Q1. _____ defines the format and the order of messages exchanged between two or more communicating entities (0.5)

1. Server
2. Client
3. **Protocol
4. Network edge

Q2. Which of this is not a network edge device? (0.5)

1. **Switch
2. Personal Computer
3. Smart Phone
4. Servers

Q3. Simple mail transfer protocol belongs to _____ layer in Internet protocol stack (0.5)

1. **Application
2. Transport
3. Network
4. Link

Q4. The amount of time required to push all the packet's bits into the link is _____ (0.5)

1. propagation delay
2. queuing delay
3. processing delay
4. **transmission delay

Q5. Identify the protocol characteristic that allows SMTP to send multiple messages over the same connection. (0.5)

1. Non-persistent connections
2. ** Persistent connections
3. Multithreading
4. Pipelining

Q6. Choose the statement that illustrates the role of Type NS records in the DNS hierarchy.(0.5)

1. Type NS records specify the mail servers for a domain, affecting email delivery.
2. Type NS records map alias names to canonical names, impacting name resolution.
3. ** Type NS records indicate the authoritative DNS servers for a domain, directing where queries should be routed.
4. Type NS records map hostnames to IP addresses, directly influencing network connectivity.

_____ is a TCP name for a transport service access point. (0.5)

1. **Port
2. Socket
3. Segment
4. Packet

Q8. For Stop-and-Wait ARQ, for 10 data packets sent, _____ acknowledgments are needed (0.5)

1. **exactly 10
2. less than 10
3. more than 10
4. only one

Q9. Which of the following is a valid Class B IP address? (0.5)

1. 10.1.1.1
2. **128.10.2.3
3. 191.255.254.255
4. 225.1.1.1

Q10. Which of the following IP addresses belongs to Class D? (0.5)

1. **224.0.0.1
2. 192.168.1.1
3. 10.0.0.1
4. 127.0.0.1

Type: DES

Q11. Consider the Go-Back-N protocol scenario with a window size of 7 (n=7). Analyse the sender and receiver side transmissions for the following scenarios with suitable sliding-window diagrams. Also, indicate the changes at both sender and receiver side windows for every data transmission.
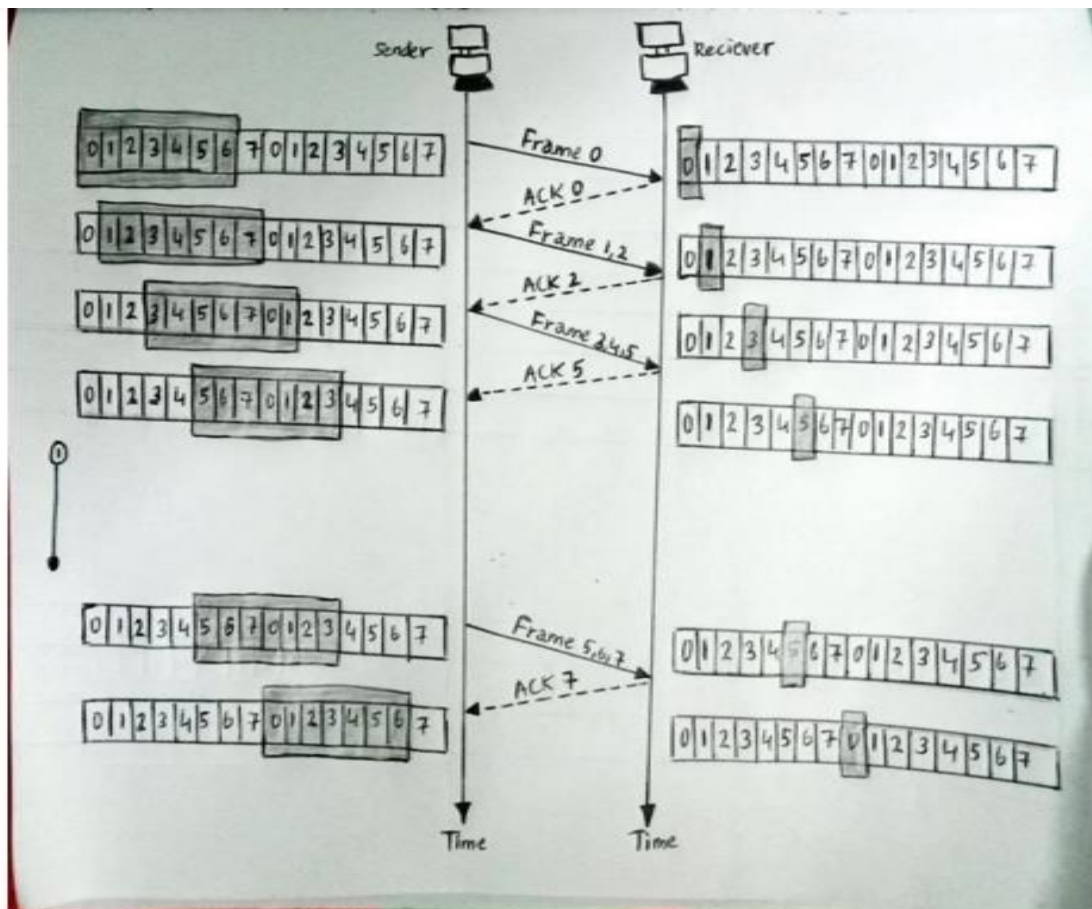
(i) Frame 0 is sent; Frame 0 is acknowledged.

