Domain Name System

Computer Networks

Computer Science Basics

Siarhei Kantarovich

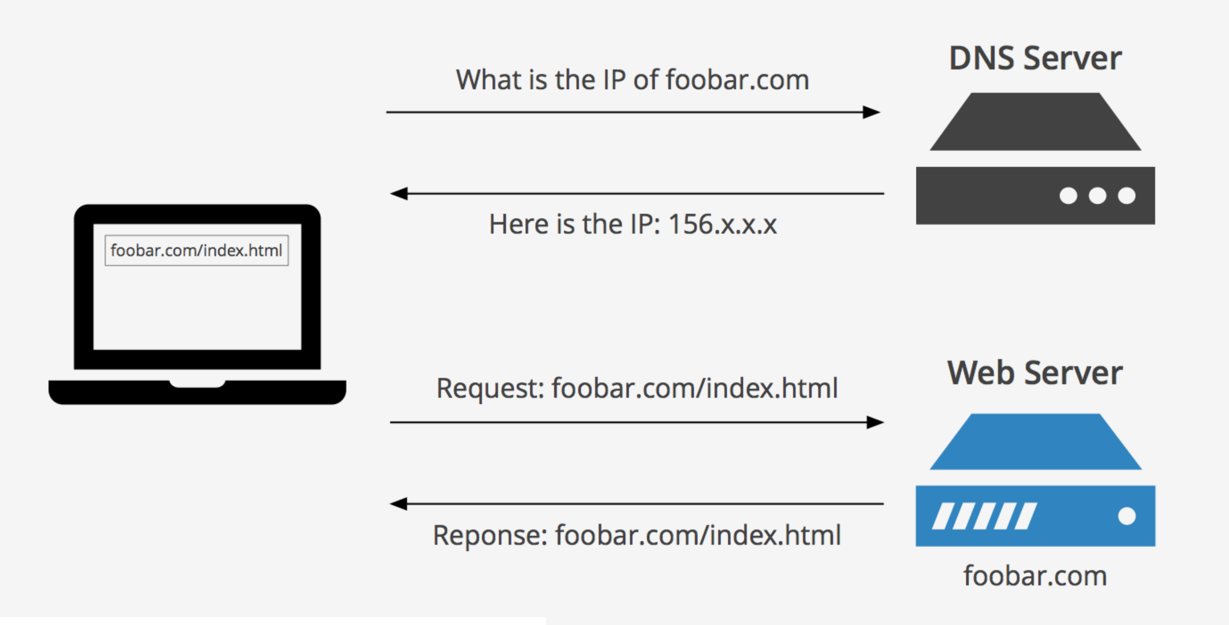
TRAINING CENTER

Computer networks - Domain name system

What is DNS?

A DNS, short for **domain name system**, is used to **resolve a particular domain name to its IP equivalent**.

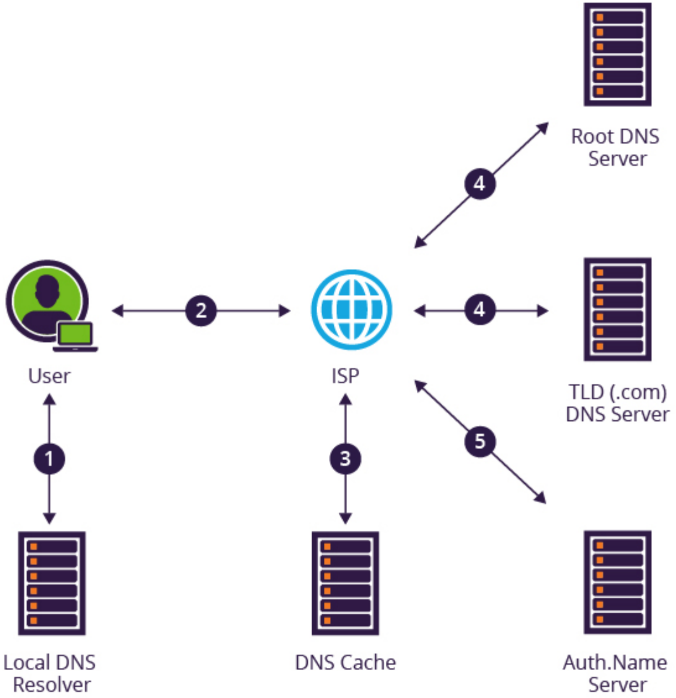
Domain names (e.g. epam.com) are simply used to be more easily read and remembered by humans, however, all domain names are associated with a particular IP address.
This can be compared to a phonebook where a person's name would correspond to the domain name (e.g. yourwebsite.com) and their phone number would correspond to the website's IP (e.g. 159.x.x.x).


