1. Session :
A session is used to save information on the server momentarily so that it may be utilized across various pages of the website. It is the overall amount of time spent on an activity. The user session begins when the user logs in to a specific network application and ends when the user logs out of the program or shuts down the machine.

Session values are far more secure since they are saved in binary or encrypted form and can only be decoded at the server. When the user shuts down the machine or logs out of the program, the session values are automatically deleted. We must save the values in the database to keep them forever.

2. Cookie :
A cookie is a small text file that is saved on the user's computer. The maximum file size for a cookie is 4KB. It is also known as an HTTP cookie, a web cookie, or an internet cookie. When a user first visits a website, the site sends data packets to the user's computer in the form of a cookie.

The information stored in cookies is not safe since it is kept on the client-side in a text format that anybody can see. We can activate or disable cookies based on our needs.

Difference Between Session and Cookies :

Cookie	Session
Cookies are client-side files on a local computer that hold user information.	Sessions are server-side files that contain user data.

Cookies end on the lifetime set by the user.	When the user quits the browser or logs out of the programmed, the session is over.
It can only store a certain amount of info.	It can hold an indefinite quantity of data.
The browser's cookies have a maximum capacity of 4 KB.	We can keep as much data as we like within a session, however there is a maximum memory restriction of 128 MB that a script may consume at one time.
Because cookies are kept on the local computer, we don't need to run a function to start them.	To begin the session, we must use the session start() method.
Cookies are not secured.	Session are more secured compare than cookies.

Cookies stored data in text file.	Session save data in encrypted form.
Cookies stored on a limited data.	Session stored a unlimited data.
In PHP, to get the data from Cookies , $_COOKIES the global variable is used	In PHP , to get the data from Session, $_SESSION the global variable is used
We can set an expiration date to delete the cookie’s data. It will automatically delete the data at that specific time.	In PHP, to destroy or remove the data stored within a session, we can use the session_destroy() function, and to unset a specific variable, we can use the unset() function.

Difference between Intranet and Internet, Working of Internet

Generally, most people are confused between the internet and the intranet. While there are exist lots of differences to differentiate them.

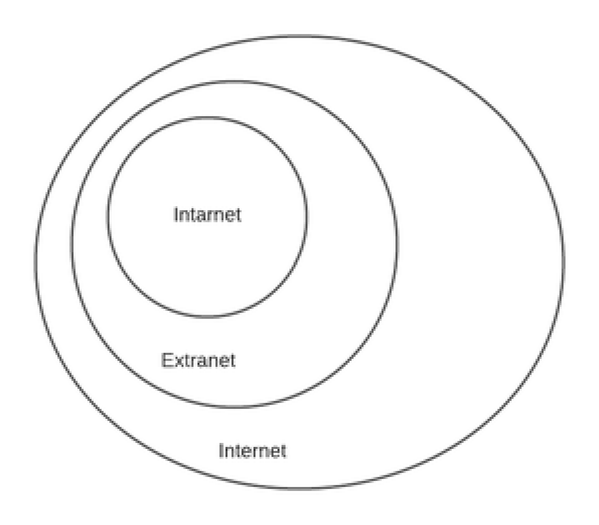
Internet:

Internet is used to connect the different networks of computers simultaneously.

It is a public network therefore anyone can access the internet. On the internet, there are multiple users and it provides an unlimited of information to the users.

Intranet:

Intranet is the type of internet that is used privately. It is a private network therefore anyone can't access the intranet. On the intranet, there is a limited number of users and it provides a piece of limited information to its users.



Types of network

Now, we shall see the difference between the internet and intranet:

S.NO	Internet	Intranet
1.	Internet is used to connect different networks of computers simultaneously.	Intranet is owned by private firms.

2.	On the internet, there are multiple users.	On an intranet, there are limited users.
3.	Internet is unsafe.	Intranet is safe.
4.	On the internet, there is more number of visitors.	In the intranet, there is less number of visitors.
5.	Internet is a public network.	Intranet is a private network.
6.	Anyone can access the Internet.	In this, anyone can’t access the Intranet.
7.	The Internet provides unlimited information.	Intranet provides limited information.

8.	Using Social media on your phone or researching resources via Google.	A company used to communicate internally with its employees and share information
9.	The Internet is a global network that connects millions of devices and computers worldwide.	An intranet is a private network that connects devices and computers within an organization.
10.	It is open to everyone and allows access to public information, such as websites and online services.	An intranet is only accessible to authorized users within the organization.
11.	It is used for communication, sharing of information, e-commerce, education, entertainment, and other purposes.	An intranet is primarily used for internal communication, collaboration, and information sharing within an organization.

12.	Users can access the Internet from any location with an Internet connection and a compatible device.	Access to an intranet is restricted to authorized users within the organization and is typically limited to specific devices and locations.
13.	Security measures, such as firewalls, encryption, and secure sockets layer (SSL) protocols, are used to protect against threats like hacking, viruses, and malware.	Intranets employ similar security measures to protect against unauthorized access and ensure the privacy and integrity of shared data.
14.	The Internet is a public network that is not owned by any particular organization or group.	Intranets are private networks that are owned and managed by the organization that uses them.
15.	Examples of Internet-based services include email, social media, search engines, and online shopping sites.	Examples of intranet-based services include internal communications, knowledge management systems, and collaboration tools

Domain Name Server

Domain Name System (DNS) is a hostname for **IP address** translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. It is required for the functioning of the Internet.

