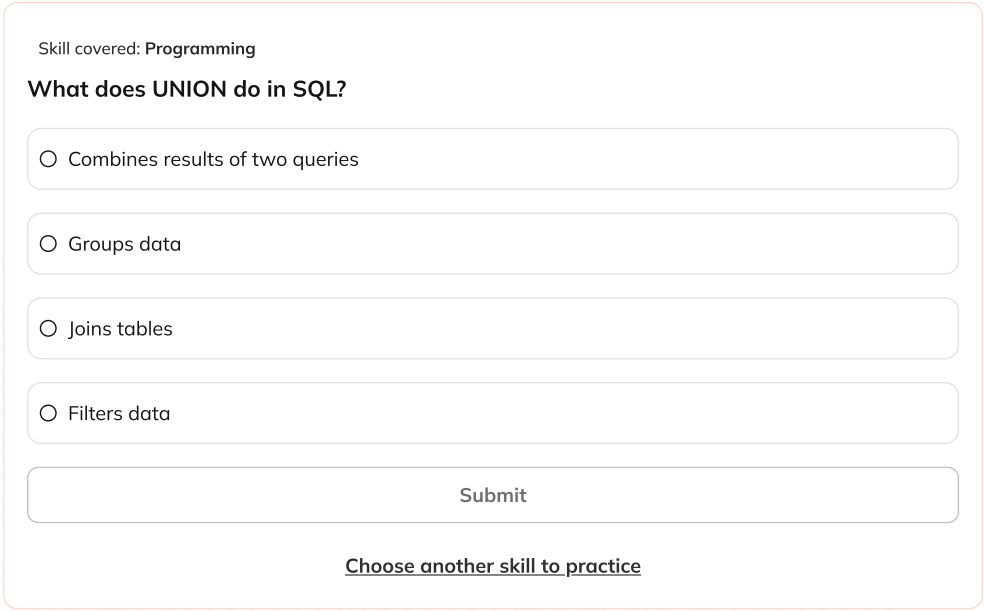


Why is the computer network so important?

Computer networks are essential for several reasons:

- **Communication**: Networks enable seamless communication through email, instant messaging, video conferencing, and VoIP, facilitating global connectivity and collaboration.
- **Resource Sharing**: They allow sharing of hardware resources (printers, scanners) and software applications (databases, programs) across multiple users and devices, optimizing efficiency and reducing costs.
- **Information Access**: Networks provide access to vast amounts of information stored on servers and databases, enabling quick retrieval and dissemination of data.
- **Business Operations**: For organizations, networks are crucial for conducting daily operations, managing transactions, maintaining customer relationships, and supporting decision-making processes.
- **Flexibility and Scalability**: Networks can be scaled up or down easily to accommodate changes in organizational needs, such as adding new users or expanding into new locations.

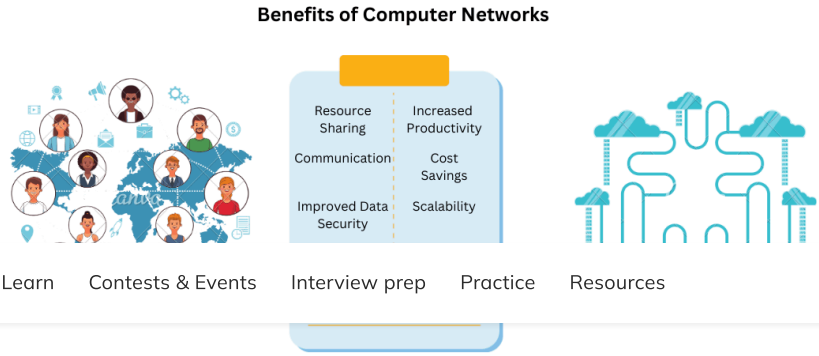
We will go through the beginner, intermediate and advanced-level sections of networking one by one.

Basic Networking Interview Questions

Let's go through some beginner-level networking interview questions.

1. What is a computer network, and what are some of its benefits?

Ans: A computer network is a group of connected devices that communicate and share resources. This can include computers, printers, servers, and other devices. Networks can be connected by wires, cables, or wireless connections. It can range in size from small local networks in a home or office to large global networks like the internet.



