🦚 राधे राधे 🦚

---

1. **What is a network?**

    - A network is a collection of computers, servers, mainframes, network devices, or other devices connected to one another to share resources and information.

2. **What is a protocol?**

    - A protocol is a set of rules that define how data is transmitted and received over a network. Examples include HTTP, FTP, TCP/IP, and SMTP.

3. **What is the OSI model?**

    - The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and implement standard networking protocols in seven layers:
        - **Physical Layer:** Transmits raw bit streams over a physical medium.
        - **Data Link Layer:** Provides node-to-node data transfer and error detection/correction.
        - **Network Layer:** Handles routing of data packets between devices across multiple networks.
        - **Transport Layer:** Manages end-to-end communication, flow control, and error recovery.
        - **Session Layer:** Establishes, manages, and terminates connections between applications.
        - **Presentation Layer:** Translates data between the application layer and the network, handling data encryption, compression, and translation.
        - **Application Layer:** Provides network services directly to end-user applications.

4. **Explain the TCP/IP model.**

    - The TCP/IP model is a four-layer conceptual model for networking that includes:
        - **Network Interface Layer:** Handles hardware addressing and defines protocols for the physical transmission of data.
        - **Internet Layer:** Manages logical addressing and routing, primarily using the IP protocol.
        - **Transport Layer:** Provides reliable data transfer and communication services between devices (TCP) and connectionless services (UDP).
        - **Application Layer:** Includes protocols for specific data communication services on a network, such as HTTP, FTP, and SMTP.

5. **What is the difference between TCP and UDP?**

    - **TCP (Transmission Control Protocol)** is connection-oriented, meaning it establishes a connection between sender and receiver before transmitting data, ensuring reliable and ordered delivery. It uses error checking, flow control, and acknowledgments.
    - **UDP (User Datagram Protocol)** is connectionless, meaning it sends data without establishing a connection, providing faster but less reliable transmission. It does not guarantee delivery, order, or error checking.

6. **What is a subnet?**

- A subnet, or subnetwork, is a segmented piece of a larger network. It improves network performance and security by dividing larger networks into smaller, more manageable sections.

7. **What is an IP address?**

   - An IP (Internet Protocol) address is a unique identifier assigned to each device connected to a network that uses the IP protocol for communication. It allows devices to locate and communicate with each other on a network.

8. **What are the differences between IPv4 and IPv6?**

   - IPv4 uses 32-bit addresses, supporting around 4.3 billion unique addresses. IPv6 uses 128-bit addresses, supporting approximately 3.4 x 10^38 unique addresses. IPv6 also includes improved security features, simplified header format, and enhanced support for Quality of Service (QoS).

9. **What is a MAC address?**

   - A MAC (Media Access Control) address is a unique identifier assigned to the network interface card (NIC) of a device. It is used for communication on the physical network segment. MAC addresses are 48 bits long and usually displayed in hexadecimal format.

10. **What is DNS?**

    - DNS (Domain Name System) translates human-readable domain names (like www.example.com) into IP addresses that networking equipment needs to deliver information. It is a hierarchical and decentralized naming system that ensures the proper resolution of domain names to IP addresses.

11. **What is DHCP?**

    - DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses and other network configuration parameters to devices on a network. This allows devices to join a network without needing a manually assigned IP address.

12. **What is a firewall?**

    - A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.

13. **What is a VPN?**

    - A VPN (Virtual Private Network) creates a secure, encrypted connection over a less secure network, such as the internet. It allows remote users to securely access an organization's internal network as if they were directly connected to it.

14. **What is a router?**

    - A router is a device that forwards data packets between computer networks. It determines the best path for data to travel from the source to the destination. Routers operate at the network layer (Layer 3) of the OSI model.

15. **What is a switch?**

    - A switch is a device that connects devices within a network and uses packet switching to forward data to its destination. Switches operate at the data link layer (Layer 2) of the OSI model and can also operate at the network layer (Layer 3) in more advanced forms.