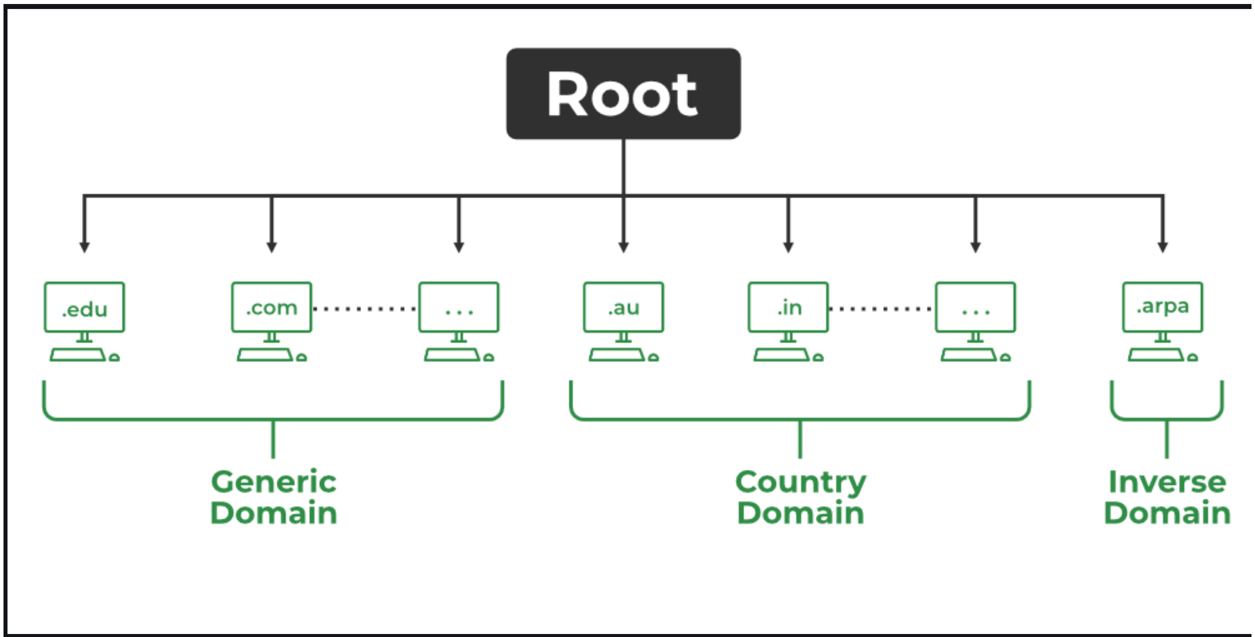
What is the Need of DNS?

Every host is identified by the IP address but remembering numbers is very difficult for people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Types of Domain

There are various kinds of domain:

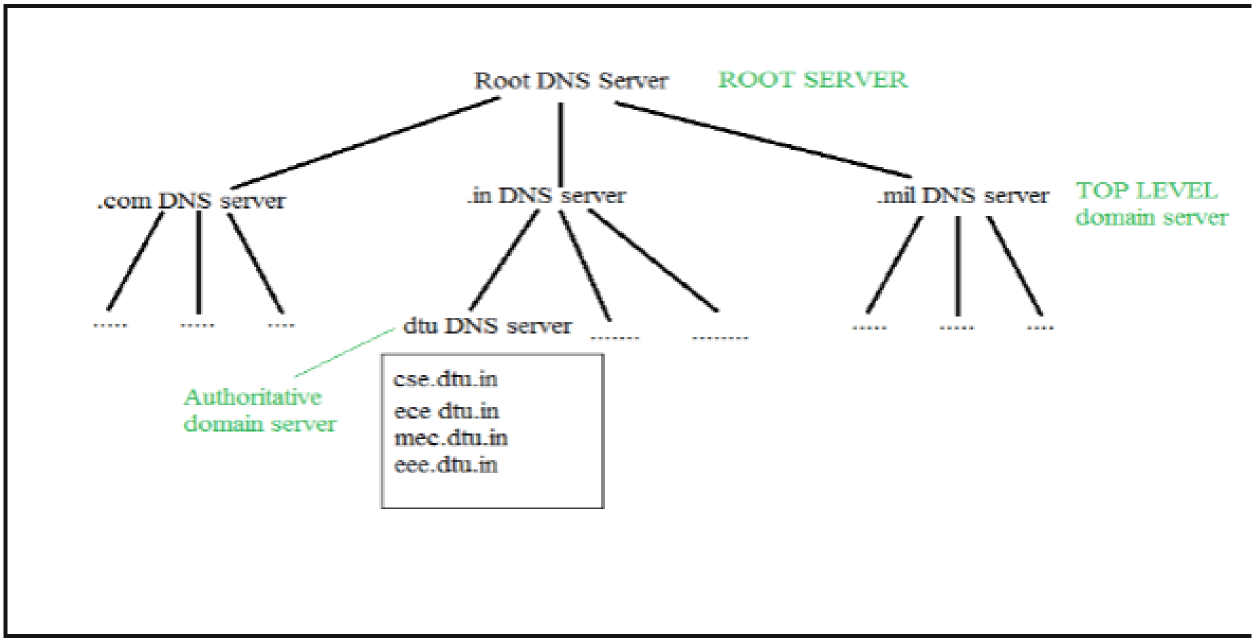
1. **Generic domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
2. **Country domain:** .in (India) .us .uk
3. **Inverse domain:** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type



Types of DNS

Organization of Domain

It is very difficult to find out the IP address associated with a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delays for that to happen organization of the database is very important.

