Top 50 Networking Interview Questions – 2023

By Great Learning Team Updated on Jan 13, 2023 5873

With many upcoming jobs promised in the Networking field, it makes sense to gain new proficiencies and enhance your skillset by preparing well in advance for the upcoming job interview. During the interview, you are likely to receive questions that test your in-depth knowledge about Networking and areas of expertise. We have enlisted the top 50 Networking Interview Questions that the interviewers typically ask to help you prepare and formulate responses in your own words.

1. What is Networking?

Networking refers to the interconnection of various computing devices to communicate and exchange information and resources such as data, software, hardware, etc. Different computing devices such as servers, desktops, laptops, smartphones, tablets connected through multiple paths for sending or receiving the data are known as Hosts. Any networking system's foundation is formed by specialised devices or mediums, also known as Network Devices. Some examples include routers, switches, modems, access points, hubs, and bridges. Networking is essential for offering faster communication, supporting businesses, sharing resources, providing entertainment, etc., in virtually every sphere of life.

2. What is Switch in Networking?

A Switch in Networking is a small hardware device that connects multiple devices such as computers, printers, wireless access points, etc., within one local area network (LAN). It is the key building block of any network and enables the connected devices to send, receive or forward information with each other. A switch operates in layer 2, also known a the OSI model's Data Link layer. Switches are the most commonly used component of networks based on Asynchronous Transfer Mode (ATM), Ethernet, InfiniBand, and more. These work by reducing the workload on the individual PCs and thereby increasing the overall bandwidth of the network. Switches use MAC addresses to support unicast, multicast, and broadcast communications to selected destination ports. These are broadly categorised into four types – Unmanaged switch, Managed switch, LAN switch, and PoE switch.

3. What is Router in Networking?

A Router is a networking device that sends, receives, and analyses data packets within the connected computer networks. A router is a layer three network device used in LAN (Local Area Network) and WAN (Wide Area Network) environments. When the data packet arrives, it inspects the destination IP address, consults its routing tables, calculates the best way to forward it and transfers it along the chosen route. Routers work on the routing protocol to prioritise the data to be transferred for each transmission. These are an essential part of modern computer networking, not just for establishing internet connections or data transmissions but also to provide additional security. By embedding firewalls and content filtering software, routers help businesses from malicious online websites and unwanted content. There are various routers available in the market depending upon their usages, such as wireless routers, edge routers, broadband routers, core routers and brouters.

4. What is Protocol in Networking?

A Protocol is an established set of rules that govern how devices exchange information within a network quickly and reliably. In other words, network protocols can be equated to a common language for two devices that enable them to have seamless communication, similar to how two people from different regions of the world may not understand each other's native language but can still communicate using a 'shared' third language.

Protocols are often classified based on the OSI (Open Systems Interconnection) model layer they belong to. Some of the most important protocols used on the internet are –

- HTTP: The HyperText Transfer Protocol (HTTP) is an application layer protocol that provides the foundation for the World Wide Web.
- TCP: The Transmission Control Protocol (TCP) is a transport layer protocol used with IP and often referenced together as TCP/IP.
- TLS/SSL: Transport Layer Security is used for encryption and previously called Secure Sockets Layer (SSL)

6. What is a Firewall in Networking?

A Firewall is a network security device that monitors all incoming and outgoing traffic and permits, blocks, or drops data packets based on a defined set of security rules. In other words, a firewall establishes a barrier between your internal network and the incoming traffic from untrusted external sources such as the internet to block malicious traffics such as viruses and hacking.

A firewall can be implemented in the form of either a software or hardware device though it is best to have both. A software firewall is a program installed on your computer to regulate traffic through applications or port numbers. In contrast, a hardware firewall is a physical device installed between your network and gateway.

7. What is Gateway in Networking?

A Gateway is a networking hardware device that acts as a 'gate' to form a passage between two network devices with two high-level protocols. A gateway is a layer three network system or device used for both LAN and WAN interconnects to serve as a transitional task. In other words, it acts as a translator between two systems that use different languages, data formats, architectures, or communication protocols.