DNS Server
What is the IP of foobar.com
Here is the IP: 156.x.x.x
foobar.com/index.html
Web Server
Request: foobar.com/index.html
Reponse: foobar.com/index.html
foobar.com

Computer networks - Domain name system

DNS resolving steps

- Website request
- Ask resolver
- Ask root server
- Ask TLD server
- Ask authoritative name servers
- Cache the IP and return it to the browser



Computer networks - Domain name system

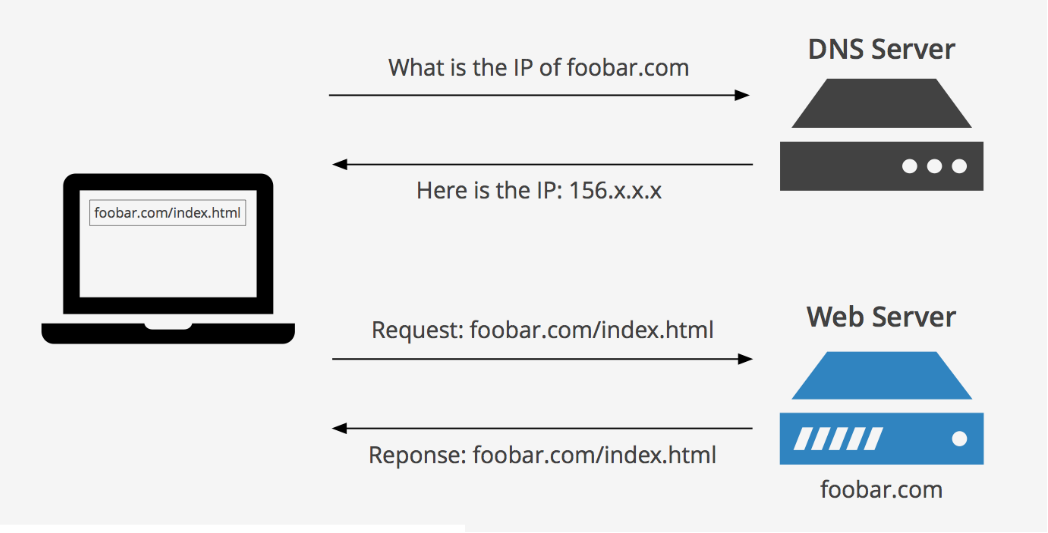
DNS resolving – step 1

Website request

The first step is, of course, to request the actual website via a web browser.

When someone types in a particular website's address (e.g. epam.com) into their address bar, the DNS lookup process begins.

Both the OS and browser **first look at their own DNS caches** to see if the information is already stored locally. If not, the resolver must be asked.


DNS Server
What is the IP of foobar.com
Here is the IP: 156.x.x.x
foobar.com/index.html
Web Server
Request: foobar.com/index.html
Reponse: foobar.com/index.html
foobar.com

Computer networks - Domain name system

DNS resolving – step 2

Ask resolver

Once the locally cached DNS records have been checked, the OS asks the resolver.

The resolver is usually your ISP (internet service provider).

It first checks its own cache to verify if the information is not already stored locally.

If it's not, it goes on to ask the root server.

