Web Tech - CA3 - JAI SHREE RAM 🚩🔱🕉️

Short Answer Type

1. The values GET, POST, HEAD etc are specified in `request line` of HTTP message.
2. `Maxage`attribute is used to extend the lifetime of a cookie.
3. Router is used to connect between two `Network`.
4. Calculate the network address for the IP/Subnet Mask: 192.168.10.22/24. - `192.168.10.22`
5. Cookies were originally designed for `Serversite`.
6. Example of a link state routing protocol is `OSPF`.
7. Find the oddly matched HTTP status codes. - `304 Not Found`
8. FTP protocol uses `TCP` port number `20` for data transfer.
9. Hashing functions like MD5 and SHA are used in IPSEC to provide `Data Integrity`.
10. How can you set a Cookie visibility scope to local Storage? - `/`
11. HTTPS makes a connection secure. It works on port number `443`.
12. JavaScript is used `To add interactivity to HTML Pages`.
13. NAT stands for `Network Address Translation`.
14. Perl array is initialized as `my @abc_array = (55,16,25,62,27);`
15. POP3 is used to `receive` email.
16. Servers receives requests for domains `by contacting remote DNS server`.
17. SMPT is used to `Transmit` email.
18. Telnet protocol uses port no `23` to establish a connection.
19. The first and last address of a subnet is generally known as `network` address and `broadcast` address.
20. The length of an IPv6 address is `128 bits`.
21. Which of the following is an anti-virus program? - `Norton`
22. Which of the following is present in both an HTTP request line and a status line? - `HTTP version number`
23. `window.print();` is the correct syntax to print a page using JavaScript.
24. `_myVar` Strings Are A Correct XML Name?
25. `DNS Server` hostnames into IP addresses.
26. `Dynamic DNS` allows client to update their DNS entry as their IP address change.
27. `Crawling` the process of fetching all the web pages linked to a web site.
28. You have an IP address of 172.16.13.5 with a 255.255.255.128 subnet mask. What is your class of address, subnet address, and broadcast address? - `Class B, Subnet 172.16.13.0, Broadcast address 172.16.13.127`
29. Inside `Script` HTML element do we put the JavaScript.
30. Domain name to IP address mapping is provided by `both DNS server and hosts file`.
31. SNMP is used for `Network management`.
32. CSS stands for `Cascading Style Sheets`.
33. Applet and Servlet communicate with `HTTP tunneling`.
34. SEO is to improve the volume and `Quality of traffic` to a web site from search engines.
35. URL defines four things: `protocol, host computer, port and path`
36. URL is a standard for specifying any kind of information on the `Internet`.

37. Websites fetched by crawler are indexed and kept in huge database, this process is called as `Indexing`.
38. `Spyware` usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else.
39. Fireball `is a device installed at the boundary of an incorporate to protect it against the unauthorized access`.
40. `Worm` is a type of independent malicious program that never required any host program.
41. `DoS Attack` can be considered as the class of computer threats.
42. SMTP uses the TCP port `25`.
43. Web server Apache uses the port number `80`.
44. SSL Certificate is related with `HTTPS` protocol.
45. `DNS` is the distributed mechanism for mapping domain name and IP address.

Long Answer Type

1. What is transport layer? How it is work.

- The transport layer is a crucial component of the OSI (Open Systems Interconnection) model and the TCP/IP protocol suite. Its primary function is to facilitate communication between devices across a network by providing reliable and efficient data transfer services.

- The transport layer ensures that data sent from one device reaches its destination accurately, completely, and in the correct order.

- The two most common protocols used at the transport layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

- **Here's how these protocols work:**

1. **Transmission Control Protocol (TCP)**:

    - TCP provides reliable, connection-oriented communication between devices. It ensures that data sent from one device is received by the other device intact and in the correct order.
    - TCP achieves reliability through mechanisms such as acknowledgments, sequence numbers, and retransmissions.
    - When data is sent using TCP, the sender breaks it into smaller units called segments. These segments are numbered and sent to the receiver.
    - The receiver acknowledges the receipt of each segment and informs the sender of any missing or out-of-order segments.
    - If the sender does not receive an acknowledgment within a specified time period, it retransmits the segment.
    - TCP also performs flow control to manage the rate of data transfer between devices, ensuring that the sender does not overwhelm the receiver with data.

2. **User Datagram Protocol (UDP)**:

    - UDP provides connectionless communication between devices, meaning it does not establish a direct connection before sending data.