(ii) Frames 1 and 2 are sent; Frames 1 and 2 are acknowledged.

(iii) Frames 3, 4, and 5 are sent; Frames 3 and 4 is acknowledged; Timer for Frame 5 expires.

(iv) Frames 5, 6, and 7 are sent; Frames 5 through 7 are acknowledged. (4)

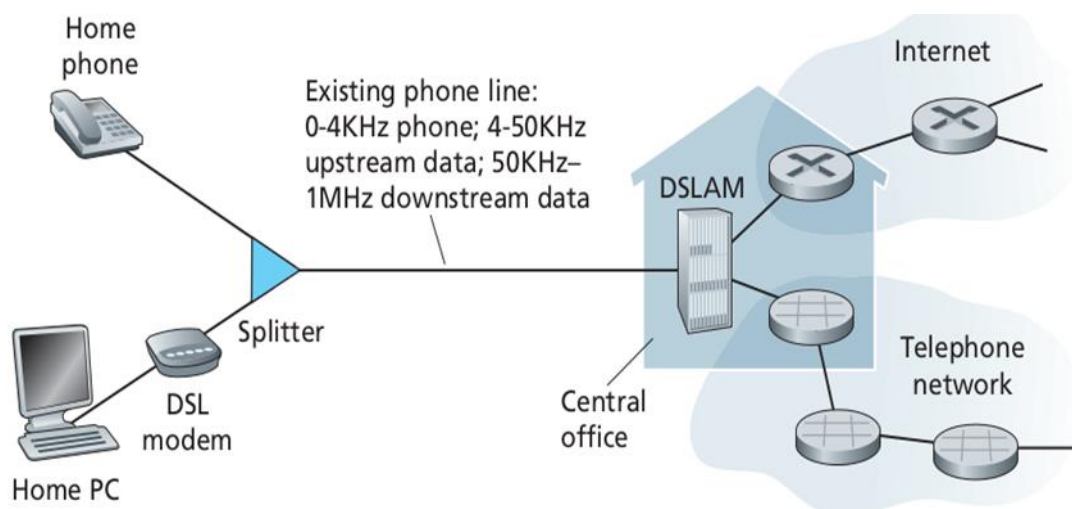**Ans: [Windows-1M, Frames-1M, Timer-1M, appropriate Ack-1M]**

