGE, EXPEDITED-DATA** | **Data and information is sent using thus primitive** |
| **CONNECT** | **Primitive for closing the connection** |
| **RESET** | **Primitive for resetting the connection** |

**Connectionless Oriented Service Primitives**

* **There are 2 types of primitives for Connectionless Oriented Service:**

| **UNIDATA** | **This primitive sends a packet of data** |
| --- | --- |
| **FACILITY, REPORT** | **Primitive for enquiring about the performance of the network, like delivery statistics.** |

**2. Write about CSMA and CSMA/CD in detail.**

**Carrier Sense Multiple Access**

**CSMA is a mechanism that senses the state of the shared channel to prevent or recover data packets from a collision. It is also used to control the flow of data packets over the network so that the packets are not lost, and data integrity is maintained. In CSMA, when two or more data packets are sent at the same time on a shared channel, the chances of collision occur. Due to the collision, the receiver does not get any information regarding the sender's data packets. And the lost information needs to be resented so that the receiver can get it. Therefore we need to sense the channel before transmitting data packets on a network. It is divided into two parts, CSMA CA (Collision Avoidance) and CSMA CD (Collision Detection).**

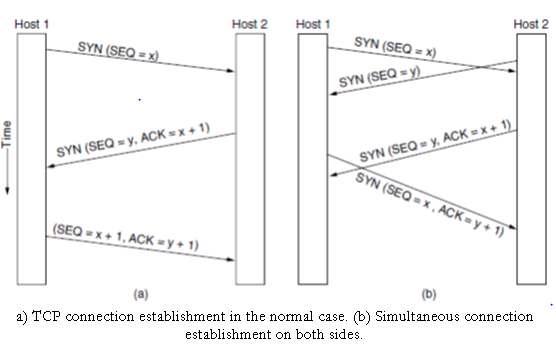
## **Difference between CSMA CA and CSMA CD**

| **S. No** | **CSMA CD** | **CSMA CA** |
| --- | --- | --- |
| **1.** | **It is the type of CSMA to detect the collision on a shared channel.** | **It is the type of CSMA to avoid collision on a shared channel.** |
| **2.** | **It is the collision detection protocol.** | **It is the collision avoidance protocol.** |
| **3.** | **It is used in 802.3 Ethernet network cable.** | **It is used in the 802.11 Ethernet network.** |
| **4.** | **It works in wired networks.** | **It works in wireless networks.** |
| **5.** | **It is effective after collision detection on a network.** | **It is effective before collision detection on a network.** |
| **6.** | **Whenever a data packet conflicts in a shared channel, it resends the data frame.** | **Whereas the CSMA CA waits until the channel is busy and does not recover after a collision.** |
| **7.** | **It minimises the recovery time.** | **It minimises the risk of collision.** |
| **8.** | **The efficiency of CSMA CD is high as compared to CSMA.** | **The efficiency of CSMA CA is similar to CSMA.** |
| **9.** | **It is more popular than the CSMA CA protocol.** | **It is less popular than CSMA CDs.** |

**3. Discuss in detail about the connection establishment and release in TCP.**

**TCP Connection Establishment:**

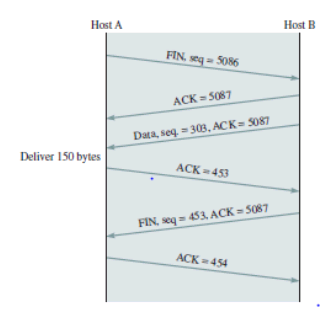
* **To establish a connection, one side, say the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives in that order, either specifying a specific source or nobody in particular.**
* **The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (e.g., a password).**
* **The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit off and waits for a response.**
* **When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the Destination port field. If not, it sends a reply with the RST bit on to reject the connection.**
* **If some process is listening to the port, that process is given the incoming TCP segment. It can either accept or reject the connection. If it accepts, an acknowledgement segment is sent back. The sequence of TCP segments sent in the normal case is shown in Fig below. Note that a SYN segment consumes 1 byte of sequence space so that it can be acknowledged unambiguously.**

****

* **In the event that two hosts simultaneously attempt to establish a connection between the same two sockets, the sequence of events is as illustrated in Fig.(b). The result of these events is that just one connection is established, not two, because connections are identified by their end points. If the first setup results in a connection identified by (x, y) and the second one does too, only one table entry is made, namely, for (x, y).**