  - Unlike TCP, UDP does not guarantee reliable delivery or ordered arrival of data. It simply sends data packets from one device to another without any acknowledgment or error-checking mechanism.
  - UDP is often used in situations where real-time communication is more critical than reliability, such as streaming media, online gaming, and VoIP (Voice over Internet Protocol).
  - Because UDP does not have the overhead of establishing and maintaining connections, it is generally faster and more efficient than TCP for certain types of applications.

- In summary, the transport layer ensures reliable and efficient communication between devices by using protocols such as TCP and UDP.
- TCP provides reliable, connection-oriented communication, while UDP offers faster, connectionless communication with fewer guarantees of reliability.
- The choice between TCP and UDP depends on the specific requirements of the application and the nature of the data being transmitted.

2. How many layers in TCP/IP protocol ? How data link layer is related to IP layer. What is doted decimal notation.

- The TCP/IP protocol suite, which is the basis of the modern internet, consists of four layers:

1. **Application Layer**:

   - This layer includes protocols that directly interact with end-users or applications, such as HTTP, FTP, SMTP, and DNS.

2. **Transport Layer**:

   - This layer is responsible for end-to-end communication and includes protocols like TCP and UDP.

3. **Internet Layer**:

   - The Internet Protocol (IP) resides in this layer, which handles addressing, routing, and fragmentation of data packets.

4. **Data Link Layer**:

   - Also known as the Network Interface Layer or Link Layer, this layer deals with the physical connection between devices and the local network topology.
   - It includes protocols like Ethernet, Wi-Fi, and PPP.

- **The relationship between the Data Link Layer and the IP layer:**

  - The Data Link Layer is responsible for the physical transmission of data between devices on the same network segment. It handles tasks such as framing, error detection, and media access control.
  - The Internet Protocol (IP) resides in the Internet Layer, one layer above the Data Link Layer. IP is responsible for routing packets across different networks to their destination using logical addresses (IP addresses).

    - The Data Link Layer and the IP layer work together to ensure that data is properly encapsulated, transmitted, and received across networks.
    - The Data Link Layer encapsulates IP packets into frames appropriate for the physical medium being used (e.g., Ethernet frames for Ethernet networks).
    - It also handles the addressing of devices on the local network, while IP deals with addressing devices globally across interconnected networks.

- **"Dotted Decimal Notation"** is a standard notation used to represent IPv4 addresses.

    - An IPv4 address is a 32-bit numerical value represented in decimal format, where each octet (8 bits) is separated by dots. Each octet is represented by its decimal value ranging from 0 to 255.
    - For example, an IPv4 address in dotted decimal notation looks like this: `192.168.1.1`.
    - This notation makes it easier for humans to read and interpret IP addresses.

3. Describe the life cycle of java applet.

- The life cycle of a Java applet refers to the sequence of events that occur from its initialization to its termination.

- Java applets are small Java programs that are designed to run within a web browser, typically to provide interactive content on a web page.

- **An overview of the typical life cycle of a Java applet:**

1. **Initialization (init)**:

    - When a web page containing a Java applet is loaded in a browser, the applet is initialized.
    - The browser loads the necessary classes and resources required for the applet to run.
    - The `init()` method of the applet is called by the browser to initialize the applet and perform any necessary setup tasks.
    - The `init()` method is typically used to initialize variables, set up the user interface, and perform any other initialization tasks required by the applet.

2. **Start (start)**:

    - After initialization, the applet enters the start-up phase.
    - The `start()` method of the applet is called by the browser to start the execution of the applet.
    - The `start()` method is where the applet begins its execution, such as starting animation, processing user input, or initiating other tasks.

3. **Running (running)**:

    - Once started, the applet enters the running state.
    - During this phase, the applet performs its main tasks, such as rendering graphics, handling user interactions, and responding to events.
    - The applet continues to execute until it is stopped or terminated.

4. **Stopping (stop)**:

    - The applet can be stopped either by the user or by the browser.
    - The `stop()` method of the applet is called when the applet is stopped.
    - The `stop()` method is typically used to pause any ongoing activities or release any resources held by the applet.

5. **Destroying (destroy)**:

    - When the applet is no longer needed, it is terminated.
    - The browser calls the `destroy()` method of the applet to perform any cleanup tasks.
    - The `destroy()` method is used to release any resources held by the applet, such as closing files, sockets, or freeing memory.

