**DNS-DOMAIN NAME SERVER**

What is DNS- domain name server (systems, service) are the internet phonebook. It maintains a directory of the domain names and translate them to human-readable names, eg. internet protocol or address. The domain names are easy to remember for people but not IP addresses.

**TCP-telephone Number**

**DNS-information**

**Information needs to have a database ,DNS has a Database which is all the records**

-DNS turns a host name(mail.yahoo.com) into an IP address

-DNS turns IP address into an Host name (reverse lookup)

DNS server 3types- DNS resolver, DNS root server and Authoritative name server

10 Type record- A,AAA,CNAME,MX and NS

DNS Resolver

A DNS resolver (recursive resolver), is designed to receive DNS queries, which include a human-readable hostname such as “www.example.com”, and is responsible for tracking the IP address for that hostname.

[www.yahoo.com--------](http://www.yahoo.com--------)> 8.8.8.8

DNS Root Server

The root server is the first step in the journey from hostname to IP address. The DNS Root Server extracts the Top-Level Domain (TLD) from the user’s query — for example, www.example.com —and provides details for the **.com** TLD Name Server. In turn, that server will provide details for domains with the .com DNS zone, including “example.com”.

There are [13 root servers worldwide](https://en.wikipedia.org/wiki/Root_name_server), indicated by the letters **A** through **M**, operated by organizations like the Internet Systems Consortium, Verisign, ICANN, the University of Maryland, and the U.S. Army Research Lab.

Authoritative DNS Server

Higher level servers in the DNS hierarchy define which DNS server is the “authoritative” name server for a specific hostname, meaning that it holds the up-to-date information for that hostname.

The Authoritative Name Server is the last stop in the name server query—it takes the hostname and returns the correct IP address to the DNS Resolver (or if it cannot find the domain, returns the message NXDOMAIN).

**Record:**

**Address Mapping record (A Record)—**

also known as a DNS host record, stores a hostname and its corresponding IPv4 address.

**IP Version 6 Address record (AAAA Record)—**

stores a hostname and its corresponding IPv6 address.

**Canonical Name record (CNAME Record)—alias record.**

can be used to alias a hostname to another hostname. When a DNS client requests a record that contains a CNAME, which points to another hostname, the DNS resolution process is repeated with the new hostname.

**Mail exchanger record (MX Record)—**specifies an SMTP email server for the domain, used to route outgoing emails to an email server.

**Name Server records (NS Record)—**

specifies that a DNS Zone, such as “example.com” is delegated to a specific Authoritative Name Server, and provides the address of the name server.

**Reverse-lookup Pointer records (PTR Record)—**

allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup).

**Certificate record (CERT Record)—**stores encryption certificates—PKIX, SPKI, PGP, and so on.

**Service Location (SRV Record) eg. global catalog—**a service location record, like MX but for other communication protocols.

**Text Record (TXT Record)—**typically carries machine-readable data such as opportunistic encryption, sender policy framework, DKIM, DMARC, etc.

**Start of Authority (SOA Record)—**this record appears at the beginning of a DNS zone file, and indicates the Authoritative Name Server for the current DNS zone, contact details for the domain administrator, domain serial number, and information on how frequently DNS information for this zone should be refreshed.

There are 4 zones where all the dns database records are stored.

1. Primary zones-

Database stored locally on server eg. HDD

-Advantage- DNS server can be loaded on any server type-standalone, server 2003, 2016,2012 r2

- Disadvantage-it causes additional network traffic eg. Server A and server B, both stored on local HDD and cant able to read each other if someone ask info to sever A which not stored in server A then Server A ask the info to server B that will cause additional network traffic.

-No fault Tolerance

-file can be hacked cause this stored in local HDD.

-NO security

1. Primary zones with active directory integrated (come with all solution from primary zone)

-stored all the database in active directory

-DNS server must be loaded on domain controller.

- no addition network traffic.

-full fault tolerance (need to have two DNS server).

-full security bcoz active directory

1. Secondary zones

* Database stored locally but not editable
* - DNS secondary zone must gety the database from primary
* -secondary gets entire copy of database.
* Used for load balancing

1. Stub zones

* - Database stored locally but not editable
* - DNS secondary zone must gety the database from primary
* Secondary gets only three resource record types
* Used for conditional forwarding
* Delegation record created on secondary zone.