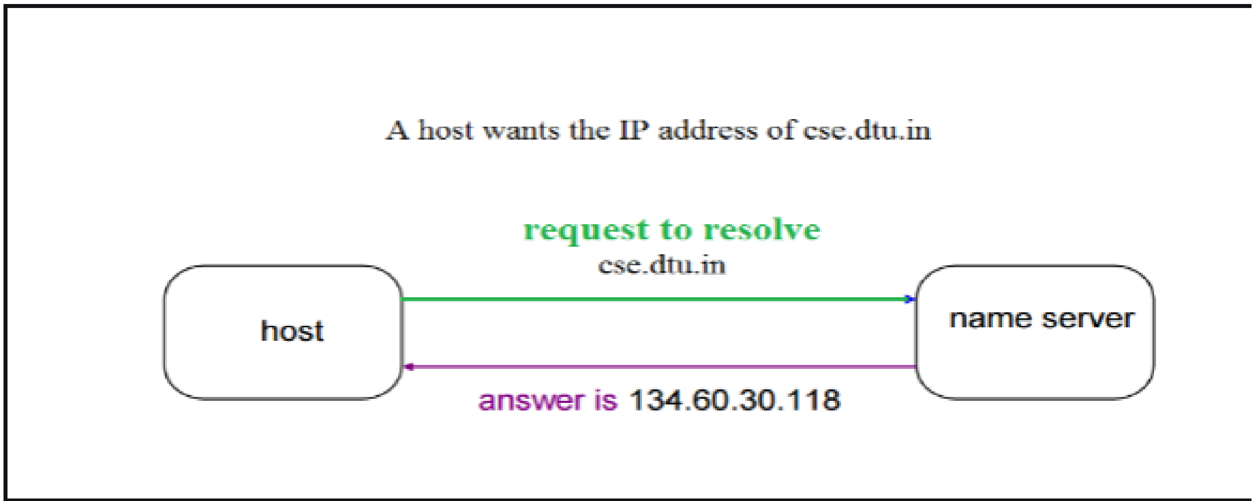


Root DNS Server

- **DNS record:** Domain name, IP address what is the validity? what is the time to live? and all the information related to that domain name. These records are stored in a tree-like structure.
- **Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.
- **Name server:** It is an implementation of the resolution mechanism.

Name-to-Address Resolution

The host requests the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.



