Protocols

Ans: It is defined as a set of rules defined for interactions between two or more nodes in any Computer network. In context to System design Interviews, we need to understand few Network protocols to understand how data transfer over the internet and the best possible protocol to choose and which is used for a particular task.

OSI vs TCP/IP

Ans:

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

TCP/IP!

Ans:
i. The protocol stack used on the Internet is the Internet Protocol Suite. It is usually called TCP/IP.
ii. The TCP/IP model is based on a five-layer model for networking, from bottom (the

link) to top (the user application).
iii. These are the physical, data link, network, transport, and application layers.

The TCP/IP Layers:

- The model consists of five separate but related layers.
- TCP/IP also defines how to interface the network layer with the data link and physical layers.
- In Fig1 the unstructured stream of bits represents frames with distinct content.

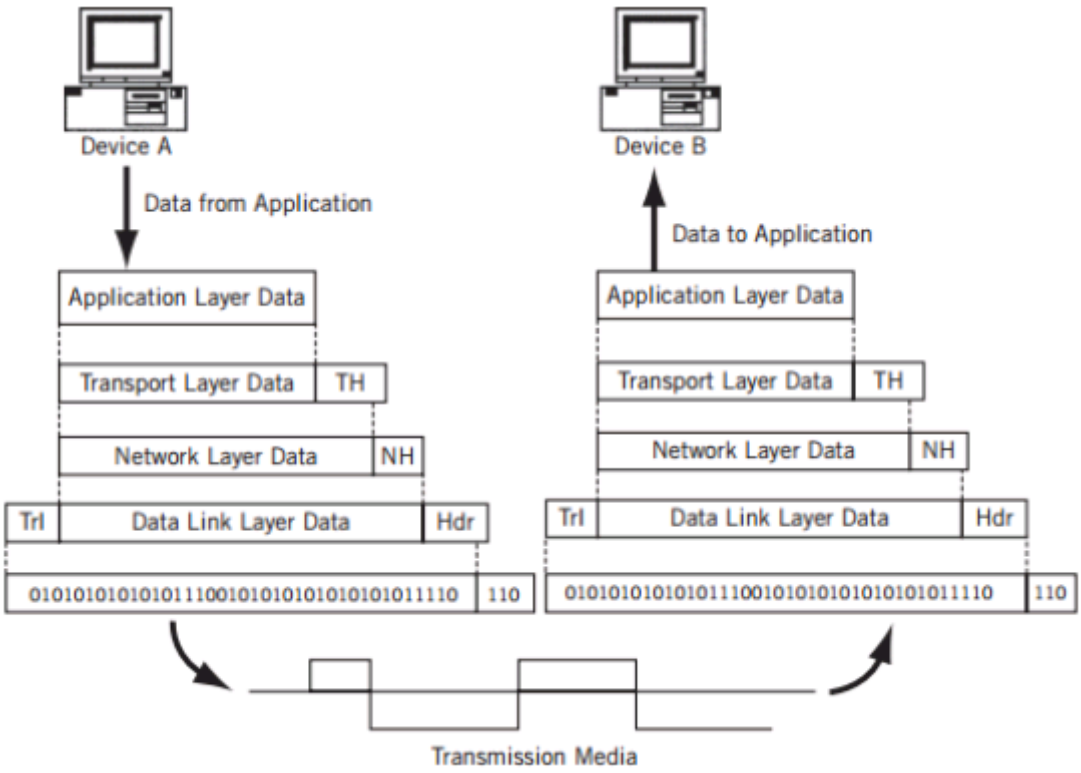


Fig1: TCP/IP encapsulation and headers

- The Physical Layer :
  i. The physical layer contains all the functions needed to carry the bit stream over a physical medium to another system.
  ii. There are other things that the physical layer must determine, or be configured to expect.
  iii. In Fig2 .The transmission framing bits are used for transmission media purposes only, such as low-level control.
  iv.Delimeter(mark start and end of packet) is added at this step

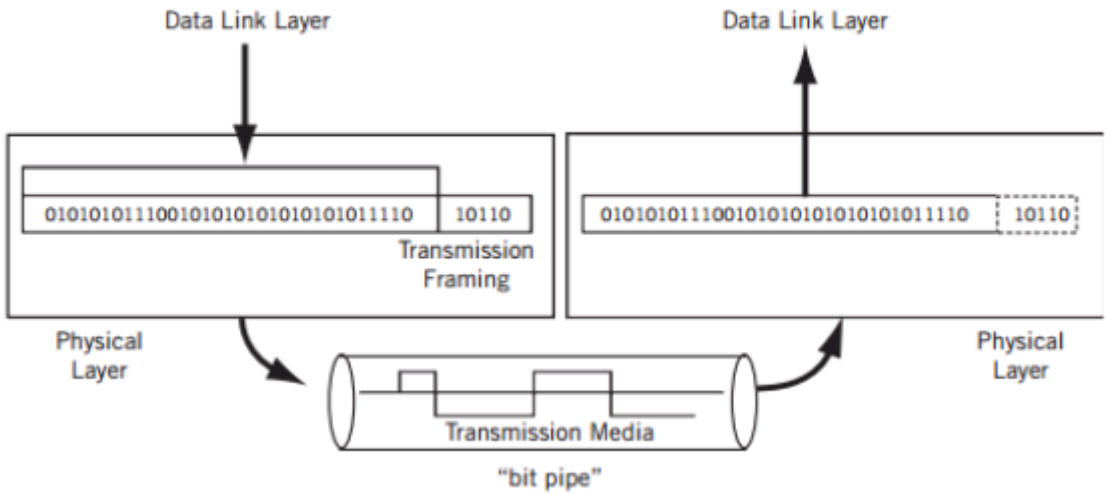


Fig2: The physical layer

i. **Data rate**—This transmission rate is the number of bits per second that can be sent. It also defines the duration of a symbol on the wire.

ii. **Bit synchronization**—The sender and receiver must be synchronized at the symbol level so that the number of bits expected per unit time is the same.

iii. **Configuration**—In a multipoint configuration, a link connects more than two devices, and in a multisystem bus topology such as a LAN, the number of systems can be very high.

iv. **Topology**—The devices can be arranged in a number of ways. In a full mesh topology, all devices are directly connected and one hop away. Systems can also be arranged as a star topology, with all systems reachable through a central system. There is also the bus and the ring.

v. **Mode**—So far, we've only talked about one of the systems as the sender and the other as the receiver. This is operation in simplex mode, where a device can only send or receive. More realistic devices use duplex mode, where all systems can send or receive with equal facility.

- **The Data Link Layer :**
  - The data link layer performs framing, physical addressing, and error detection, this layer also performs access control.
  - In LANs, this media access control (MAC) forms a sublayer of the data link layer and has its own addressing scheme known (not surprisingly) as the MAC layer address.
  - In addition, the data link layer can perform some type of flow control.
  - The unit of communication at the data link layer is a frame.
  - Fig3, showing that data link layer frames have both header and trailer.

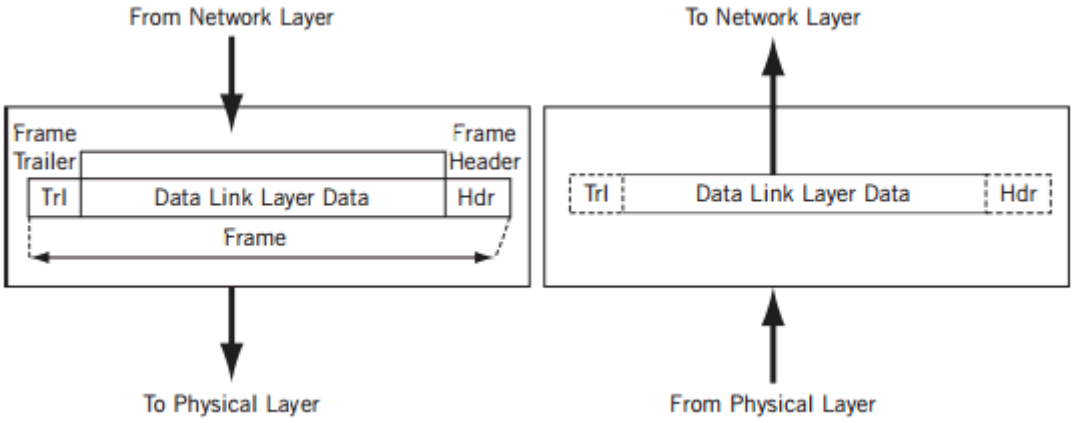


Fig3: The data link layer

- **The Network Layer:**
  i. At the network layer, TCP/IP supports the Internet Protocol (IP).
  ii. The Internet Protocol (IP)is the transmission mechanism used by the TCP/IP protocols
  iii. IP transports data in packets called datagrams, each of which is transported separately.
  iv. The network layer delivers data in the form of a packet from source to destination.
  v. The biggest difference between the network layer and the data link layer is that the data link layer is in charge of data delivery between adjacent systems, while the network layer delivers data to systems that are not directly connected to the source.
  vi. Fig4 shows the relationship between the network layer and the transport layer above and the data link layer below.
  vii. These data units are packets with their own destination and source address formats.
  viii. The network layer uses one or more routing tables to store information about reachable systems.