6. **Termination**:

    - Once the `destroy()` method completes execution, the applet is terminated, and its memory resources are released.
    - The browser unloads the applet's classes and resources, freeing up memory and system resources.

- It's important to note that the life cycle of a Java applet can vary slightly depending on the specific implementation and browser environment.
- The general sequence of `initialization`, `start`, `running`, `stopping`, and `termination` remains consistent across most Java applets.

4. For a 5 Kbytes packets sent over a 10 Mbps transmission link, what is the transmission time of the packet?

- Given,

    - Bandwidth : $10 Mbps = 10*10^6 bps$

    - Packet Size : $5KB = 5*8*2^{10}Bits$

    - Transmission Time : $$Packet Size \over Bandwidth$$

    - i.e Required Transmission Time = $${5*8*2^{10}\over10*10^{6}}=0.004096 seconds = 4.096 ms$$

5. Discuss the IP address and Class type with minimum and maximum range.

- IP addresses are unique numerical identifiers assigned to devices connected to a network used for communication between devices over the internet or local networks.

- IP addresses are divided into classes to efficiently allocate addresses based on the size of the network.

- There are five classes of IP addresses: A, B, C, D, and E. However, classes D and E are reserved for special purposes, such as multicasting and experimental use, respectively.

- The commonly used classes for regular network addressing are A, B, and C.

- **IP address classe along with their minimum and maximum ranges:**

1. **Class A**:
    - Class A IP addresses are designed for large networks with a large number of hosts.
    - The first octet (8 bits) is reserved for the network portion, and the remaining three octets (24 bits) are used to identify hosts.
    - The range of Class A IP addresses starts from 0.0.0.0 and ends at 127.255.255.255.
    - The minimum address in Class A is 0.0.0.0, and the maximum address is 127.255.255.255.
    - Class A networks can accommodate up to 16 million hosts per network.
2. **Class B**:
    - Class B IP addresses are used for medium-sized networks.
    - The first two octets (16 bits) are reserved for the network portion, and the remaining two octets (16 bits) are used to identify hosts.
    - The range of Class B IP addresses starts from 128.0.0.0 and ends at 191.255.255.255.
    - The minimum address in Class B is 128.0.0.0, and the maximum address is 191.255.255.255.
    - Class B networks can accommodate up to 65,534 hosts per network.
3. **Class C**:
    - Class C IP addresses are used for small networks.
    - The first three octets (24 bits) are reserved for the network portion, and the remaining octet (8 bits) is used to identify hosts.
    - The range of Class C IP addresses starts from 192.0.0.0 and ends at 223.255.255.255.
    - The minimum address in Class C is 192.0.0.0, and the maximum address is 223.255.255.255.
    - Class C networks can accommodate up to 254 hosts per network.
4. **Class D**:
    - Class D IP addresses are reserved for multicast addresses, which are used for one-to-many communication.
    - Multicast addresses are used to send data packets to multiple recipients simultaneously.
    - The range of Class D IP addresses starts from 224.0.0.0 and ends at 239.255.255.255.
5. **Class E**:
    - Class E IP addresses are reserved for experimental or research purposes.
    - They are not intended for regular use in networking applications.
    - The range of Class E IP addresses starts from 240.0.0.0 and ends at 255.255.255.255.

- The range of IP addresses within each class determines the number of available hosts and the size of the network that can be accommodated.

6. Discuss TCP/IP, POP, IPV$, VOIP, SMTP

1. **TCP/IP (Transmission Control Protocol/Internet Protocol)**:

- TCP/IP is a suite of communication protocols used to interconnect network devices on the internet. It provides end-to-end communication by specifying how data should be packetized, addressed, transmitted, routed, and received.
- TCP/IP consists of multiple protocols, including:
  - **TCP (Transmission Control Protocol):** Ensures reliable and ordered delivery of data packets between devices by establishing a connection, acknowledging received packets, and retransmitting lost packets.
  - **IP (Internet Protocol):** Defines the addressing scheme and routing of packets across networks. It is responsible for delivering packets from the source host to the destination host based on their IP addresses.
- TCP/IP is the foundation of the modern internet and is used for various applications, such as web browsing, email, file transfer, and more.

2. **POP (Post Office Protocol)**:

    - POP is a protocol used for retrieving emails from a remote mail server to a local email client. It operates over TCP/IP.
    - The most common version is POP3 (Post Office Protocol version 3), which allows users to download emails from the server to their local device and typically deletes the messages from the server once downloaded.
    - POP3 is widely supported by email clients, but it lacks features like synchronization between devices and server-based storage of emails.