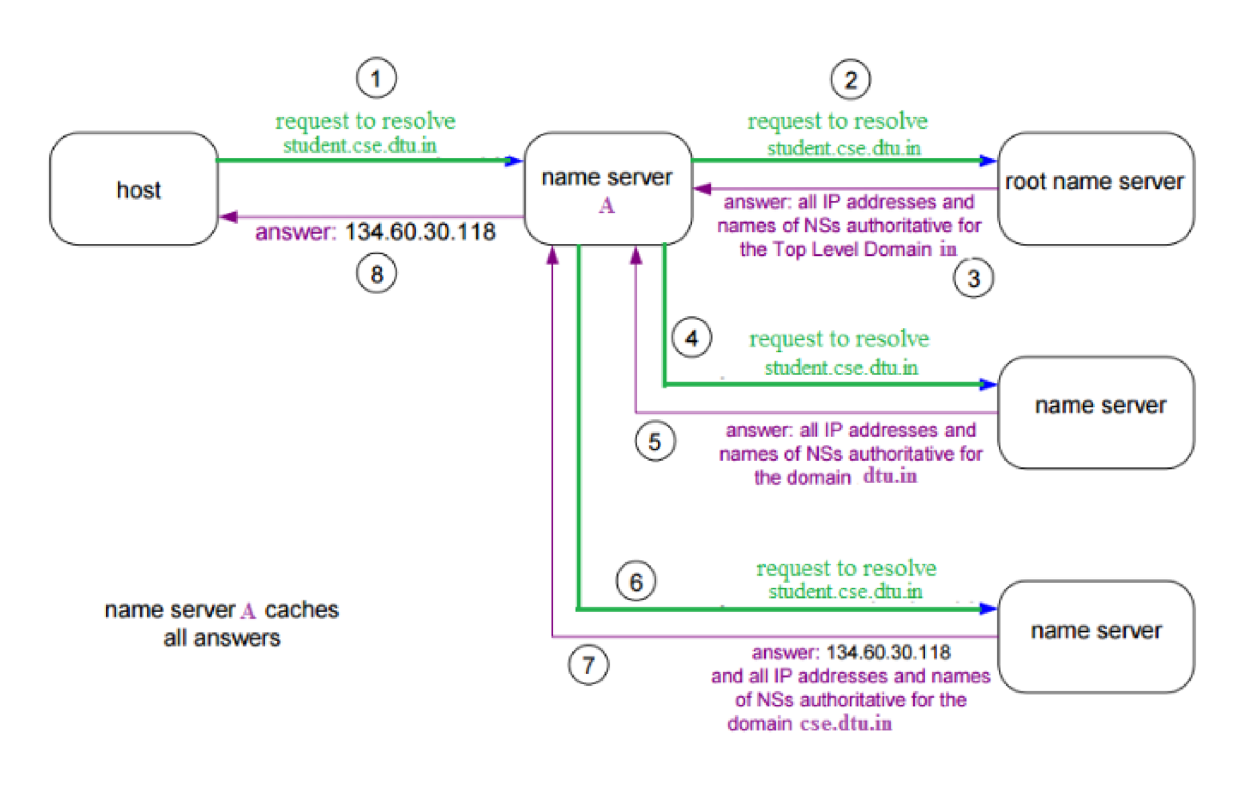
Name-to-Address Resolution

- **Hierarchy of Name Servers Root name servers:** It is contacted by name servers that can not resolve the name. It contacts the authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.
- **Top-level domain (TLD) server:** It is responsible for com, org, edu, etc, and all top-level country domains like uk, fr, ca, in, etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.
- **Authoritative name servers** are the organization's DNS servers, providing authoritative hostnames to IP mapping for organization servers. It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top-level domain server and then to the authoritative domain name server which actually contains the IP

address. So the authoritative domain server will return the associative IP address.

Domain Name Server

The client machine sends a request to the local name server, which, if the root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to a top-level domain (TLD) or authoritative name server. The root name server can also contain some hostName to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.



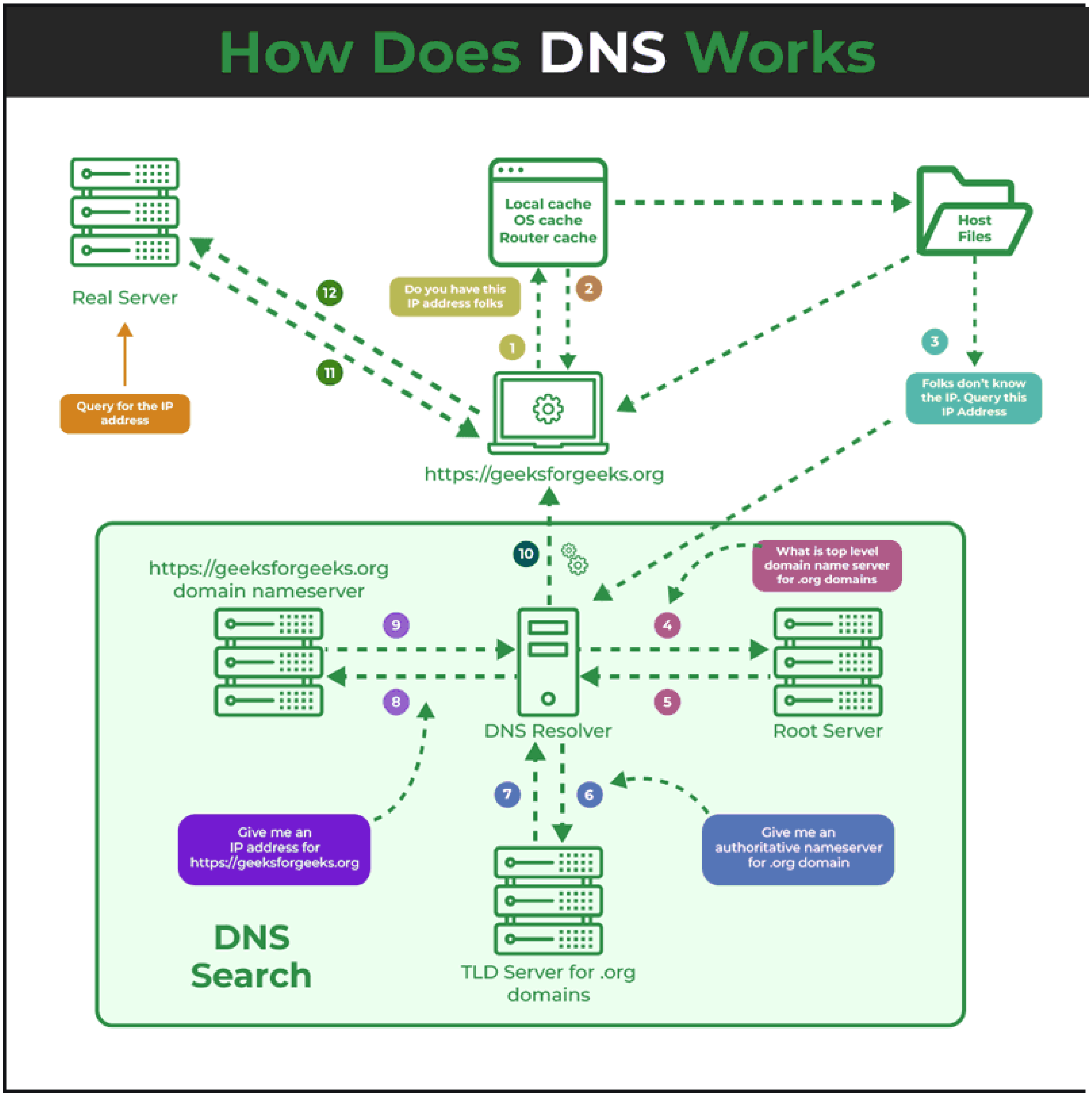
host
1
request to resolve student.cse.dtu.in
name server A
answer: 134.60.30.118
8
2
request to resolve student.cse.dtu.in
root name server
answer: all IP addresses and names of NSs authoritative for the Top Level Domain in
3
4
request to resolve student.cse.dtu.in
name server
5
answer: all IP addresses and names of NSs authoritative for the domain dtu.in
6
request to resolve student.cse.dtu.in
name server
7
answer: 134.60.30.118 and all IP addresses and names of NSs authoritative for the domain cse.dtu.in
name server A caches all answers

Domain Name Server

How Does DNS Work?