Some of the benefits of computer networks include:

a. **Resource sharing** - Users on a network can share resources like printers, storage, and applications.

b. **Communication** - Networks enable users to communicate and collaborate in real time, regardless of their physical location.

c. **Improved data security** - Networks can be configured with security features such as firewalls and access controls to protect against unauthorised access.

d. **Increased productivity** - With shared resources and improved communication, networks can increase productivity and efficiency in the workplace.

e. **Cost savings** - By sharing resources, networks can reduce hardware and software costs.

f. **Scalability** - Networks can be easily expanded to accommodate new users and devices.

g. **Centralised management** - Network administrators can manage resources, users, and security from a central location, improving efficiency and security.

2. What is the difference between a LAN and a WAN?

Ans: The following is the difference between a LAN and a WAN.

LAN (Local Area Network)	WAN (Wide Area Network)
It covers a small geographical area, typically within a building or campus.	It covers a larger geographical area, typically spanning multiple cities or countries.
Operates at high speeds, typically up to 10 Gbps.	Operates at lower speeds, typically up to 10 Mbps.
Managed by a single organisation or individual.	Often managed by multiple organisations or service providers.
Generally less expensive to set up and maintain.	Generally more expensive to set up and maintain.
Limited to a small number of devices, typically up to a few hundred.	It can support a large number of devices, typically up to thousands or millions.
Typically uses Ethernet or Wi-Fi technology.	Uses a variety of technologies, including leased lines, satellite links, and VPNs.
Provides high levels of security and control over network resources.	Often requires additional security measures to protect data and resources.
Examples include home networks, office networks, and school networks.	**Examples** include the Internet, corporate WANs, and service provider networks.

Also see, Personal Area Network

3. What is an IP address, and how do networking protocols use IP addresses?

Ans: An IP address is a unique identifier assigned to every device that connects to a network. It is a numerical label that allows devices to communicate with each other over the internet or a local network. An IP address consists of a network ID and a host ID, separated by dots. The network ID identifies the network, and the host ID identifies a particular device on the network.

Networking protocols use IP addresses to route data packets between devices. For example, when a computer wants to send data to another device on the network or internet, it needs the IP address of the recipient device to send the data to the correct destination.

IP addresses are divided into classes based on their range. Class A: 1-126, Class B: 128-191, Class C: 192-223.

An example in IP address: **192.168.1.10** is a **32-bit address** used in **IPv4**. It is represented in binary as 11000000.10101000.00000001.00001010. It belongs to **class A.**

4. What is a router, and what is its role in a network?

Ans: A router is a networking device that connects multiple networks and routes data packets between them. Its primary role in a network is to forward data between networks. These networks are based on the destination IP address of the packets. Routers work at the network layer of the OSI model. It uses routing tables to determine the best path for data to reach its destination.

They also provide other services like network address translation (NAT). It enables devices on a private network to access the internet using a single public IP address. Routers are essential components of modern computer networks. They are used by internet service providers, businesses, and homes to connect devices and enable communication between them.

5. What is a firewall, and how does it improve network security?

Ans: A firewall is a network security tool that monitors and controls incoming and outgoing network traffic. It acts as a barrier between a secure internal network and untrusted external networks, such as the internet.

Firewalls use rules to determine whether network traffic should be allowed or blocked based on specific criteria. It can be the source and destination of the traffic, the type of traffic, and the intended use of the network. By filtering out unauthorised or malicious traffic, firewalls improve network security by preventing attacks such as hacking, malware infections, and data theft.

6. What is a DNS server, and what is its purpose?

Ans: A DNS (Domain Name System) server is a network server that translates domain names into their corresponding IP addresses. DNS is used to map human-readable domain names, such as www.codingninjas.com, to the numeric IP addresses that computers use to communicate with each other.

When a user types a domain name into a web browser or other network application, the app sends a request to a DNS server to resolve the domain name into an IP address. The DNS server then looks up the IP address for the domain name and returns it to the requesting app.

DNS servers are a critical component of the internet infrastructure. They are essential for allowing users to access websites and other network resources. It is done by using easy-to-remember domain names.

7. What is a MAC address, and how is it used in networking?

Ans: A MAC (Media Access Control) address is a unique identifier assigned to a network interface controller (NIC). It is used as a network address in communications within a network segment.

MAC addresses are used at the data link layer of the network stack. It controls access to the network media and ensures each device has a unique address. They are used by network devices such as switches to direct traffic to the correct destination device on the local network segment.

MAC addresses are typically represented as a string of six pairs of hexadecimal digits, such as 00:1B:44:11:3A:B7. They are assigned by the network interface manufacturer and stored in the device's hardware.

