1. What is a Network?
   A network is a group of connected devices (like computers and phones) that share data and resources. It allows communication between devices using cables or wireless signals.
2. What is a Protocol?
   A protocol is a set of rules that devices follow to communicate in a network. It helps different devices understand and exchange data properly.
3. What is an IP Address?
   An IP address is a unique number given to each device in a network. It helps in identifying and locating devices for sending and receiving data.
4. What is the difference between IPv4 and IPv6?
   IPv4 uses 32-bit addresses and supports around 4 billion devices. IPv6 uses 128-bit addresses and can support a much larger number of devices.
5. What is a MAC Address?
   A MAC address is a unique hardware ID given to a device's network card. It helps in identifying devices on a local network.
6. What is a Subnet?
   A subnet is a smaller part of a network created to organize and manage traffic better. It helps improve network speed and security.
7. What is DNS?
   DNS stands for Domain Name System. It changes website names (like google.com) into IP addresses that computers understand.
8. What is DHCP?
   DHCP stands for Dynamic Host Configuration Protocol. It automatically gives IP addresses to devices when they join a network.
9. What is the difference between a Hub, a Switch, and a Router?
   A hub sends data to all devices, a switch sends it to the right device, and a router connects different networks and manages traffic between them.
10. What is a Firewall?
    A firewall is a security tool that blocks harmful data and allows safe data. It protects the network from unauthorized access.
11. What is NAT (Network Address Translation)?
    NAT changes private IP addresses into a public IP before sending data to the internet. It helps save IP addresses and improves security.
12. What is the OSI Model?
    The OSI model explains how data moves through a network in 7 steps (layers). Each layer has a special job in sending or receiving data.
13. What is the difference between the OSI and TCP/IP models?
    The OSI model has 7 layers, while the TCP/IP model has 4 layers. Both describe how data travels, but TCP/IP is used in real networks.
14. What are TCP and UDP?
    TCP and UDP are communication protocols. TCP is reliable and checks for errors, while UDP is faster but doesn't check for errors.
15. What is the difference between TCP and UDP?
    TCP makes sure data reaches correctly and in order, making it reliable but slower. UDP sends data quickly but may lose or mix up data.
16. What is a Socket?
    A socket is a connection point between two devices to send or receive data. It uses an IP address and port number for communication.
17. What is a Port Number?
    A port number helps identify specific services or applications on a device. It makes sure the data goes to the correct program.

18. What is a VLAN?
    A VLAN is a virtual LAN that lets devices in different places act like they are on the same network. It improves management and security.
19. What is a VPN?
    A VPN is a secure connection over the internet. It hides your data and location, helping you stay private and safe online.
20. What is Bandwidth?
    Bandwidth is the amount of data that can be sent over a network in a certain time. Higher bandwidth means faster data transfer.
21. What is Latency?
    Latency is the time it takes for data to travel from the sender to the receiver. Lower latency means faster communication.
22. What is Throughput?
    Throughput is the actual amount of data successfully transferred over a network in a given time. It shows how efficiently the network works.
23. What is a Gateway?
    A gateway connects two different networks and allows data to flow between them. It acts like a bridge between different systems or protocols.
24. What is the difference between an Intranet and the Internet?
    The internet is a public network used globally, while an intranet is a private network used inside a company or organization.
25. What is a Ping Command?
    Ping checks if a device is reachable over the network and shows how fast the connection is. It's useful for testing network problems.
26. What is Traceroute?
    Traceroute shows the path data takes to reach a destination. It helps find where delays or problems happen in a network.
27. What is a Proxy Server?
    A proxy server acts as a middleman between users and the Internet. It improves security, speeds up access, and hides user identity.
28. What is Load Balancing?
    Load balancing spreads network traffic across multiple servers. This helps avoid overload and keeps services fast and reliable.
29. What is the difference between Unicast, Multicast, and Broadcast?
    Unicast sends data to one device, multicast to a group, and broadcast to all devices in a network.
30. What is an ARP (Address Resolution Protocol)?
    ARP finds the MAC address of a device when only its IP address is known. It helps send data to the right hardware on a network.
31. What is ICMP (Internet Control Message Protocol)?
    ICMP is used to send error messages and test tools like ping. It helps with network troubleshooting and diagnostics.
32. What is a Default Gateway?
    A default gateway is the device that routes data from a local network to other networks, usually the Internet.
33. What is SSL/TLS?
    SSL/TLS are security protocols that encrypt data sent over the internet. They keep your online activities private and safe.
34. What is a DMZ in networking?
    A DMZ (Demilitarized Zone) is a part of a network where public servers are placed. It adds a security layer by separating internal systems from the internet.