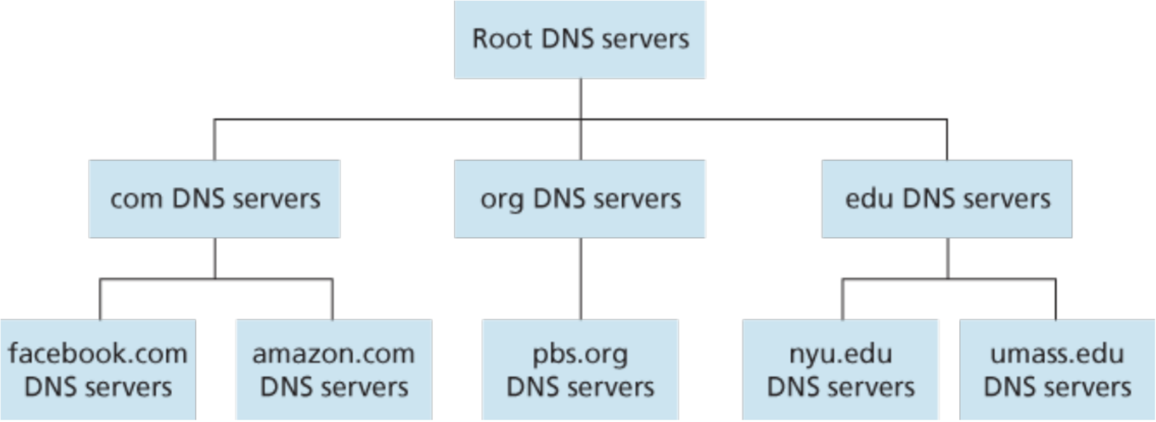


Figure 2.17 Portion of the hierarchy of DNS servers

Computer networks - Domain name system

DNS resolving – step 3

Ask root server

The next step is to ask the root server.

The root server looks at the last section of the request (the .com portion).

Although the root server cannot locate the IP address of the website, it tells the resolver where the top level domain (TLD) servers are for .com.

The resolver then stores this information for later use..