8. What is the difference between a hub, a switch, and a router?

Ans: The following table consists of the difference between a hub, a switch, and a router.

Property	Hub	Switch	Router
Layer	Physical Layer	Data Link Layer	Network Layer
Broadcasts	Broadcasts all incoming traffic to all connected devices.	Forwards traffic only to the intended device.	Forwards traffic to the destination network.
Addresses	Does not have a MAC address.	It has a MAC address.	It has a MAC and an IP address.
Collision Domain	Shares a single collision domain.	Creates a separate collision domain for each port.	Creates a separate collision domain for each port.
Packet Filtering	Does not filter packets.	Can filter packets based on MAC address.	Can filter packets based on MAC and IP addresses.
Routing	Cannot route traffic.	It cannot route traffic between networks, but can route traffic between different VLANs.	Can route traffic between networks.

9. What is a subnet mask, and how is it used in networking? Given the IP address 192.168.10.0/24, how many subnets and hosts per subnet can be created if you use a subnet mask of 255.255.255.192?

Ans: A subnet mask is a 32-bit value used in conjunction with an IP address to divide it into a network and host portions. It is used to identify which part of an IP address identifies the network and which part identifies the host. The subnet mask is applied to the IP address by performing a logical AND operation. It is used to help determine a network's size and scope and enables efficient traffic routing.

The subnet bits will be borrowed from the host bits using a subnet mask of 255.255.255.192 (or /26 in CIDR notation). In this case, there will be 2 bits borrowed, which means there will be 4 subnets (2^2) and 62 hosts per subnet (2^6-2, as 2 addresses are reserved for network and broadcast addresses). So answer will be **4 subnets** and **62 hosts per subnet**.

10. What is the OSI model, and how is it used in networking?

Ans: The OSI (Open Systems Interconnection) model is a conceptual model that describes the communication functions of a network. It consists of seven layers, each with a specific function. These functions work together to provide end-to-end communication between devices on a network:

a. **Physical Layer**: This layer is responsible for transmitting raw bits over a communication channel, defining the electrical and physical specifications for the connection.

b. **Data Link Layer**: This layer provides reliable transmission of data frames over a physical link by adding error detection and correction, flow control, and access control.

c. **Network Layer**: This layer provides logical addressing and routing services to allow data to be transferred between different networks. It defines protocols for forwarding and routing data through intermediate network nodes.

d. **Transport Layer**: This layer provides end-to-end delivery of data by ensuring that packets are delivered reliably and in order and by managing congestion and flow control.

e. **Session Layer**: This layer establishes, manages, and terminates communication sessions between applications on different devices. It also provides services such as checkpointing and recovery in case of a failure.

f. **Presentation Layer**: This layer is responsible for formatting and presenting data to the application layer. It defines data compression, encryption, and conversion protocols between different data formats.

g. **Application Layer**: This layer provides services to the end-user applications, such as email, file transfer, and remote login. It defines the protocols that applications use to exchange data and interact with the network.

The OSI model is used as a reference framework for designing, implementing, and troubleshooting network protocols and systems. By dividing network communication into a series of independent layers, the OSI model helps to ensure that each layer can be developed and tested separately, promoting interoperability and reducing complexity. It also provides a common language for network engineers and developers to describe and understand network communication.

11. What is the TCP/IP model?

The TCP/IP model is a conceptual model that describes the communication protocols used on the internet and other computer networks. It consists of four layers, each with its own specific function and set of protocols.

a. **Application Layer**: The application layer is responsible for providing services to user applications, such as email, file transfer, and web browsing. Protocols at this layer include HTTP, FTP, SMTP, and DNS.

b. **Transport Layer**: The transport layer provides reliable communication between applications on different devices. It manages flow control, error checking, and fragmentation of data. The two most common protocols used at this layer are TCP and UDP.

c. **Internet Layer**: The internet layer is responsible for packet forwarding between networks and routing packets to their destinations. It provides an addressing scheme that uniquely identifies each device on a network. The main protocol used at this layer is the Internet Protocol (IP).

d. **Network Interface Layer**: The network interface layer is responsible for data transmission between devices on the same network. It provides hardware addressing and error checking. It may include protocols for managing the physical medium, such as Ethernet, Wi-Fi, or Bluetooth.

