What is DNS?

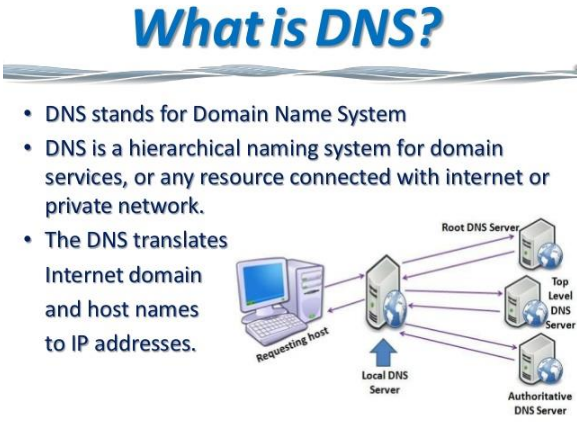
Computers are and were only able to communicate using numbers. Paul Mockapetris came up with a system that automatically mapped IP addresses to the domain name, and then DNS was born.

How Does DNS Domain Work?

Nameservers - store DNS records which are the actual file that says “this domain" maps to "this IP address." They are distributed all around the world. These nameservers are called the root nameservers. TLD (top-level domains) - are the two or three characters like .com that end a domain name.

Each TLD has its own set of nameservers that store the authoritative information for keeping the DNS records for that domain.

Your browser will ask your local resolving name server if they have the DNS records for the domain cached. The resolving name server is typically your ISP (Internet Service Provider). If it's a popular website like youtube.com, they will likely have the record in their cache.



What is DNS?

- DNS stands for Domain Name System
- DNS is a hierarchical naming system for domain services, or any resource connected with internet or private network.
- The DNS translates Internet domain and host names to IP addresses.

What Are DNS Records?

The primary purpose of a DNS server is to create DNS records. It provides essential information about the hostname and the domain, and especially the IP address. In simple words, a DNS system can’t work without its records. There are many types of DNS records.

Address Mapping record, also known as A Record, is among the most common type of DNS. It is also known as the host record. Its primary purpose is to store a hostname. Furthermore, it is also a corresponding IPv4 address.

IP Version 6 Address record is commonly known as the AAAA Record. It is pretty helpful for storing hostname along with IPv6 address.

Canonical Name record is the CNAME Record. It is a commonly used DNS entry. It is also used to identify a hostname or a domain name and point it to another hostname. When you request a record that is CNAME, the resolution process takes place under a new hostname.

MX Record or Mail exchanger record is a type of DNS record that helps to move the emails as per the preference of the domain owner. It works on the outgoing emails and routes them to the specific email server.

NS Record or Name Server records is a type of record used to specify a DNS zone. For instance, "abc.com is a domain name that is authorized to a specific AND or Authoritative Name Server. Thus, the NS record provides the complete address for that particular name server.

PTR Record or Reverse-lookup Pointer records are records that allow the resolution center of DNS to receive the hostname or give the IP address to the relevant person. It is also known as the DNS lookup as it is associated with the DNS resolution center.

CERT or certificate record might not be too familiar, but it is pretty helpful. Its primary purpose is to store certificates like PGP, SPKI, PKIX, etc. these certificates are encrypted and provide several uses to the websites.

SRV Record or Service Location is a type that resembles the Mail exchanger record a lot. Where the MX record is helpful for emails, the SRV is ideal for the service location of other protocols of communication. It is not as popular or as widely used as the MX record but has its uses.

SOA Record or Start of Authority is quite a crucial type. Because it appears at the start of the zone file, you get information about the specific AND for the required DNS zone. Furthermore, it also provides details of contacts regarding the administration of a particular domain. Also, it offers information about the serial number of a specific domain and concerning information about the flow of DNS information in any specific zone.

DNS Zone

Every domain name, a part of the DNS system, has several DNS settings, also known as DNS records. For these DNS records to be kept in order, the DNS zone was created.

A DNS zone refers to a particular portion or administrative space within the global Domain Name System (DNS). Each DNS zone represents a boundary of authority subject to management by certain entities. The total of all DNS zones, organized in a hierarchical tree-like order of cascading lower-level domains, form the DNS namespace.