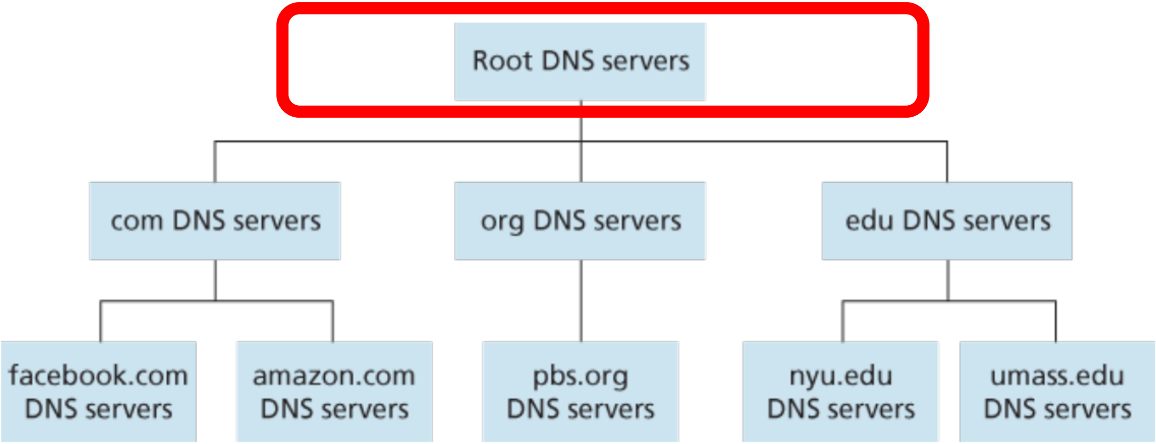
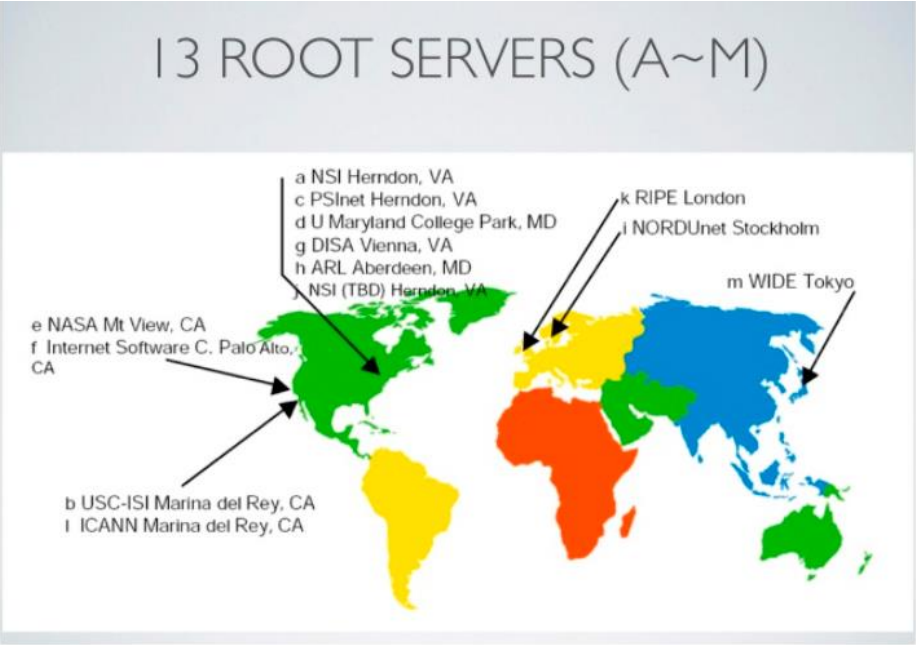
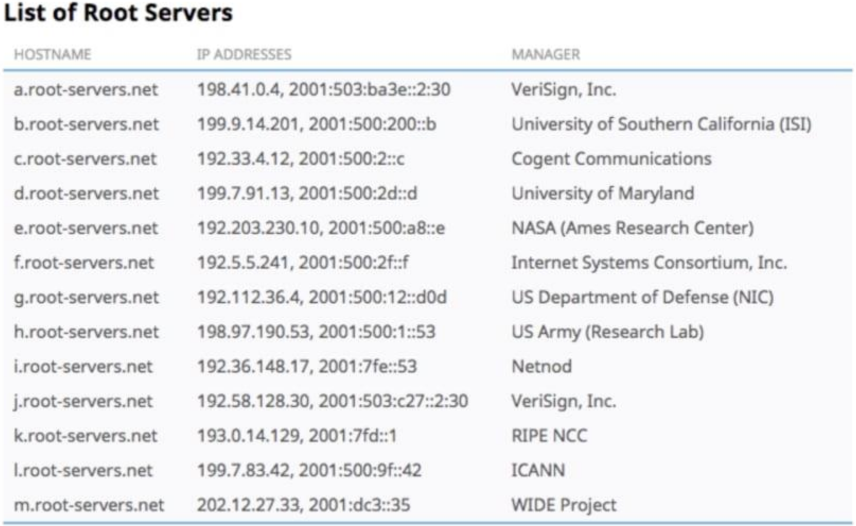


Figure 2.17 Portion of the hierarchy of DNS servers

Computer networks - Domain name system





List of Root Servers

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Credits: https://iana.org

Computer networks - Domain name system

DNS resolving – step 4

Ask TLD server

The resolver goes on to ask the TLD servers the IP address of the website in question.

Although the TLD servers can't provide us with the required information, they know where to direct our request.

The TLD servers provide the resolver with a list of name servers for that website.

Again, the resolver stores this information for later use.

