DNS and how it works?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names. Web browsers interact through IP addresses. DNS translates domain names to IP addresses so browsers can load Internet Resources.

The process of DNS resolution involves converting a hostname into a computer-friendly IP address. An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device. When a user wants to load a webpage, a translation must occur between what a user types into their web browser and the machine-friendly address necessary to locate the domain of the website.

DNS servers

There are 4 DNS servers involved in loading a website:

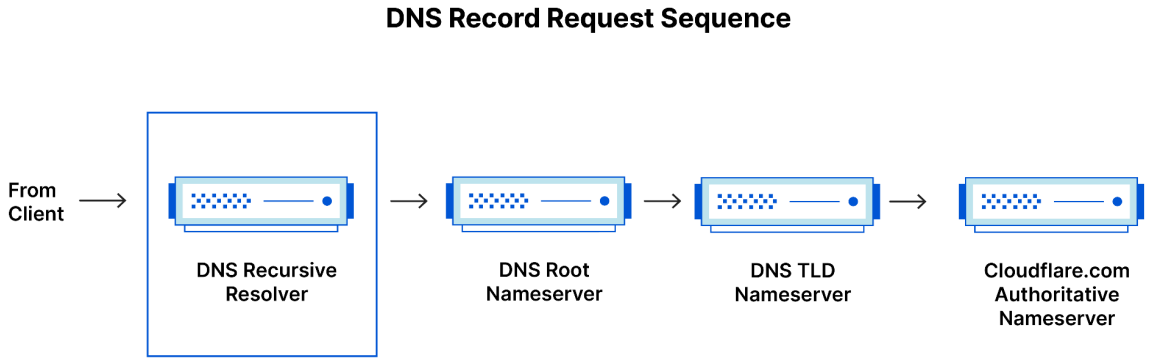
- **DNS recursor:** The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.
- **Root Nameserver:** The root server is the first step in translating human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
- **TLD Nameserver:** The top level domain server can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and if hosts the last portion of a hostname.
- **Authoritative Nameserver:** This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor that made the initial request.

What's the difference between an authoritative DNS server and a recursive DNS resolver?

Both concepts refer to servers that are integral to the DNS infrastructure, but each performs a different role and lives in different locations inside the pipeline of a DNS query. One way to think about the difference is that the recursive resolver is at the beginning of the DNS query and the authoritative nameserver is at the end.

Recursive DNS Resolver

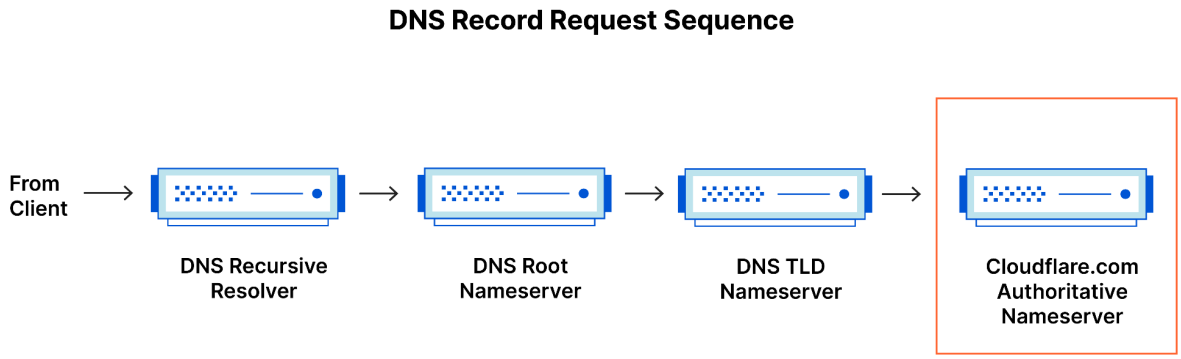
The recursive resolver is the computer that responds to a recursive request from a client and takes the time to track down the DNS record. It does this by making a series of requests until it reaches the authoritative DNS nameserver for the requested record. Luckily, recursive DNS resolvers don't always need to make multiple requests in order to track down the records needed to respond to a client; Caching is a data persistence process that helps short-circuit the necessary requests by serving the requested resource record earlier in the DNS lookup.