The gateway acts as the entry and exit point for a network to manage the data inflows and outflows. It stores information about the routing paths of networks in communication and transmits data across them using the packet switching technique.

8. What is Hub in Networking?

A Hub is a networking device that allows you to connect multiple computing devices to a single network. It also acts as a multi-port repeater to amplify signals that deteriorate after travelling through a series of connecting cables. A hub has many ports to connect multiple wires from different branches. It can be used for both digital and analog data to broadcast messages primarily. Hubs are passive physical devices that do not have any software associated with them. They are not intelligent devices and do not perform any message filtering. Hubs are mainly used in home networks or small organisations for network monitoring and connectivity. There are two types of hubs – Active Hub and Passive Hub.

9. What is Computer Networking?

Computer Networking is the practice of sharing information and resources using the interconnection of multiple devices within a network system. It allows users to create and store files in one computer system so that they can access them from another computer(s) within the same network. The main benefits of computer networking include –

- File sharing
- Resource sharing
- Sharing devices such as printers, scanners, or fax machines
- Sharing software on remote systems
- and sharing a single internet connection
- Increasing storage capacity using network-attached storage devices
- Improved communication using emails, instant messaging, videos, etc.

10. What is Bridge in Networking?

A Bridge is a networking device that connects multiple LANs to create a single, aggregated network segment. This process of aggregating networks to form a larger LAN is known as Network Bridging. Bridges work as the layer 2 network or data link layer of the OSI model and transmit data as data frames. A wireless bridge connects networks having wireless segments. Bridges help improve network performance by separating a network into different sections or segments with different bandwidth. It can block or forward the incoming data frame after inspecting it for the destination MAC address. Switches are preferred over bridges in modern LANs as bridges generally connect fewer networks.

11. What is ARP in Networking?

The acronym ARP stands for Address Resolution Protocol (ARP) which is a communication protocol used to find the MAC (Media Access Control) address of a host from its IP address. It is an important protocol in networking used to convert a 32-bit Internet Protocol (IP) address, typically for IPv4, to a 48-bit MAC address in a LAN.

There are four types of ARP –

- Proxy ARP
- Gratuitous ARP
- Reverse ARP
- Inverse ARP

12. What is DNS in Networking?

DNS stands for Domain Name System, which, at its most basic, works like the phone book for the internet. You can think of DNS like your smartphone's contact list, which matches contact's names with their phone numbers and email addresses.

DNS is a hierarchical host naming system connected to the internet or any private network. The process involves converting the domain names of participating entities or hosts to a computer-friendly IP address. DNS has been one of the foundations of the functionality of the internet since 1985. Though we don't realise it, we use DNS to check our emails or while browsing on our smartphones every day. Whenever you connect to the internet, the DNS server that you use is automatically established by your network provider.

13. What is Ping in Networking?

A Ping is a software utility used to verify the reachability of a specific IP address on a network. It was first developed by Michael Muss in 1983 to quickly test various points of the network and get a response. It works by sending Internet Control Message Protocol (ICMP) echo requests to the host of a destination computer and then waiting for an echo reply. The ping is initiated several times to get responses echoed back to the source provides important information such as –

- consistency in the network connection
- bytes sent and received
- approximate duration of the round-trip time
- packets sent, received, or lost

14. What is Server in Networking?

A network server is computer hardware or software that acts as a central repository unit and provides data or information to other computers within the network. Hosting certain files or programs on one of the many networking servers enables users to access them by connecting to that server via   LAN or WAN. There are many types of servers, such as web servers, email servers, file servers and more. A major advantage of this approach is that if a user loses their data, they can access their most important files stored on the network server. Additionally, multiple users can make changes to a single document or have access to shared devices such as a printer or a scanner. By offering a centralised location to store files, a network server helps improve file management and data security.

