DNS

DNS translates and maps alphabetic domain names like websites' web addresses or names to the numeric IP addresses of computers or servers. And it is also capable of performing the reverse process. It uses User Datagram Protocol or UDP and its service uses port number 53 to operate.

Some Domain name examples like .com, .gov, .edu, .org are some of the Top-level Domains that are also called TLD names.

Example of a domain name is www.google.com which has its IP address 142.250.187.238. Machines over the internet uses IP address to communicate with one another however we as humans cannot remember all the IP address of our favourite websites. That's where DNS comes into the picture. It uses common human readable name like google.com and maps it to its complicated, hard to remember IP address 142.250.187.238.

In short, the main feature of the DNS is to map the google.com name to its corresponding IP address. Its like the NAT we discussed earlier, like NAT translate private IP address to public IP address and vice-versa, DNS does the same with the domain name like google.com to its IP address and vice-versa.

- To check the IP address of google.com

```
host google.com
```

- To check the name server interface is using

```
# Linux

systemd-resolve --status | grep "DNS Servers"

# Windows

ipconfig /all

netsh interface ipv4 show dnsservers
```

Types of name servers

There are three types of name servers. These are - Root servers, Primary servers and Secondary servers.

- Root Server -Root Server is the top level server which consists of the entire DNS tree. It does not contain the information about domains but delegates the authority to the other server. Think of these as the internet's supreme directory assistance. When you want to find a website like www.inventyourshit,com, your computer first asks one of the 13 root name servers "Where can I find information about .com domains?" The root server then points you toward the .com name servers.
- Primary Servers - Primary Server stores a file about its zone. It has authority to create, maintain, and update the zone file. These are the name servers that actually hold the address records for a particular domain, like a local directory listing. Your computer then asks the authoritative name server designated for inventyourshit.com "What is the IP address for www.inventyourshit.com The authoritative server responds with the IP address you need to access that website.
- Secondary Server - Secondary Server transfers complete information about a zone from another server which may be primary or secondary server. The secondary server does not have authority to create or update a zone file.

How DNS Works ?

Let's understand how DNS works step by step. We will consider the picture below for this.

- Before passing any request on the wild internet. The requested website is first checked in the local DNS cache stored on the machine. If any entry for the target website is not found, the DNS request flow moved to the next step.
- When we type www.example.com into the browser, it asks the local DNS Server for its IP address. Here the local DNS is at ISP end.
- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that **I do not know the IP address of www.example.com but know the IP address of DNS Server.**
- The local DNS server then asks the .com DNS Server the same question.
- The .com DNS Server replies the same that it does not know the IP address of www.example.com but knows the DNS IP address of example.com.
- Then the local DNS asks the example.com DNS server the same question.
- Then example.com DNS server replies with IP address of www.example.com.
- Now, the local DNS sends the IP address of www.example.com to the computer that sends the request.