papergrid
Date: / /

DNS

Domain name system

(1) DNS:
Domain name system, a system where Domain names are converted to IP

(2) lets take an example:
there is a person who speaks french and a other person who speaks English, In order for them to communicate and understand each other we need a translator

Similarly,
Computer understands IP address and human understands english.
In order to communicate between them DNS acts as a translator.

DNS maintains a table where names are mapped to Numbers.
i.e website domain name are mapped to their host IP address.

(2) DNS History

The idea of mapping human-readable hostnames to numerical addresses originated in 1970s, with ARPANET, the predecessor of internet

The Stanford Research institute (SRI) was responsible for maintaining a text file called host.txt that mapped hostnames to computer addresses on ARPANET

papergrid

Date: / /

To add an entity to host file, users would call SRI staff during business hours & they would add the host & its associated numeric address manually to the file

In 1980, it was understood that a centralized, manually updated host file was not a scalable approach.

John postel of the university of Southern California's team was responsible for the ARPANET assigned number list, assigned the task of creating an automated naming system to paul mockapetris.

Paul mockapetris created the solution, the Domain name system.

In 1984, four UC Berkeley students wrote the first DNS name server implementation for Unix & named it BIND.
BIND was ported to Windows NT

In 1987 DNS was formalized in RFC 1035

papergrid

Date: / /

(3) How DNS works :-

DNS Servers:-

Servers are computer storing HTML files, images, sounds, videos etc.

Server that work together to provide IP address of the requested website to the web browser are called DNS servers.

(4) There are 4 types of DNS servers.

1) DNS recursive resolver / DNS Resolver

2) Root name server

3) Top level domain / TLD name server

4) Authoritative name server.

→) DNS Resolver

(5)

A DNS Resolver, also known as a resolver, is a server on the internet that converts domain names into IP address.

When you use the internet, every time you connect to a website using its domain name (such as computerhope.com), your computer need to know that website's IP address so your computer contacts a DNS resolver & gets the current IP address of computerhope.com

papergrid
Date: / /

Usually the resolver is one part of a larger decentralized DNS. When you send your request to the DNS resolver, the resolver access other servers in the DNS to obtain the address, then sends you the response.

The DNS resolver contacted by your computer is usually chosen by your ISP. However you can configure your network to use a different DNS provider if you choose. This configuration can be modified in your operating system's network settings.

(6) → Root Name Server

There are 13 sets of Root name servers logically named as
letter.root-servers.net
where letter ranges from a to m
& operated by 12 different organization.

each set has a number of servers based around the world.
information page exists for all root server at address
letter.root-server.org
where letter ranges from a to m

Details of all root name servers can be found on website www.root-server.org

7) why overide dns

papergrid
Date: / /

(7) -> Top level Domain / TLD name Server.

TLD name Server Stores the information of all Domains sharing a common domain extension.
domains. .com .net .in .edu
for example.
.Com TLD name Server Store all information about .Com extensions.
.net TLD name server Stores all information about .net websites.

Top level Domain.
TLD is actually divided into two distinct sub-categories: they are organizational hierarchy & geographical hierarchy.

-> organization hierarchy: The example of these Top level Domains are given below

Domain purpose.
.com Commercial organization
.edu educational organization
.gov government institutions.
.mil military groups.
.net major network support centers
.org non profit organization & others.
.int international organizations.

-> Geographical Hierarchy: These are TLD that are localized to some certain geographical areas of operation and they are closely connected to the

papergrid
Date: / /

Main TLDs
. in → india.
. uk
. us

8 → Authoritative name servers.

An authoritative name server provides actual answer to your DNS queries.
it provides the original and definitive answers to DNS queries
It doesnot provides just cached answers that were obtained from another name server. therefore it only returns answer to queries about Domain name that are installed in its Configuration system.

There are two types of Authoritative Name servers:

1) Master Servers (primary name server)
A master server stores the original master copies of all zone records.
a host master only make changes to master server zone records.
Each slave server gets updates via special automatic updating mechanism of the DNS protocol.
All slave [redacted] server maintains an identical copy of the master records.

2) Slave server (secondary name server).
A slave server is exact replica of master servers. it is used to share DNS server load. and to improve DNS zone availability in case master servers fails.
it is recomended that you should at least have 2 slave servers and one master server for each domain name.

9 → Summary of the DNS process - a DNS example.

lets assume we type www.google.com in web browser
Since webbrowser needs IP address, it forwards the query to the computer os

computer OS is configured to forward query to DNS resolver.

DNS resolver checks the cache. whether it has a IP address of requested website or not?
DNS query is forwarded to Root name server,
Root name servers checks the extension of website whether it is .com/.net/.org etc
based on extension the root name server provides the IP address of TLD name server to DNS Resolver

papergrid
Date: / /

DNS resolver now contacts TLD name server, which then provides the IP address of authoritative name server

finally authoritative name server provides exact IP address

DNS Resolver stores this IP address in cache for future purpose.

now operating systems forwards it to web browser.

Web browser then contacts the google.com server & loads the Requested website

(10)

→ DNS Queries.