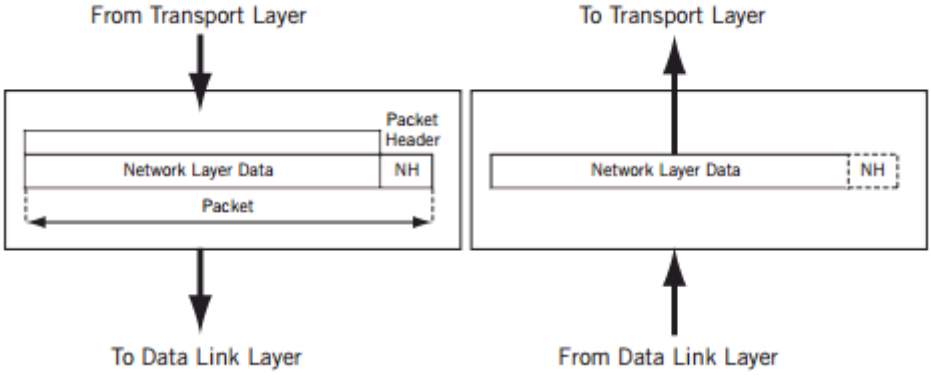


Fig4: The Network Layer

ix. The unit of communication at the network layer is a datagram.

- **The Transport Layer :**
  i. Process-to-process delivery is the task of the transport layer.
  ii. This process of dividing message content into packets is known as segmentation.
  iii. The network layer forwards each and every packet independently, and does not recognize any relationship between the packets.
  iv. The transport layer, in contrast, can make sure the whole message.
  v. This function of the transport layer involves some method of flow control and error control (error detection and error correction) at the transport layer, functions which are absent at the network layer.
  vi. There are two very popular protocol packages at the transport layer:
  TCP—This is a connection-oriented, “reliable” service that provides ordered delivery of packet contents.
  UDP—This is a connectionless, “unreliable” service that does not provide ordered delivery of packet contents.
  vii. Fig5 , showing how data are broken up if necessary and reassembled at the destination.
  viii. The unit of communication at the transport layer is a segment, user datagram, or apacket, depending on the specific protocol used in this layer.

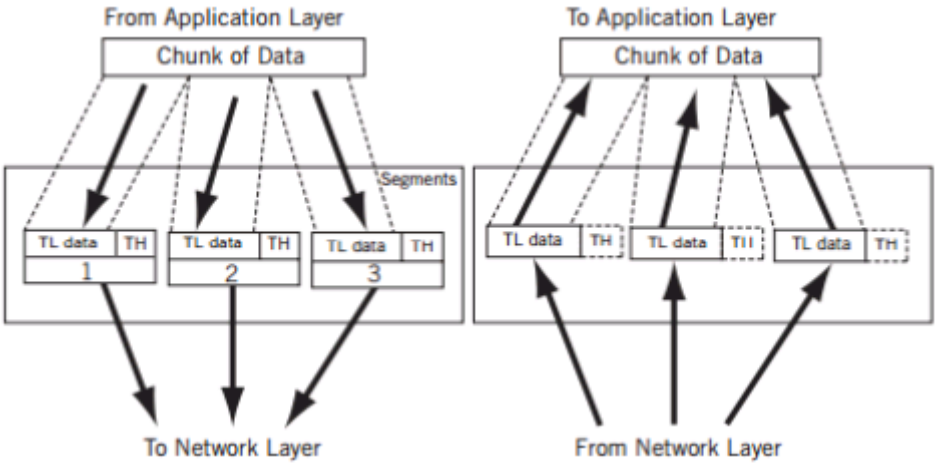


Fig5: The transport layer

- **The Application Layer :**
  i. The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.
  ii. The application layer allows a user to access the services of our private internet or the global Internet.
  iii. Many protocols are defined at this layer to provide services such as electronic

mail, file transfer, accessing the World Wide Web, and so on.
iv. The unit of communication at the application layer is a message.

OSI and every Layer protocols

Ans:

Layer	Name	Function	Protocols
Layer 7	Application	To allow access to network resources.	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	To translate, encrypt and compress data.	MPEG, ASCH, SSL, TLS
Layer 5	Session	To establish, manage, and terminate the session	NetBIOS, SAP
Layer 4	Transport	The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine.	TCP, UDP
Layer 3	Network	To provide internetworking. To move packets from source to destination	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	To organize bits into frames. To provide hop-to-hop delivery	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	To transmit bits over a medium. To provide mechanical and electrical specifications	RS232, 100BaseTX, ISDN, 11.

TCP protocol

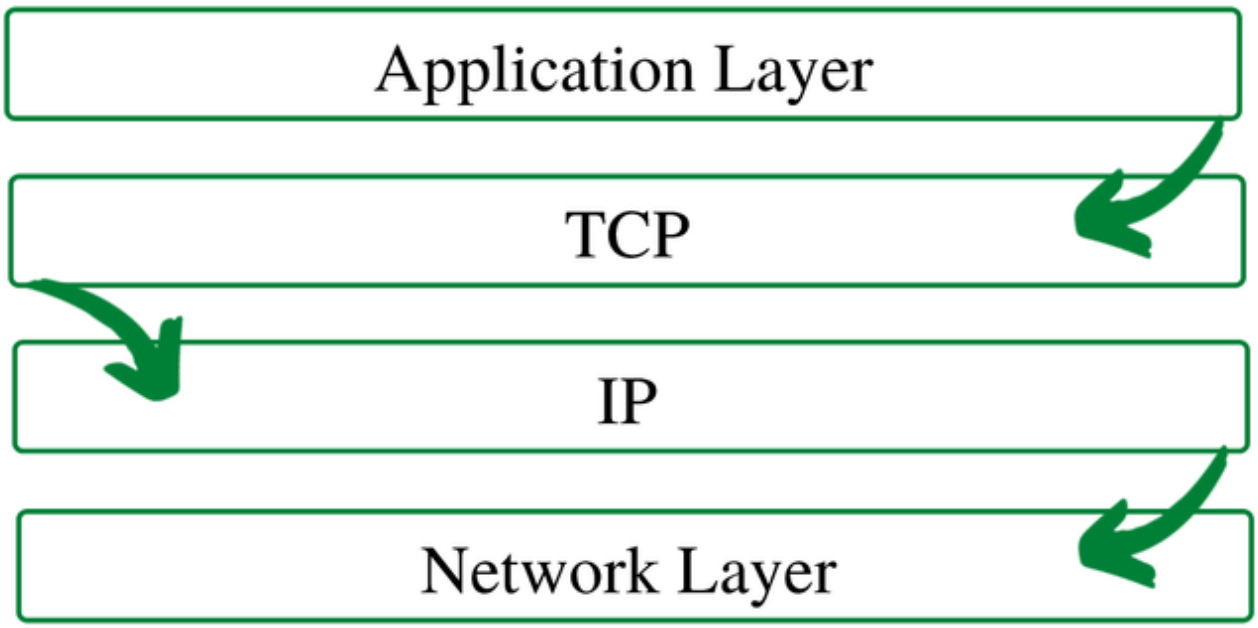
Ans: TCP stands for **Transmission Control Protocol**. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

Working

- *For example,* When a user requests a web page on the internet, somewhere in the world, the server processes that request and sends back an HTML Page to that user. The server makes use of a protocol called the HTTP Protocol. The HTTP then requests the TCP layer to set the required connection and send the HTML file.
- Now, the TCP breaks the data into small packets and forwards it toward the Internet Protocol (IP) layer. The packets are then sent to the destination through

different routes.

