Basics of Networking 2: DNS

Daniel STAN

May 27, 2024

Original content by Eric Milard 🇫🇷 *Éléments de réseau 2* Contrib and Speakers: Daniel Stan, Nidà Meddouri, Elloh Adja, Suzana Dedefa, Christian Diaconu
Version: v1.0, feedback and remarks to: `daniel.stan@epita.fr`

Outline

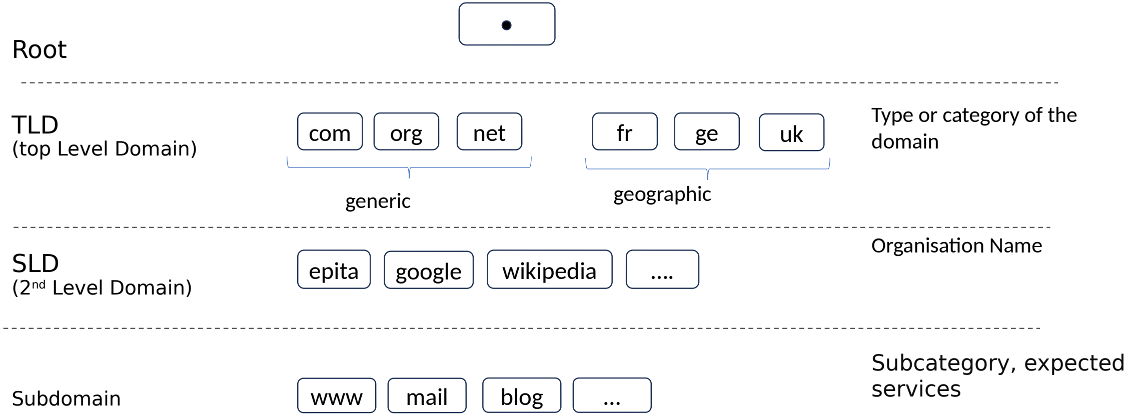
1. Domain Names at a glance
2. Iterative Queries on a system
3. Recursive Resolution

Motivation: When I connect to a server, what happens?

```
dstan@flan:~$ ping epita.fr
PING epita.fr(2606:4700:20::ac43:4796 (2606:4700:20::ac43:4796)) 56 data bytes
64 bytes from 2606:4700:20::ac43:4796 (2606:4700:20::ac43:4796): icmp_seq=1 ttl=51 time=12.5 ms
64 bytes from 2606:4700:20::ac43:4796 (2606:4700:20::ac43:4796): icmp_seq=2 ttl=51 time=11.4 ms
64 bytes from 2606:4700:20::ac43:4796 (2606:4700:20::ac43:4796): icmp_seq=3 ttl=51 time=11.2 ms
64 bytes from 2606:4700:20::ac43:4796 (2606:4700:20::ac43:4796): icmp_seq=4 ttl=51 time=10.7 ms
64 bytes from 2606:4700:20::ac43:4796 (2606:4700:20::ac43:4796): icmp_seq=5 ttl=51 time=10.3 ms
```

- Traduction mechanism from a **name** to an **IP address**
  - ...and from IP back to name (reverse)
  - and to store arbitrary data
  - This is called a **resolution**, or **lookup**.
- Why:
  - Easier to **remember** a name than an IP.
  - Flexibility: since an IP address may change, do not **hardcode** it. Ex: **DynDNS**.
  - Resilience: store more than one IP for a name. Ex: **Round Robin**, **IPv4/IPv6 dual stack**

The entry hierarchy



Root

•

TLD
(top Level Domain)

com org net

generic

fr ge uk

geographic

Type or category of the domain

SLD
(2nd Level Domain)

epita google wikipedia ....

Organisation Name

Subdomain

www mail blog ...