Q12. Illustrate the following access networks with neat diagrams:

i.DSL

ii. Ethernet. (3)

Ans: [DSL explanation-1M, DSL Diagram-0.5M, Ethernet explanation-1M, Ethernet diagram-0.5M]

Digital subscriber line (DSL):

A residence typically obtains DSL Internet access from the same local telephone company (telco) that provides its wired local phone access. Thus, when DSL is used, a customer's telco is also its ISP. As shown in above figure, each customer's DSL modem uses the existing telephone line to exchange data with a digital subscriber line access multiplexer (DSLAM) located in the telco's local central office (CO). The home's DSL modem takes digital data and translates it to high-frequency tones for transmission over telephone wires to the CO; the analog signals from many such houses are translated back into digital format at the DSLAM. The residential telephone line carries both data and traditional telephone signals simultaneously, which are encoded at different frequencies:

  • A high-speed downstream channel, in the 50 kHz to 1 MHz band

  • A medium-speed upstream channel, in the 4 kHz to 50 kHz band

  • An ordinary two-way telephone channel, in the 0 to 4 kHz band

Ethernet:
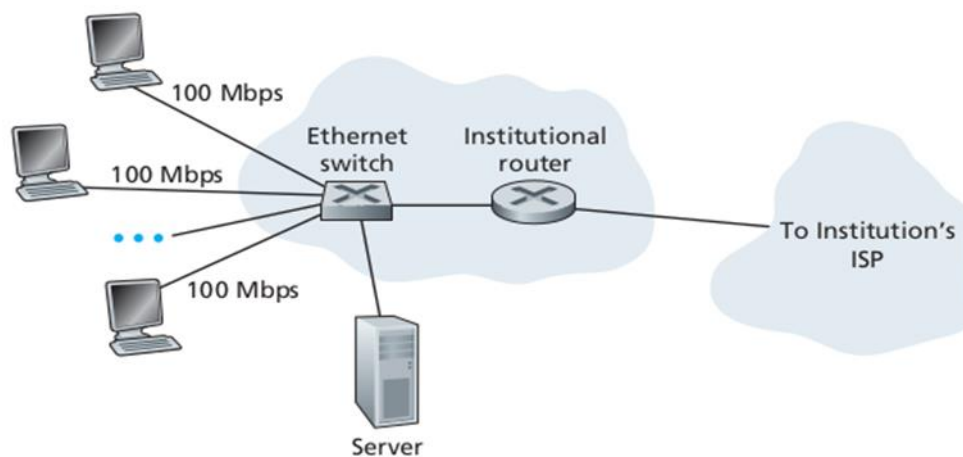
Although there are many types of LAN technologies, Ethernet is by far the most prevalent access technology in corporate, university, and home networks. As shown in above figure, Ethernet users use twisted-pair copper wire to connect to an Ethernet switch. The Ethernet switch, or a network of

such interconnected switches, is then in turn connected into the larger Internet. With Ethernet access, users typically have 100 Mbps access to the Ethernet switch, whereas servers may have 1 Gbps or even 10 Gbps access. Increasingly, however, people are accessing the Internet wirelessly from laptops, smartphones, tablets, and other devices (see earlier sidebar on "A Dizzying Array of Devices"). In a wireless LAN setting, wireless users transmit/receive packets to/from an access point that is connected into the enterprise's network (most likely including wired Ethernet), which in turn is connected to the wired Internet. A wireless LAN user must typically be within a few tens of meters of the access point. Wireless LAN access based on IEEE 802.11 technology, more colloquially known as WiFi, is now just about everywhere—universities, business offices, cafes, airports, homes, and even in airplanes.