15. What is VLAN in Networking?

VLAN is a virtual extension of LAN which works as a subnetwork for the collection of devices that communicate with one another within one logical network. The devices are physically apart but configured to communicate as if they are attached to the same wire. Implementing VLANs offers more flexibility than non-virtual network solutions and reduced security risks. It also helps in reducing traffic congestion as individual VLANs works as a separate LAN. Having a VLAN is cost-effective for organisations as it helps to expedite network operations and facilitates flexible teamwork.

16. What is NAT in Networking?

NAT is an acronym for Network Address Translation. It is a process of mapping multiple local private addresses to a public one inside a private network. It can be configured to assign only one address for the entire network for both security and economic purposes. NAT allows a router to act as an interface between the public network or the internet and a private or local network. It can also be used to enable selective access outside the network and conserve private IP addresses used within an organisation hidden from the world.

17. What is Networking in Computer?

Networking in a computer system refers to connecting two or more computers within an information system. The primary purpose of networking is to share data, communicate with one another (mainly for business purposes) and provide technical support.

The computers may be physically linked through optical cables, telephone lines or using wireless technology such as radiofrequency waves, infrared beams or satellites using a variety of network topologies. The most common types of networking in computers include –

- LAN or Local Area Network: A LAN comprises a collection of small devices in one physical location and may include both wireless or wired devices.
- WAN or Wide Area Network: A WAN connects devices over a large geographical area comprising of multiple LANs.
- Enterprise Network: Enterprise networks are built for large organisations and may use both LAN and WAN across their campus or data centres.
- Service-provider Network: Service-provider network uses WAN to offer simple connectivity to individual users of an organisation as well as supply internet or cellular services to their customers.

18. What is a Router in Networking?

A Router is a networking device that connects two or more sub-networks or packet-switched networks. Most routers pass data traffic between LANs and WANs with the help of IP routing protocols. A router is more capable than other network devices such as a hub or a switch. It analyses data sent over a network, determines its path and changes how it is packaged to send it over to a different network. Routers are most commonly used in home networking to connect multiple computers using a shared internet connection.

19. What is Port in Networking?

A Port is a communication endpoint in networking through which information flows from a program on the computer to another computer on the network. Think of a port as a docking point where all private boats are docked.

Ports are numbered, and each port is associated with a distinct service. They allow computers to differentiate between different kinds of incoming and outgoing traffic over the same network connection. Some ports are reserved for specific protocols, such as HTTP (HyperText Transfer Protocol) uses port 80, FTP (File Transport Protocol) uses port 21, emails received on a local computer use TCP port 25. Each host can have 65535 ports per IP address, and the use of these ports is managed by IANA (Internet Assigned Numbers Authority).

20. What is DHCP in Networking?

DHCP stands for Dynamic Host Configuration Protocol. It is a network protocol used on IP addresses to automate the process of configuring devices and allow for seamless communication on the network.

A DHCP server automatically assigns IP addresses to each host on the network, thus allowing them to use services such as DNS and any other communication protocol to communicate with other endpoints. This process simplifies the management of IP addresses on the same network and greatly reduces the errors made by manually assigning them. Using DHCP, IP conflicts are reduced, and it is easy to change addresses or endpoints.

21. What is Router in Networking and How it works?

A router is a virtual networking device that serves two main functions: receive, analyse and forward data packets to intended IP addresses and allow multiple computing devices to share the same internet connection.

How does it work?

A Router analyses the destination IP addresses of data packets and decide their routing path. To direct these data packets effectively, the router uses a routing protocol, compares it with its internal routing table and identifies the best path from the list to the network destination. It then forwards the data packet down the most efficient path to the given IP address. Routers also help to filter out unwanted interference, provides high-speed internet connectivity, allows users to configure ports as per their requirements and carry out data encapsulation or decapsulation processes.

22. What is IP address in Networking?

IP address stands for Internet Protocol address and is a unique identifying number for each device connected to the network. An IP address is expressed as a set of four numbers with each number in the set ranging from 0 to 255, for example – 192.152.1.34.