- The TCP layer in the user's system waits for the transmission to get finished and acknowledges once all packets have been received.



Features of TCP/IP

1. Segment Numbering System

- TCP keeps track of the segments being transmitted or received by assigning numbers to each and every single one of them.
- A specific *Byte Number* is assigned to data bytes that are to be transferred while segments are assigned *sequence numbers*.
- *Acknowledgment Numbers* are assigned to received segments.

2. Flow Control

- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- The receiver continually hints to the sender on how much data can be received (using a sliding window)

3. Error Control

- TCP implements an error control mechanism for reliable data transfer
- Error control is byte-oriented
- Segments are checked for error detection
- Error Control includes – *Corrupted Segment & Lost Segment Management, Out-of-order segments, Duplicate segments*, etc.

4. Congestion Control

- TCP takes into account the level of congestion in the network
- Congestion level is determined by the amount of data sent by a sender
- **Full duplex**
  It is a full-duplex means that the data can transfer in both directions at the same time.

Advantages of TCP

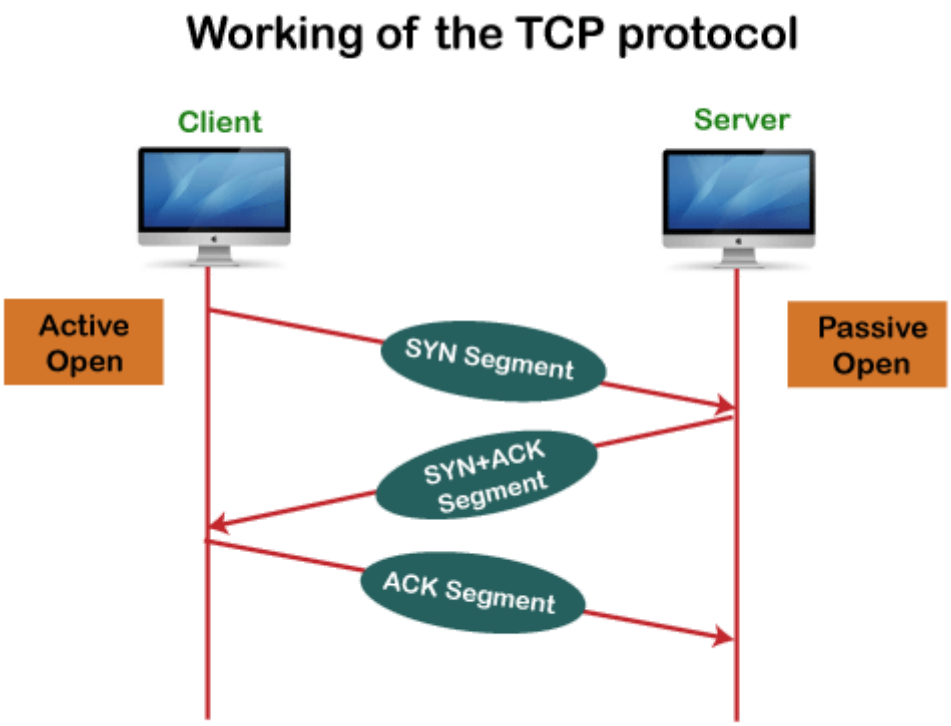
- It provides a connection-oriented reliable service, which means that it guarantees the delivery of data packets. If the data packet is lost across the network, then the TCP will resend the lost packets.
- It provides a flow control mechanism using a sliding window protocol.
- It provides error detection by using checksum and error control by using Go Back or ARP protocol.
- It eliminates the congestion by using a network congestion avoidance algorithm that includes various schemes such as additive increase/multiplicative decrease (AIMD), slow start, and congestion window.

Disadvantage of TCP

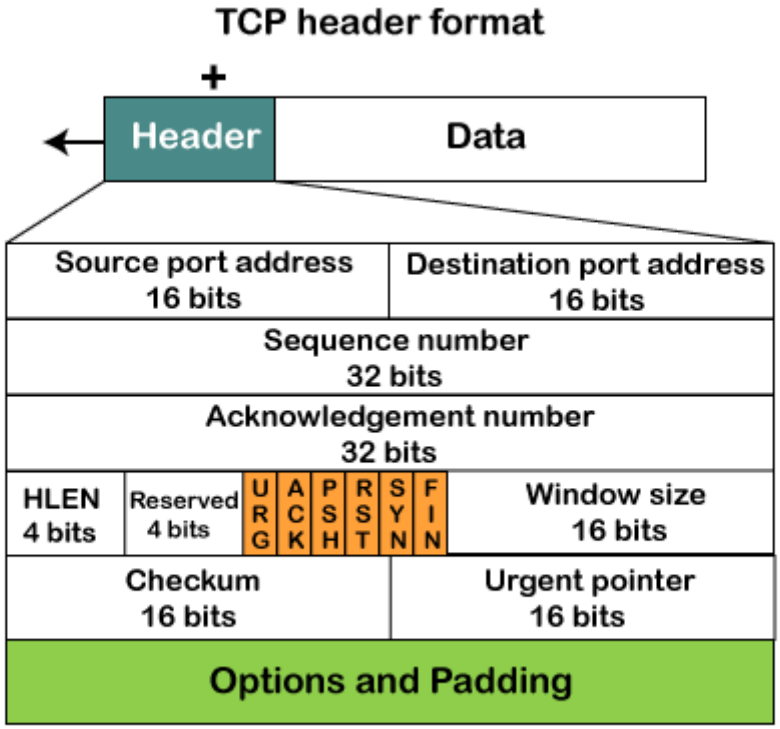
- It increases a large amount of overhead as each segment gets its own TCP header, so fragmentation by the router increases the overhead.

Working of TCP

In TCP, the connection is established by using three-way handshaking. The client sends the segment with its sequence number. The server, in return, sends its segment with its own sequence number as well as the acknowledgement sequence, which is one more than the client sequence number. When the client receives the acknowledgment of its segment, then it sends the acknowledgment to the server. In this way, the connection is established between the client and the server.



TCP Header Format



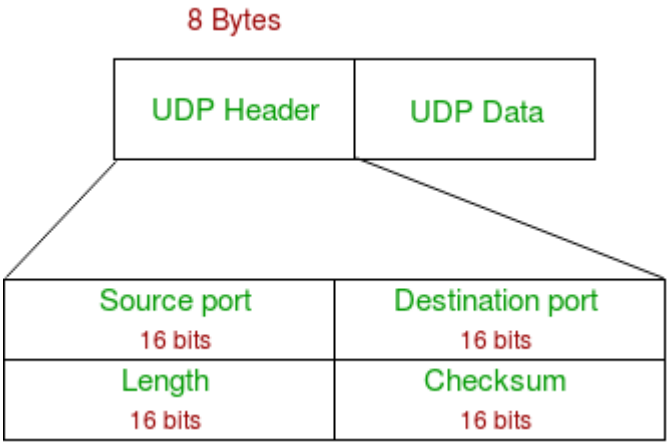
UDP!

Ans: User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection prior to data

transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.The UDP enables process to process communication.For real-time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth.
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth,unlike TCP.

UDP Header –

UDP header is an **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contains all necessary header information and the remaining part consist of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



1. **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
2. **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
3. **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
4. **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.

- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol

Network Layer(IP) is an connection less protocol in TCP/IP

Ans:

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.

Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

IP Addressing:

i. IP is responsible for addressing and routing in the TCP/IP environment.

ii. An IP address is 32-bits in length, grouped into four 8-bit octets and each octet is represented by a decimal number from 0-255.

iii. Four decimal numbers are separated by periods in a format called dotted decimal notation.