**TCP Connection Termination:**

* **TCP provides for a graceful closure that involves independent termination of each direction of the connection. A termination is initiated when an application tells TCP that it has no more data to send.**
* **The TCP entity completes transmission of its data and upon receiving acknowledgement from the receiver, issues a segment with the FIN bit set.**
* **Upon receiving a FIN segment, A TCP entity informs its application that the other entity has terminated its transmission of data.**
* **For e.g. as shown in fig below the TCP entity in host A terminates its transmission first by issuing a FIN segment. Host B sends an ACK segment to acknowledge receipt of the FIN segment from A. The FIN segment uses one byte, so the ACK is 5087 as shown in the example.**
* **After B receives the FIN segment, the direction of the flow from B to A is still open. In the fig below host B sends 150 bytes in one segment, followed by a FIN segment. Host A then sends an acknowledgment. The TCP in host A then enters the TIME\_WAIT state and starts the TIME\_WAIT timer with an initial value set to twice the maximum segment lifetime (2MSL).**
* **The only valid segment that can arrive while host A is in the TIME\_WAIT state is a retransmission of the FIN segment from host B(if host A’s ACK was lost, and host B’s retransmission time-out has expired).**
* **If such a FIN segment arrives while host A is in the TIME\_WAIT state, then the ACK segment is retransmitted and the TIME\_WAIT timer is restarted at 2MSL. When the TIME\_WAIT timer expires, host A closes the connection and then deletes the record of the connection.**

****

**4. Explain the Services of Transport layer.**

**Process to process delivery:**

**While Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source-destination hosts to correctly deliver a frame and the Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16-bit address used to identify any client-server program uniquely.**

**End-to-end Connection between hosts:**

**The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-oriented protocol that uses a handshake protocol to establish a robust connection between two end hosts. TCP ensures reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol that ensures best-effort delivery. It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.**

**Multiplexing and Demultiplexing:**

**Multiplexing allows simultaneous use of different applications over a network that is running on a host. The transport layer provides this mechanism which enables us to send packet streams from various applications simultaneously over a network. The transport layer accepts these packets from different processes differentiated by their port numbers and passes them to the network layer after adding proper headers. Similarly, Demultiplexing is required at the receiver side to obtain the data coming from various processes. Transport receives the segments of data from the network layer and delivers it to the appropriate process running on the receiver’s machine.**

**Congestion Control:**

**Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur. As a result, retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open loop congestion control to prevent the congestion and closed-loop congestion control to remove the congestion in a network once it occurs. TCP provides AIMD- additive increase multiplicative decrease, leaky bucket technique for congestion control.**

**Data integrity and Error correction:**

**The transport layer checks for errors in the messages coming from the application layer by using error detection codes, computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.**

**Flow control:**

**The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.**

**5. Write about electronic mail in detail**

**Electronic Mail (e-mail) is one of most widely used services on the Internet. This service allows an Internet user to send a message in formatted manner (mail) to the other Internet user in any part of the world. Messages in mail not only contain text, but it also contains images, audio and videos data. The person who is sending mail is called the sender and the person who receives mail is called the recipient. It is just like postal mail service. Components of E-Mail System : The basic components of an email system are : User Agent (UA), Message Transfer Agent (MTA), Mail Box, and Spool file. These are explained below.**

**User Agent (UA) : The UA is normally a program which is used to send and receive mail. Sometimes, it is called a mail reader. It accepts a variety of commands for composing, receiving and replying to messages as well as for manipulation of the mailboxes.**

**Message Transfer Agent (MTA) : MTA is actually responsible for transfer of mail from one system to another. To send mail, a system must have a client MTA and a system MTA. It transfers mail to the mailboxes of recipients if they are connected in the same machine. It delivers mail to peer MTA if the destination mailbox is on another machine. The delivery from one MTA to another MTA is done by Simple Mail Transfer Protocol.**

**Mailbox : It is a file on the local hard drive to collect mail. Delivered mails are present in this file. The user can read it and delete it according to his/her requirement. To use the e-mail system each user must have a mailbox . Access to the mailbox is only to the owner of the mailbox.**