16. **What is NAT?**

    - NAT (Network Address Translation) modifies the IP address information in IP packet headers while in transit across a traffic routing device. It allows multiple devices on a local network to share a single public IP address, improving security and conserving IP addresses

17. **What is a VLAN?**

    - A VLAN (Virtual Local Area Network) groups together devices on a network into logical subnets, regardless of their physical location. This helps improve network management and security by isolating broadcast domains and segmenting network traffic.

18. **What is an IDS?**

    - An IDS (Intrusion Detection System) monitors network traffic for suspicious activity and potential threats, alerting administrators of detected anomalies. IDSs can be network-based (NIDS) or host-based (HIDS).

19. **What is an IPS?**

    - An IPS (Intrusion Prevention System) not only detects but also prevents identified threats in real-time by taking corrective action, such as blocking traffic or resetting connections. It is a proactive extension of an IDS.

20. **What is SSL/TLS?**

    - SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols designed to provide secure communication over a computer network. They use encryption to protect data and ensure privacy and data integrity.

21. **What is a DMZ in network security?**

    - A DMZ (Demilitarized Zone) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually the internet. It acts as a buffer zone between the internal network and the external world.

22. **What is a honeypot?**

    - A honeypot is a security mechanism that creates a decoy to attract attackers and detect, deflect, or study hacking attempts. It appears to be a legitimate part of the network but is isolated and monitored.

23. **What is a proxy server?**

   - A proxy server acts as an intermediary for requests from clients seeking resources from other servers. It provides increased security and privacy by hiding the client's IP address and filtering traffic.

24. **What is port scanning?**

    - Port scanning is a technique used to identify open ports and services available on a networked device. It is often used for security assessments and by attackers to find vulnerabilities.

25. **What are the common network ports and their associated services?**

    - Common ports include:
      - 20: FTP data transfer
      - 21: FTP command (File Transfer Protocol)
      - 22: SSH (Secure Shell)
      - 23: Telnet (Terminal Network)
      - 25: SMTP (Simple Mail Transfer Protocol)
      - 53: DNS (Domain Name System)
      - 69: TFTP (Trivial)
      - 80: HTTP (Hypertext Transfer Protocol)
      - 88: Kerberos - Network Authentication System
      - 110: POP3 (Post Office Protocol 3)
      - 143: IMAP (Internet Message Access Protocol)
      - 443: HTTPS (HTTP Secure)
      - 636: LDAP
      - 902: VMware
      - 993: IMAP Secure
      - 995: POP3 Secure
      - 3306: MySQL

26. **What is a network topology?**

    - Network topology refers to the arrangement of different elements (links, nodes, etc.) in a computer network. It can be physical (layout of cables and devices) or logical (path that data takes).

27. **What is a mesh network?**

    - A mesh network is a network topology in which each node relays data for the network and all nodes cooperate in the distribution of data. This provides high reliability and redundancy.

28. **What is a star topology?**

    - In a star topology, all devices are connected to a central hub or switch. Communication between devices is managed through this central point. It is easy to install and manage but can be affected by the failure of the central hub.

29. **What is a ring topology?**

    - In a ring topology, each device is connected to two other devices, forming a circular data path. Data travels in one direction until it reaches its destination. Ring topology can be disrupted by a single point of failure.

30. **What is a bus topology?**

    - In a bus topology, all devices share a common communication line or bus. Data is sent in one direction, and all devices receive the data but only the intended recipient processes it. It is simple to set up but can be prone to collisions and signal degradation.

31. **What is a hybrid topology?**

    - A hybrid topology combines two or more different types of topologies to form a resultant topology. It leverages the strengths and mitigates the weaknesses of each combined topology.

32. **What is the difference between a hub and a switch?**

    - A hub broadcasts data to all devices in a network segment, while a switch forwards data only to the specific device it is intended for.

