Discuss five client error status codes while doing a client request

1. **400 Bad Request:** The server cannot process the request due to invalid syntax or missing information. Example: A user submits a form with incomplete fields or invalid characters.
2. **401 Unauthorized:** The client lacks proper authentication credentials to access the requested resource. Example: A user attempts to access a protected page without providing valid login credentials.
3. **403 Forbidden:** The client is authenticated but lacks authorization to access the resource. Example: A user tries to view another user's private information without necessary permissions.
4. **404 Not Found:** The requested resource cannot be found on the server. Example: A user types an incorrect URL or clicks a broken link.
5. **410 Gone:** The requested resource has been permanently removed from the server. Example: A user tries to access a blog post that was removed from website.

Discuss the different sections of domain name space

The domain name space is divided into three sections: generic domains, country domains, and inverse domain.

Generic Domains: It defines the registered hosts according to their generic behaviour. It uses three-character labels, and these labels describe the organization type. Example- .com, .edu, .mil, .org, .net

Country Domain: It uses two-character country abbreviations. Example- .in, .us, .uk

Inverse Domain: The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Discuss Persistence timer in TCP

To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer. When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged. The probe causes the receiving TCP to resend the acknowledgment which was lost.

Briefly discuss five approaches to congestion control

Open Loop Congestion Control

1. **Retransmission Policy:** Retransmission timers are designed to prevent congestion and optimize efficiency.

2. **Window Policy:** Selective repeat window is adopted as it sends the specific packet that has been lost.
3. **Discarding Policy:** Router partially discards the corrupted or less sensitive packages and maintain the quality of a message.
4. **Acknowledgment Policy:** The receiver sends acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver sends an acknowledgment only if it has to send a packet or if a timer expires.
5. **Admission Policy:** If there is a congestion in the network, router denies establishing a virtual network connection to prevent further congestion.

Closed Loop Congestion Control

1. **Backpressure:** Congested node stops receiving packets from upstream node.
2. **Choke Packet Technique:** Whenever the resource utilization exceeds the threshold value, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic.
3. **Implicit Signalling:** The source guesses that there is congestion in a network.
4. **Explicit Signalling:** If a node experiences congestion it can explicitly sends a packet to the source to inform about congestion.

Explain the working of Reverse Address Resolution Protocol

1. **RARP Request:** The device needing an IP address broadcasts a RARP request packet containing its MAC address.

2. **Server Response:** A RARP server on the network, maintaining a table of MAC-to-IP mappings, receives the request.

3. **Matching Address:** If the server finds a matching MAC address in its table, it sends a unicast RARP reply packet containing the corresponding IP address back to the device.

4. **IP Assignment:** The device receives the reply, obtains its IP address, and configures its network interface based on it.

Discuss transmission impairment in computer networks

1. **Attenuation:** The strength of signal decreases with increasing distance which causes loss of energy. Amplifiers are used to amplify the attenuated signal.
   Attenuation(dB) = $10\log_{10}(P2/P1)$
   P1 is the power at sending end and P2 is the power at receiving end.
   Attenuation(dB) = $20\log_{10}(V2/V1)$
   V1 is the voltage at sending end and V2 is the voltage at receiving end.
2. **Distortion:** It means changes in shape of the signal. In composite signals, every component arrives at different time which leads to distortion.
3. **Noise:** The random or unwanted signal that mixes up with the original signal is called noise. Types of noise:
   - **Thermal noise:** is generated due to the random motion of electrons in a wire.

- **Induced noise:** is generated in a circuit by a varying magnetic or electrostatic field produced by another circuit.
- **Crosstalk:** happens when signal in one wire affects the signal in the other wire.
- **Impulse**: is a signal with high energy

Explain the factors which affect the performance of a network.

1. **Network Infrastructure:** Network Infrastructure consists of routers, switches or services like IP Addressing, wireless protocols, etc.