Example: 172.24.208.192

Divided into two parts: network ID and host ID, In the above address, host ID 208.192 resides on network 172.24.

I) IP Address Classes :

IP Addresses are categorized in Classes A to E. Only IP addresses in the A, B, and C classes are available for host assignment.

- **Class A:**
  i. Value of the first octet is between 1 and 127.
  ii. Addresses beginning with 127 are reserved for loopback.
  iii. IP registry assigns the first octet, leaving the last three octets to be assigned to hosts.
  iv. Intended for large corporations and government.
- **Class B :**
  i. Value of the first octet is between 128 and 191.
  ii. IP registry assigns the first two octets, leaving the third and fourth octets to be assigned to hosts.
  iii. Intended for use in medium to large networks.
- **Class C :**
  i. Value of the first octet is between 192 and 223.
  ii. IP address registry assigns the first three octets.
  iii. These networks are limited to 254 hosts per network.
  iv. Intended for small networks.
- **Class D:**
  i. Value of the first octet is between 224 and 239.

ii. Reserved for multicasting.

- **Class E :**
  i. Value of the first octet is between 240 and 255.
  ii. Reserved for experimental use and can't be used for address assignment.

II) Private IP Addresses:

Due to the popularity of TCP/IP and the Internet, we are running out of unique IP addresses, A series of addresses have been reserved for private networks (networks whose hosts can't be accessed directly through the Internet.)

- Reserved addresses:
  i. Class A addresses beginning with 10.
  ii. Class B addresses from 172.16 to 172.31.
  iii. Class C addresses from 192.168.0 to 192.168.255.
  The addresses in those ranges can't be routed across the Internet.

III) Internet Protocol Version 6 :
IPv6 solves some problems in IPv4:
i. Limits of the 32-bit address space
ii. Lack of built-in security
iii. Complicated setup
iv. Lack of built-in quality of service (QoS)
v. Better routing and better improvement for multicasting.

IV) IPv6 :

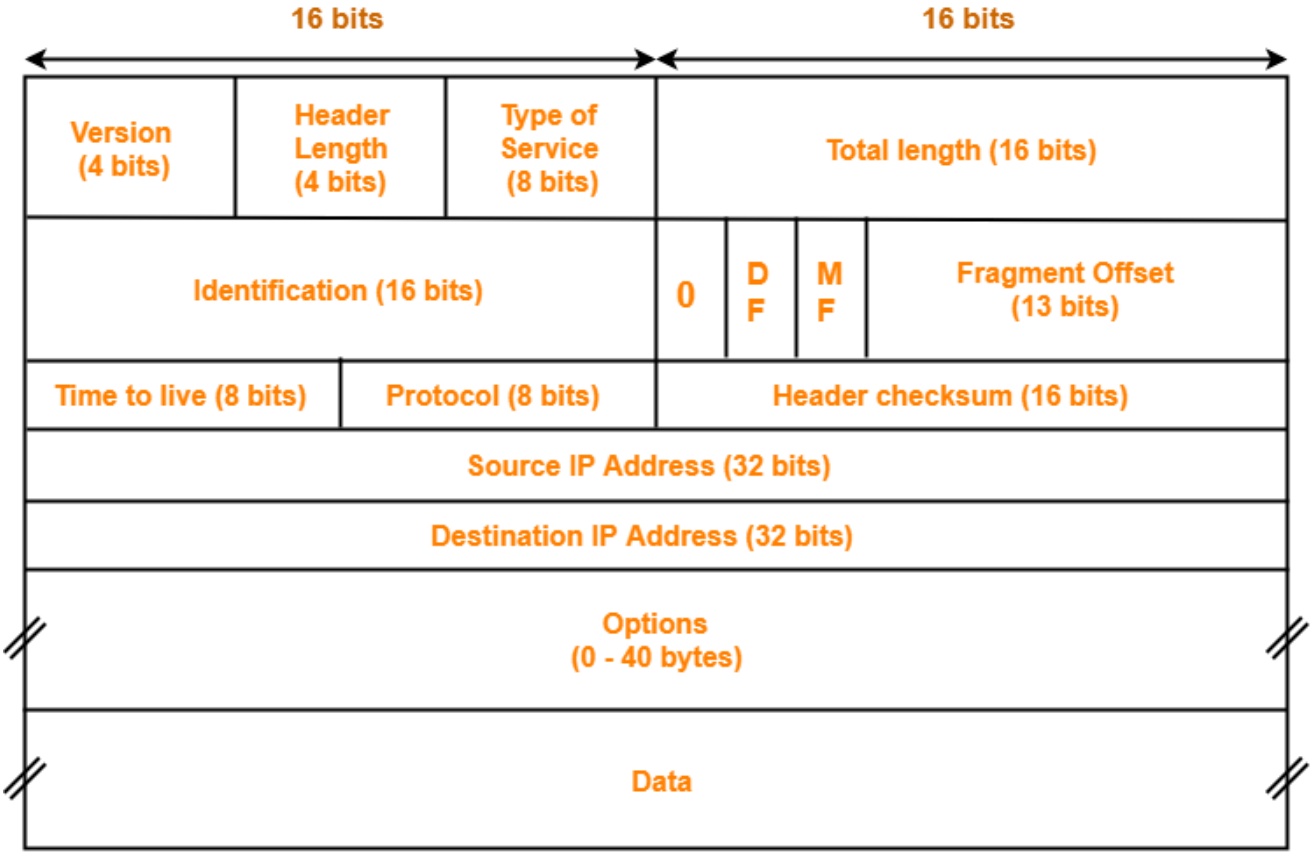
i. An IPv6 address is 128 bits instead of 32 bits in IPv4 IP Security (IPSec) protocol is incorporated into IPv6. IPv6 is autoconfiguring (no IP address to assign and no subnet mask to determine Microsoft Internet Protocol Version 6 (IPv6)
ii. IPv6 Addresses Specified in hexadecimal format, 8 blocks of 4 hex values.
iii. 16-bit sections separated by a colon

iv. Examples –FE80:0000:0000:D1AC:F0CD:00B9:0000:B00D
–2001:1B20:0302:442A:1100:2FEA:00A4:002B

v. You can remove leading zeros
–FE80:0:0:D1AC:F0CD:B9:0:B00D
–2001:1B20:302:442A:1100:2FEA:A4:2B

vi. Consecutive block of zeros can be replaced by ::
– FE80::D1AC:F0CD:B9:0:B00D

ipv4 header



IPv4 Header

Application Layer Protocols

Ans:•

```
TELNET is an abbreviation for TErminaL NETwork.
• TELNET is a general-purpose client-server application program.
• Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side
• There are two types of login:
        • Local Login
        • Remote login

**SSH is more secured remote login protocol and it can provide security to telnet using the concept of tunnneling**
```

```
FTP:
FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files. It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP
```

```
promotes sharing of files via remote computers with reliable and efficient
data transfer. The Port number for FTP is 20 for data and 21 for control.

>ftp machinename
```

```
SMTP:
It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP
protocol. Using a process called “store and forward,” SMTP moves your email
on and across networks. It works closely with something called the Mail
Transfer Agent (MTA) to send your communication to the right computer and
email inbox. The Port number for SMTP is 25.

**Command**
MAIL FROM:<mail@abc.com?
```

```
DNS:
It stands for Domain Name System. Every time you use a domain name,
therefore, a DNS service must translate the name into the corresponding IP
address. For example, the domain name www.abc.com might translate to
198.105.232.4.
The Port number for DNS is 53.

**Command**
ipconfig /flushdns
```

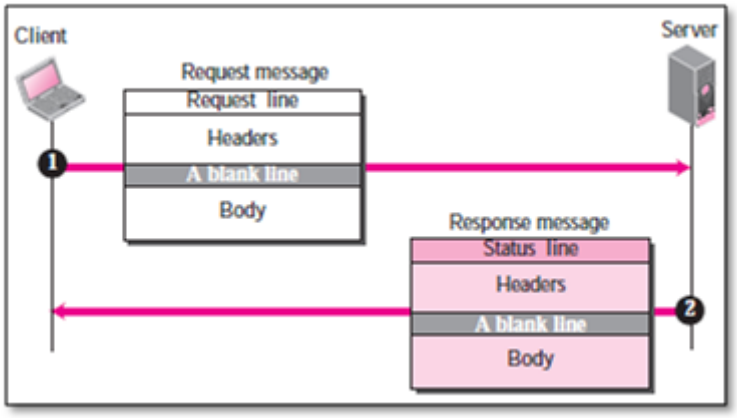
```
DHCP:
It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP
addresses to hosts. There is a lot of information a DHCP server can provide
to a host when the host is registering for an IP address with the DHCP
server. Port number for DHCP is 67, 68.

**Command**
clear ip dhcp binding {address | * }
```