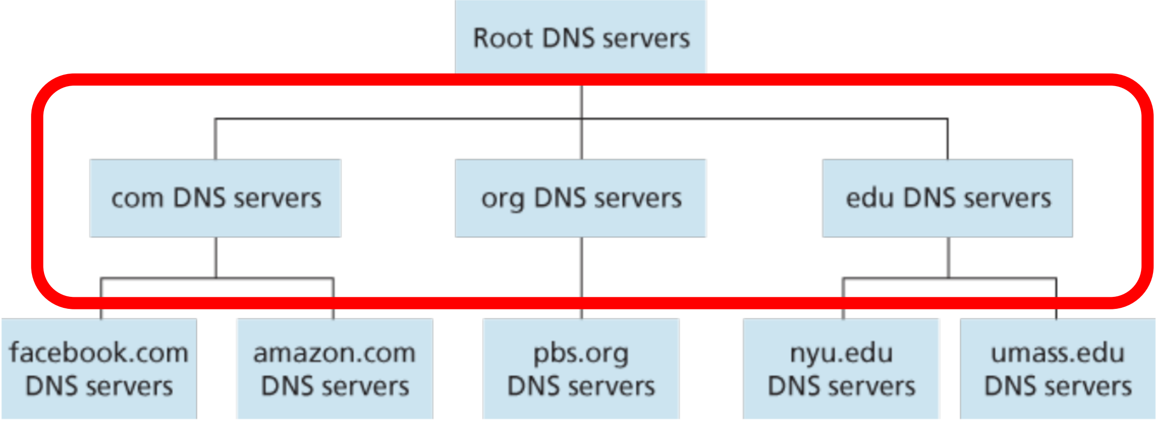


Figure 2.17 Portion of the hierarchy of DNS servers

Computer networks - Domain name system

DNS resolving – step 5

Ask authoritative name servers

Finally, now that the resolver knows what the authoritative name servers are, it can query these name servers and retrieve the required IP information.

The authoritative name servers contain all the necessary information regarding a particular domain.