The working of DNS starts with converting a hostname into an IP Address. A domain name serves as a distinctive identification for a website. It is used in place of an IP address to make it simpler for consumers to visit websites. Domain Name System works by executing the database whose work is to store the name of hosts which are available on the Internet. The top-level domain server stores address information for top-level domains such as .com and .net, .org, and so on. If the Client sends the request, then the DNS resolver sends a request to DNS Server to fetch the IP Address. In case, when it does not contain that particular IP Address with a hostname, it forwards the request to another DNS Server. When IP Address has arrived at the resolver, it completes the request over Internet Protocol.

For more, you can refer to Working of DNS Server.


How Does DNS Works
Local cache
OS cache
Router cache
Host Files
Real Server
Query for the IP address
Do you have this IP address folks
1
2
3
Folks don't know the IP. Query this IP Address
11
12
https://geeksforgeeks.org
10
https://geeksforgeeks.org domain nameserver
What is top level domain name server for .org domains
9
4
8
5
DNS Resolver
Root Server
7
6
Give me an IP address for https://geeksforgeeks.org
Give me an authoritative nameserver for .org domain
DNS Search
TLD Server for .org domains

How Does DNS Work?

Authoritative DNS Server Vs Recursive DNS Resolver

Parameters	Authoritative DNS Server	Recursive DNS Resolver

Function	Holds the official DNS records for a domain	Resolves DNS queries on behalf of clients
Role	Provides answers to specific DNS queries	Actively looks up information for clients
Query Handling	Responds with authoritative DNS data	Queries other DNS servers for DNS data
Client Interaction	Doesn’t directly interact with end-users	Serves end-users or client applications
Data Source	Stores the DNS records for specific domains	Looks up data from other DNS servers
Caching	Generally, doesn’t perform caching	Caches DNS responses for faster lookups

Hierarchical Resolution	Does not participate in the recursive resolution	Actively performs recursive name resolution
IP Address	Has a fixed, known IP address	IP address may vary depending on ISP
Zone Authority	Manages a specific DNS zone (domain)	Does not manage any specific DNS zone

What is DNS Lookup?

DNS Lookup or DNS Resolution can be simply termed as the process that helps in allowing devices and applications that translate readable domain names to the corresponding IP Addresses used by the computers for communicating over the web.

DNS Servers Involved in Loading a Webpage

Upon loading the webpage, several DNS Servers are responsible for translating the domain name into the corresponding IP Address of the web server hosting the website. Here is the list of main DNS servers involved in loading a Webpage.

- Local DNS Resolver
- Root DNS Servers
- Top-Level Domain (TLD) DNS Servers

- Authoritative DNS Servers
- Web Server

This hierarchical system of DNS servers ensures that when you type a domain name into your web browser, it can be translated into the correct IP address, allowing you to access the desired webpage on the internet.

For more information you can refer DNS Look-Up article.

What is DNS Resolver?

DNS Resolver is simply called a DNS Client and has the functionality for initiating the process of DNS Lookup which is also called DNS Resolution. By using the DNS Resolver, applications can easily access different websites and services present on the Internet by using domain names that are very much friendly to the user and that also resolves the problem of remembering IP Address.

What Are the Types of DNS Queries?

There are basically three types of DNS Queries that occur in DNS Lookup. These are stated below.

- **Recursive Query:** In this query, if the resolver is unable to find the record, in that case, DNS client wants the DNS Server will respond to the client in any way like with the requested source record or an error message.
- **Iterative Query:** Iterative Query is the query in which DNS Client wants the best answer possible from the DNS Server.

- **Non-Recursive Query:** Non-Recursive Query is the query that occurs when a DNS Resolver queries a DNS Server for some record that has access to it because of the record that exists in its cache.

What is DNS Caching?

DNS Caching can be simply termed as the process used by DNS Resolvers for storing the previously resolved information of DNS that contains domain names, and IP Addresses for some time. The main principle of DNS Caching is to speed up the process of future DNS lookup and also help in reducing the overall time of DNS Resolution.

FAQs On Domain Name System (DNS)

Q.1: What do you mean by level 3 DNS Server?

Answer:

Q.2: Is Domain Name System (DNS) a protocol?

Answer:

Domain Name System (DNS)

Q.3: How can you categorize a DNS as a TCP or UDP?