33. **What is ARP?**

    - ARP (Address Resolution Protocol) is used to map an IP address to a MAC address within a local network segment.

34. **What is ICMP?**

    - ICMP (Internet Control Message Protocol) is used for error messages and operational information queries, such as ping and traceroute.

35. **What is a socket?**

    - A socket is an endpoint for sending or receiving data across a computer network.

36. **What is a three-way handshake in TCP?**

    - A three-way handshake is a process used in TCP to establish a connection between a client and server. It involves SYN, SYN-ACK, and ACK packets.

37. **What is a ping command?**

    - The ping command is used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the originating host to a destination computer.

38. **What is traceroute?**

    - Traceroute is a network diagnostic tool used to track the pathway taken by a packet on an IP network from source to destination.

39. **What is an IPsec?**

    - IPsec (Internet Protocol Security) is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet in a communication session. It operates at the network layer to provide end-to-end security.

40. **What is a network packet?**

- A network packet is a formatted unit of data carried by a packet-switched network.

41. **What is QoS?**
    - QoS (Quality of Service) is a feature that manages data traffic to reduce packet loss, latency, and jitter on a network.
42. **What is SNMP?**
    - SNMP (Simple Network Management Protocol) is used for managing devices on IP networks and collecting and organizing information about managed devices.
43. **What is a man-in-the-middle attack?**
    - A man-in-the-middle attack is a security breach where a malicious actor intercepts and possibly alters the communication between two parties without their knowledge.
44. **What is spoofing?**
    - Spoofing is a technique where an attacker disguises themselves as another user or device on a network to gain access to data or resources.
45. **What is a DDoS attack?**
    - A DDoS (Distributed Denial of Service) attack overwhelms a network or service with traffic from multiple sources, causing it to become unavailable.
46. **What is a VPN tunnel?**
    - A VPN tunnel is an encrypted connection established between two points over a public network. It allows secure data transmission between the VPN client and server, protecting data from interception and unauthorized access.
47. **What is a zero-day exploit?**
    - A zero-day exploit targets a previously unknown vulnerability in software or hardware that has not yet been patched by the vendor.
48. **What is encryption?**
    - Encryption is the process of converting data into a coded format to prevent unauthorized access.
49. **What is a network interface card (NIC)?**
    - A NIC (Network Interface Card) is a hardware component that allows a computer or device to connect to a network. It provides the necessary interface for communicating over a network using a specific protocol like Ethernet or Wi-Fi.
50. **What is CSMA/CD?**
    - CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is a network protocol used in Ethernet networks to manage data transmission and avoid collisions. Devices listen to the

network for a carrier signal before transmitting and back off for a random time if a collision is detected.

51. **What is CSMA/CA?**

    - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is a network protocol used in wireless networks to avoid collisions. Devices listen for a clear channel before transmitting and use acknowledgments to confirm successful transmission.

52. **What is a cryptographic hash function?**

    - A cryptographic hash function is an algorithm that takes an input and produces a fixed-size string of characters, which is typically a digest that uniquely represents the input data.

53. **What is a firewall rule?**

    - A firewall rule defines how a firewall should filter and control incoming and outgoing network traffic. Rules specify criteria such as IP addresses, port numbers, and protocols to allow or block specific types of traffic.

54. **What is network segmentation?**

    - Network segmentation divides a network into smaller, isolated sections to improve security and performance. Segmentation can prevent the spread of malware, limit the impact of breaches, and manage network traffic more effectively.

55. **What is a stateful firewall?**

    - A stateful firewall monitors the state of active connections and makes decisions based on the context of the traffic, not just the individual packets. It tracks the state of connections and uses this information to allow or block traffic.

56. **What is a stateless firewall?**

    - A stateless firewall filters packets based solely on predefined rules without considering the state of the traffic. It inspects each packet individually, allowing or blocking it based on static rules.

