Computer networking interview questions

**1. What does PoP stand for?**

Post Office Protocol (PoP) is an email protocol used by local email clients to retrieve emails from a remote server over a TCP/IP connection. POP3 typically uses port 110 for non-encrypted communication and port 995 for encrypted (SSL/TLS) communication.

**2. What is OSI model?**

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and implement network communications by dividing them into seven distinct layers.

**3. Identify the layer which provides service to the user.**

The layer in the OSI model that provides services directly to the user is the Application Layer (Layer 7).

**Examples of Protocols at the Application Layer:**

HTTP (Hypertext Transfer Protocol): Used for web browsing.

FTP (File Transfer Protocol): Used for file transfers.

SMTP (Simple Mail Transfer Protocol): Used for email transmission.

DNS (Domain Name System): Used for resolving domain names to IP addresses.

**4. What is a HUB?**

A hub is a basic networking device used to connect multiple Ethernet devices, making them act as a single network segment. It operates at the Physical Layer (Layer 1) of the OSI model.

**5. What does a set of rules define?**

Protocol in networking indeed defines a set of rules and conventions for communication between network devices.

**6. What is HTTP?**

HTTP, or HyperText Transfer Protocol, is the foundation of data communication on the web. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands. HTTP is used to request and deliver web pages, images, videos, and other resources over the Internet.

**7. What is the length of the MAC address?**

A Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communications on the physical network segment. The length of a MAC address is:

48 bits, which is equivalent to 6 bytes.

**8. What does port number 143 refer to?**

Port number 143 is associated with the Internet Message Access Protocol (IMAP). IMAP is a standard protocol used by email clients to retrieve messages from a mail server over a TCP/IP connection.

**9. What does TCP/IP stand for?**

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It is a suite of communication protocols used to interconnect network devices on the internet and private networks.

**10. What is a proxy server also known as?**

A proxy server is also known as a proxy or application-level gateway. It acts as an intermediary between a client seeking a resource and the server providing that resource.

**11. What is SNMP and why is it important?**

SNMP (Simple Network Management Protocol) is a protocol used for monitoring and managing network devices. It is important because it allows network administrators to collect and organize information about network performance, detect issues, and ensure efficient network operation.

**12. What is the collection of the hyperlinked document on the internet known as?**

The collection of hyperlinked documents on the internet is known as the **World Wide Web** **(WWW)** or simply the **Web**.

**13. Why are parity bits used?**

Parity bits are used for error detection in digital communication and data storage. They help ensure data integrity by allowing the detection of errors in transmitted or stored data.

**14. What is the location of a resource on the internet given by?**

The location of a resource on the internet is given by URL.

**15. What is SMTP?**

Simple Mail Transfer Protocol (SMTP) is a standard protocol used for sending and receiving email messages between servers.

**Port 25 :** The default port for SMTP communication.

**Port 465 :** Used for SMTPS, which is SMTP over SSL/TLS, providing encrypted communication.

**16. What is a router?**

A router is a networking device that forwards data packets between computer networks, directing the data along the most efficient routes. It connects multiple networks, manages traffic, and ensures that data reaches its destination.

**17. What is a switch?**

A switch is a networking device that connects devices within a local area network (LAN), forwarding data packets to their intended destination based on the device's MAC address. It operates at the data link layer (Layer 2) of the OSI model.

**18. What is a repeater?**

A repeater is a networking device that regenerates or amplifies incoming electrical or optical signals before retransmitting them. Repeaters operate at the physical layer (Layer 1) of the OSI model and are commonly used in telecommunications and networking to ensure reliable data transmission over extended distances.

**19. What is FTP?**

FTP stands for File Transfer Protocol. It's a standard network protocol used to transfer files between a client and a server on a computer network. FTP operates on a client-server architecture, where the client initiates a connection to the server to perform file transfer operations. The **default port number** for FTP (File Transfer Protocol) is **21.**

**20. What is MIME?**

MIME stands for Multipurpose Internet Mail Extensions. It is a standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs.

**21. Identify the major difference between SNMPv3 and SNMPv2.**

The major difference between SNMPv3 (Simple Network Management Protocol version 3) and SNMPv2 (Simple Network Management Protocol version 2) lies in their security features.

**22. What is a LAN?**

LANs(Local Area Networks) are commonly used to connect computers, servers, printers, and other devices within a specific location to facilitate communication and resource sharing. They are characterized by high data transfer rates, low latency, and typically do not require leased telecommunication lines.