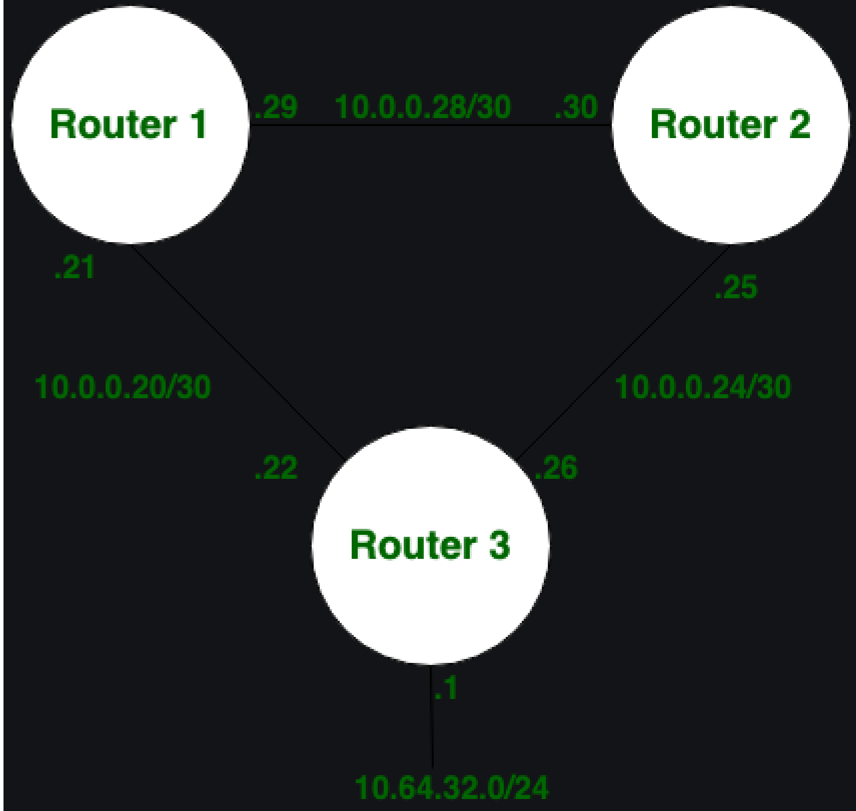
Answer:

TCP UDP.

Dynamic and Static Routing

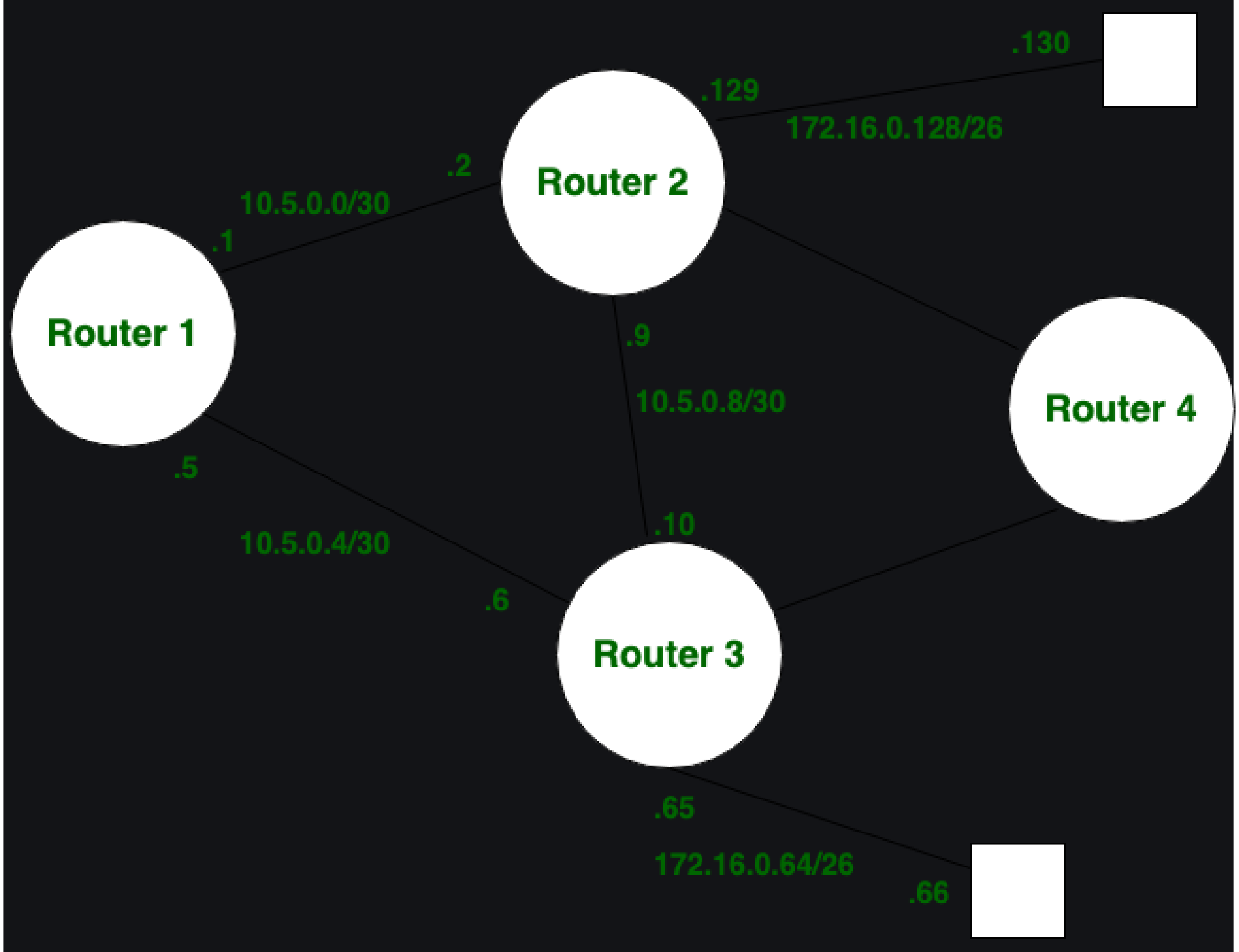
Static Routing:

Static Routing is also known as **non-adaptive** routing which doesn’t change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing.