**Spool file : This file contains mails that are to be sent. User agent appends outgoing mails in this file using SMTP. MTA extracts pending mail from the spool file for their delivery. E-mail allows one name, an alias, to represent several different email addresses. It is known as a mailing list. Whenever a user has to send a message, the system checks the recipient's name against the alias database. If a mailing list is present for a defined alias, separate messages, one for each entry in the list, must be prepared and handed to MTA. If for a defined alias, there is no such mailing list, the name itself becomes the naming address and a single message is delivered to the mail transfer entity.**

**Services provided by E-mail system :**

**Composition – The composition refers to the process that creates messages and answers. For composition any kind of text editor can be used.**

**Transfer – Transfer means sending a procedure of mail i.e. from the sender to recipient.**

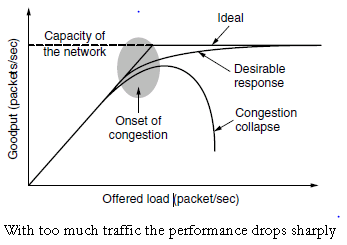
**Reporting – Reporting refers to confirmation for delivery of mail. It helps users to check whether their mail is delivered, lost or rejected.**

**Displaying – It refers to present mail in form that is understood by the user.**

**Disposition – This step concerns the recipient about what the recipient will do after receiving mail i.e save mail, delete before reading or delete after reading.**

**6. What are the reasons for congestion? What are the problems with congestion?**

**Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called congestion. The network and transport layers share the responsibility for handling congestion.**

****

1. **Common reasons for congestion on routers - Congestion can occur on a router when packets arrive at a greater rate than possible to forward. Congestion can be sporadic or long term. When congestion occurs, packets must be discarded by the router. Congestion occurs at a bottleneck when:  
   i. Packets arrive on several channels to be forwarded on a single channel.  
   ii. Incoming channels have a higher bandwidth than outgoing channels.  
   iii. Channel bandwidth is sufficient but router CPU processing is too slow to handle bookkeeping (queuing, routing table updates, etc).  
   iv. Router lacks sufficient memory buffer space.  
   v. Under an end-to-end reliable protocol (e.g. TCP), even with infinite memory, congestion can get worse because packets have timed out (e.g. moving from queue back to front on router or due to delay in acknowledging on a receiver) resulting in duplicates, adding to the congestion.**

**Effects of network congestion :**

**Queueing delay**

**Packet Loss**

**Slow Network**

**Blocking of new connections**

**Low throughput**

**7. With an example explain the Dynamic routing algorithms used in computer networks.**

**Dynamic routing is known as a technique of finding the best path for the data to travel over a network. In this process a router can transmit data through various different routes and reach its destination on the basis of conditions at that time of communication circuits.**

**Dynamic routers are smart enough to take the best path for data based on the condition of the present scenario at that time of the network. In case one section fails in the network to transfer data forward dynamic router will use its algorithm (in which they use routing protocols to gather and share information of the current path among them) and it will re-route the previous network over another network in real-time. And this amazing capability and functionality to change paths in real-time over the network by sharing status among them is the key functionality of Dynamic Routing. OSPF (open shortest path first) and RIP are some protocols used for dynamic routing.**

**8. Explain about HTTP**

**HTTP represents "Hypertext Transfer Protocol." HTTP is the protocol that can transfer information over the network. It is the Internet protocol suite method and defines commands and functions used for sharing web page data.**

**HTTP uses a server-client model. A client, for example, maybe a laptop or telephone device. The HTTP server is frequently a web host running web server software, such as Apache or IIS.**

**HTTP also represents commands such as GET and POST, which are used to handle submissions on websites. The CONNECT command can act as a fast connection that is encrypted using a secure socket layer (SSL).**

**HTTP is equivalent to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in how the messages are sent from the client to the server and from the server to the client. SMTP messages are saved and advanced, while HTTP messages are delivered directly.**

**9. What are TCP and UDP protocols?**

**TCP is a transport layer connection-oriented protocol. It provides a reliable connection and protected data transmission between the connected machines over a network. It first establishes a secure link and then sends the data.**

**TCP sends the data from one device to the other in the form of data blocks. It is slow in data transmission but has more functionalities such as flow control, error control, and congestion control in the system.**

**The TCP header is 20–60 bytes and therefore, it contains several pieces of information to improve the reliability. But, the overhead is raised. Because of its reliability, protocols like HTTP, FTP, etc., use TCP for secured data transmission over the network.**