POP3 and IMAP

Parameter	POP3	IMAP
Full Form	POP3 is an abbreviation for Post Office Protocol 3.	IMAP is an abbreviation for Internet Message Access Protocol.
Introduction	The POP is an Internet standard protocol on the application layer that the local email clients use for retrieving emails from any remote server over the TCP/IP connection.	The IMAP is a protocol that allows distant users to access their emails directly from the server and read them on any device at any location feasible for them.
Complexity	POP3 is a very simplified protocol. It can only download the emails on the local computer from the inbox.	The IMAP protocol is very complex. It allows all the users to view their email folders easily and read them on the mail server itself (from any device they want).
Email Organization	A user cannot organize the emails on the server using POP3.	IMAP allows its users to organize their available emails on the server.
Need to Download	POP3 downloads the mail first and then allows its users to read them.	You can partially read your emails before downloading them in the case of IMAP.
Multiaccess	POP3 only allows a single device at a time to access the emails.	IMAP allows multiple devices at a time to access and read the available mails.
Updating of Emails	A user cannot update or create emails on the mail server by using the POP3 protocol.	You can use the IMAP protocol for updating or creating emails. It is easy to do so with a web interface or email software.
Search Emails	You cannot search for mail content on any mail server using the POP3 protocol. The user needs to download the mail first and then search for the required content.	You can easily search for mail content on any mail server using IMAP without downloading them.
Change and Delete	POP3 does not allow its users to alter or delete any email available on the mail server.	IMAP allows its users to use an email software or a web interface to alter or delete the available emails.
Speed	POP3 is very fast.	IMAP is slow as compared to POP3.
Syncing of Mails	It does not allow syncing of a user's emails.	Users can sync their emails using this protocol.
Direction	**Unidirectional** – The changes that you make on a device have zero effect on the content available on the server.	**Bi-directional** – Whenever you make changes on the device or server, it shows on the other side as well.

HTTP

Ans:
HTTP stands for Hypertext Transfer Protocol. It is used to access data on the WWW (World Wide Web). It is a protocol which governs the communication between the client and server.
There are three important features of HTTP:
i. HTTP is **Connectionless**
After a request is made, the client disconnects from the server and waits for a response. The server must re-establish the connection after it processes the request.
ii. HTTP is **Media Independent**
Any type of data can be sent by HTTP as long as both the client and server know how to handle the data content.
iii. HTTP is **Stateless**
This is a direct result of HTTP being connectionless. The server and client are aware of each other only during a request. Afterwards, each forgets the other. For this reason neither the client now the browser can retain information between different requests across the web pages.
Working:
i. A browser contacts a server to establish a TCP connection with it.
ii. The HTTP software on the client sends a request to the server. The HTTP software on the server interprets this request and sends the response to the client.
iii. **HTTP Commands:**
a. **GET** : Request by a client to obtain a web page from the server.
b. **PUT** : Request by a client to store a web page on the server.
c. **POST** : Request by a client to update contents of a web page on the server.
d. **DELETE:** Request by a client to remove a web page from the server.



Extra

HTTP status codes that indicate what kind of response has been sent back. They are 3 digit codes that are grouped by the first number in the code. Each code has a

corresponding “reason phrase” to make human interpretation easier.

- **1XX** - informational response e.g. `102 Processing`
- **2XX** - successful response e.g. `200 OK`
- **3XX** - redirection response e.g. `302 Found`
- **4XX** - client error response e.g. `404 Not Found`
- **5XX** - server error response e.g. `500 Internal Server Error`

Other features of HTTP include sessions, which can be established and maintained either server side, or client side with **HTTP cookies.** HTTP also supports authentication in a variety of ways.

Domain Name System(DNS) in detail!

Ans:: **DNS** is a client/server application program used to help other application programs. DNS is used to map a host name in the application layer to an IP address in the network layer.

NEED FOR DNS.

- To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet.
- However, people prefer to use names instead of numeric addresses. Therefore, we need a system that can map a name to an address or an address to a name.

```
(for example, www.amazon.com) to machine readable IP addresses (for
example, 192.0.2.44).
```

Note: DNS should be maintain NAMESPACE property(the names must be unique because the addresses are unique.

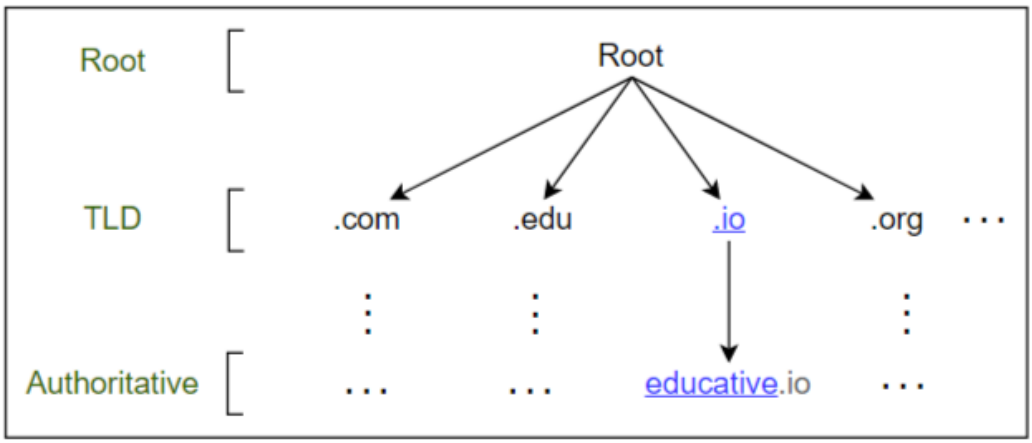
- **Hierarchy:** DNS name servers are in a hierarchical form. The hierarchical structure allows DNS to be highly scalable because of its increasing size and query load. In the next lesson, we’ll look at how a tree-like structure is used to manage the entire DNS database.

DNS hierarchy

1. **DNS resolver:** Resolvers initiate the querying sequence and forward requests to the other DNS name servers. Typically, DNS resolvers lie within the premise of the user’s network. However, DNS resolvers can also cater to users’ DNS queries