The authority over each DNS zone is delegated to a legal entity or organization (i.e., a country-code top-level domain registry) or a company/individual registered to use a certain sub-domain within the system.

DNS Zone File

The DNS Zone file represents the actual file, which contains all the records for a specific domain. In a DNS Zone file, each line can hold only one record, and each DNS Zone file must start with the TTL (Time to Live), which specifies for how long the records should be kept in the DNS Server's cache.

The other mandatory record for a DNS Zone file is the SOA (Start of Authority) record - it specifies the primary authoritative name server for the DNS Zone.

After these two records are specified, additional records, such as A or NS records, can be added. When adding a record for a hostname, the hostname must end with a period (.). Hostnames, which do not end with a period, are considered relative to the primary domain name for which the DNS Zone was created. For example, when specifying the "www" record, there is no need to place a period after it.

Comments in the DNS Zone file must be started with a semicolon (;) and the start of a multiple line comment is represented by brackets ("("), and comments must again start with a semicolon. When the multiple lines end, they must be closed again with a bracket (")"), placed on a single line.

```
EXAMPLE:
$ORIGIN example.com. ; designates the start of this zone
file in the name space
$TTL 1h ; The default expiration time of a resource
record without its own TTL value
example.com. IN SOA ns.example.com. root.example.com. (
2008120710 ; serial number of this zone file
1d ; slave refresh (1 day)
1d ; slave retry time in case of a problem (1 day)
4w ; slave expiration time (4 weeks)
1h ; minimum caching time in case of failed lookups (1
hour)
)
example.com. NS dns1.ntchosting.com. ; ns.example.com is
the nameserver for example.com
example.com. NS dns2.ntchosting.com. ; ns.somewhere.com
is a backup nameserver for example.com
example.com. MX 10 mx1.ntchosting.com
example.com. MX 10 mx2.ntchosting.com ; mail.example.com
is the mailserver for example.com
example.com. A 209.25.134.47 ; ip address for
"example.com"
www A 209.25.134.47
```

DNS in the Security Industry

DNS is invaluable to the Internet community, however, it is not without vulnerability. When it was created, the internet was a much smaller and safer place, so there was little security in mind. b. As the internet has grown, malicious actors have found weaknesses in the DNS system. A DNS attack could result in denial of service and other threats.

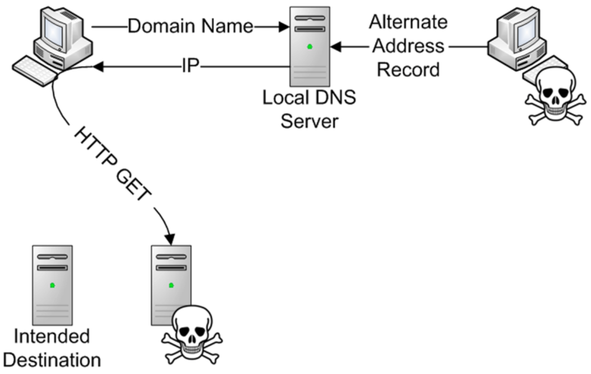
DNS protection is the straightforward way to prevent your daily net usage from any potential risk or vulnerability which can cause your organization great harm.

Website owners can protect their servers from DNS attacks to protect both their websites and users. This is the only way by which you can protect your system from ransomware, malware, hijack attacks from malicious websites and users.

DNS Attacks

DNS Cache Poisoning can corrupt the working of the DNS system. The cybercriminals try to insert their malicious content in your browser's cache and set the IP addresses to their malicious websites, which cause you to visit the unauthorized website when you enter the domain name of your favorite website.

DNS Cache Poisoning



The resemblance is so striking that you will not be able to spot any difference. Not only this, but it can also have control over your system and download & install ransomware, viruses, spyware on it.

Why Is DNS Important?

So, why exactly is DNS so important? DNS is important because of its critical role as the backbone of the internet. If a DNS is not responding, you won't connect to other websites on the internet.

This is because when a web browser is opened, and the desired website is to be visited, you do not have to go through the stress of remembering and entering a long number (IP address). You enter a domain name and end up exactly where you are supposed to.

If the DNS cannot translate the domain name to the correct IP address, you won't access any website. Without DNS, the majority of the internet as we know it breaks down.