Intermediate-Level Networking Interview Questions

After going through some beginner-level questions, now it's time to cover some intermediate-level networking interview questions.

12. What is a VPN, and how does it improve network security and privacy?

Ans: A VPN (Virtual Private Network) is a secure network connection that allows users to access the internet or a private network remotely as if they were directly connected to the network. VPNs use encryption and tunnelling protocols to provide confidentiality, integrity, and authenticity for data transmitted over public networks.

By using a VPN, data is transmitted securely over the internet, preventing unauthorised access, interception, or eavesdropping. VPNs also enable users to bypass geographical restrictions and protect their online activity and privacy by masking their IP address and encrypting their traffic.

13. What is the difference between a static IP address and a dynamic IP address?

Ans: The following is the difference between a static IP address and a dynamic IP address.

Static IP Address	Dynamic IP Address
Assigned manually by a network administrator or ISP.	Assigned automatically by a DHCP server.
It remains constant and does not change.	It can change each time a device connects to the network.
Ideal for servers, web hosting, or devices that require a fixed IP address.	Ideal for home or small business networks with devices that don't require a fixed IP address.
They are more secure as they are not susceptible to IP spoofing or DNS attacks.	They are less secure as they can be more easily targeted by IP spoofing or DNS attacks.
They are more expensive, as they require more configuration and administration.	They are more cost-effective, as they can be easily managed and do not require manual configuration.
Requires manual reconfiguration if network topology changes.	Automatically adapts to network topology changes.
Provides better network performance as obtaining a new IP address upon connection is unnecessary.	May experience slower network performance due to the time needed to obtain a new IP address upon connection.

14. What is network latency, and how can it be minimised in a network?

Ans: Network latency is the time delay between sending a data packet from one network device to another. Various factors, such as distance, network congestion, and equipment performance, can cause it. High latency can lead to poor network performance, slow response times, and decreased productivity.

To minimise network latency, network administrators can implement various solutions such as using faster network hardware, optimising network configurations, reducing network congestion, implementing quality of service (QoS) policies, and using content delivery networks (CDNs) to reduce the distance data needs to travel.

15. What is Quality of Service (QoS), and how is it used to prioritise network traffic?

Ans: Quality of Service (QoS) is a networking technology that enables network administrators to prioritise certain types of network traffic over others. QoS ensures that important or time-sensitive data, such as voice or video traffic, is given priority over less important data, such as email or web browsing. This helps improve network performance, reduce network congestion, and ensure critical applications or services receive the necessary bandwidth and resources to operate

optimally.

16. What is a VLAN, and how is it used to segment a network?

Ans: A VLAN (Virtual Local Area Network) is a logical network that is created within a physical network infrastructure. VLANs allow network administrators to logically segment a network, separating devices into different broadcast domains, even if they are physically connected to the same network switch. VLANs can be used to improve network performance, increase security, and simplify network management. By grouping devices into different VLANs; administrators can control traffic flow and prioritise traffic. They can also provide access control based on VLAN membership, improving overall network efficiency and security.

17. What is network address translation (NAT), and how does it improve network security?

Ans: Network Address Translation (NAT) is a technique used to modify IP address information in the packet headers while packets are in transit over the internet. NAT provides an additional layer of security by masking the internal IP addresses of a private network. This makes it harder for an attacker to launch a direct attack on a specific device on the network. Additionally, NAT can be used to conserve IP addresses by allowing multiple devices on a private network to share a single public IP address.

18. What is a load balancer, and how is it used to distribute network traffic across multiple servers?

Ans: A load balancer is a device or software that distributes network traffic across multiple servers to optimise resource usage, maximise throughput, and minimise response time. The load balancer acts as a reverse proxy server, distributing incoming network traffic across multiple backend servers based on predefined algorithms, such as round-robin or weighted round-robin.

Load balancers can improve network performance and availability by directing traffic away from servers that are overburdened or offline, automatically scaling resources up or down based on demand, and providing failover capabilities in case of server failures. Load balancing is commonly used in web applications, streaming services, and other high-traffic online services.

19. What is a network protocol, and what are some common network protocols used in networking?

A network protocol is a set of rules and procedures that govern the communication between devices on a network. Network protocols define how data is transmitted, received, and processed, including error checking, authentication, and encryption.