Dynamic Routing:

Dynamic routing is also known as **adaptive** routing which changes the routing table according to the change in topology. Dynamic routing uses complex routing algorithms and it does not provide high security like static routing. When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.



Difference between Static and Dynamic Routing:

S.NO	Static Routing	Dynamic Routing
1.	In static routing routes are user-defined.	In dynamic routing, routes are updated according to the topology.

2.	Static routing does not use complex routing algorithms.	Dynamic routing uses complex routing algorithms.
3.	Static routing provides high or more security.	Dynamic routing provides less security.
4.	Static routing is manual.	Dynamic routing is automated.
5.	Static routing is implemented in small networks.	Dynamic routing is implemented in large networks.
6.	In static routing, additional resources are not required.	In dynamic routing, additional resources are required.
7.	In static routing, failure of the link disrupts the rerouting.	In dynamic routing, failure of the link does not interrupt the rerouting.

8.	Less Bandwidth is required in Static Routing.	More Bandwidth is required in Dynamic Routing.
9.	Static Routing is difficult to configure.	Dynamic Routing is easy to configure.
10.	Another name for static routing is non-adaptive routing.	Another name for dynamic routing is adaptive routing.

Proxy server

What is a proxy server and how does it work?

Every computer that is connected to the network has an IP (Internet Protocol) address that identifies the device uniquely. Similarly, the **proxy server** is a computer on the network that has its own IP address. But sometimes, we want to access those websites or servers that are restricted and we do not want to show our identity (IP address). In such a scenario, the **proxy server** comes into existence. We can achieve the same by using the **proxy server**. It provides varying levels of functionality, security, and privacy that depend on the use case, needs, or policies of the company. In this section, we will discuss **what is a proxy server**, its **types, advantages, need**, and **working of proxy servers**.

Proxy Server

The **proxy server** is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.

In other words, we can say that the proxy server allows us to access any websites with a different IP address. It plays an intermediary role between users and targeted websites or servers. It collects and provides information related to user requests. The most important point about a proxy server is that it does not **encrypt traffic**.

There are two main purposes of proxy server:

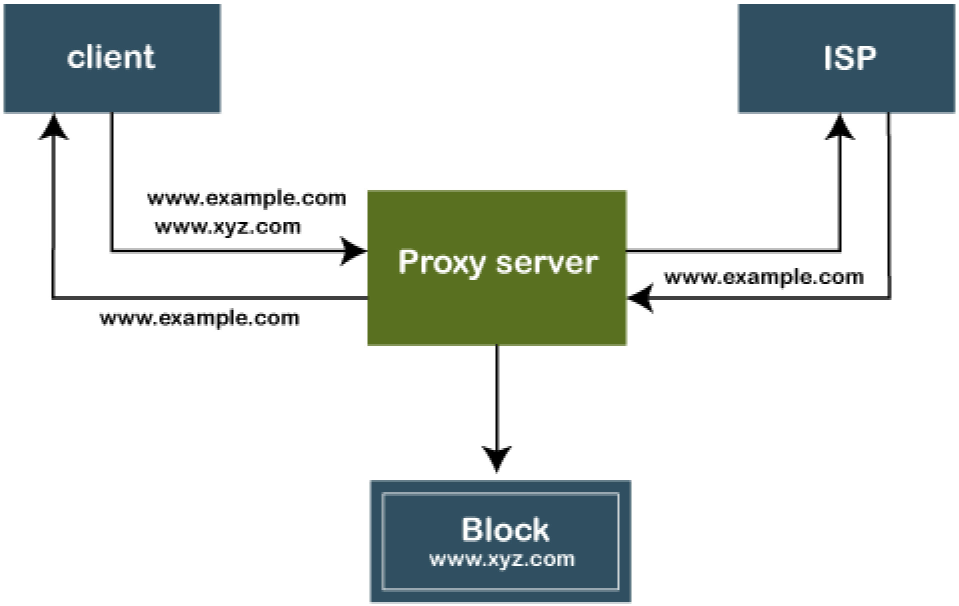
ADVERTISEMENT
ADVERTISEMENT

ADVERTISEMENT

- To keep the system behind it anonymous.
- To speed up access to a resource through caching.

Mechanism of Proxy Server

The following figure depicts the mechanism of the proxy server.