2. **Applications Used in the Network:** Applications that have poor performance can take large bandwidth. Complicated applications need maintenance

3. **Network Issues:** Network issue like congestion, hardware failure, packet loss can affect network performance

4. **Network Security:** Security measures such as firewalls and encryption that are implemented to protect the network can introduce processing overhead.

Write the functions of physical, network and transport layers.

Functions of the Physical Layer

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock.
- **Bit rate control:** The Physical layer also defines the transmission rate
- **Physical topologies:** Physical layer specifies how the different devices are arranged in a network
- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination.
- **Logical Addressing:** The sender & receiver's IP addresses are placed in the header to distinguish each device uniquely.

Functions of the Transport Layer

- **Segmentation and Reassembly:** Transport layer accepts the message from the session layer, and breaks it into smaller units. It then reassembles the message at the destination station.
- **Service Point Addressing:** The transport layer header includes service point address to deliver the message to the correct process.

What are physical & logical addresses? Discuss the working of Address Resolution Protocol.

Physical Addresses (MAC Addresses): A unique 48-bit address assigned to the hardware interface of a network device

Logical Addresses (IP Addresses): A unique address that identifies the device on the network.

Working of ARP:

1. **ARP Request:** When a device needs to send data to another device on the same network, it first checks its ARP cache for the MAC address associated with the destination IP address.
2. **Broadcast:** If the MAC address isn't found in the cache, the device sends an ARP request broadcast packet to all devices on the local network.
3. **ARP Reply:** The device with the matching IP address responds with an ARP reply packet containing its MAC address.
4. **Cache Update:** The sender device updates its ARP cache with the learned MAC address and can now directly send data to the destination device using its physical address.

Discuss the two node instability problem in distance vector routing. Also discuss solutions to this problem.

Two-Node Instability Problem: This problem occurs when two directly connected routers share information about a failed link prematurely, leading to a looping situation and unstable operation.

- Imagine this scenario: Routers A and B connect to Router X. Suddenly, the link between A and X breaks.
- A updates its routing table, marking X as unreachable.
- B receives this update, marks X as unreachable too, and informs A, believing it's helpful.
- A, mistakenly assuming B has a better path to X, updates its table with a route going through B.
- This creates a loop between A and B because each thinks the other has access to X.

Solution:

1. **Split Horizon:** This technique prevents a router from sharing a route back to the neighbour it originally learned from. Example: A wouldn't share the route to X with B anymore.

2. **Poison Reverse:** This method involves marking a failed route with an unreachable metric when sharing it with other routers. Example: A would tell B that X is unreachable, stopping the loop from forming.

Explain the process of fragmentation of IP packets and their reassembly at receiver's end with the help of an example.

Fragmentation is the breaking of an IPV4 packet that exceeds the MTU of the data link layer into smaller IPV4 packets. Fragmentation relies on following fields in the IPV4 header:

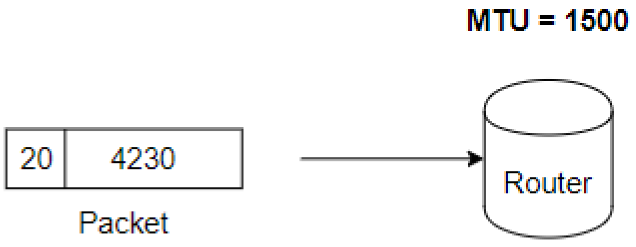
- **Identification:** To identify fragments, we use a 16-bit field. When the packet is fragmented, the identification field is copied into the fragmented packet headers.
- **Fragment offset**: This is a 13-bit field that is used to order the data into fragments. All the fragments except the last one should have data in multiples of 8.
- **MF (More fragments):** It is a one-bit flag that specifies if there are more fragments of the frame. All the fragmented packets have this flag set to 11 except the last packet which sets this flag to 00.
- **DF (Don't fragment):** It is a one-bit flag that tells the routers whether to fragment the packet or not. If it is set to 00 then the packet can be fragmented.