Here are some common network protocols used in networking:

a. **TCP/IP (Transmission Control Protocol/Internet Protocol)** - a protocol suite that enables the communication between devices on the internet and other networks.

b. **HTTP (Hypertext Transfer Protocol)** - a protocol for transmitting and receiving web pages, including text, images, and other multimedia content.

c. **FTP (File Transfer Protocol)** - a protocol for transferring files between devices on a network.

d. **DNS (Domain Name System)** - a protocol for converting human-readable domain names into IP addresses that can be used by network devices to connect to a website or other resource.

e. **DHCP (Dynamic Host Configuration Protocol)** - a protocol for assigning IP addresses and other network configuration settings to devices on a network.

f. **SMTP (Simple Mail Transfer Protocol)** - a protocol for sending and receiving email messages.

g. **POP (Post Office Protocol)** - a protocol for downloading email messages from a mail server to a local email client.

h. **IMAP (Internet Message Access Protocol)** - a protocol for accessing email messages stored on a remote mail server.

i. **SNMP (Simple Network Management Protocol)** - a protocol for managing and monitoring network devices and resources.

Advanced-Level Networking Interview Questions

At last, let's see some advanced-level networking interview questions.

20. What is BGP (Border Gateway Protocol), and how is it used in routing between autonomous systems?

Ans: Border Gateway Protocol (BGP) is a protocol used to exchange routing information between different autonomous systems (AS) on the internet. It is responsible for routing traffic between different ISPs and ensuring that packets reach their destination across multiple networks. BGP considers factors such as path length, route stability, and AS path to determine the best route for traffic.

It allows for flexible policy control over routing decisions and can be used to implement traffic engineering. BGP is typically used in large-scale networks such as internet service provider (ISP) backbones and is critical for the proper functioning of the internet. It also supports security mechanisms such as Route Origin Validation (ROV) to prevent routing attacks.

21. What is MPLS (Multiprotocol Label Switching), and how is it used to improve network performance and efficiency?

Ans: Multiprotocol Label Switching (MPLS) is a technique used to improve the performance and efficiency of network traffic routing. MPLS works by assigning labels to packets at the ingress edge of the network based on destination addresses or other criteria. These labels are then used to guide the packet through the network instead of examining the packet header at each hop.

This reduces the processing time and resources required for packet forwarding and can also improve traffic engineering and quality of service (QoS). MPLS is commonly used in service provider networks to provide VPN services, traffic engineering, and QoS. It is also used in enterprise networks to improve network performance.

22. What is SDN (Software-Defined Networking), and how is it used to manage and automate network configuration and control centrally?

Ans: Software-Defined Networking (SDN) is an approach to network architecture that allows network administrators to manage and automate network configuration and control through software-based controllers. In an SDN architecture, the network control plane is separated from the data plane, allowing network administrators to centrally manage network functions and policies.

This enables greater flexibility and scalability in network management and improved network performance and security. SDN is often used in data centres and enterprise networks to manage virtualised infrastructure and cloud environments and can also be used in service provider networks to improve service delivery and reduce operational costs.

23. What is network virtualisation, and how is it used to create multiple virtual networks on a single physical network infrastructure?

Ans: Network virtualisation is the process of creating multiple virtual networks on a single physical network infrastructure. It enables the creation of logical networks that are independent of the underlying physical network, allowing network administrators to partition the network into multiple segments with their own network policies and configurations.

Network virtualisation can be achieved through various technologies, such as virtual LANs (VLANs), virtual private networks (VPNs), and software-defined networking (SDN). This approach to network architecture provides greater flexibility, scalability, and efficiency in network management and improved network traffic security and isolation.

24. What is a packet analyser, and how is it used to troubleshoot network issues?

Ans: A packet analyser, also known as a network analyser or protocol analyser, is a tool used to capture, analyse, and decode network traffic. It enables network administrators to identify and diagnose network problems by inspecting individual packets and their contents, including headers, payloads, and protocols.

By analysing network traffic behaviour, packet analysers can identify issues such as network congestion, security breaches, and misconfigurations. They also provide insight into network performance, usage, and trends. Packet analysers are essential for troubleshooting complex network issues and are widely used in network engineering, security, and forensics.

25. What is a distributed denial-of-service (DDoS) attack, and what are some strategies for mitigating such attacks?

Ans: A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to overwhelm a network, server, or website with a flood of traffic from multiple sources, making it inaccessible to legitimate users.