IP addresses are not random strings of numbers. They are allocated by the Internet Assigned Numbers Authority (IANA) to help maintain the internet's security. It was developed in the 1970s and formed the foundation of the internet protocol suite. All the devices connected over the same network can find, send or exchange information with the other connected device using the IP Address protocol. There are two main versions of the IP addresses – IPv4 and IPv6.

23. What is Socket in Networking?

A Socket is a software structure that allows for communication between two or more programs running on the same or different machines within a network node. It can be seen as the endpoint of two-way communication commonly used in client-server applications. A socket can be created by linking the IP number of a system with a software port number where IP number and port number are separated by a ':'.

24. What is Routing in Networking?

Routing is a process of selecting a path for traffic across one or more networks. Network routing protocols use metrics to determine the optimal path for data packet delivery. For example, in the case of packet-switching networks such as the internet, routing helps to determine the best paths for Internet Protocol (IP) packets to travel from source to their destination.

Routing is performed by layer 3 or network layer for the process of most efficient path determination. It can be classified into three categories –

- Static routing
- Dynamic routing
- Default routing

25. What is a Switch in Networking?

A network switch is a hardware device that connects multiple devices (such as computers, printers, servers, etc.) to a network to facilitate the sharing of information and resources. The devices can communicate with each other and share information regardless of whether they are in the same building or not. The most common form of the network switch is the Ethernet switch.

Switches in networking work on either layer 2 of the OSI model or layer 3 or the network layer. Layer 2 switches forward data packets based on the destination MAC address, while layer 3 switches forward data based on the destination IP addresses. Some switches can perform both functions.

26. What is Bandwidth in Networking?

The network bandwidth refers to the maximum transfer capacity of a wired or wireless network communication. In other words, it is a measure of the amount of data that can be sent and received at a time. While bandwidth is traditionally expressed in bits per second (bps), modern network links with greater capacity are often measured in megabits or gigabits per second. For example, having 5 Mbps bandwidth means you can receive up to 5 megabits of data per second.

The more bandwidth a connection has, the more data it can send or receive at a given time. Contrary to a common belief, bandwidth does not increase the connection’s speed; it only makes the network seem faster. Increased bandwidth does not mean increasing the transmission speed of the data.

27. What is Host in Networking?

A host refers to a computer device (or server) that is linked with other devices connected within a network. The network hosts are assigned at least one network address configured manually by an administrator or automatically assigned by means of DHCP.

A network host commonly acts as a sever offering services, information resources, software applications, etc., to users or other hosts in the network. A host participating in networks that use an internet protocol suite has its unique IP address and is called an IP host. The IP host is responsible for storing data and transfer it to other machines or computers, called remote terminals.

28. What is Switching in Networking?.

Switching is a process of exchanging information or data between different computer networks or a network segment using multiple layers of the OSI model. Adding a switch to the network helps reduce traffic congestion and increase network performance.

Communication takes place through network switching in three phases –

- by establishing a dedicated circuit link between the sender and the receiver through nodes or switching centres
- transfer of data once the circuit is established
- once the communication is complete, the circuit disconnects.

29. What is Subnetting in Networking?

Subnetting is a process of partitioning a bigger network into smaller networks. The primary purpose of subnetting is to reduce network congestion by splitting into subnets or subnetworks, thereby creating a resilient computer network. Creating a subnet allows you to limit the network traffic and avoid backlogs. Subnetting works by dividing broadcast domains to reduce the load imparted on the network. It is crucial for large organisations and businesses to have full control over traffic and improve network speed and performance. Subnetting also enhances network security as the division between each subnet allows enterprises to enforce access controls.

30. What is Domain in Networking?

A network domain refers to the grouping of multiple devices, computers, workstations and database servers that share different data types within the same network infrastructure. The use of domains in networking first appeared in 1965 when it was initially applied to name the radio stations based on the geographical location and the broadcast frequency. Domains can be identified using a Domain Name System or DNS that translates the domain name into IP addresses. A full domain name is represented as a sequence of symbols specified by dots. This allows users to memorise user-friendly names instead of remembering IP addresses.

