Computer Networks Interview Questions

Q1. What happens when a URL is entered in the browser ?

Ans. You enter a URL into a web browser

1. Browser checks cache for DNS entry to find the corresponding IP address of the website.
2. If not found in cache, ISP's (Internet Service Provider) DNS server initiates a DNS query to find the IP address of the server that hosts the domain name.
3. The browser looks up the IP address for the domain name via DNS
4. The browser sends a HTTP *request* to the server
5. The server sends back a HTTP *response*
6. The browser begins rendering the HTML
7. The browser sends requests for additional objects embedded in HTML (images, css, JavaScript) and repeats steps 3-5.
8. Finally, Done.

Q2. What is DNS ? Explain it's working .

Ans. DNS is the Domain Name System. It is considered as the devices/services directory of the Internet. It is a decentralized and hierarchical naming system for devices/services connected to the Internet. It translates the domain names to their corresponding IPs. For e.g. google.com to 8.8.8.8. It uses port 53 by default.

Working:-

1. The user logs onto their Internet Service Provider (ISP) to use the Internet.
2. The user opens up a web browser and types a URL into the address bar.
3. The computer then asks the ISP's DNS servers for the specific IP address for a given site.
4. Once the DNS server that holds this specific IP address for a site is found, the DNS server responds with the appropriate IP address, and the user's computer then gives this address to the user's browser.
5. The browser opens a connection to the server using the IP address provided and retrieves the page from the site requested.
6. The browser displays the requested page on the computer screen.

Q3. What is a 3-way handshake / how TCP connection is established ?

Ans. A three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server.

- Step 1: In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.
- Step 2: In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of the segment that is received and SYN signifies what sequence number it should be able to start with the segments.
- Step 3: In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.

Q4. What is a firewall ?

Ans. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.A firewall can be hardware, software, or both.

Working:-

Firewalls can be configured in several different ways. For example, a basic firewall may allow traffic from all IP addresses except those flagged in a blacklist. A more secure firewall might only allow traffic from systems or IP addresses listed in a whitelist.

Q5.What is VPN ?

Ans. A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks.

Working:-

1. The VPN software on your computer encrypts your data traffic and sends it (via your Internet Service Provider) to the VPN server through a secure connection.
2. The encrypted data from your computer is decrypted by the VPN server.
3. The VPN server will send your data on to the internet and receive a reply, which is meant for you, the user.
4. The traffic is then encrypted again by the VPN-server and is sent back to you.
5. The VPN-software on your device will decrypt the data so you can actually understand and use it.

Q6. What are the HTTP and the HTTPS protocol?

Ans. HTTP is the HyperText Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on the World Wide Web (WWW). It helps the web browsers and web servers for communication. It is a 'stateless protocol' where each command is independent with respect to the previous command. HTTP is an application layer protocol built upon the TCP. It uses port 80 by default. HTTPS is the HyperText Transfer Protocol Secure or Secure HTTP. It is an advanced and secured version of HTTP. On top of HTTP, SSL/TLS protocol is used to provide security. It enables secure transactions by encrypting the communication and also helps identify network servers securely. It uses port 443 by default.

Q7. What is Stop-and-Wait Protocol?

In Stop and wait protocol, a sender after sending a frame waits for an acknowledgment of the frame and sends the next frame only when acknowledgment of the frame has been received.

Q8. What are Unicasting, Anycasting, Multicasting and Broadcasting?

- Unicasting: If the message is sent to a single node from the source then it is known as unicasting. This is commonly used in networks to establish a new connection.
- Anycasting: If the message is sent to any of the nodes from the source then it is known as anycasting. It is mainly used to get the content from any of the servers in the Content Delivery System.
- Multicasting: If the message is sent to a subset of nodes from the source then it is known as multicasting. Used to send the same data to multiple receivers.

- Broadcasting: If the message is sent to all the nodes in a network from a source then it is known as broadcasting. DHCP and ARP in the local network use broadcasting.

Q9.What is NIC and its function?

Ans. A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.