57. **What is a demilitarized zone (DMZ)?**

    - A DMZ (Demilitarized Zone) is a physical or logical subnetwork that separates an internal local area network (LAN) from other untrusted networks, typically the internet. It contains and exposes an organization's external-facing services to reduce the risk to the internal network.

58. **What is a honeynet?**

    - A honeynet is a network of honeypots designed to attract and analyze potential attackers. It mimics a real network to deceive attackers and gather intelligence on their methods and tools.

59. **What is network sniffing?**

    - Network sniffing is the process of monitoring and capturing data packets traveling across a network.

60. **What is SSL/TLS handshake?**

    - The SSL/TLS handshake is a process that establishes a secure connection between a client and server. It involves the exchange of keys, the negotiation of encryption algorithms, and the authentication of the server (and optionally the client) to set up a secure communication channel.

61. **What is a secure shell (SSH)?**

    - SSH (Secure Shell) is a protocol for securely accessing and managing network devices over an unsecured network. It provides encrypted communication, authentication, and command execution capabilities, replacing older, less secure protocols like Telnet.

62. **What is a wireless access point (WAP)?**

    - A WAP (Wireless Access Point) allows wireless devices to connect to a wired network using Wi-Fi. It acts as a bridge between the wired and wireless portions of the network, providing connectivity and managing wireless traffic.

63. **What is WPA2?**

    - WPA2 (Wi-Fi Protected Access 2) is a security protocol and security certification program developed to secure wireless computer networks. t uses stronger encryption (AES) and authentication methods (802.1X) than its predecessor, WPA.

64. **What is a rogue access point?**

    - A rogue access point is an unauthorized WAP installed on a network, often used to gain unauthorized access or conduct man-in-the-middle attacks.

65. **What is a network ACL?**

    - A network ACL (Access Control List) is a set of rules used to control network traffic and restrict access to network resources. ACLs can be applied to routers, switches, and firewalls to permit or deny traffic based on criteria like IP addresses and port numbers.

66. **What is a VPN concentrator?**

    - A VPN concentrator is a device that provides secure, remote access to multiple VPN connections.

67. **What is a network bridge?**

    - A network bridge connects and filters traffic between two or more network segments, functioning at the data link layer (Layer 2) of the OSI model.

68. **What is a BGP?**

    - BGP (Border Gateway Protocol) is a protocol used to exchange routing information between autonomous systems on the internet. It ensures that data can be routed efficiently and accurately across the interconnected networks that make up the internet.

69. **What is a DHCP lease?**

- A DHCP lease is a temporary IP address assignment given by a DHCP server to a client device for a specified period.

70. **What is a network load balancer?**

    - A network load balancer distributes incoming network traffic across multiple servers to ensure no single server becomes overwhelmed. It improves performance, reliability, and availability by balancing the load.

71. **What is a multicast?**

    - Multicast is a method of sending network traffic from one sender to multiple receivers in a single transmission.

72. **What is port forwarding?**

    - Port forwarding redirects communication requests from one address and port number to another, often used to make services on a private network available to external users.

73. **What is NAT overload (PAT)?**

    - NAT overload, also known as PAT (Port Address Translation), allows multiple devices on a local network to share a single public IP address by using different port numbers. It conserves IP addresses and allows multiple devices to access the internet simultaneously.

74. **What is a network monitoring tool?**

    - A network monitoring tool continuously observes a network for performance issues, failures, and security threats.

75. **What is a VLAN hopping attack?**

    - A VLAN hopping attack exploits network misconfigurations to send packets to different VLANs, potentially gaining unauthorized access to network resources.

76. **What is an SSL VPN?**

    - An SSL VPN uses Secure Sockets Layer (SSL) to provide secure remote access to network resources over an encrypted connection.

77. **What is an IPsec VPN?**

    - An IPsec VPN uses the IPsec protocol suite to create a secure and encrypted communication channel over the internet.