31. What is ACL in Networking?

ACL is an acronym for Access Control Lists. It is a set of rules used to control the network traffic and reduce network attacks. ACL works as a network filter and can only be configured on devices with packet filtering capabilities such as routers. The primary purpose of using an ACL is to provide network security. It contains a set of conditions that are applied on an interface basis to determine whether to allow or deny network traffic entering or leaving a network interface. The best place to configure an ACL is on the edge router that acts as a gateway for all outside networks. There are four types of ACLs based on their usage –

- Standard ACL
- Extended ACL
- Dynamic ACL
- Reflexive ACL

32. What is Multiplexing in Networking?

Multiplexing is a process of combining multiple data streams into one signal over a single medium. The hardware device used for multiplexing is known as a Multiplexer that combines the ‘n’ number of input signals into a single output signal. There are two main types of multiplexers – analog and digital. Analog multiplexing involves analog signals that are multiplexed according to their frequency and wavelength. When digital signals are multiplexed in the form of frames and packets, the process is called digital multiplexing. Multiplexing in networking allows effective utilisation of the bandwidth when multiple signals share one medium.

33. What is the purpose of Virtual Private Networking (VPN)?

A Virtual Private Networking (VPN) refers to an encrypted connection to another network over the internet. In simple terms, VPN connects your computer, smartphone or tablet to another computer (also called a server) and allows you to browse the internet using that computer’s internet connection. VPN can be used to –

- to access region-restricted websites
- shield your browsing activity
- protect your computer from untrustworthy Wi-Fi hotspots
- protect yourself from being logged while using torrent
- gain anonymity by hiding your location
- conduct work remotely and prevent unauthorised users from prying on the traffic
- provides a secure connection for safe data transfer while working remotely
- reduce the risk of data leakage

34. What is ISP in Networking?

ISP stands for Internet Service Provider. ISP refers to a company that provides internet access and services, including internet transit, web hosting, domain name registration and email services, to name a few. An ISP serves as a gateway to access everything available on the internet, usually for a fee.

There are three levels of ISP. A Tier 1 ISP sits at the top of the internet access pyramid with access to all networks on the internet. These ISPs then sell access to Tier 2 ISPs which further sell access directly to organisations and individuals. ISPs are responsible for maintaining network infrastructure, routing network traffic and enabling users to establish internet connectivity.

35. What is VLSM in Networking?

VLSM stands for Variable Length Subnet Masking. It is a subnet design strategy that allows subnet masks to have variable sizes within the same network. In other words, it involves a process of subnetting a subnet. VLSM enables network engineers to divide an IP address into different sized subnets and allocate it according to the network needs. This means that more than one mask is used for different subnets of a single class A, B, or C networks, thereby increasing the usability of subnets. The network administrator must use the relevant supporting routing protocol to use VLSM such as Intermediate System-to-Intermediate System (IS-IS), Routing Information

Protocol v2 (RIPv2), Border Gateway Protocol (BGP), and Open Shortest Path First (OSPF).

36. What is Subnet in Networking?

A subnet, also known as a subnetwork, is a logical partition of an IP network. Simply put, it is a network within a network. The primary purpose of the subnet is to ensure the efficient and faster transmission of data within a network. The IP addresses of computers that belong to a subnet are divided into two fields – the routing prefix or network number and the host identifier or the rest field. The subnetting of a network enhances its routing efficiency, keeps users connected and runs efficient network management. The strategic placement of subnets ensures that traffic destined for a device stays within the subnet, thereby reducing the network’s load.