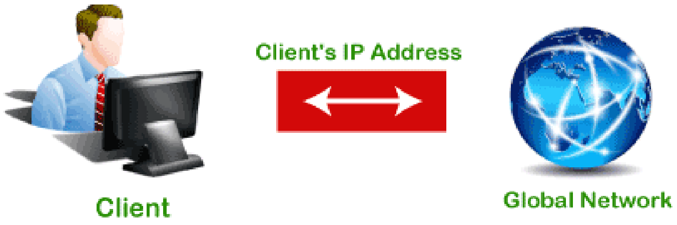


Mechanism of Proxy Server

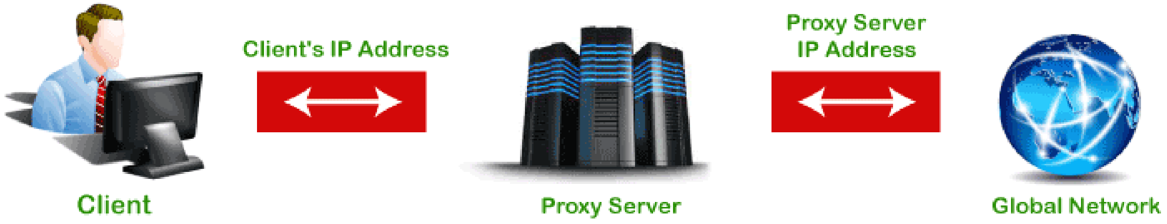
The proxy server accepts the request from the client and produces a response based on the following conditions:

1. If the requested data or page already exists in the local cache, the proxy server itself provides the required retrieval to the client.
2. If the requested data or page does not exist in the local cache, the proxy server forwards that request to the destination server.
3. The proxy servers transfer the replies to the client and also being cached to them.

Therefore, it can be said that the proxy server acts as a client as well as the server.



Communication without proxy server



Communication with proxy server

Types of Proxy Servers

There are many types of proxy servers available. The two most common types of proxy servers are **forward** and **reverse proxy servers**. The other proxy server has its own feature and advantages. Let's discuss each in detail.

1. **Open or Forward Proxy Server:** It is the most widely recognized type of intermediary worker that is gotten to by the customer. An open or forward proxy server refers to those sorts of intermediaries that get demands from web clients and afterward peruse destinations to gather the mentioned information. After collecting the data from the sites, it forwards the data to the internet users directly. It bypasses the firewall made by authorities. The following image shows

forward proxy configuration.

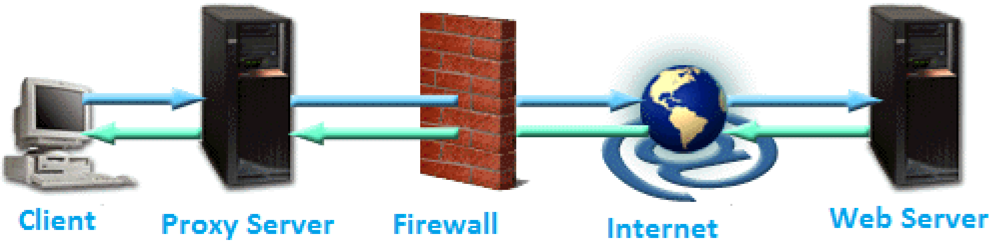


Fig: Forward Proxy Server

2. **Reverse Proxy Server:** It is a proxy server that is installed in the neighborhood of multiple other internal resources. It validated and processes a transaction in such a way that the clients do not communicate directly. The most popular reverse proxies are **Varnish** and **Squid**. The following image shows the reverse proxy configuration.

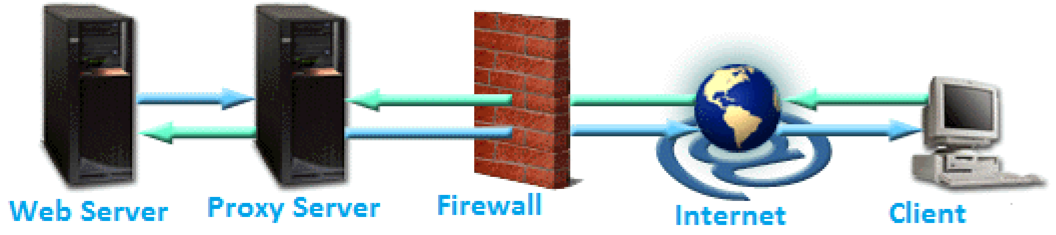


Fig: Reverse Proxy Server

3. **Split Proxy Server:** It is implemented as two programs installed on two different computers.

4. **Transparent Proxy:** It is a proxy server that does not modify the request or response beyond what is required for proxy authentication and identification. It works on port 80.

5. **Non-Transparent Proxy:** It is an intermediary that alters the solicitation reaction to offer some extra types of assistance to the client. Web demands are straightforwardly shipped off the intermediary paying little mind to the worker from where they started.

6. **Hostile Proxy:** It is used to eavesdrop upon the data flow between the client machine and the web.
7. **Intercepting Proxy Server:** It combines the proxy server with a gateway. It is commonly used in businesses to prevent avoidance of acceptable use policy and ease of administration.
8. **Forced Proxy Server:** It is a combination of Intercepting and non-intercepting policies.
9. **Caching Proxy Server:** Caching is servicing the request of clients with the help of saved contents from previous requests, without communicating with the specified server.
10. **Web Proxy Server:** The proxy that is targeted to the world wide web is known as a web proxy server.
11. **Anonymous Proxy:** The server tries to anonymizing the web

Web Servers: Introduction, Working, Configuring, Hosting and Managing a Web server, Client-side Technologies, Serverside Technologies, and hybrid technologies