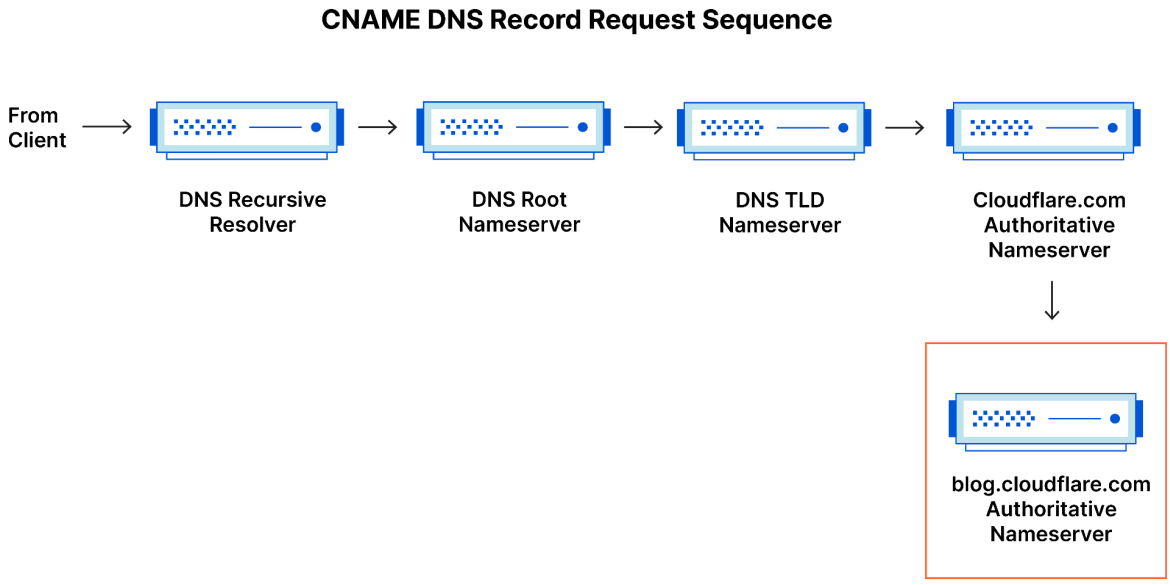
Authoritative DNS server

An authoritative DNS server is a server that actually holds, and is responsible for, DNS resource records. This is the server at the bottom of the DNS lookup chain that will respond with the queried resource record, ultimately allowing the web browser making the request to reach the

IP address needed to access a website or other web resources. An authoritative nameserver can satisfy queries from its own data without needing to query another resource, as it is the final source of truth for certain DNS records.



It's worth mentioning that in instances where the query is for a subdomain such as foo.example.com, an additional nameserver will be added to the sequence after the authoritative nameserver, which is responsible for storing the subdomain.



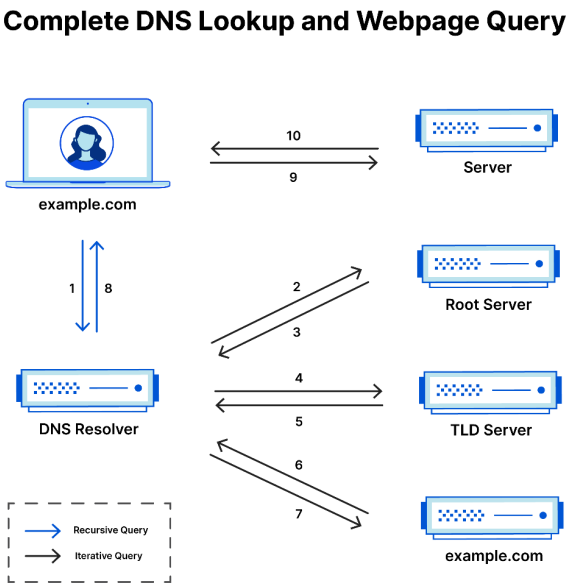
What are the steps in a DNS lookup?