37. What is Node in Networking?

A network node is a communication point that can analyse, receive, send and forward information. In networking, nodes are simply data points or devices over an extensive network such as a personal computer, modem, servers, bridges, printers that connect over Wi-Fi or ethernet. Generally, nodes are programmed to receive or store data from one node to another, back up files online and download files. So they can perform a variety of functions based on the application. In a network connection, multiple nodes are required to form a connection, with each node having an exclusive address for the network like a MAC (Media Access Control) or DCL (Data Link Control). This address helps to recognise and keep track of data being transmitted on the network.

38. What is Networking?

Networking can be defined as the process of connecting various devices or systems such as computers, servers or peripherals to allow the exchange of data, applications and resources located on network nodes. The networking hardware includes devices such as network cables, routers, network cards and distributors. Three main types of networks include – Local Area Network (LAN), Wide Area Network (WAN) and the internet. The main benefits of Networking include –

- Increased manageability
- A cost-effective way of sharing compared to non-network resources
- Security
- easy and faster inter-personal communication using various technologies such as email, online chat, voice messaging, video conferencing, etc.

39. What is a Server in Networking?

A network server is a computer or system that is dedicated to managing resources over a shared network. A device that makes the request is called a client, and the one that receives the request to share resources is called a server. In functionality, an individual system can both act as a server and a client at the same time. Network servers help in the management of different tasks for system administrators and can also act as a central file storage unit. These are also capable of running an intranet and exercise various security control measures. Some examples of network servers include web servers, database servers, FTP servers, proxy servers and more. In a corporate environment, servers are often stored in a glasshouse, while remote servers are located in a data centre. Mainframe computers and minicomputers were some of the first servers.

40. What is STP in Networking?

Spanning Tree Protocol (STP) is a network protocol designed to build a loop-free topology in the network. It is a layer 2 protocol that prevents broadcasts storms on networks with redundant paths. The standardised STP protocols are specified as IEEE 802.1D. STP runs on 802.1D-compliant bridges and switches to prevent loops in a network. The configuration of STP requires a well-planned network topology by the administrator. STP increases the reliability of the network exponentially by introducing redundancy that is as important as backups in case an active link within the network fails.

41. What is Subnet Mask in Networking?

A subnet mask is a 32-bit number used to separate IP addresses into a network address and a host address. It is used to determine whether a host is on the local subnet or a remote network to reduce heavy network traffic. A subnet mask uses the same format as an IPv4 address, with each section containing a number from 0 to 255. For instance, a typical subnet mask for a Class A network is 255.0.0.0. One can determine the type and number of IP addresses or a local network using its default subnet mask. A subnet mask is generally used by the router to maximise IP addressing efficiency.

42. What is RIP in Networking?

Routing Information Protocol (RIP) is a distance-vector routing protocol that employs the hop count to find the best path between the source and destination network. RIP works on the application layer of the OSI model and uses port number 520.

RIP considers the lowest hop count as a metric to count the number of networks to reach the destination. It has an AD value of 120, and the maximum hop count is 15. The hop count of 16 is considered unreachable. In most networking environments, RIP is a trusted choice for routing as it is easy to configure, scalable and requires far less complex than its counterparts.

43. What is VPN in Networking?

VPN or Virtual Private Network is a service that provides anonymity, security and privacy to the users by creating a safe and encrypted private connection across a public network connection. VPN makes use of tunnelling protocols to establish connection security between the client and the VPN server.

The use of VPNs is legal in most countries across the globe. VPNs do not really make connections completely anonymous, but they add a layer of security and privacy. While individuals mostly use remote access VPNs, businesses make use of site-to-site VPNs.

44. What is ATM in Networking?

ATM stands for Asynchronous Transfer Mode and is a switching technique used by telecommunication networks to encode data into small fixed-size packets called cells. These cells are ideal for time-division multiplexing (TDM) and transmit them over a physical medium.

Each ATM cell is 53 bytes long with a 5-byte header and a 48-byte payload. Since all the data is encoded into identical cells, the transmission is simple and uniform. This reduces packet overload and ensures that mixed traffic is handled efficiently. ATM is the core protocol used for Synchronous Optical Network (SONET), Fiber Distributed Data Interface (FDDI) and other high-speed networks. ATM networks can easy to work with and are scalable both in size and speed.