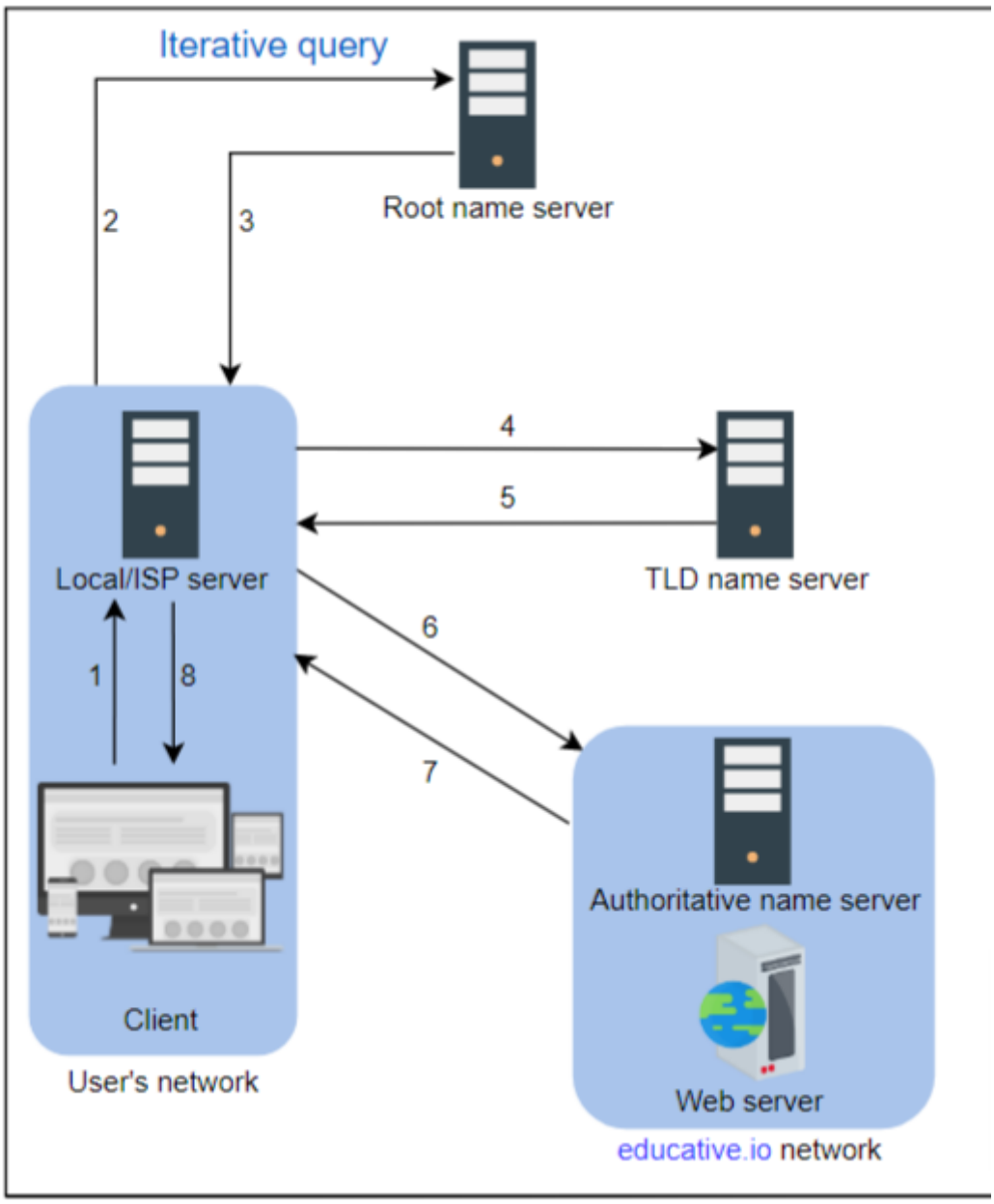
through caching techniques, as we will see shortly. These servers can also be called local or default servers.

2. **Root-level name servers:** These servers receive requests from local servers. Root name servers maintain name servers based on top-level domain names, such as `.com`, `.edu`, `.us`, and so on. For instance, when a user requests the IP address of educative.io, root-level name servers will return a list of top-level domain (TLD) servers that hold the IP addresses of the `.io` domain.
3. **Top-level domain (TLD) name servers:** These servers hold the IP addresses of authoritative name servers. The querying party will get a list of IP addresses that belong to the authoritative servers of the organization.
4. **Authoritative name servers:** These are the organization's DNS name servers that provide the IP addresses of the web or application servers.



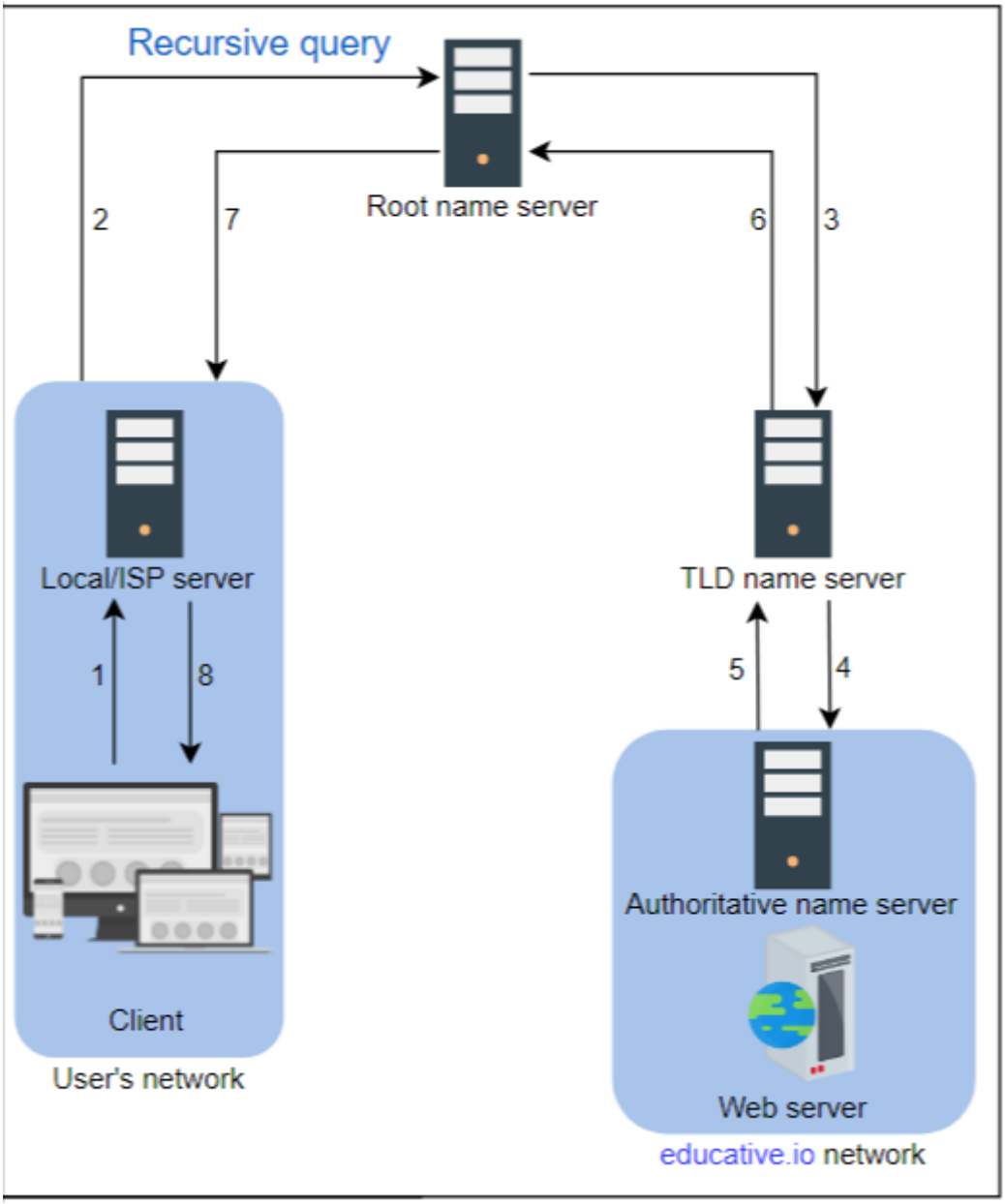
here are two ways to perform a DNS query:

1. **Iterative:** The local server requests the root, TLD, and the authoritative servers for the IP address.