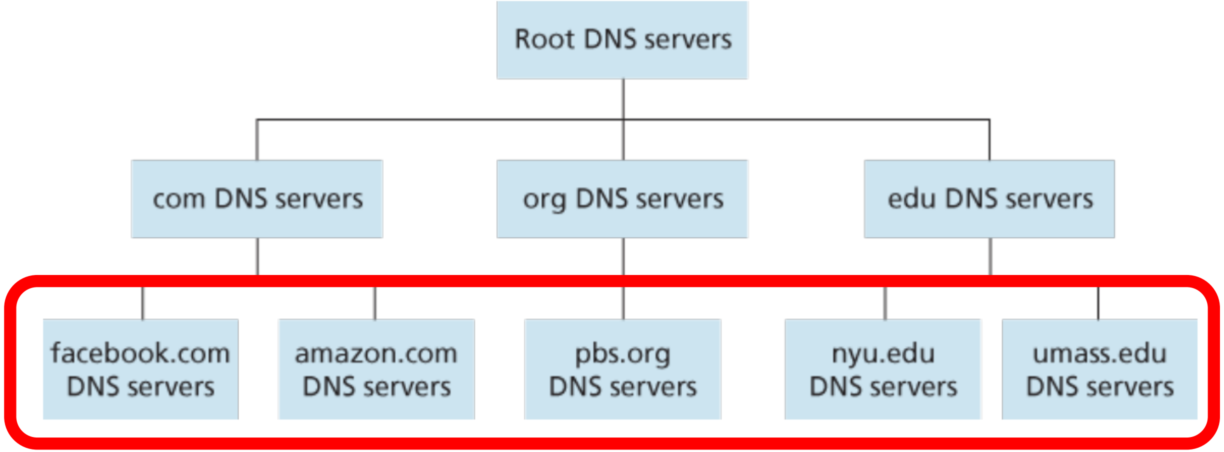


Figure 2.17 Portion of the hierarchy of DNS servers

Computer networks - Domain name system

DNS resolving – step 6

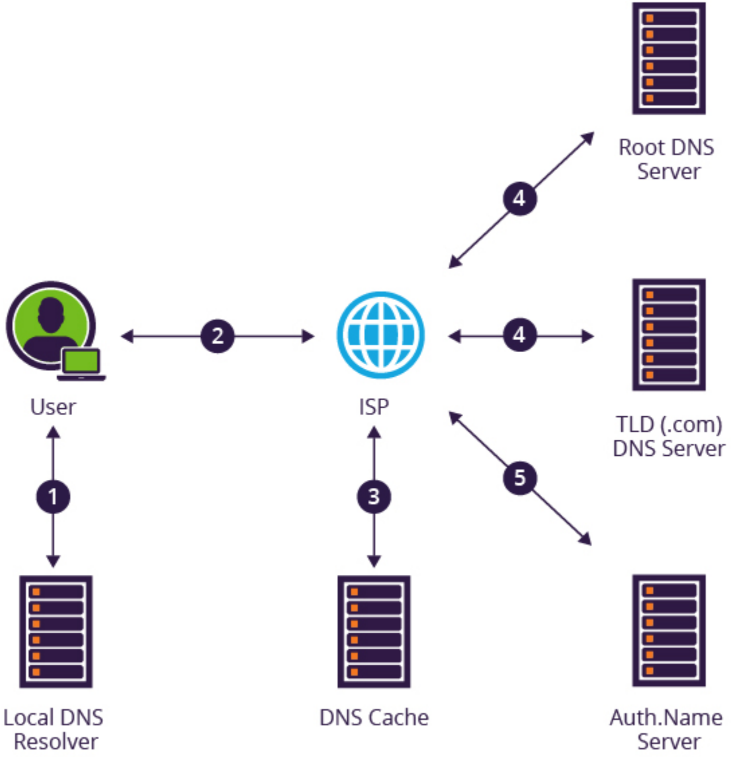
Cache the IP and return it to the browser

Now that the resolver knows the IP of said domain, it will cache it for later use.

At this point, the IP is delivered to your OS where it is locally cached as well.

The OS then passes this information on to the browser.

Once the browser knows the IP address of the website, it can then begin requesting and receiving information from the website's origin server.



Computer networks - Domain name system

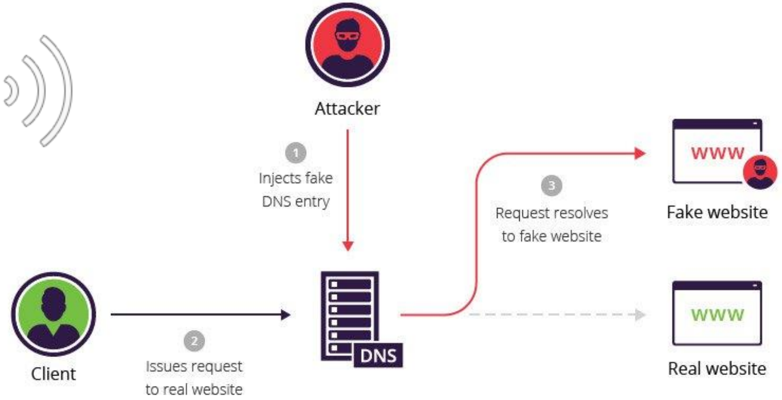
DNS security

The DNS Security Extensions (DNSSEC)

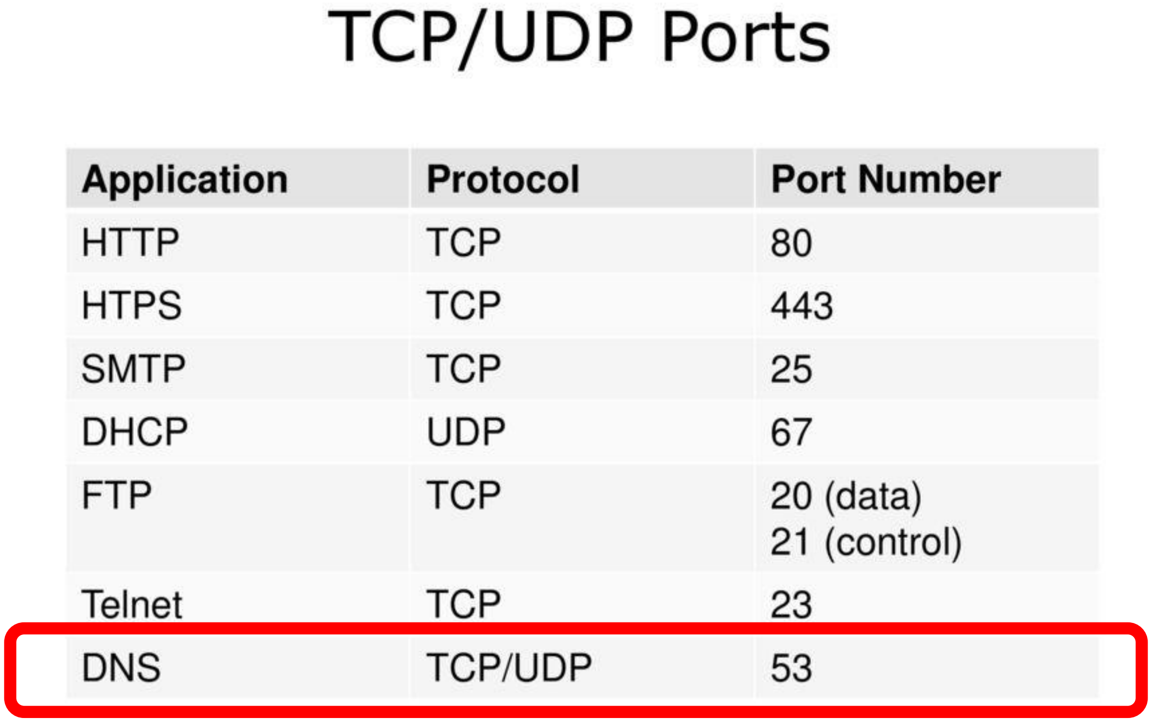
DNSSEC strengthens authentication in DNS using *digital signatures* based on *public key cryptography*. With DNSSEC, it's not DNS queries and responses themselves that are cryptographically signed, but rather DNS data itself is signed by the owner of the data.