78. **What is a network tap?**

    - A network tap is a hardware device that provides a way to access the data flowing across a computer network for monitoring and analysis.

79. **What is a service level agreement (SLA)?**

    - An SLA is a contract between a service provider and a customer that specifies the performance, availability, and other service-related expectations and obligations.

80. **What is a time-to-live (TTL) value?**
    - A TTL value is a field in an IP packet that specifies the maximum number of hops the packet can take before being discarded.
81. **What is a network redundancy?**
    - Network redundancy involves adding extra or backup components to a network to ensure it remains operational in case of a failure.
82. **What is a remote access VPN?**
    - A remote access VPN allows individual users to connect securely to a private network from a remote location.
83. **What is a site-to-site VPN?**
    - A site-to-site VPN connects entire networks to each other, such as a branch office network to a headquarters network.
84. **What is an Ethernet frame?**
    - An Ethernet frame is a data packet on an Ethernet network that includes the payload data along with source and destination MAC addresses and error-checking information.
85. **What is a network hub?**
    - A network hub is a simple device that connects multiple computers in a local network, broadcasting data to all connected devices.
86. **What is a FQDN?**
    - An FQDN (Fully Qualified Domain Name) specifies the exact location of a domain within the DNS hierarchy, including the hostname and all domain levels.
87. **What is a link-local address?**
    - A link-local address is an IP address that is valid only for communication within the local network segment or subnet.
88. **What is a network collision?**
    - A network collision occurs when two devices on the same network segment transmit data simultaneously, causing the data to interfere and become corrupted.
89. **What is the difference between unicast, multicast, and broadcast?**
    - Unicast is one-to-one communication, multicast is one-to-many communication, and broadcast is one-to-all communication within a network.
90. **What is a wildcard mask?**
    - A wildcard mask is used in network configurations to specify a range of IP addresses in access control lists (ACLs) and routing policies.

91. **What is a private IP address?**

    - A private IP address is an IP address used within a private network, not routable on the internet.
    - Class A: 10.0.0.0 - 10.255.255.255
    - Class B: 172.16.0.0 - 172.31.255.255
    - Class C: 192.168.0.0 - 192.168.255.255

92. **What is a public IP address?**

    - A public IP address is an IP address that is routable on the public internet and can be accessed by external networks. It is assigned by ISPs and used for communication between devices on different networks.

93. **What is a broadcast domain?**

    - A broadcast domain is a network segment where a broadcast packet sent by any device is received by all other devices in the same segment.

94. **What is a collision domain?**

    - A collision domain is a network segment where data packets can collide with each other when being sent on a shared medium.

95. **What is a subnet mask?**

    - A subnet mask is a 32-bit number that divides an IP address into the network and host portions. It determines the range of IP addresses within a subnet by masking the network part and leaving the host part.

96. **What is an autonomous system (AS)?**

    - An autonomous system (AS) is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet.

97. **What is dynamic routing?**

    - Dynamic routing is a method where routers automatically update their routing tables based on network changes and current conditions.

98. **What is static routing?**

    - Static routing involves manually configuring fixed routes in a router's routing table.

99. **What is a routing table?**

    - A routing table is a data table stored in a router or networked computer that lists the routes to particular network destinations. It includes information on network paths and metrics used to determine the best route for data packets.

100. **What is a default gateway?**

  - A default gateway is a device that routes traffic from a local network to devices on other networks, often used to connect a local network to the internet.

101. **What is two-factor authentication (2FA)?**

  - 2FA (Two-Factor Authentication) is a security mechanism that requires two forms of verification before granting access to an account or system. It typically combines something the user knows (password) with something they have (smartphone, hardware token) or something they are (biometric).

102. **What is a broadcast storm?**

  - A broadcast storm occurs when there is an excessive amount of broadcast traffic on a network, overwhelming devices and causing network performance issues. It can be caused by misconfigurations, loops, or faulty devices.

💖 Thank You 💖