## 

**UDP is a transport layer, connectionless protocol. It provides quick transmission of data between the connected machines over a network. There is no overhead of creating, maintaining, and terminating a connection in UDP.**

**It is mainly used to transmit real-time data where we cannot afford any transmission delays. UDP sends the data from one device to the other in the form of continuous data streams.**

**The UDP header is of fixed size, i.e., 8 bytes. It is unreliable but faster in speed. Due to its transmission speed, protocols like DNS, DHCP, RIP, etc., use UDP for proper data transmission over the network.**

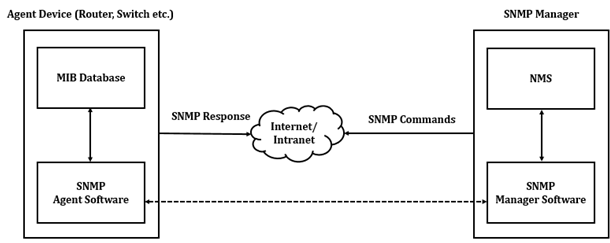
**10. What is the difference between Broadcasting and Multicasting?**

**Difference between Broadcast and Multicast :**

| **S.No.** | **Broadcast** | **Multicast** |
| --- | --- | --- |
| **1.** | **It has one sender and multiple receivers.** | **It has one or more senders and multiple receivers.** |
| **2.** | **It sent data from one device to all the other devices in a network.** | **It sent data from one device to multiple devices.** |
| **3.** | **It works on star and bus topology.** | **It works on star, mesh, tree and hybrid topology.** |
| **4.** | **It scales well across large networks.** | **It does not scale well across large networks.** |
| **5.** | **Its bandwidth is wasted.** | **It utilises bandwidth efficiently.** |
| **6.** | **It has one-to-all mapping.** | **It has one-to-many mapping.** |
| **7.** | **Hub is an example of a broadcast device.** | **Switch is an example of a multicast device.** |

**\*11. Write short notes on(a) SNMP**

**Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices and their functions. SNMP provides a common language for network devices to relay management information within single- and multi-vendor environments in a local area network (LAN) or wide area network (WAN). The most recent iteration of SNMP, version 3, includes security enhancements that authenticate and encrypt SNMP messages as well as protect packets during transit.**

****

**Components of SNMP**

**There are four main components in an SNMP-managed network:**

**SNMP agent: This program runs on the hardware or service being monitored, collecting data about various metrics like bandwidth use or disk space. When queried by the SNMP manager, the agent sends this information back to the management system. An agent may also proactively notify the NMS if an error occurs. Most devices come with an SNMP agent preinstalled; it typically just needs to be turned on and configured.**