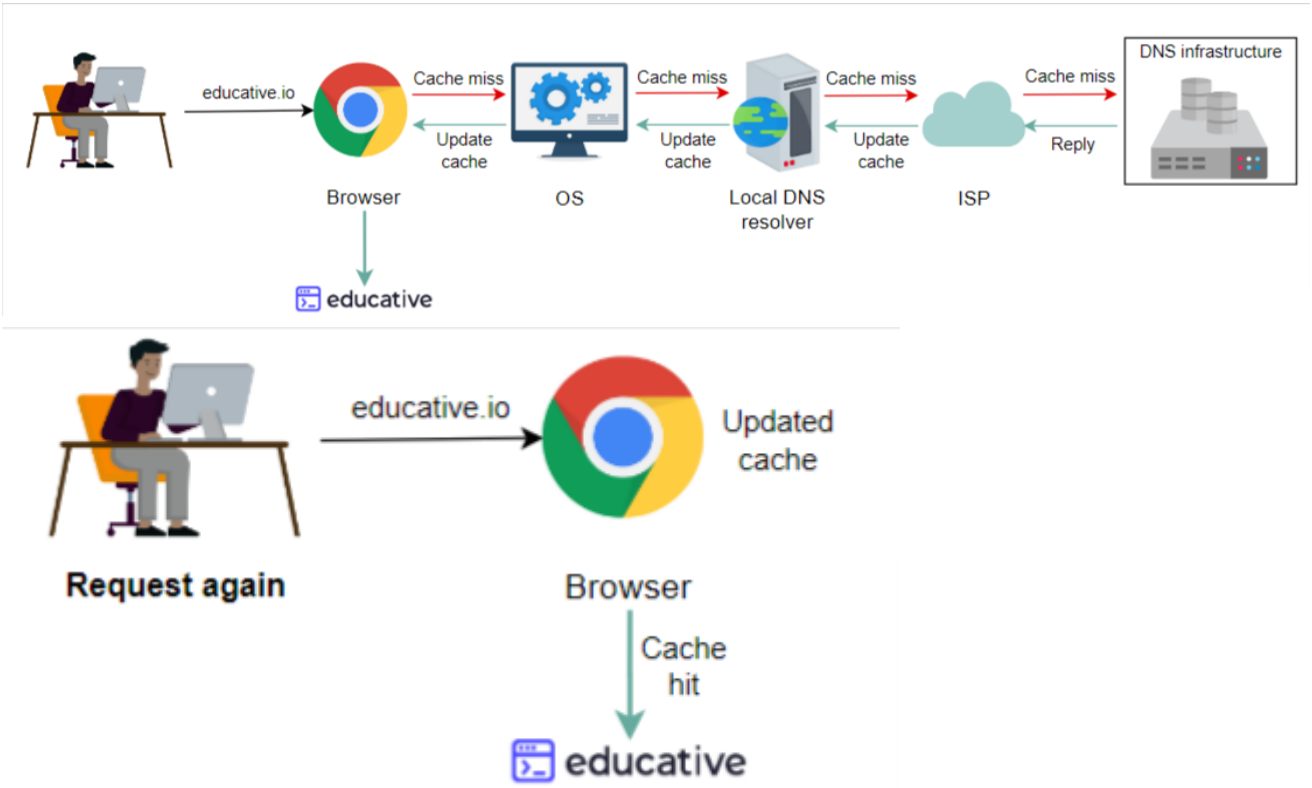
2. **Recursive:** The end user requests the local server. The local server further requests the root DNS name servers. The root name servers forward the requests to other

name servers.



Caching

It refers to the temporary storage of frequently requested resource records. A ***record*** is a data unit within the DNS database that shows a name-to-value binding. Caching reduces response time to the user and decreases network traffic. When we use caching at different hierarchies, it can reduce a lot of querying burden on the DNS infrastructure. Caching can be implemented in the browser, operating systems, local name server within the user's network, or the ISP's DNS resolvers.



DNS as a distributed system

Although the DNS hierarchy facilitates the distributed Internet that we know today, it's a distributed system itself. The distributed nature of DNS has the following advantages:

- It avoids becoming a single point of failure (SPOF).
- It achieves low query latency so users can get responses from nearby servers.
- It gets a higher degree of flexibility during maintenance and updates or upgrades. For example, if one DNS server is down or overburdened, another DNS server can respond to user queries.

There are 13 logical root name servers (named letter **A** through **M**) with many instances spread throughout the globe. These servers are managed by 12 different organizations.

cmd command lines

```
1.  nslookup www.google.com
2.  dig www.google.com
```

GeoDNS

Ans:Between the request of a visitor and the response of the authoritative nameserver, there is a long way. That is especially true if the server is on another continent. What

we can do to improve this process is to provide more nameservers, closer to the users, and have a system that redirects queries to the closest server. A smart load balancing mechanism that can locate the origin of the queries.
GeoDNS is a such a system that provides strategically located name servers on different continents and a process of distributing the traffic based on the locations of the queries.

Working
When a user sends a query, a DNS server will analyze it, reading the IP. Based on this information, the query will be sent to the closest nameserver. This will reduce the waiting time significantly.

`Example:_Imagine this. You have servers in the USA, in Germany, and in India. A visitor from Italy will get the answer to its request from Germany. A Canadian will get it from the American server and a Chinese from the Indian. The traffic will be optimized for speed and load balancing._`

- Who need it?
Ans:It is for global sites that will have traffic from different countries and substantial traffic: companies that need 100% uptime and low latency.
E-commerce platforms that don't want to miss a sale, Content companies, who needs a CDN network for fast content delivery on a global scale; Banking and Fintech companies with international clients, and more.

MultiCast DNS?

Ans:The multicast DNS (mDNS) protocol resolves hostnames to IP addresses within small networks that do not include a local name server.

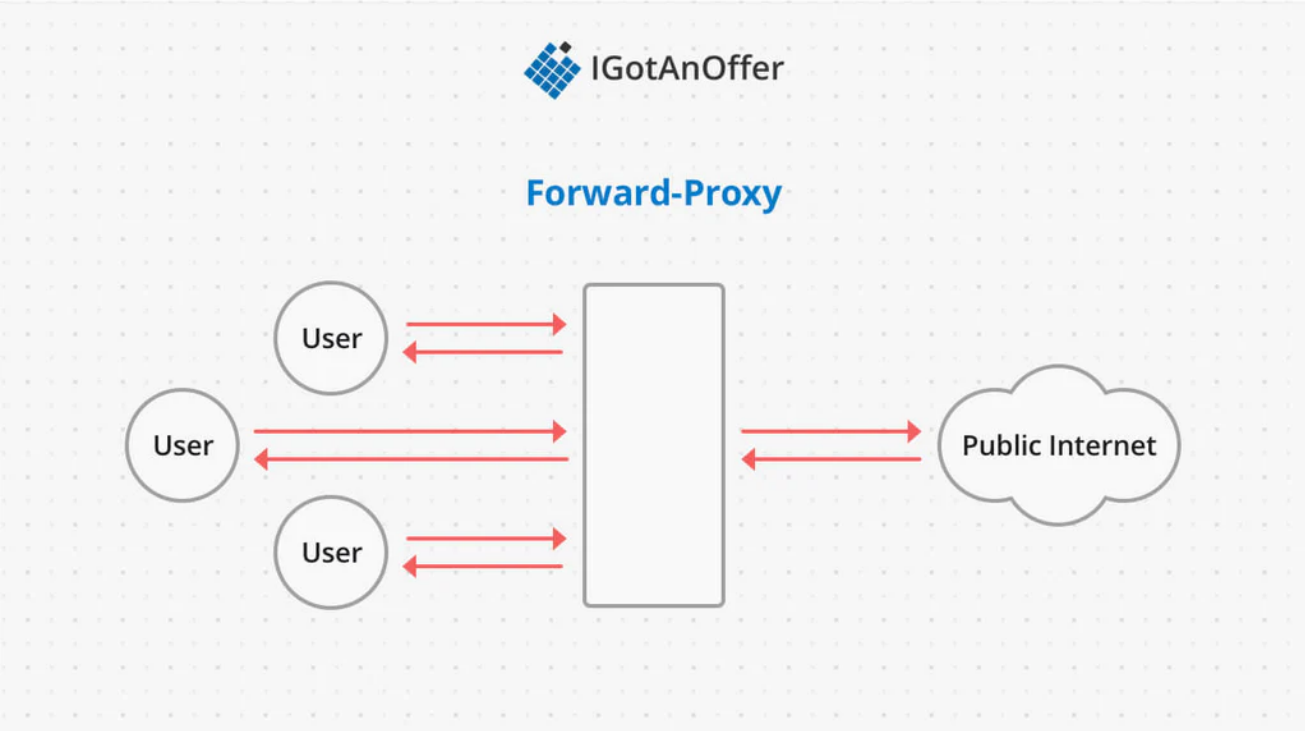
- It is a zero-configuration service, using essentially the same programming interfaces, packet formats and operating semantics as unicast Domain Name Service (DNS).
- It was designed to work as either a stand-alone protocol or compatibly with standard DNS servers. When an mDNS client needs to resolve a hostname, it sends an IP multicast query message that asks the host having that name to identify itself. That target machine then multicasts a message that includes its IP address.
- All machines in that subnet can then use that information to update their mDNS caches.
- Any host can relinquish its claim to a name by sending a response packet with a time to live (TTL) equal to zero.