Some strategies for mitigating DDoS attacks include:

a. Implementing DDoS mitigation services and solutions, such as firewalls, load balancers, and intrusion detection systems.

b. Configuring network devices to filter and block traffic from known malicious sources, such as blacklisting IP addresses and blocking specific protocols.

c. Utilising Content Delivery Networks (CDNs) to distribute traffic and provide redundancy, reducing the impact of attacks.

d. Increasing network bandwidth and server capacity to handle larger volumes of traffic, reducing the impact of the attack.

e. Having a well-defined incident response plan in place, with clear roles and responsibilities assigned, to quickly respond to and recover from attacks.

f. Educating users and employees on identifying and reporting suspicious activities, such as phishing emails and botnets, which can be used to launch DDoS attacks.

26. What is a virtual private cloud (VPC), and how is it used to securely connect a private network to a public cloud infrastructure?

Ans: A Virtual Private Cloud (VPC) is a virtual network infrastructure that allows organisations to create isolated network environments in a public cloud infrastructure, such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. A VPC provides the ability to create private subnets with their own IP address ranges and configure routing tables, network gateways, and security rules to control access to resources within the VPC.

A VPC allows organisations to securely connect their private network to a public cloud infrastructure, enabling them to take advantage of cloud services while maintaining control over their network architecture and security. This can be done using virtual private network (VPN) connections or dedicated connections provided by the cloud provider. By using a VPC, organisations can isolate their resources in a private network and reduce the risk of unauthorised access or data breaches.

27. What is a software-defined WAN (SD-WAN), and how is it used to simplify network management and improve network performance?

Ans: Software-defined WAN (SD-WAN) is a technology that simplifies the management of network connections and improves network performance by decoupling network hardware from its control mechanism. It enables businesses to route traffic between branch offices, data centres, and public clouds over the most optimal path, increasing network efficiency and reducing downtime.

SD-WAN allows network administrators to centrally manage network traffic, policies, and security across multiple locations without relying on individual devices' manual configuration. Additionally, SD-WAN provides cost savings by using less-expensive broadband links instead of costly MPLS

connections.

28. What is a multicast, and how is it used to transmit data to multiple recipients simultaneously?

Ans: Multicast is a method of transmitting data to multiple recipients simultaneously, using a single stream of data. It is often used for applications that require the same data to be sent to multiple recipients, such as video or audio streaming, stock quotes, or real-time traffic updates.

Multicast traffic is delivered to a group of recipients who have expressed interest in receiving the data using a specific multicast IP address. Multicast uses a tree-based delivery mechanism, where data is transmitted from a single source to multiple receivers via intermediate network nodes.

It is an efficient way to reduce network traffic and improve network performance, as it eliminates the need to transmit the same data multiple times to different recipients.

29. What is the difference between TCP and UDP, and what are some scenarios in which one protocol might be preferred over the other?

Ans: The difference between TCP and UDP are mentioned below.

TCP	UDP
Transmission Control Protocol.	User Datagram Protocol.
Connection-oriented protocol.	Connectionless protocol.
Reliable data delivery.	Unreliable data delivery.
Requires established connection before transmitting data.	No connection establishment required.
Guarantees data delivery with retransmission.	No retransmission or guarantee of data delivery.
Ordered data transmission.	No ordered data transmission.
Slower transmission speed.	Faster transmission speed.
Uses flow control and congestion control mechanisms.	No flow control or congestion control mechanisms.
Suitable for applications that require accurate data transmission and error-free delivery, such as email, file transfer, and web browsing.	Suitable for applications that require faster data transmission and can tolerate data loss, such as video streaming, gaming, and VoIP.

TCP is typically preferred when reliability and error-free data transmission are important, such as when transferring large files or making important transactions. On the other hand, UDP is preferred when speed and efficiency are more important than reliability, such as in real-time applications like video streaming or online gaming, where a slight loss of data or delay is acceptable.

You can read related articles such as Congestion Control in Computer Networks here.

30. What happens when you enter “www.google.com” in the web browser?

Ans: When you enter "www.google.com" in the web browser, the following steps occur:

a. The browser first checks its cache to see if it has a copy of the requested webpage.

b. If the webpage is not in the cache, the browser sends a request to a DNS (Domain Name System) server to obtain the IP address of the server that hosts the website.

c. Once the IP address is obtained, the browser initiates a TCP (Transmission Control Protocol) connection with the server.

d. The browser sends an HTTP (Hypertext Transfer Protocol) request to the server for the webpage.