→ Recursive query :-
In a recursive query, a DNS client provides a hostname and the DNS Resolver must provide an answer it responds to the client with either the requested resource record or an error message if it can't find an ~~answer~~ record

The recursive query is between a DNS Client and its local DNS server

papergrid

Date: / /

DNS response Codes.

Code 0: No error
Code 1: Format error - query cannot be interpreted.
Code 2: Server failure - process impossible
Code 3: Name error - domain name does not exist
Code 4: DNS query type not implemented on the DNS server
Code 5: Refused - name server refuses due to policy

→ Iterative Query:
In iterative query, a DNS Client provides a hostname & the DNS resolver returns the best answer it can if the DNS resolver has the relavant DNS record in its cache, it returns them if not it refers the DNS client to Root server. The iterative query is between local DNS servers and other DNS servers

→ Non recursive Query:

A non recursive is a query in which DNS resolver already knows the answer. it immediately returns a DNS record because it already stores it in local cache.

(11) :

DNS caching and Time to Live

To improve efficiency, reduce DNS traffic across internet, and improve performance, DNS cache servers are used. These servers store DNS query results in a cache and can serve it immediately in response to a query without requiring recursive DNS queries.

The DNS records are stored in a cache for a period of time called time to live, defined in configuration of each DNS record.

Time to live is very significant because it determines the freshness of DNS record.

DNS records can be cached at several layers.

→ Browser DNS caching: Modern web browsers are designed to cache DNS records. This enables providing an IP address immediately in response to a user request without needing to contact external servers.

→ operating System DNS caching: All operating system comes with DNS resolver called stub resolver.

when max TTL is used

which are record place where a DNS query can be resolved before it leaves the local device.

→ Recursive Resolver DNS caching :- A DNS resolver operated by a third party receives DNS queries and checks its local cache to see if it already has the IP for requested host.

(iv) → DNS Resource Record :- are used to store hostname, IP address & others info in DNS server

| name | ttl | record class | record type | record data |

name → is an alphanumeric identifier of the DNS record

TTL → time to live specifies how long the record should be kept in local cache

Record class :- indicates the namespace → typically IN, the internet namespace

Record type :- is the DNS record type - for ex A, CName, MX, PTR

Record data → Containing the DNS values, for example the IP address for a hostname

papergrid
Date: / /

Common DNS Record types

1) Address Mapping record (A) - record that hold a hostname and its corresponding IPV4 address

2) IP version 6 Address record (AAAA) :- record that holds a hostname and its corresponding IPV6 address

3) Canonical name (CNAME) :- used to create aliases of domain names, can be used to alias a domain to another domain

4) Mail exchange record (MX) :- specifies a mail exchange server for domain name, used in SMTP protocol to route emails to correct email server

5) Name server record (NS) :- delegates a DNS zone to use a specific authoritative name server

6) Reverse-lookup pointer record (PTR) :- used to look up domain names based on an IP address.

7) Certificate Record (CERT) :- stores encryption certificate such as PKIX, SPKI, PGP etc

papergrid
Date: / /

20 → DNS Hierarchy

DNS uses hierarchy to manage its distributed system. The DNS hierarchy, also called the domain name space, is an inverted tree structure.

The DNS tree has a single Domain at the top of the structure called the root domain. A period or dot (.) is the designation for root domain

~~Below the top level domains~~

Below the root domain are the top-level Domain that Divide the DNS hierarchy into segments.
Below the top level domains, the domain name space is further divided into subdomains representing individual organization

Domain and subdomain.

A domain is a label of the DNS tree. Each node on the DNS tree represent a domain. Domains under the top-level domains represent individual organization or entities.
These domains can be further divided into subdomains to ease administration of an organization's host computers.

(2)

For example.

Company A creates a domain called companya under .com top level domain.
Company A has seperate LAN for its location in
- chicago
- washington
- providence.

Therefore company A network administrator decides to create a seperate subdomain for each division.

Any domain in a subtree is considered part of all domains above it.
Therefore chicago.companya.com is part of the companya.com domain and both are part of .com domain.

Domain names that end in a period for root are called fully Qualified domain name (FQDNs)

Each computer that uses DNS is given a DNS hostname that represents the computer's position within DNS hierarchy
Therefore the hostname for host1 is
host1.washington.companya.com.

papergrid
Date: / /

Domain Delegation

Domain delegation gives an organization authority for a domain
Having Authority for a domain means that the organization network administrator is responsible for maintaining the DNS database of hostnames and address information for that domain.

A group of domain and subdomain for which an organization has authority is called zone.
All host information for a zone is maintained in single, Authoritative database.

For example, the Companya.Com domain is delegated to company A. creating the companya.Com. Zone. There are three subdomains within Companya.Com domain
Chicago.Companya.Com
Washington - Companya.Com
Providence.Companya.Com

The company A Administrator maintains all information for the zone in a single database and also has authority to create and delegate subdomains.

papergrid
Date: / /

→ Zone transfer

Zone transfer is the process of copying the content of the zone file on a primary DNS server to secondary DNS server, using zone transfer provides fault tolerance by synchronizing the zone file in a primary DNS server with the zone file in a secondary DNS server

The secondary DNS server can perform name resolution if the primary DNS server fails

transfer modes are used

→ Full transfer

Full transfer when you bring a new DNS server online & configure it to be a secondary server for an existing zone in your environment. it will perform a full transfer of all the zone information in order to replicate all the existing resource record for that zone.