Reassembly

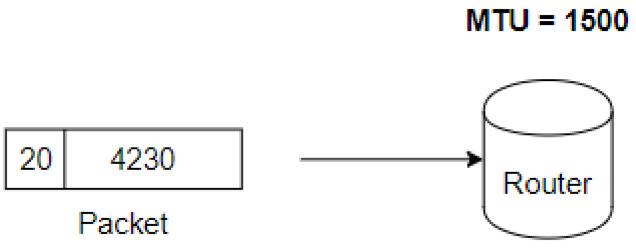
The steps of the process of reassembly are as follows:

1. The destination identifies that the packet has been fragmented using the MF and fragment offset fields.
2. The destination categorizes the incoming packets according to their identification fields. Two packets with the same identification field are put in the same category.
3. The packets within a category are sequenced using the MF and fragment offset. First, the packets with MF equal to 11 are sorted in ascending order based on their fragment offset values. Then the packet having an MF equal to 00 and a fragment offset not equal to 0 is placed at the end, since it's the last packet.

Example:



The size of the incoming packet is greater than the MTU so the router fragments the packet into smaller ones.



The first fragmented packet contains 1,480 bytes of data as it is divisible by 8, and 1,480 + 20 = 1,500, which is equal to the MTU

Packet 1

Identification: 231

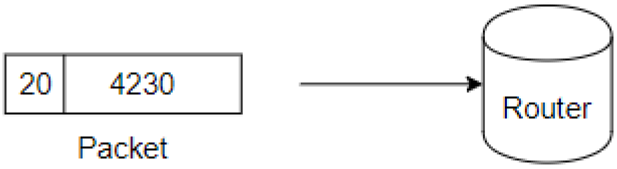
Fragment offset: 0

MF : 1

Header length : 5

The header length is 5 because it has a scaling factor of 4, meaning 5 x 4 = 20

MTU = 1500



The second fragmented packet contains 1,480 bytes of data as it is divisible by 8, and 1,480 + 20 = 1,500 which is equal to the MTU

Packet 1

Identification: 231

Fragment offset: 0

MF : 1

Header length : 5

Packet 2

Identification: 231

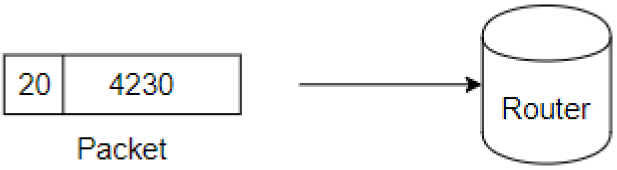
Fragment offset: 185

MF : 1

Header length : 5

The fragment offset is calculated by dividing the data in the first packet by 8 (1,480 / 8 = 185) and then adding it to the offset of the previous packet which is 0, so 185 + 0 = 185