Every DNS zone has a *public/private key pair*.

The zone owner uses the zone's *private key* to sign DNS data in the zone and generate digital signatures over that data. As the name "private key" implies, this key material is kept secret by the zone owner.
The zone's *public key*, however, is published in the zone itself for anyone to retrieve. Any recursive resolver that looks up data in the zone also retrieves the zone's public key, which it uses to *validate* the authenticity of the DNS data. The resolver confirms that the digital signature over the DNS data it retrieved is valid. If so, the DNS data is legitimate and is returned to the user. If the signature does not validate, the resolver assumes an attack, discards the data, and returns an error to the user.



Computer networks - Domain name system



TCP/UDP Ports

Application	Protocol	Port Number
HTTP	TCP	80
HTPS	TCP	443
SMTP	TCP	25
DHCP	UDP	67
FTP	TCP	20 (data) 21 (control)
Telnet	TCP	23
DNS	TCP/UDP	53

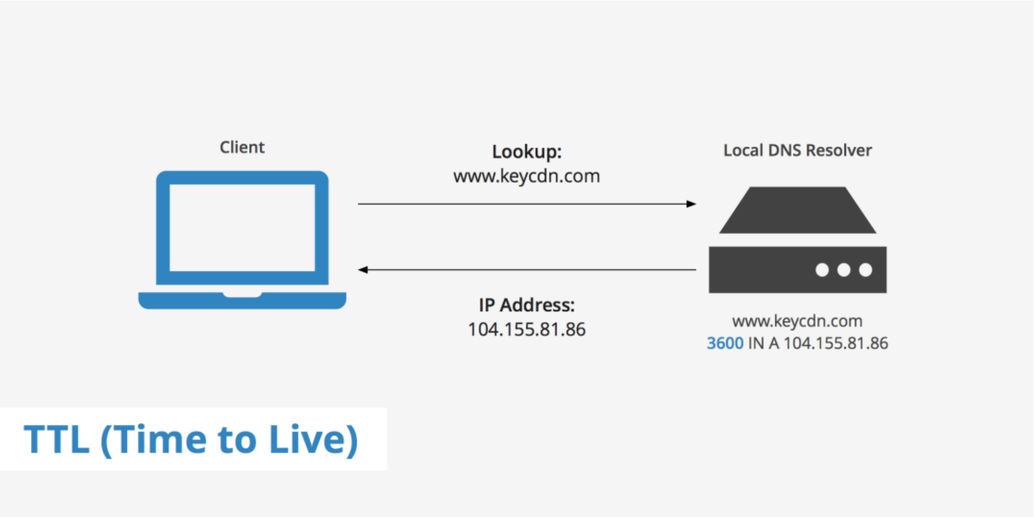
Computer networks - Domain name system

DNS resolving – TTL

What is TTL?