Full zone transfer can be very time-consuming and resource-intensive, especially in situation where there isn't sufficient Bandwidth between primary and secondary DNS server

↗ mechanism under transfer

papergrid
Date: / /

Incremental transfer :

when using incremental zone transfer, the secondary server retrieves only resource record that have changed within a zone. so it remains synchronized with the primary DNS server.

when incremental transfer are used the database on the primary server and the secondary server are compared to see if any differences exists.
if the zones are identified as same, no zone transfer is performed, if there is any difference then the zone transfer is initiated

* Database are compared based on the serial number of the start of authority resource record

→ explanation (pic)
if there is any change in primary DNS server it sends an NOTIFY message
now slave asks for start of autority request as it has to compare 2 values (serial number, it has with new serial numbers)

If serial number is different, then zone transfer takes place

Zone transfer can also be initiated by master

papergrid

Date: / /

Is entire process safe?

lets say we want to make money transfer
lets open bankpage & assume we are getting
correct results
So browsers contacts authoritative name
Server for IP
lets assume there is a attacker & he
poisons the IP address and direct the
user to his machine and we are not
aware.

How to protect this?
DNS has something called DNS security
extension which does 2 things. it ~~can~~

Authenticate our response.
So our computer can check if the response
was sent by Authoritative name server
or attacker

Integrity
DNS security checking message integrity
i.e is message/Response was changed
in mean time.
So it can compare with algorithm which
value is correct & for some reason
values seems to be incorrect,
it simply discards it & not use
it any more.

(13) Record types

→ CNAME : CNAME can be used to alias one name to another. CNAME stands for canonical name.

A common example is when you have both example.com and www.example.com pointing to the same Application & hosted by same server. TO avoid two different records its common to create.

An A record for example.com pointing to server IP address

A CNAME record for www.example.com pointing to example.com

As a result, example.com points to the server IP address & www.example.com points to the same address via example.com, if IP address changes, you only need to update it one place, ie just edit record for example.com

(14) → MX Record

mail exchange record directs to a email server The MX record indicates how emails be routed in accordance with SMTP

Lik CNAME, an MX Record must allways point to another domain

ex of mx record.

example.com	record type	priority	value	TTL
@	MX	10	mailhost1.example.com	4500
@	MX	20	mailhost2.example.com	4500

The priority number before the domains for

papergrid
Date: / /

These mx records indicates preference.

The lower priority value is preferred. The server will always try mail host1 first because 10 is lower than 20, in the request a message reply (failure) the server will default to mailhost2.

(15) → A record

The address record (A record) yields an IPv4 address that corresponds to a host name. There can be multiple IP addresses pointing to a single hostname & there can also be multiple hostnames each maps to same IP address.

(within one step)

There must be a valid A record in the DNS for the host name.

→ AAAA Records operate in the exact same way as A record, except they point to an IPv6 address.

(16) → PTR Record

The Domain name system or DNS correlates domain names with IP address.

A DNS PTR record provides domain name associated with IP address.

PTR record is exactly the opposite of A record.

DNS PTR records are used in reverse DNS lookup.

papergrid
Date: / /

in DNS lookup, query that starts with the IP address & looks up the domain name.

DNS PTR records are stored under the IP address - reversed and with .in-addr.arpa added
in-addr.arpa has to be added because PTR record are stored within the .arpa top-level domain in DNS

use
Anti-Spam → some email anti spam filter use reverse DNS to check Domain names of email address & see if associated IP address are likely to be used by legitimate email servers

Troubleshooting email delivery issues : email delivery problems can result from a misconfigured or missing PTR record, if a domain has no PTR record email services may block all emails from that domain.

Logging
System logs typically record only IP address, a reverse DNS lookup can convert these into domain names for logs that are more human readable.

SOA Record : The DNS start of authority record stores important information about a domain or zone such as email address, when the domain was last updated, & how long the server need to wait before refreshes. SOA Record are also important for zone transfers

→ notify mechanism

papergrid
Date: / /

RNAME: RNAME value represents the administrator's email address, which can be confusing because it's missing @ sign, in SOA record admin @example.com.

MNAME: This is name of primary name server for the zone. Secondary server receive update to the zone from primary server.

REFRESH: length of time (in seconds) secondary server should wait before asking primary server for the SOA Record to see if it has been updated.

RETRY: The length of time a server should wait for asking an unresponsive primary name server for an update again.

EXPIRED: If a secondary server does not get a response from the primary server for this amount of time, it should stop responding to queries for the zone.

Zone serial number: A zone serial number is a version number for the SOA record. When the serial number changes in a zone file this alerts secondary name server that they should update their copies of the zone file via zone transfer.

§ TTL → The interval at which the SOA record itself is refreshed