MTU = 1500



The third fragmented packet contains the left over data which is 1270 bytes

MF = 0 as it is the last fragment

Packet 1

Identification: 231

Fragment offset: 0

MF : 1

Header length : 5

Packet 2

Identification: 231

Fragment offset: 185

MF : 1

Header length : 5

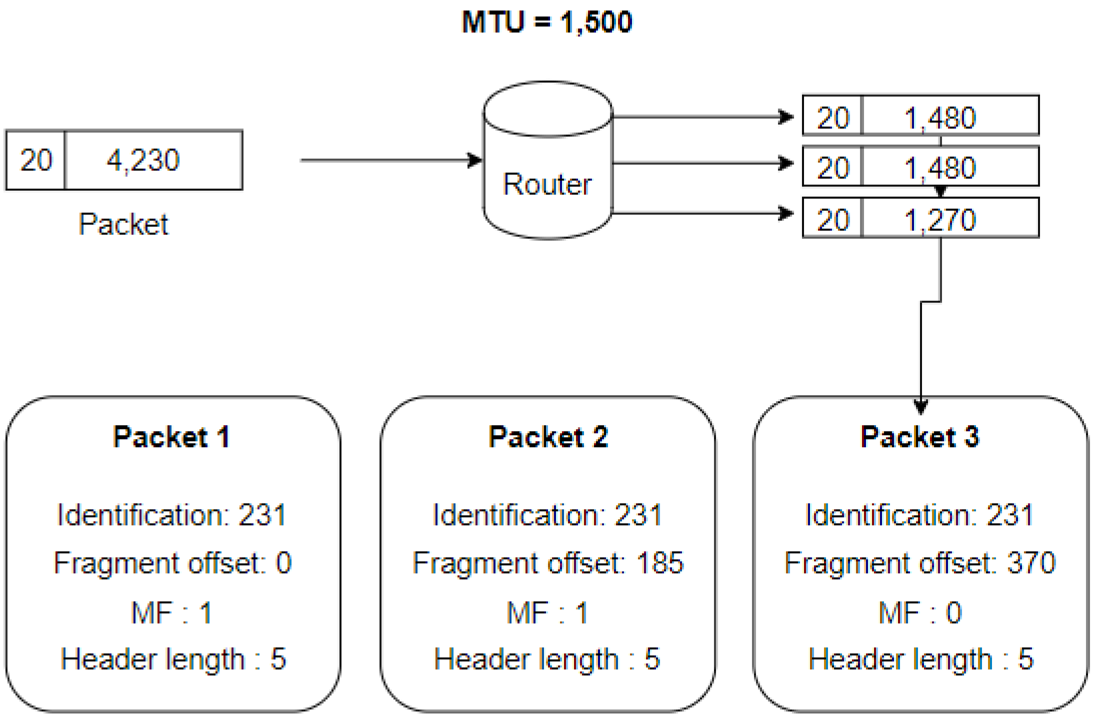
Packet 3

Identification: 231

Fragment offset: 370

MF : 0

Header length : 5

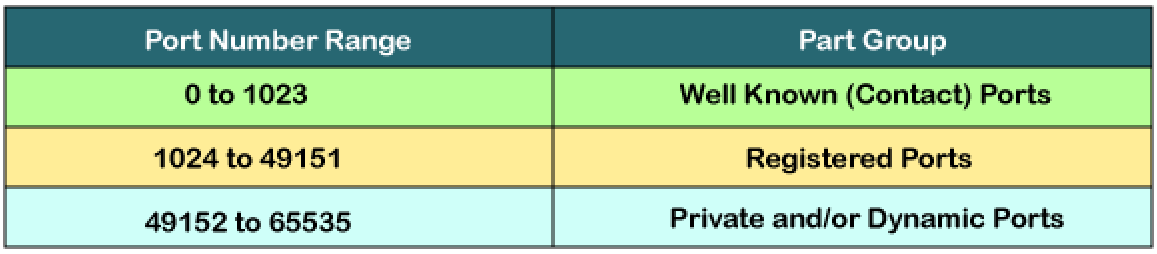


Explain the process of queuing in user datagram protocol(UDP)

UDP provides a process to process communication. The client generates the processes that need services while the server generates the processes that provide services. The queues are available for both the processes, i.e., two queues for each process. The first queue is the incoming queue that receives the messages, and the second one is the outgoing queue that sends the messages. The queue functions when the process is running. If the process is terminated, then the queue will also get destroyed

What are different categories of ports? Write uses of UDP.

1. **Well-known ports:** They are used with those protocols that serve common applications and services such as HTTP, IMAP, SMTP, etc.
2. **Registered ports:** The registered ports are used for the user processes.
3. **Dynamic ports:** They are assigned to the client application dynamically when a client creates a connection.



Port Number Range	Part Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

UDP is used for:

Multicasting, Online gaming, Real-time applications, DNS, DHCP, Voice over Internet Protocol services, Routing update protocols, Simple request-response communication

What is TCP? Discuss connection establishment in TCP.

TCP is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. It lies between the Application and Network Layers.