**23. What is a computer network?**

A computer network is a system of interconnected devices (like computers, servers, and routers) that communicate to share resources and data. Key components include nodes (devices), transmission media (cables/wireless), network interface cards (NICs), switches, and routers.

**24. Explain the difference between a LAN, MAN, and WAN.**

**LAN** is for small, localized areas.

**MAN** is for larger areas like cities.

**WAN** spans very large areas, potentially worldwide.

**25. What is the TCP/IP model? How does it differ from the OSI model?**

The TCP/IP model is a four-layer framework used for network communications:

**Application Layer :** Interfaces with applications (e.g., HTTP, FTP).

**Transport Layer :** Manages data transfer (e.g., TCP, UDP).

**Internet Layer :** Handles addressing and routing (e.g., IP).

**Network Interface Layer :** Deals with physical hardware connections.

**Differences :**

**Layers :** TCP/IP has 4 layers, OSI has 7.

**Origin :** TCP/IP is practical and widely used, developed for the internet; OSI is more theoretical and detailed.

**Application Layer Functions :** TCP/IP combines OSI's application, presentation, and session layers into one.

**26. What is an IP address? What are the different types of IP addresses?**

An IP address (Internet Protocol address) is a unique numerical identifier assigned to each device connected to a network, enabling it to communicate with other devices.

**Types of IP Addresses :**

**IPv4 Addresses :** 32-bit number, written as four decimal numbers separated by dots (e.g., 192.168.1.1).

**IPv6 Addresses :** 128-bit number, written as eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

**27. What is a subnet mask? How is it used in networking?**

A subnet mask is a 32-bit number used in networking to divide an IP address into the network and host portions.

**Usage :**

**Identifying Networks and Hosts :** Determines if an IP address is within the same local network.

**Subnetting :** Divides a large network into smaller subnets for efficient management and reduced traffic.

**Routing :** Helps routers direct packets to the correct network segment.

**28. What is a DNS server?**

A DNS server (Domain Name System server) translates domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers use to identify each other on the network.

**29. What is DHCP?**

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network configuration parameters (subnet mask, default gateway, DNS servers) to devices on a network.

**30. Explain the difference between TCP and UDP.**

**TCP:**

1. Connection-oriented.

2. Ensures reliable data transfer with error checking and correction.

3. Data is delivered in order and without duplication.

4. Suitable for applications requiring reliability, like web browsing and email.

**UDP:**

1. Connectionless.

2. Faster but does not guarantee reliable data transfer.

3. Data can be lost, duplicated, or received out of order.

4. Suitable for applications where speed is crucial and some data loss is acceptable, like video streaming and online gaming.

**31. What is HTTP and HTTPS?**

HTTP (HyperText Transfer Protocol) is a protocol for transmitting web pages over the internet. HTTPS (HyperText Transfer Protocol Secure) is the secure version of HTTP, using encryption (SSL/TLS) to protect data in transit.

**32. What is the purpose of ARP?**

The purpose of ARP (Address Resolution Protocol) is to map IP addresses to their corresponding MAC addresses within a local network.

**33. What is ICMP and what are its uses?**

ICMP (Internet Control Message Protocol) is used for network diagnostics and error reporting. Its uses include :

1. Echo requests and replies (e.g., ping) to check connectivity.

2. Network error reporting (e.g., destination unreachable).

3. Network congestion control and troubleshooting.

**34. Explain the function of the SSL/TLS protocol.**

SSL/TTLS (Secure Sockets Layer/Transport Layer Security) protocol encrypts data transmitted over the internet to ensure privacy, data integrity, and secure authentication between clients and servers.

**35. What is Telnet and SSH?**

**Telnet** is a network protocol used for remote access to a computer or network device, providing a command-line interface. It is not secure as it transmits data in plain text.

**SSH** (Secure Shell) is a secure network protocol for remote access and management of computers and network devices, encrypting data to protect against attacks.

**36. What is a modem?**

A modem (modulator-demodulator) is a device that converts digital data from a computer into analog signals for transmission over telephone lines and vice versa.

**37. What is a firewall?**

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

**38. What is a gateway in networking?**

A gateway in networking is a device that connects different networks, enabling communication between devices on different protocols or network architectures. It acts as a translator, forwarding data between networks with different protocols.

**39. What is a proxy server and how does it work?**

A proxy server acts as an intermediary between users and the internet. It receives requests from users, forwards them to web servers, receives responses, and sends them back to users. It can enhance security, privacy, and performance by caching data and filtering requests.