**SNMP-managed devices and resources: These are the nodes on which an agent runs.**

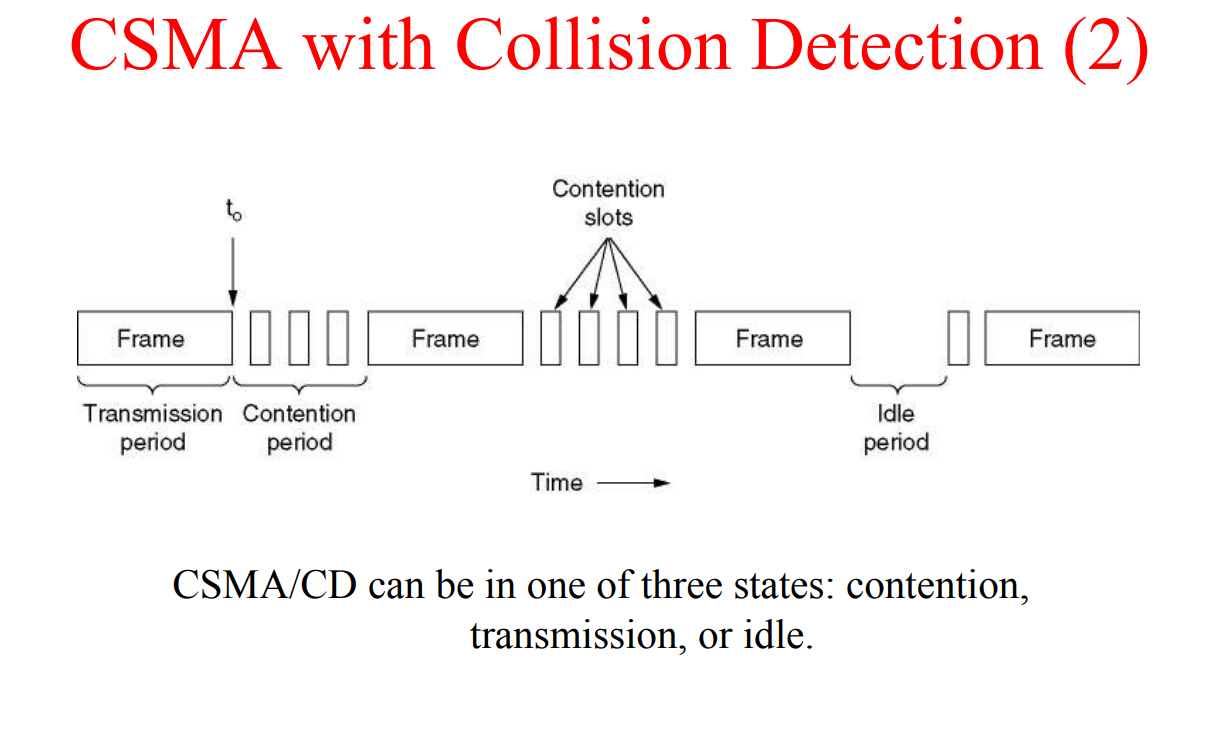
**SNMP manager (aka NMS): This software platform functions as a centralised console to which agents feed information. It will actively request agents to send updates via SNMP at regular intervals. What a network manager can do with that information depends heavily on how feature-rich the NMS is. There are several free SNMP managers available, but they are typically limited in their capabilities or the number of nodes they can support. At the other end of the spectrum, enterprise-grade platforms offer advanced features for more complex networks, with some products supporting up to tens of thousands of nodes.**

**Management information base (MIB): This database is a text file (.mib) that itemises and describes all objects used by a particular device that can be queried or controlled using SNMP. This database must be loaded into the NMS so that it can identify and monitor the status of these properties. Each MIB item is assigned an object identifier (OID).**

**What is CSMA with CDs? What are the three different states a CSMA/CD can be in?**

## **CSMA CD**

**The Carrier Sense Multiple Access/ Collision Detection protocol is used to detect a collision in the media access control (MAC) layer. Once the collision was detected, the CSMA CD immediately stopped the transmission by sending the signal so that the sender does not waste all the time to send the data packet. Suppose a collision is detected from each station while broadcasting the packets. In that case, the CSMA CD immediately sends a jam signal to stop transmission and waits for a random time context before transmitting another data packet. If the channel is found free, it immediately sends the data and returns it.**

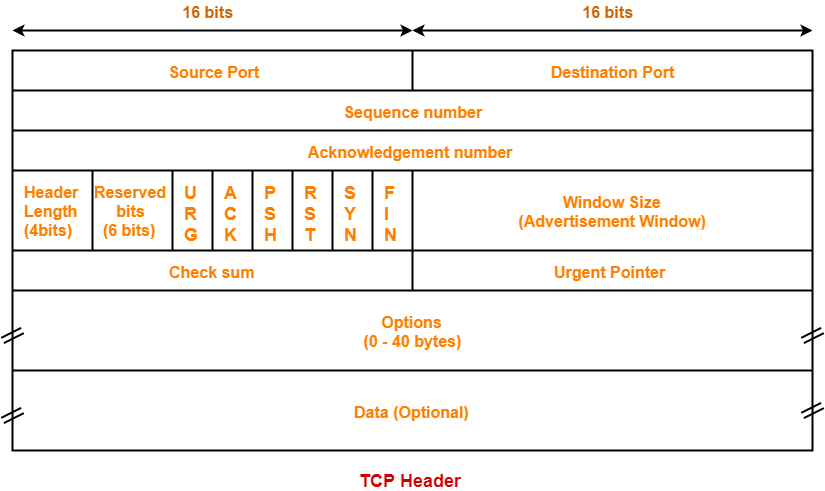
****

**13.**

**\*14. Explain the structure of TCP Header format.**

**TCP Header-**

**The following diagram represents the TCP header format-**

****

**Let us discuss each field of TCP header one by one.**

## **1. Source Port-**

* **Source Port is a 16 bit field.**
* **It identifies the port of the sending application.**