TCP uses Three-Way Handshake for connection establishment

1. SYN (Synchronize): The client initiates the connection by sending a SYN packet to the server, containing:

   - The client's initial sequence number (ISN)
   - The port number of the server it wants to connect to

2. SYN-ACK (Synchronize-Acknowledge): The server responds with a SYN-ACK packet, containing:

   - The server's own ISN
   - An acknowledgement of the client's ISN (by incrementing it by 1)

3. ACK (Acknowledge): The client acknowledges the server's ISN with an ACK packet, completing the handshake.

What is silly window syndrome? Discuss the syndrome created by sender and its solutions

Silly Window Syndrome is a problem that arises due to poor implementation of TCP. It degrades the TCP performance and makes the data transmission extremely inefficient. The problem is called so because:

1. It causes the sender window size to shrink to a silly value.
2. The window size shrinks to such an extent that the data being transmitted is smaller than TCP Header.

The two major causes of this syndrome are as follows:

1. Sender window transmitting one byte of data repeatedly.
2. Receiver window accepting one byte of data repeatedly.

Cause-1: Sender window transmitting one byte of data repeatedly –
Suppose only one byte of data is generated by an application . The poor implementation of TCP leads to transmit this small segment of data. Every time the application generates a byte of data, the window transmits it. This makes the transmission process slow and inefficient. The problem is solved by Nagle’s algorithm.

Nagle's algorithm suggests:

1. Sender should send only the first byte on receiving one byte data from the application.
2. Sender should buffer all the rest bytes until the outstanding byte gets acknowledged.
3. Sender should wait for 1 RTT (Round Trip Time).

After receiving the acknowledgement, sender should send the buffered data in one TCP segment. Then, sender should buffer the data again until the previously sent data gets acknowledged.

Explain cryptography. What is public and private cryptography? What are the different types of firewalls?

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

Public Key Cryptography: Two keys are used one key is used for encryption and another key is used for decryption. One key is used to encrypt the plain text to convert it into cipher text and another key is used by the receiver to decrypt the cipher text to read the message.

Private Key Cryptography: The same key is used for encryption and decryption. In this key is symmetric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public-key cryptography.

Types of Firewall

1. **Packet Filter:** It controls network access based on the source and destination IP addresses, protocols, and ports.
2. **Stateful Inspection Firewalls:** It is used to control how data packets move through a firewall.
3. **Application Layer Firewalls:** These firewalls can examine application layer information like an HTTP request.
4. **Next-generation Firewalls:** It includes features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.
5. **Circuit-level gateways:** It provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security
6. **Software Firewall:** It protects our system from any external attacks such as unauthorized access, malicious attacks, etc.
7. **Hardware Firewall:** A hardware firewall is a physical appliance that is deployed to enforce a network boundary.
8. **Cloud Firewall:** It protects a private network from any unwanted access by filtering data at the cloud level.

Explain the terms Internet, Intranet and Extranet. What are virtual private networks? Explain how these can be implemented. Explain the advantages and disadvantages of virtual private networks.

- **Internet:** The global network of interconnected computer networks, accessible to anyone with an internet connection.
- **Intranet:** A private network within an organization, accessible only to authorized employees.
- **Extranet:** A controlled extension of an organization's intranet that allows authorized external users, like partners or suppliers, limited access to specific resources.

A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet.

VPN implementation

- **Remote Access VPN:** Establishes secure connections for individuals to access their organization's network remotely.
- **Site-to-Site VPN:** Creates secure connections between geographically dispersed offices or networks.
- **Split Tunneling:** Directs only specified traffic through the VPN tunnel, while allowing other traffic to directly access the internet.

Advantages of VPN:

- **Security:** Encrypts data, protecting it from interception
- **Privacy:** Hides your internet traffic from your ISP
- **Remote Access:** Enables secure access from anywhere with an internet connection.

Disadvantages of VPN:

- **Performance:** Encryption and tunneling can add overhead, potentially slowing down internet speed.
- **Cost:** Implementing and maintaining a VPN infrastructure can increase the cost.
- **Complexity:** Setting up and managing VPNs can be technically challenging for some users.