TTL, otherwise known as time to live, is a commonly used setting for defining how long a DNS record should remain in a DNS resolver's cache. Using TTL helps improve website speed since if the DNS lookup is already cached locally, it can be retrieved **much faster** than if a DNS server is required to complete the full lookup process.

Caching DNS records obviously is very beneficial in terms of improving speeds as well as the reducing the amount of load DNS resolvers around the globe experience. However, setting your TTL too high can cause issues. For instance, if a change to a DNS record must be made, you'll need to wait for the TTL to expire before the change will take effect. This is called the propagation period.



Computer networks - Domain name system

DNS resolving – request types

Recursive Query

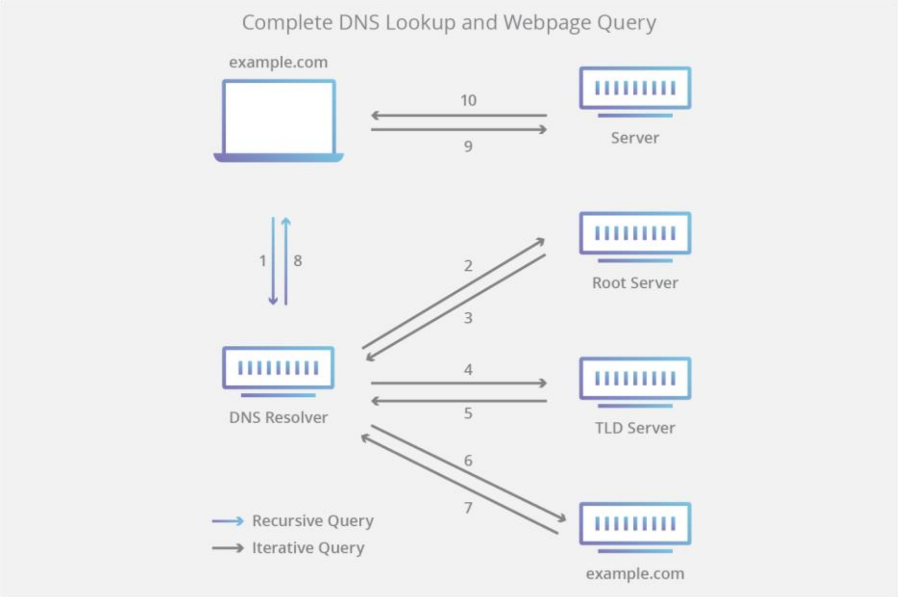
In Recursive name query, the DNS client requires that the DNS server respond to the client with either the requested resource record or an error message i.e. the record or domain name doesn’t exist.

If DNS server is not able to resolve the requested query then it forwards the query to another DNS server until it gets an answer or the query fails.

Iterative Query

An iterative name query is one in which a DNS client allows the DNS server to return the best answer it can give based on its cache or zone data. If the queried DNS server does not have an exact match for the queried name, the best possible information it can return is a referral (that is, a pointer to a DNS server authoritative for a lower level of the domain namespace).

The DNS client can then query the DNS server for which it obtained a referral. It continues this process until it locates a DNS server that is authoritative for the queried name, or until an error or time-out condition is met.



Computer networks - Domain name system

DNS records

Type	Description	Function
A	Address Record	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host
CNAME	Canonical Name Record	Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.
MX	Mail Exchange Record	Maps a domain name to a list of message transfer agents for that domain
AAAA	IPv6 Address Record	Returns a 128-bit IPv6 address
TXT	Text Record	Sender Policy Framework, DKIM, DMARC, DNS-SD, etc.
PTR	Pointer Record	Pointer to a canonical name. Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing reverse DNS lookups

Type	Description	Function
SRV	Service locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.
SPF	Sender Policy Framework	SPF(99) (from RFC 4408) was specified as part of the Sender Policy Framework protocol as an alternative to storing SPF data in TXT records, using the same format. It was later found that the majority of SPF deployments lack proper support for this record type, and support for it was discontinued in RFC 7208.
NS	Name Server record	Delegates a DNS zone to use the given authoritative name servers
SOA	Start of [a zone of] Authority Record	Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.