45. What is a Gateway in Networking?

A gateway is basically a hardware device or a node that acts as a critical stopping point for incoming and outgoing data within a computer network. It may be a router, server, firewall or any other device that filters traffic between two networks. For instance, if you have a wireless network at home, your gateway is the modem or the combination of router and modem. In the enterprise, a gateway can also act as a firewall or a proxy server. A gateway is one of the many ways that the data is moved over the internet. It also allows us entry into different networks to send emails, check web pages, buy online and more. A gateway can operate up to layer 5 of the OSI model.

46. What is Checksum in Networking?

Checksum is an error detection method used to verify the integrity of a data transfer within a network. It is typically used to compare two data sets using different algorithms to ensure data is transmitted without any error. The transmitter computes a numerical value in a block of data and sends it along with each data frame. At the receiver’s end, a new checksum is calculated and matched against the existing checksum to retrieve the numerical value. If the received checksum values match the sent one, the transmission is considered to be successful. A mismatched checksum indicates an error or data corruption.

47. What is Telnet in Networking?

Telnet, developed in 1969, is a networking protocol used on the local area network connections (LANs) and the internet to provide a two-way interactive communication facility. TELNET stands for TErminal NETwork. The users get connected to the server with the help of the Telnet protocol and can access any information on a remote computer. The computer which starts connection is termed as the local computer, and the computer which accepts the connection is termed as a remote computer. It operates of client/server principle via a virtual terminal connection consisting of an 8-bit byte oriented data connection over the TCP/IP. The format of a telnet command has a prefix character or IAC (Interpret As Command), which has code 255, followed by a command code and option code.

48. What is BGP in Networking?

BGP stands for Border Gateway Protocol and is classified as the routing protocol of the global internet network. Think of it as the postal service of the internet that finds the most efficient route to deliver the letter to its recipient. It facilitates data routing and reachability between autonomous systems (AS) on the internet using an arbitrary topology. BGP also helps conserve network bandwidth, support network security and facilitate coordination among multiple BGPs within the autonomous system (AS). Using BGP gives you more control over route selection and route advertisement by continually calculating the best path. That is why BGP is the routing protocol of the internet.

49. What is Ethernet in Networking?

Ethernet is a computer network technology used to connect multiple computers or devices over a wired connection and create a local area network (LAN). It provides a simple interface by connecting devices together with a cable to share information. Ethernet works on layer 1 (physical) and layer 2 (data link layer) of an OSI model and can connect up to 1024 personal computers. An Ethernet network may use various topologies such as a star, bus, ring, etc. Wired Ethernet networks are connected via fibre optic cables, while the wireless Ethernet network uses wireless NICs. Ethernet network is very reliable, and data is transmitted as well as received at very high speed. To ensure the security of the data, Ethernet makes use of firewalls.

50. What is RFC in Networking?

RFC stands for Request For Comments and is mainly used to develop standard network protocols. It is a technical document published by the Internet Engineering Task Force (IETF) that contains various networking protocols, procedures, applications and technologies. Almost all network protocols on the internet are built using RFCs. The final version of the document is published and sequentially numbered, which then becomes the standard. All standard network protocols such as FTP, HTTP, TCP, UDP, IP, etc., are defined as RFCs which form the base for cross-platform network communication.

This brings us to the end of the blog on Networking Interview Questions. We hope you are now well-equipped with the kind of questions that may be asked during an Interview. You can also prepare with these free networking courses.

Also, if you're interested to become a network architect, there are a few things you should know. First, you'll need to have a strong understanding of networking concepts and principles. Second, you should be able to design and implement networks that are both efficient and reliable. And lastly, you'll need to be able to troubleshoot and resolve any networking issues that may arise. If you have these skills and knowledge, then you may be well suited for a career as a network architect.

Wondering where to learn the highly coveted in-demand networking skills for free? Check out these free networking courses.