## **2. Destination Port-**

* **Destination Port is a 16 bit field.**
* **It identifies the port of the receiving application.**

| **NOTE** **It is important to note-**   * **A TCP connection is uniquely identified by using-**   **Combination of port numbers and IP Addresses of sender and receiver**   * **IP Addresses indicate which systems are communicating.** * **Port numbers indicate which end to end sockets are communicating.** |
| --- |

## **3. Sequence Number-**

* **Sequence number is a 32 bit field.**
* **TCP assigns a unique sequence number to each byte of data contained in the TCP segment.**
* **This field contains the sequence number of the first data byte.**

## **4. Acknowledgement Number-**

* **Acknowledgment number is a 32 bit field.**
* **It contains the sequence number of the data byte that the receiver expects to receive next from the sender.**
* **It is always the sequence number of the last received data byte incremented by 1.**

## **5. Header Length-**

* **Header length is a 4 bit field.**
* **It contains the length of the TCP header.**
* **It helps in knowing from where the actual data begins.**

### **Minimum and Maximum Header length-**

| **The length of TCP header always lies in the range-**  **[20 bytes , 60 bytes]** |
| --- |

* **The initial 5 rows of the TCP header are always used.**
* **So, minimum length of TCP header = 5 x 4 bytes = 20 bytes.**
* **The size of the 6th row representing the Options field varies.**
* **The size of the Options field can go up to 40 bytes.**
* **So, maximum length of TCP header = 20 bytes + 40 bytes = 60 bytes.**

**15. What are the protocols associated with WWW? Explain them.**

**A web browser loads a webpage using various protocols:**

**It uses the Domain Name System (DNS) protocol to convert a domain name into an IP address.**

**It uses the HyperText Transfer Protocol (HTTP) to request the webpage contents from that IP address.**

**It may also use the Transport Layer Security (TLS) protocol to serve the website over a secure, encrypted connection.**

**16. What are the different services provided by transport layer**

**The services provided by the transport layer protocols can be divided into five categories:**

* **End-to-end delivery**
* **Addressing**
* **Reliable delivery**
* **Flow control**
* **Multiplexing**

**17. Repeated Question**

**18. Are the TCP Connections half- duplex? How are the Connections released in TCP?**

**No TCP is full duplex, A TCP connection is a full-duplex connection. To understand the connection release, we can consider them to be a pair of simplex connections. We can then imagine that each simplex connection is being released independently. Releasing a TCP connection is symmetric. Either port can send a TCP segment with the FIN bit set, meaning it has no more information to send when the FIN is acknowledged that direction is shut down. Still, data can continue to flow continually in the other direction.**

**19. Explain flow control in the transport layer in detail.**

**Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asks for the retransmission of packets. This increases network congestion and thus, reduces the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.**

**20. Explain the working of domain name system**

**DNS stands for Domain Name System.**

* **DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.**
* **DNS is required for the functioning of the internet.**
* **Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.**
* **DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilise user-friendly names when looking for other hosts instead of remembering the IP addresses.**
* **For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than the IP address.**

**21. Explain about the TCP Congestion Control.**

**CONGESTION CONTROL**

**Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens, or remove congestion after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal)**

**Congestion Policy**

* **TCP's general policy for handling congestion is based on three phases: slow start, congestion avoidance, and congestion detection. In the slow-start phase, the sender starts with a very slow rate of transmission, but increases the rate rapidly to reach a threshold.**
* **When the threshold is reached, the data rate is reduced to avoid congestion. Finally if congestion is detected, the sender goes back to the slow-start or congestion avoidance phase based on how the congestion is detected.**

**22. What is DNS? What resource records are associated with it? Explain.**

**DNS stands for Domain Name System**

**DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilise user-friendly names when looking for other hosts instead of remembering the IP addresses.**

**We can define DNS Resource Records simply as DNS Server database entries. Resource Records are usually a name to IP Address (**[**IPv4**](https://www.omnisecu.com/tcpip/internet-layer-ip-addresses.php) **or** [**IPv6**](https://www.omnisecu.com/tcpip/ipv6/index.php)**) mapping (or vice versa). DNS Resource Records are used to answer DNS client queries. Resource Records are added to the DNS server for the portion of the DNS namespace which the DNS Server is hosting.**