3. **IPv6 (Internet Protocol version 6)**:

    - IPv6 is the latest version of the Internet Protocol, designed to replace IPv4 due to the exhaustion of IPv4 addresses.
    - IPv6 addresses are 128 bits in length, providing a much larger address space compared to the 32-bit addresses used in IPv4.
    - IPv6 addresses are represented in hexadecimal notation and are structured in eight groups of four hexadecimal digits separated by colons.
    - IPv6 adoption is increasing to accommodate the growing number of internet-connected devices and to support new technologies.

4. **VoIP (Voice over Internet Protocol)**:

    - VoIP is a technology that enables voice communication and multimedia sessions over the internet or other IP networks.
    - Instead of traditional circuit-switched networks, VoIP converts voice signals into digital packets and transmits them over IP networks.
    - VoIP services can include voice calls, video calls, instant messaging, and other forms of communication.
    - VoIP offers cost savings, flexibility, and integration with other IP-based services, but it may suffer from quality issues related to network latency, packet loss, and bandwidth limitations.

5. **SMTP (Simple Mail Transfer Protocol)**:

  - SMTP is a protocol used for sending emails between servers. It is part of the TCP/IP protocol suite.
  - SMTP operates on port 25 by default and is responsible for delivering outgoing emails from the sender's email client to the recipient's mail server.
  - SMTP uses a store-and-forward mechanism, where emails are temporarily stored on mail servers and forwarded to their final destination.
  - SMTP is widely used for sending transactional emails, newsletters, and other types of electronic messages over the internet.

7. For a 5 Kbytes packets sent over a 10 Mbps transmission link, what is the transmission time of the packet?

- `ALREADY ANSWERED – In question No 5`

8. You have been allocated a class B network address of 135.1.0.0 and and need to create 4 subnets each with around 200 hosts what is the easiest mask to use to satisfy the criteria?

- To create `4` subnets from a Class B network address `135.1.0.0` and accommodate around `200` hosts each, we need to determine the subnet mask that will provide enough host addresses for each subnet.

- Given that we need around 200 hosts per subnet, we need to find the subnet mask that can accommodate at least `200` host addresses. The subnet mask will determine the number of bits allocated for the network portion and the host portion.

- Let's calculate:

  - To accommodate around `200` hosts, we need at least `8` bits for the host portion (since (2^8 = 256)) and we need to reserve `1` address for network and `1` for broadcast, leaving `254` usable addresses).

  - We need to create `4` subnets, which means we need to borrow additional bits for the network portion to create enough subnets.

  - Considering we are given a Class B network address `135.1.0.0`, which has a default subnet mask of `16` bits for the network portion (Class B: `16` network bits, `16` host bits), we can extend the subnet mask to borrow more bits for subnetting while still accommodating the required number of hosts per subnet.

  - The easiest way to achieve this is to use a subnet mask of `21` bits for the network portion. This would give us:

    - `16` bits for the Class B network portion.
    - `5` bits for subnetting (which allows for `32` subnets: (2^5 = 32)).
    - `11` bits for host addresses within each subnet (which allows for `2048` hosts per subnet: $(2^{11}-2 = 2046)$ usable host addresses after reserving `1` address for the network and `1` for the broadcast).

- So, the easiest subnet mask to use to satisfy the criteria would be `135.1.0.0/21`. This would allow for the creation of 4 subnets, each with around 200 hosts.

9. Discuss the IP layer. What does UDP do.

- The IP (Internet Protocol) layer is a fundamental component of the TCP/IP protocol suite and the OSI model.
- It is responsible for routing packets of data between devices in a network, regardless of the underlying physical network topology.
- The primary functions of the IP layer include addressing, routing, and fragmentation of data packets.

1. **Addressing**:
    - IP addresses uniquely identify devices on a network. Each device connected to a network is assigned an IP address, which consists of a network portion and a host portion.
    - IPv4 addresses are 32 bits in length, typically represented in dotted-decimal notation (e.g., 192.168.1.1).
    - IPv6 addresses are 128 bits in length, represented in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
2. **Routing**:
    - The IP layer uses routing algorithms to determine the best path for data packets to reach their destination.
    - Routers and switches are devices that operate at the IP layer and make decisions about how to forward packets based on their destination IP addresses.
    - IP routers maintain routing tables that contain information about network paths and make forwarding decisions based on these tables.
3. **Fragmentation**:
    - IP layer fragmentation occurs when a packet is too large to be transmitted over a network link with a smaller maximum transmission unit (MTU).
    - The IP layer fragments the original packet into smaller fragments, each of which can be transmitted across the network link.
    - At the destination, the IP layer reassembles the fragments into the original packet before passing it to the higher-layer protocols.