Q13. Given that HTTP is stateless, elaborate how websites implemented by Ecommerce companies can able to track customer's sessions and preferences across multiple visits. Illustrate its working with suitable diagram. (3)

Ans: [How cookies works-2M, explanation and appropriate Diagram-1M]

To manage user sessions and personalize content, HTTP uses cookies. Defined in [RFC 6265], cookies are small data packets sent by servers to clients (browsers) that are stored and sent back with

subsequent requests. They allow websites to identify users, manage sessions, and customize content based on user preferences, making them essential for many modern web applications.
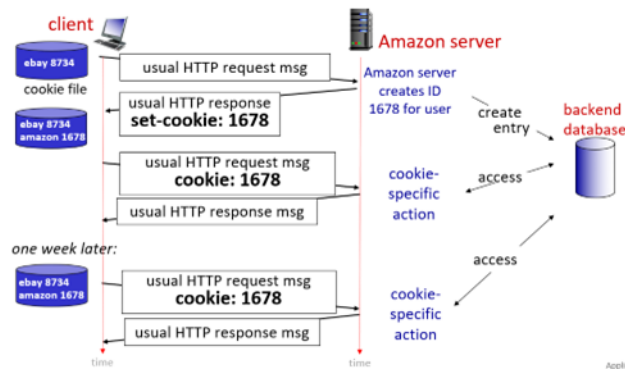
•   Initial Visit: Susan visits Amazon.com for the first time. Amazon generates a unique ID (e.g., 1678) and sends it to Susan's browser via the Set-Cookie header.

•   Cookie Storage: Susan's browser stores this ID in its cookie file.

•   Subsequent Requests: Each time Susan requests a page from Amazon, her browser includes the Cookie: 1678 header, allowing Amazon to track her actions.

•   Return Visit: If Susan returns to Amazon later, her browser continues to send the same cookie ID, enabling Amazon to recognize her and provide personalized recommendations and services.

Q14. Explain the concepts of multiplexing and demultiplexing in the transport layer.

Which transport layer protocol is to be used for the following cases. Justify your answer.

i) An application that needs to protect the boundaries of its messages.

ii) An application needs a stream-oriented environment in which it accepts the responsibility

of delivering the bytes in-order to the other side. (3)

Ans:[Multiplexing-0.5 M,Demultiplexing & ports-0.5 M, Protocol-1M, Proper Justification-1M]

Multiplexing: This process occurs at the sender's side where the transport layer combines data from multiple applications into a single data stream for transmission. Each application's data is tagged with a unique source port number, allowing the transport layer to keep track of different data streams.

Demultiplexing: At the receiver's side, the transport layer uses the destination port numbers included in the data packets to direct the data to the correct application. Each application listens on a specific port number, ensuring that data is delivered to the appropriate process.

Port Numbers: They are used to identify which application the data should be sent to or received from. This tagging allows multiplexing and demultiplexing to manage multiple data streams efficiently and accurately.

i.   UDP. UDP is a transport layer protocol that helps in transmitting each message as an

    independent user datagram thus helps in preserving the message boundary.

ii.   TCP. TCP gives a connection-oriented transport layer protocol which transmits a stream of bytes in order and reliably to the receiver.

Describe Classful Addressing of IPv4 in detail. Discuss why all the addresses in IPv4 cannot be assigned to computers.

An organization is granted a network address 172.16.0.0/16.

i) Find the first and last addresses in the block

ii) Find the maximum number of interfaces that can be used by organisation. (3)

Ans: [Classful addressing-1M, All address can't be used-0.5M, first and last address-1M, interfaces-0.5M]

IPv4 (Internet Protocol version 4) is a 32-bit addressing scheme used to identify devices on a network. In classful addressing, the 32-bit IPv4 address is divided into different parts based on predefined address classes.

1. Class A
* Range: 0.0.0.0 to 127.255.255.255

2. Class B
* Range: 128.0.0.0 to 191.255.255.255

3. Class C
* Range: 192.0.0.0 to 223.255.255.255

4. Class D
* Range: 224.0.0.0 to 239.255.255.255

5. Class E
* Range: 240.0.0.0 to 255.255.255.255

Why Not All IPv4 Addresses Can Be Assigned

* Reserved Network and Broadcast Addresses: Each network in IPv4 has two addresses that cannot be assigned to hosts: the network identifier and the broadcast address.

