What is a DNS Server?

The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP address for those sites. Browsers then use those addresses to communicate with origin servers or CDN edge servers to access website information. This all happens thanks to DNS servers: machines dedicated to answering DNS queries.

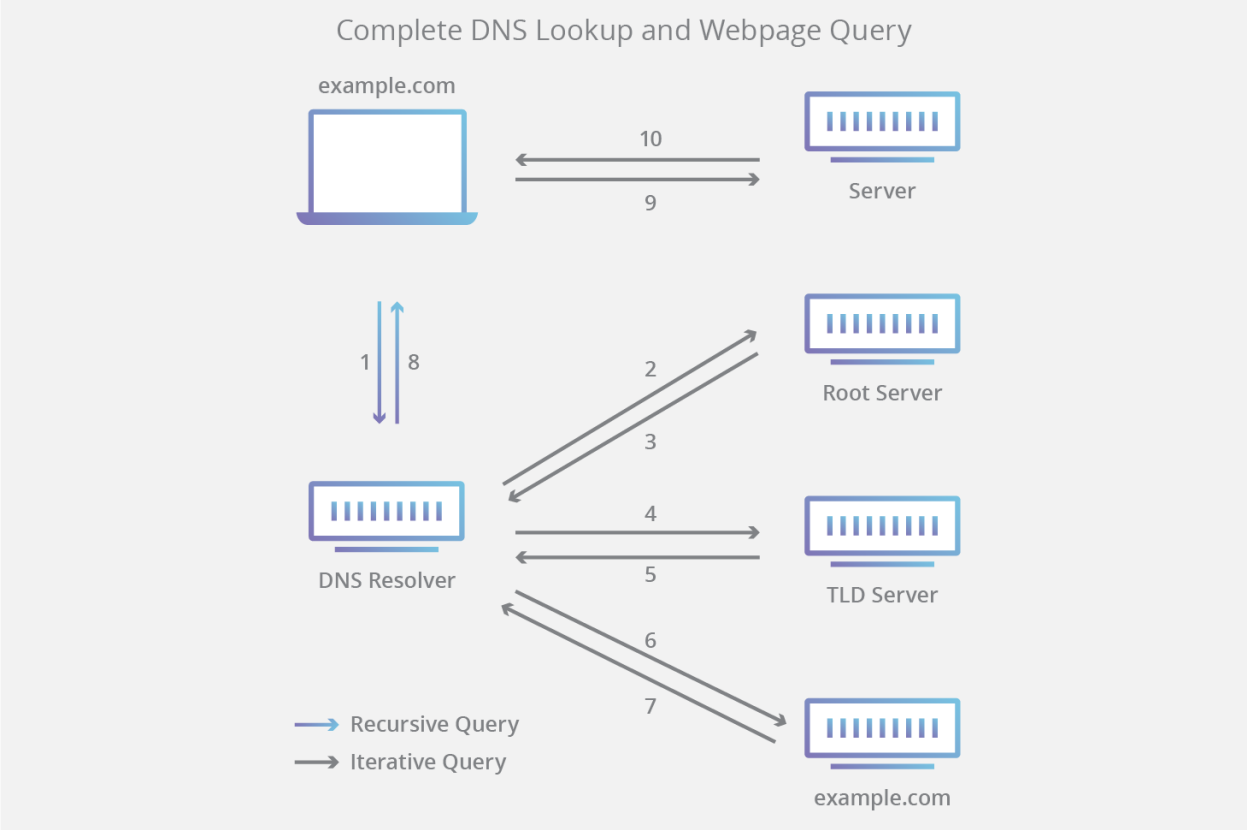
What is a server?

A server is a device or program dedicated to providing services to other programs, referred to as 'clients'. DNS clients, which are built into most modern desktop and mobile operating systems, enable web browsers to interact with DNS servers. For more, see The Client-Server Model.

How do DNS servers resolve a DNS query?

In a typical DNS query without any caching, there are four servers that work together to deliver an IP address to the client: recursive resolvers, root nameservers, TLD nameservers, and authoritative nameservers.

The DNS recursor (also referred to as the DNS resolver) is a server that receives the query from the DNS client, and then interacts with other DNS servers to hunt down the correct IP. Once the resolver receives the request from the client, the resolver then actually behaves as a client itself, querying the other three types of DNS servers in search of the right IP.



First the resolver queries the root nameserver. The root server is the first step in translating (resolving) human-readable domain names into IP addresses. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net) that stores the information for its domains.

Next the resolver queries the TLD server. The TLD server responds with the IP address of the domain's authoritative nameserver. The recursor then queries the authoritative nameserver, which will respond with the IP address of the origin server.

The resolver will finally pass the origin server IP address back to the client. Using this IP address, the client can then initiate a query directly to the origin server, and the origin server will respond by sending website data that can be interpreted and displayed by the web browser.

What is DNS Caching?

In addition to the process outlined above, recursive resolvers can also resolve DNS queries using cached data. After retrieving the correct IP address for a given website, the resolver will then store that information in its cache for a limited amount of time. During this time period, if any other clients send requests for that domain name, the resolver

can skip the typical DNS lookup process and simply respond to the client with the IP address saved in the cache.

Once the caching time limit expires, the resolver must retrieve the IP address again, creating a new entry in its cache. This time limit, referred to as the time-to-live (TTL) is set explicitly in the DNS records for each site. Typically the TTL is in the 24-48 hour range. A TTL is necessary because web servers occasionally change their IP addresses, so resolvers can't serve the same IP from the cache indefinitely.

What happens when DNS servers fail?

DNS servers can fail for multiple reasons, such as power outages, cyberattacks, and hardware malfunctions. In the early days of the Internet, DNS server outages could have a relatively large impact. Thankfully, today there is a lot of redundancy built into DNS. For example, there are many instances of the root DNS servers and TLD nameservers, and most ISPs have backup recursive resolvers for their users. (Individual users can also use public DNS resolvers, like Cloudflare's 1.1.1.1.) Most popular websites also have multiple instances of their authoritative nameservers.

In the case of a major DNS server outage, some users may experience delays due to the amount of requests being handled by backup servers, but it would take a DNS outage of very large proportions to make a significant portion of the Internet unavailable. (This actually happened in 2016 when DNS provider Dyn experienced one of the biggest DDoS attacks in history). Cloudflare offers a Managed DNS Service that comes with built-in DNS security aimed at protecting DNS servers from attacks as well as other common sources of server failure.