For most situations, DNS is concerned with a domain name being translated into the appropriate IP address. To learn how this process works, it helps to follow the path of a DNS lookup as it travels from a web browser, through the DNS lookup process, and back again. Lets take a look at the 8 steps in a DNS lookup:

- A user types “example.com” into a web browser and the query travels into the Internet and is received by a DNS recursive resolver;
- The resolver then queries a DNS root nameserver;
- The root server then responds to the resolver with the address of a Top Level Domain DNS server which stores the information for its domains. When searching for example.com, our request it pointed toward the .com TLD;
- The resolver then makes a request to the .com TLD;
- The TLD server then responds with the IP address of the domain’s nameserver;
- Lastly, the recursive resolver sends a query to the domain’s nameserver;
- The IP address for example.com is the returned to the resolver from the nameserver;
- The NDS resolver then responds to the web browser with the IP address of the domain requested initially;

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

- The browser makes a HTTP request to the IP address;
- The server at that IP returns the webpage to be rendered in the browser;

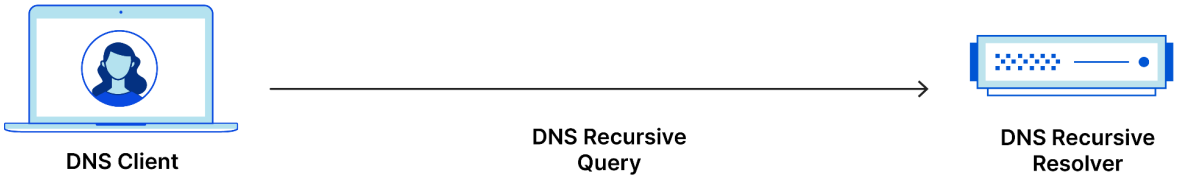


What is a DNS resolver?

The DNS resolver is the first stop in the DNS lookup, and it is responsible for dealing with the client that made the initial request. The resolver starts the sequence of queries that ultimately leads to a URL being translated into the necessary IP address;

Note: A typical uncached DNS lookup will involved both recursive and iterative queries;

It's important to differentiate between a recursive DNS query and a recursive DNS resolver. The query refers to the request made to a DNS resolver requiring the resolution of the query. A DNS recursive resolver is the computer that accepts a recursive query and processes the response by making the necessary requests.



What are the types of DNS queries?

There are three types of queries. By using a combination of these queries, an optimized process for DNS resolution can result in a reduction of distance traveled.

- **Recursive query:** A DNS client requires that a DNS server will respond to the client with either the requested resource record or an error message if the resolver can't find the record;
- **Iterative query:** DNS client will allow a DNS server to return the best answer it can. If the queried DNS server does not have a match for the query name, it will return a referral to a DNS server authoritative for a lower level of the domain namespace. The DNS client will then make a query to the referral address. This process continues with additional DNS servers down the query chain until either an error or timeout occurs;
- **Non-recursive query:** A DNS resolver client queries a DNS server for a record that it has access to either because it's authoritative for the record or the record exists inside of its cache. Typically, a DNS server will cache DNS records to prevent additional bandwidth consumption and load on upstream servers;

What is DNS caching? Where does DNS caching occur?

The purpose of caching is to temporarily store data in a location that results in improvements in performance and reliability for data requests. DNS caching involves storing data closer to the requesting client so that the DNS query can be resolved earlier and additional queries further down the DNS lookup chain can be avoided, thereby improving load times and reducing bandwidth/CPU consumption. DNS data can be cached in a variety of locations, each of which will store DNS records for a set amount of time determined by a time-to-live.

Modern web browsers are designed by default to cache DNS records for a set amount of time. The purpose here is obvious; The closer the DNS caching occurs to the web browser, the fewer processing steps must be taken in order to check the cache and make the correct requests to an IP address. When a request is made for a DNS record, the browser cache is the first location checked for the requested record.

The operating system level DNS resolver is the second and last local stop before a DNS query leaves your machine. The process inside your operating system that is designed to handle this query is commonly called a “stub resolver” or DNS client. When a stub resolver gets a request from an application, it first checks its own cache to see if it has the record. If it does not, it then sends a DNS query, outside the local network to a DNS recursive resolver inside the Internet service provider (ISP).

When the recursive resolver inside the ISP receives a DNS query, like all previous steps, it will also check to see if the requested host-to-IP-address translation is already stored inside its local persistence layer.

The recursive resolver also has additional functionality depending on the types of records it has in its cache:

- If the resolver does not have the *A records*, but does have a *NS records* for the authoritative nameservers, it will query those name servers directly, bypassing several steps in the DNS query. This shortcut prevents lookups from the root and .com nameservers and helps the resolution of the DNS query occur more quickly;
- If the resolver does not have the *NS records*, it will send a query to the TLD server, skipping the root server;
- In the unlikely event that the resolver does not have records pointing to the TLD servers, it will then query the root servers. This event typically occurs after a DNS cache has been purged

References

What is DNS? | How DNS works | Cloudflare