What are the benefits of subnetting a network?

1. It reduces network traffic
2. It helps overcome limitations of LAN
3. It protects one network from another
4. Maintenance is easy in case of small networks.

What is a Private network address?

A private network address is a non-routable IP address used within a private network, like home or office network address. Devices using private addresses are invisible to external systems. It is cheap, secure and scalable.

What is meant by segmentation?

Segmentation is the process of dividing a larger network into smaller, self-contained subnetworks.

Benefits of segmentation:

1. Enhanced Security
2. Improved Performance
3. Simplified Management

What is host ID and network ID?

A network ID is the fragment of IP address that tells us which network the host belongs. Host ID is the fragment of an IP address that uniquely classifies a host on a specified network

What is the role of the TTL field in IP header?

It is an 8-bit field in IPv4 header. It is also called Datagram's lifetime. It prevents the datagram to loop through the network by restricting the number of hops taken by a packet before delivering to the destination.

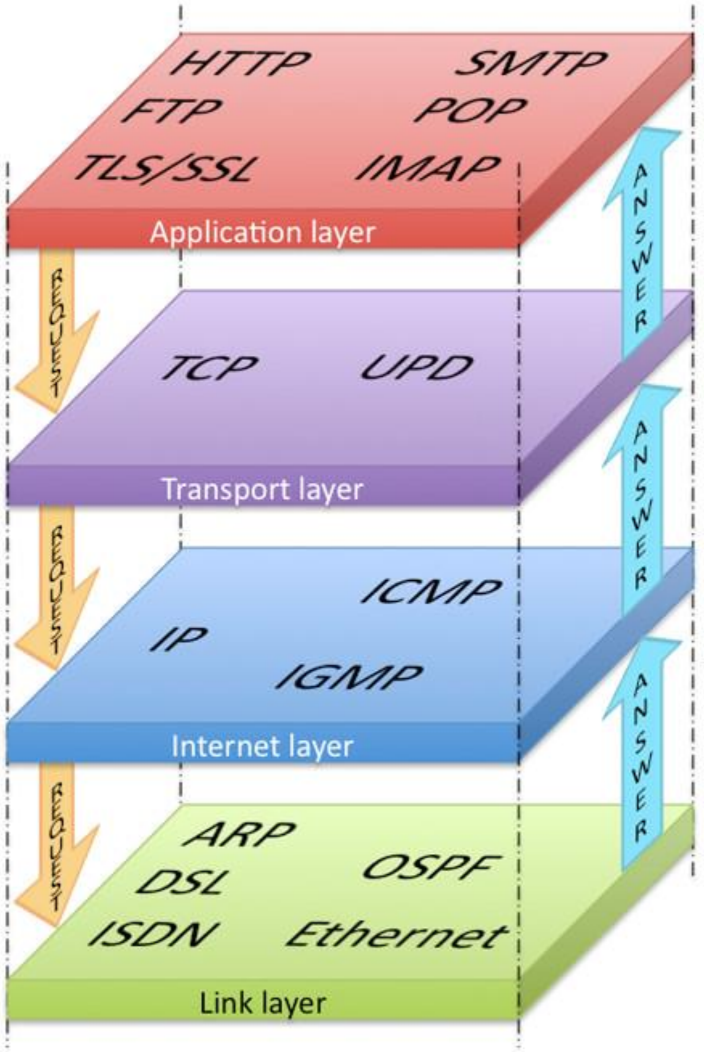
What is the size of an Ethernet address? Describe its parts (if any).

Ethernet address, also known as a Media Access Control (MAC) address, has a size of 6 bytes. These 6 bytes, or 48 bits, are further divided into two parts:

1. Organizationally Unique Identifier (OUI): - The first 3 bytes (24 bits) of the address represent the OUI. It prevents collisions between devices made by different manufacturers.

2. Locally Administered Address (LAA): - The last 3 bytes (24 bits) of the address represent the LAA. It ensures no two devices made by the same manufacturer have the same MAC address.

Draw the TCP/IP stack. Label the protocols in their position.



Define the term Computer Network.

A computer network is a system of interconnected computers that can share resources and communicate with each other. Types of computer network:

- **Local Area Network (LAN):** A small network that connects devices in a limited area, such as a home, office, or school.
- **Metropolitan Area Network (MAN):** A network that covers a larger area such as a city or town.
- **Wide Area Network (WAN):** A large network that connects devices over a wide geographical area, such as a country.

What is MTU? Why is it required?

Maximum Transmission Unit (MTU) determines the maximum size of a data packet that can be transmitted over that network. If the size of a data packet exceeds the MTU, it needs to be fragmented into smaller fragments that can be transmitted over the network. Different networks have different MTU sizes

Under what conditions an ICMP error message is generated? Under what conditions an ICMP error message is not generated? Discuss.

ICMP (Internet Control Message Protocol) error messages are generated to report various issues encountered during IP packet delivery such as:

1. Destination Unreachable
2. Time Exceeded
3. Parameter Problem
4. Redirect
5. Echo Request/Reply

ICMP error messages are NOT generated during:

1. First Fragment of a Fragmented Packet
2. ICMP Error Message Itself
3. Broadcast or Multicast
4. Packet Filtering

What is ICMP echo request and reply?

ICMP Echo Request: It is initiated by a device (pinger) wanting to check connectivity with another device (pinged). It is sent as an ICMP message containing the pinger's IP address and a timestamp.

ICMP Echo Reply: Upon receiving the echo request, the pinged device responds with an ICMP echo reply message. It includes the pinger's IP address, the original timestamp, and its own timestamp.

Explain the TCP transmission policy

Same as silly window syndrome

Explain the role of DNS in a network.

1. DNS (Domain Name System) is a client/server network communication protocol. DNS clients send requests to the server while DNS servers send responses to the client.
2. DNS implements a distributed database to store the name of all the hosts available on the internet.
3. DNS translates the domain name into IP addresses.

Explain adaptive flow control in detail and its usage.

Adaptive flow control is used in computer networks to manage the rate of data transmission between two end points. It uses real-time feedback from the network and congestion signals to adjust the rate of data transmission in real-time.

Applications:

1. **TCP/IP networks:** To manage data traffic.
2. **Wireless networks:** Used in wireless networks with limited bandwidth.
3. **Data centres:** To manages data transfers between servers and storage devices.
4. **Multimedia streaming:** To ensures smooth delivery of video and audio content over congested networks.

Firewalls

A firewall is a network security device, which monitors all incoming and outgoing traffic and accepts, rejects or drops that specific traffic based on a defined set of security rules. There are two types of firewall:

1. **Host- based Firewalls:** It is installed on each network node and controls each incoming and outgoing packet. It comes as a part of the operating system. It protects each host from attacks and unauthorized access.
2. **Network-based Firewalls:** It filters all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. It may have two or more network interface cards (NICs).

NAT

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. It also performs translation of port numbers.

Types of NAT:

1. **Static NAT:** In this, a single unregistered IP address is mapped with a legally registered IP address. This is generally used for Web hosting.
2. **Dynamic NAT:** In this, an unregistered IP address is translated into a registered IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
3. **Port Address Translation (PAT):** It is also known as NAT overload. In this, many local IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic. It is most frequently used as it is cost-effective