35. What is Port Forwarding?
    Port forwarding directs data from the internet to a specific device or service in your network. It's used for things like hosting a game server.
36. What is a Packet?
    A packet is a small unit of data sent over a network. Large messages are broken into packets and reassembled at the destination.
37. What is Packet Switching?
    Packet switching breaks data into small packets and sends them independently. It's fast and efficient for data transmission.
38. What is the difference between Static and Dynamic IP?
    A static IP doesn't change and is set manually, while a dynamic IP is given automatically and may change each time you connect.
39. What is Network Congestion?
    Network congestion happens when too much data tries to travel at once, slowing down the network. It's like traffic on a busy road.
40. What is a Mesh Network?
    In a mesh network, each device connects to many others. This makes the network stronger and keeps it working even if one device fails.
41. What is a Subnet Mask?
    A subnet mask separates the IP address into the network and host parts. It helps identify which part of the IP belongs to the network and which to the device.
42. What is a MAC Address?
    A MAC (Media Access Control) address is a unique ID given to a device's network card. It's used for communication inside a local network.
43. What is DHCP (Dynamic Host Configuration Protocol)?
    DHCP automatically gives IP addresses to devices on a network. It saves time and avoids manual IP setup.
44. What is NAT (Network Address Translation)?
    NAT changes private IP addresses into a public IP address so devices can access the internet. It helps save IP addresses and adds a layer of security.
45. What is DNS (Domain Name System)?
    DNS translates domain names like google.com into IP addresses. It helps browsers find websites easily.
46. What is a VPN (Virtual Private Network)?
    A VPN creates a secure, private connection over the internet. It protects your data and hides your IP address.
47. What is an IP Address?
    An IP address is a unique number given to every device connected to a network. It helps identify and locate the device.
48. What are IPv4 and IPv6?
    IPv4 uses 32-bit addresses and supports fewer devices. IPv6 is newer and uses 128-bit addresses, allowing many more devices to connect.
49. What is the difference between TCP and UDP?
    TCP is reliable and ensures data reaches correctly, while UDP is faster but doesn't guarantee delivery. TCP is like a phone call; UDP is like a text message.
50. What is a Switch?
    A switch connects multiple devices in a network and sends data to the right one. It works at the data link layer (Layer 2).
51. What is a Hub?
    A hub connects network devices but sends data to all of them, not just the one that needs it. It's slower and less smart than a switch.

52. What is a Router?
    A router connects different networks and sends data between them. It's commonly used to connect a home network to the internet.
53. What is the OSI Model?
    The OSI model is a framework with 7 layers that explain how data moves through a network. It helps understand how networks work.
54. What is the TCP/IP Model?
    The TCP/IP model is a 4-layer model used to describe how data is sent over the Internet. It's based on real-world protocols.
55. What is the difference between the OSI and TCP/IP models?
    The OSI model has 7 layers and is more of a guide, while the TCP/IP model has 4 layers and is used in real networks.
56. What is a Protocol in Networking?
    A protocol is a set of rules for how data is sent and received. Examples are TCP, IP, HTTP, and FTP.
57. What is Bandwidth?
    Bandwidth is the maximum amount of data that can move through a network in a given time. More bandwidth means faster speed.
58. What is a VLAN (Virtual LAN)?
    A VLAN groups devices on different physical networks into a single virtual network. It improves security and organization.
59. What is the difference between Public and Private IP addresses?
    Public IPs are used on the internet and are unique, while private IPs are used inside networks and can repeat in different places.
60. OSPF vs RIP:

Feature	OSPF	RIP
Speed	Fast	Slow
Updates	When changes happen	Every 30 seconds
Path decision	Cost-based	Hop count
Use	Big networks	Small networks

61. . What is the difference between static and dynamic routing?

- Static routing: Manually set routes.
- Dynamic routing: Routers learn paths automatically using protocols like OSPF or RIP.

62. What is routing?
    Routing means choosing the best path for data to travel from the sender to the receiver across networks.
63. What is a routing table?
    A routing table is like a map in a router that helps it decide where to send data.
64. What is OSPF?
    OSPF is a routing protocol that finds the best path using a method called Dijkstra's algorithm.. What is RIP?
    RIP is a simple routing protocol that uses hop count to choose the best path. Less used today.
65. What is BGP?
    BGP is the routing protocol used between big networks on the internet (like between Google and ISPs).

66. What is a reverse proxy?
    A reverse proxy is a server that receives requests from users and forwards them to the right web server. It also hides the real servers and protects sensitive data from direct access.

67. What is the role of the address in a packet traveling through a datagram network?
In a datagram network, the address in the packet helps send data from the sender to the final receiver. It is used for end-to-end delivery.

68. Can a routing table in the datagram network have two entries with the same destination address?
No, it can't. Each destination address in the routing table must be unique to avoid confusion about where to send the packet.

69. What kind of arithmetic is used to add data items in checksum calculation?
One's complement arithmetic is used in checksum calculations. It helps find errors in data by adding binary numbers in a special way.
70. Define piggybacking.
Piggybacking is when a device adds an acknowledgment (ACK) to the data it's sending. This way, it saves space and makes communication more efficient.

71. What are the advantages and disadvantages of piggybacking?
Advantage: It uses network bandwidth better by sending data and ACKs together.
Disadvantage: If there's too much delay, it can cause missed ACKs and re-sending of data.

72. Which technique is used in byte-oriented protocols?
Byte stuffing is used. It adds extra bytes to the data to avoid confusion when the data has patterns that look like control signals.

73. Name of the software layers or User support layer in the OSI model.

Application layer
Presentation layer Session layer
74. Name the hardware layers or network support layers in the OSI model.
Network layer
Datalink layer
Physical layer

75. Define the HTTPS protocol.
The full form of HTTPS is the Hypertext Transfer Protocol Secure. It is an advanced version of the HTTP protocol. Its port number is 443 by default. It uses the SSL/TLS protocol for providing security.

76. Name some services provided by the application layer in the Internet model?
Some services provided by the application layer in the Internet model are as follows: Mail services, Directory services, File transfer, Access management, and Network virtual terminal.