**There are different types of Resource Records. Most important types of Resource Records are 1) IPv4 host address (A), 2) IPv6 host address (AAAA, pronounced "quad-A") 3) CNAME (Alias), 4) Pointer (PTR), 5) Mail Exchanger (MX) 6 ) Service (SRV)**

| **DNS Resource Record Type** | **Explanation** |
| --- | --- |
| **A Record** | **IPv4 Host Record, used for mapping a Domain Name to an IPv4 address** |
| **AAAA Record (pronounced "quad-A")** | **IPv6 Host Record, used for mapping a Domain Name to an IPv6 address** |
| **CNAME Record (Canonical Names)** | **Alias Record, used for mapping an alias of a DNS domain name. CNAME Records are useful to use more than one name for a single host. CNAME Records allow using different names for the same host.** |
| **MX Record** | **Mail Exchanger, used for mapping a DNS domain name to the mail server. MX (Mail Exchanger) Records are used by e-mail applications to locate mail servers for a DNS domain, based on the destination email address. MX (Mail Exchanger) Record stores the mail server information for a particular domain.** |
| **PTR Record** | **Pointer, used for reverse lookup (IP Address to Domain Name resolution)** |
| **SRV Record** | **SRV record, used to map available services. Mainly used by Active Directory in Microsoft Windows Servers** |

**23. What are the five basic functions supported in e-mail systems? Explain.**

**Services provided by E-mail system :**

**Composition – The composition refers to the process that creates messages and answers. For composition any kind of text editor can be used.**

**Transfer – Transfer means sending a procedure of mail i.e. from the sender to recipient.**

**Reporting – Reporting refers to confirmation for delivery of mail. It helps users to check whether their mail is delivered, lost or rejected.**

**Displaying – It refers to present mail in form that is understood by the user.**

**Disposition – This step concerns the recipient what will the recipient do after receiving mail i.e save mail, delete before reading or delete after reading.**

**24 Explain the following networks i) ARPANET ii) Internet**

**ARPANET stands for Advanced Research Projects Agency NET. ARPANET was the first network which consisted of distributed control. It was the first to implement** [**TCP/IP**](https://www.geeksforgeeks.org/tcp-ip-model/) **protocols. It was basically the beginning of the Internet with the use of these technologies. It was designed with a basic idea in mind that was to communicate with scientific users among an institute or university**

**Characteristics of ARPANET :**

1. **It is basically a type of WAN.**
2. **It used the concept of Packet Switching Network.**
3. **It used Interface Message Processors(IMPs) for subnetting.**
4. **ARPANETs software was split into two parts- a host and a subnet.**

**The Internet, sometimes called simply "the Net," is a worldwide system of computer networks -- a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers). The Internet is a public, cooperative and self-sustaining facility accessible to hundreds of millions of people worldwide.**

**25. With an example explain the sliding window Flow control mechanism.**

**Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in the Transmission Control Protocol.**

**In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.**

**26. Discuss about the header format of UDP.**

**UDP header is an 8-bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.**

1. **Source Port: Source Port is a 2 Byte long field used to identify the port number of the source.**
2. **Destination Port: It is a 2 Byte long field, used to identify the port of the destined packet.**
3. **Length: Length is the length of UDP including the header and the data. It is a 16-bits field.**
4. **Checksum: Checksum is 2 Bytes long. It is the 16-bit one’s complement of the one’s complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.**

**28 Give the general principles of various congestion control algorithms.**

## Principles of Congestion Control

**As per control theory, the computer network, which is also a system, is divided into two groups. They are open-loop and closed-loop solutions.**

## The open-loop solutions

**It provides an excellent design to ensure that the problem does not occur in the first place. The designing tools include deciding to accept new traffic, discarding packets and scheduling the packets at various network points. The open-loop solution's decisions are independent of the current state of the network.**

## Closed-loop solutions

**It makes the decision based on the concept of a feedback loop. The feedback Notes loop enables the closed-loop system to monitor the procedure to detect when and where congestion occurs. After that, it passes the information to the places where they can take actions.**

**The system's monitoring depends on the percentage of all packets discarded for drawback of buffer area, the average queue lengths, the multiple packets that time out and are retransmitted, the normal packet delay and the standard deviation of packet delay.**

**Secondly, hosts or routers share packets periodically to directly know about congestion so that the traffic around congested areas can be routed to alternate destination routes.**

**29 Write the structure of TCP pseudo header and explain how it is used in checksum calculation.**