* Private IP Addresses: Private address ranges are reserved for internal use and cannot be used on the public internet.

These include:

* Class A: 10.0.0.0 to 10.255.255.255

* Class B: 172.16.0.0 to 172.31.255.255

* Class C: 192.168.0.0 to 192.168.255.255

These private addresses allow devices within local networks to communicate but need Network Address Translation (NAT) to access the public internet.

* Loopback and Special-Purpose Addresses: Certain addresses (like those used for loopback or reserved for multicast) are not assignable to devices on the internet.

The address range 127.0.0.0 to 127.255.255.255 is reserved for loopback testing. Any address within this range, such as 127.0.0.1, refers to the device itself (localhost).

Multicast and Experimental Addresses:

Class D and Class E addresses are reserved for multicast and experimental purposes, respectively, and cannot be assigned to hosts.

i) First Address of the block: 172.16.0.0

Last Address of the block: 172.16.255.255

ii) Maximum number of interfaces that can be connected $=2^{16}-2$

Q16. Explain the working of DNS caching. Discuss its impact on network performance and reliability. (3)

Ans: [How caching works-2M, Performance-0.5M, Reliability-0.5M]

How it Works:

Caching Process: When a DNS server receives a response to a query, it stores the information in its local cache. This cached data remains available for a set period, often up to two days, before it is discarded.

Query Handling: For subsequent queries requesting the same hostname, the DNS server can return the cached IP address directly. DNS caching not only speeds up the resolution process but also decreases the load on DNS servers and reduces overall network traffic.

• Performance Impact: DNS caching improves response time by avoiding the need for repeated queries up the DNS hierarchy. This is particularly beneficial where multiple users may request the same hostname within a short period as the server can provide almost instant responses.

• Reliability Impact: While caching improves performance, it can sometimes result in outdated information being served. If a hostname's IP address changes, the DNS server will continue to serve the cached (old) IP address until the cached entry's TTL (Time to Live) expires. This delay can lead to temporary issues if a host changes its IP address before all DNS caches across the Internet are updated.

Q17. In a block of addresses, we know the IP address of one host is 25.34.12.56/16. Find the following.

      i) Limited broadcast address

      ii) Direct Broadcast address

      iii) Network address

      iv) Address space of that block. (2)

Ans: [Each Answer-0.5 M]

i) Limited broadcast Address: 255.255.255.255

ii) Direct Broadcast Address: 25.34.255.255

iii) Network Address: 25.34.0.0

iv) Address space of the block$=2^{16}$ Addresses.

Q18. Suppose router A wants to send 1500 bytes packet to router B with transmission rate of 100Mbps then what is the transmission delay involved in sending packet from A to B?. Also, if the distance between the A and B is 480 km and the propagation speed in the transmission medium is $2.4*10^8$ m/s , then what is the propagation delay? . (2)

Ans: [Transmission delay-1M, Propagation delay-1M]

Transmission Delay = Packet length/Transmission Rate (L/R)

$$= (1500*8)/(100*10^6)$$

$$= 0.12ms$$

Propagation Delay = Distance/Speed (D/S)

$$= (480*10^3)/(2.4*10^8)$$

$$= 2ms$$

Q19. Find the class of the following IP addresses and subnet mask of that block

    i)0xD022360C

    ii)0xEE220201

    iii)0x72220208

    iv)0x810E0608. (2)

Ans: [Each answer-0.5 M]

    i)   Class C, Subnet mask : 255.255.255.0

    ii)   Class D, No subnet mask

    iii)   Class A, Subnet mask: 255.0.0.0

    iv) Class B, Subnet mask: 255.255.0.0