UDP (User Datagram Protocol):

- UDP is a connectionless transport-layer protocol that operates on top of the IP layer.

- Unlike TCP (Transmission Control Protocol), UDP does not establish a connection before transmitting data and does not provide reliable, ordered delivery of packets.

- UDP is a lightweight protocol that offers low overhead and minimal error checking.

- **Here's what UDP does:**

1. **Connectionless Communication**:
    - UDP operates in a connectionless manner, meaning it does not establish a virtual circuit or maintain a connection state between the sender and receiver.
    - Each UDP packet (datagram) is treated as an independent unit and is transmitted without prior setup or acknowledgment.
2. **Minimal Header Overhead**:
    - UDP headers are simpler compared to TCP headers, containing only basic information such as source port, destination port, length, and checksum.
    - This minimal overhead makes UDP suitable for applications where low latency and high throughput are more important than reliability, such as real-time multimedia streaming, online gaming, DNS (Domain Name System), and SNMP (Simple Network Management Protocol).
3. **Unreliable Delivery**:
    - UDP does not provide mechanisms for error recovery, flow control, or congestion control.
    - Packets sent via UDP may be lost, duplicated, or delivered out of order without any notification to the sender or receiver.
4. **Multicast and Broadcast Support**:
    - UDP supports multicast and broadcast transmission, allowing a single packet to be sent to multiple recipients simultaneously.
    - This makes UDP suitable for applications that require one-to-many or one-to-all communication, such as multimedia broadcasting and network discovery protocols.

- UDP is a simple, lightweight transport-layer protocol that operates on top of the IP layer and provides connectionless communication with minimal overhead.
- While UDP sacrifices reliability for efficiency, it is well-suited for applications that prioritize real-time data transmission and low latency.

10. Why IP layer fragmentation is required.

- IP layer fragmentation is required to ensure that data packets can be transmitted across networks with varying maximum transmission unit (MTU) sizes.

- The MTU is the maximum size of a data packet that can be transmitted over a particular network link without fragmentation.

- If a packet's size exceeds the MTU of a network link, fragmentation is necessary to break the packet into smaller fragments that can fit within the MTU and be transmitted successfully.

- **why IP layer fragmentation is required?**

1. **Network Heterogeneity**:
    - Networks in the internet can have different MTU sizes depending on the underlying technologies and configurations.

- For example, Ethernet networks typically have an MTU of 1500 bytes, while older networks like dial-up connections may have smaller MTUs.
- When a packet travels through multiple networks with different MTUs, fragmentation allows it to adapt to each network's limitations.

2. **Path MTU Discovery**:
   - Path MTU Discovery is a mechanism that allows a sender to dynamically determine the minimum MTU along the path to the destination.
   - By sending packets with the "Don't Fragment" (DF) flag set, the sender can receive ICMP (Internet Control Message Protocol) messages indicating that a packet was too large to be forwarded without fragmentation.
   - The sender can then adjust the size of subsequent packets or enable fragmentation as needed to ensure successful delivery.

3. **Efficient Utilization of Network Resources**:
   - Fragmentation allows for the efficient utilization of network resources by ensuring that packets are transmitted as efficiently as possible given the constraints of each network link.
   - Without fragmentation, large packets may be unnecessarily dropped or require retransmission, leading to wasted bandwidth and increased latency.

4. **Handling of Large Packets**:
   - Fragmentation allows large packets to be transmitted across networks that do not support their size.
   - This is particularly important for protocols and applications that may generate large data packets, such as multimedia streaming, file transfers, or virtual private network (VPN) tunnels.

- However, while fragmentation ensures that packets can traverse networks with different MTUs, it also introduces overhead and complexity.
- Fragmented packets require additional processing and may increase the likelihood of packet loss, reordering, or duplication.
- Modern networks and protocols often strive to minimize fragmentation by using techniques such as Path MTU Discovery and optimizing packet sizes to avoid the need for fragmentation whenever possible.