Note: to remember just think like this I called a Ice cream truck at my home and bought some ice cream,while the truck driver go back to the company many of my socity people bought the ice cream even though I was the who called him...

Proxies

A proxy is a server that sits between a client and application server to provide some intermediary service to the communication. There are two kinds of proxies that provide different services: forward proxies and reverse proxies.

Forward Proxies



A forward proxy sits between a pool of clients and the public internet. The goal of a forward proxy is to protect the particular client pool by filtering outgoing requests and incoming responses.

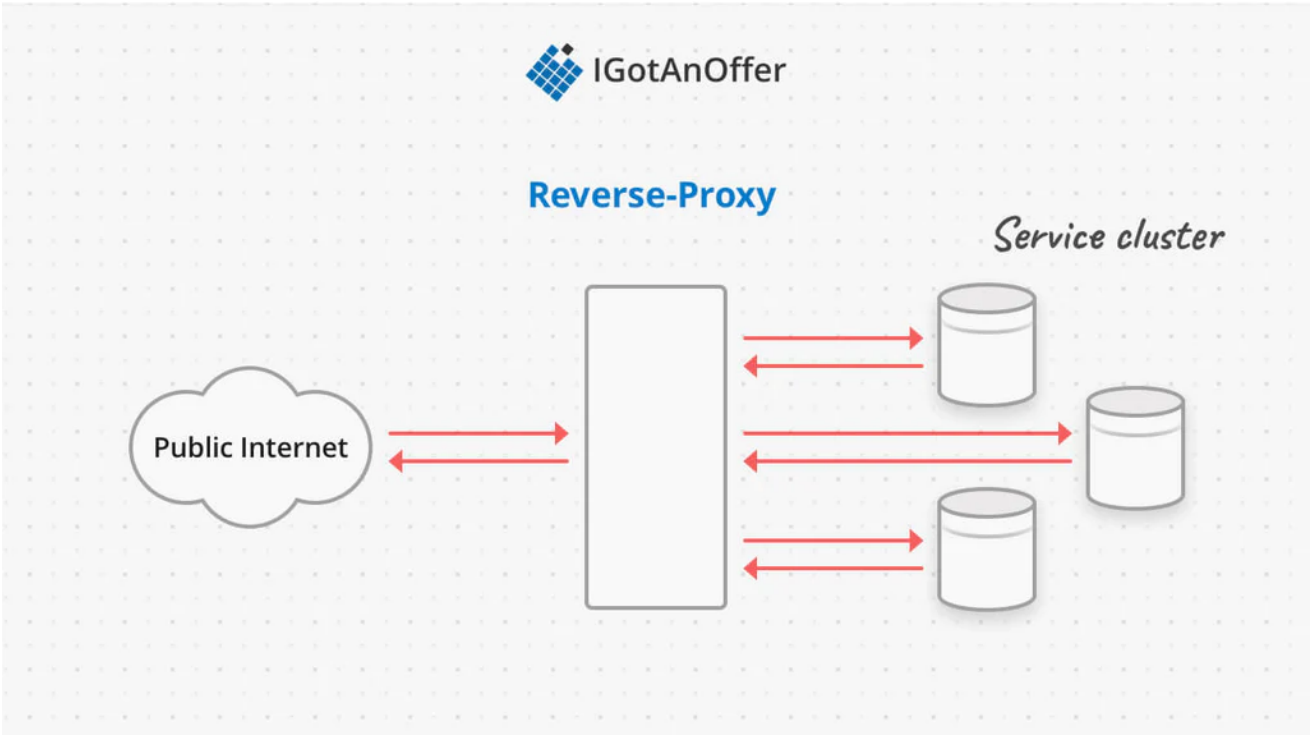
The common use cases for forward proxies are:

- Enforcing “terms of use” on a network
- Blocking malicious websites
- Anonymizing network traffic by using the IP address of the proxy instead of the client

For example, a school network might decide to block requests going out to certain social media websites. Alternatively a business network might try to mitigate phishing

attacks by not allowing employee requests to known malicious domain names.

Reverse Proxies



A reverse proxy sits between the public internet and a pool of servers. Because of their location in the system as an intermediary, reverse proxies can provide a number of services, including:

- Anonymizing the cluster servers
- SSL termination
- Load balancing
- Caching
- Filtering requests
- Attack prevention (e.g. DOS detection)

For example, if a company wanted to expose a public API for querying data, but not modifying it, they could filter out any requests that used an HTTP verb other than GET before passing the requests on to the servers that actually process and generate the responses.

As another example, a service could use a reverse proxy to handle TLS termination (the description of HTTPS requests) so that the application servers don't have to handle encryption/decryption. The proxy would then pass on the requests to the servers within a private network so the communication is still secure.

Note That VPN are more reliable than proxies

VPN

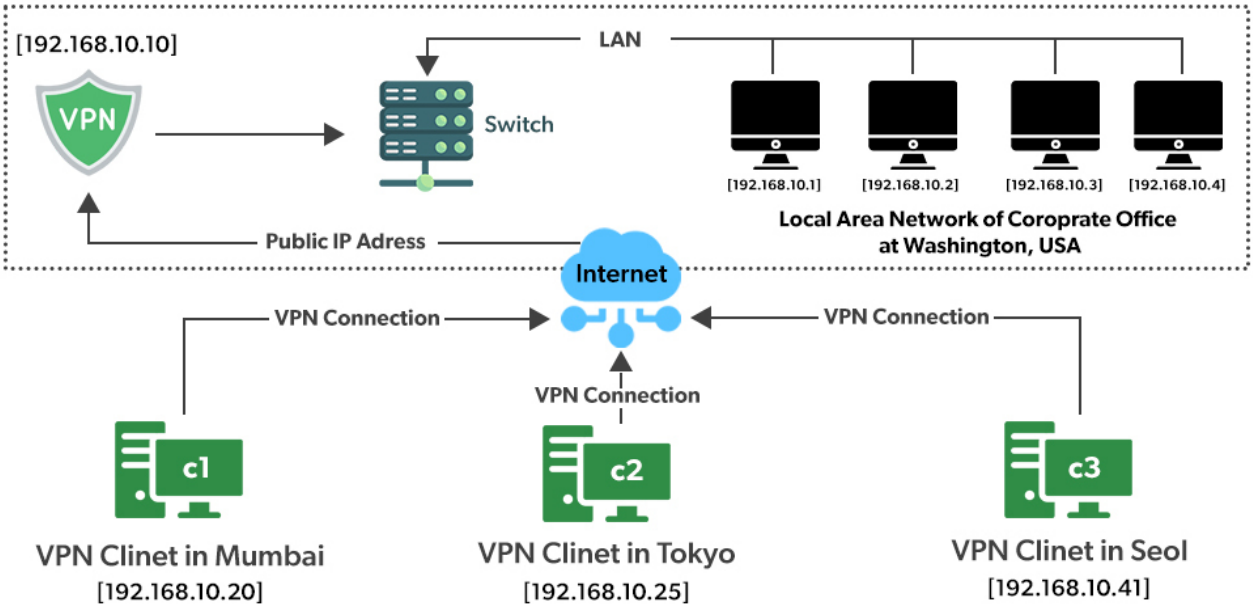
VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet.

Lets understand VPN by an example:

Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

The situation is described below:

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the intuitive way of extending the local network even across the geographical borders of the country.



1. VPN also ensures security by providing an encrypted tunnel between client and VPN server.
2. VPN is used to bypass many blocked sites.
3. VPN facilitates Anonymous browsing by hiding your ip address.
4. Also, most appropriate Search engine optimization(SEO) is done by analyzing the data from VPN providers which provide country-wise stats of browsing a particular product. This method of SEO is used widely my many internet marketing managers to form new strategies.
   Using VPN is legal in most of the countries,. The legality of using a VPN service depends on the country and its geopolitical relations with another country as well. A reliable and secure VPN is always legal if you are not intended to use it for any illegal activities like committing fraud online, cyber theft, or in some countries downloading copyrighted content.