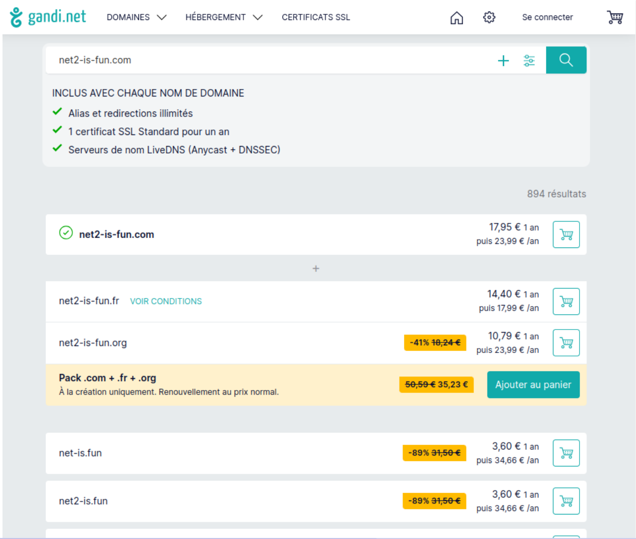
Subcategory, expected services

Fully Qualified Domain Name (FQDN)

A FQDN is **globally unique**.

- It contains at least a TLD and a SLD : *epita.fr*, *ionis-group.com*...
- It can contain **arbitrary** subdirectories: *cri.epita.fr*,*pie.cri.epita.fr*,*fleet.pie.crie.epita.fr*
- If a domain name is not a FQDN, it may be completed by the system using some default suffix.

In practice: How to buy a domain?



net2-is-fun.com

INCLUS AVEC CHAQUE NOM DE DOMAINE

- ✓ Alias et redirections illimités
- ✓ 1 certificat SSL Standard pour un an
- ✓ Serveurs de nom LiveDNS (Anycast + DNSSEC)

894 résultats

✓ **net2-is-fun.com** — 17,95 € 1 an, puis 23,99 € /an

net2-is-fun.fr VOIR CONDITIONS — 14,40 € 1 an, puis 17,99 € /an

net2-is-fun.org — -41% ~~18,24 €~~ — 10,79 € 1 an, puis 23,99 € /an

Pack .com + .fr + .org
À la création uniquement. Renouvellement au prix normal. — ~~50,59 €~~ 35,23 €

net-is.fun — -89% ~~31,50 €~~ — 3,60 € 1 an, puis 34,66 € /an

net2-is.fun — -89% ~~31,50 €~~ — 3,60 € 1 an, puis 34,66 € /an

Usually, one buys an **SLD**: *epita.fr*, *ionis-group.com*, *google.com* to an ICANN accredited *registrar* (🇫🇷 *registraire*).

← example of a Registrar interface.

Usually, if you own a domain name, you can register **any subdomain**.

Public database of domain name owners: **whois**.

Exercice: who owns *epita.fr*? *tudo.re*? *gouv.fr*?

Iterative Queries

A software for DNS queries

DNS Protocol: 53/udp (but 53/tcp too)
Plenty of clients: `host`, `nslookup`, `dig`

```
dstan@flan:~$ host epita.fr 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

epita.fr has address 104.26.7.225
...

dstan@flan:~$ nslookup epita.fr 8.8.8.8
...

dstan@flan:~$ dig epita.fr @8.8.8.8

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> epita.fr @8.8.8.8
...
;; ANSWER SECTION:
epita.fr.    300 IN  A 104.26.6.225
```

What server to use? Resolvconf file

Any system stores[1] at least one known and reliable DNS server: `/etc/resolv.conf`

```
dstan@flan:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND −− YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd−resolved stub resolver.
# run ”systemd−resolve −−status” to see details about the actual nameservers.

nameserver 192.168.101.254
nameserver 127.0.0.53
search lrde.epita.fr int.ionis−it.com
```

- ⚠ **8.8.8.8** is a popular public DNS server administrated by google, handy for testing purposes, do not use in production! ⚠
- Mostly the same scheme on Windows systems
- Default server when using `dig`, `host`, ...

[1] it has to be an IP address and not a domain name.

Exceptions: hosts file

Some exceptions can be stored in `/etc/hosts` file.

```
dstan@flan:~$ cat /etc/hosts
127.0.0.1 localhost
::1       ip6-localhost ip6-loopback
127.0.1.1 flan
```

Good practice: my local hostname (here: `"flan"`) harcoded as **127.0.0.1**.
This is not **DNS queries** anymore:

```
dstan@flan:~$ host flan
Host flan not found: 3(NXDOMAIN)
dstan@flan:~$ getent hosts flan
127.0.1.1         flan
dstan@flan:~$ getent hosts epita.fr
2606:4700:20::ac43:4796 epita.fr
2606:4700:20::681a:7e1 epita.fr
```

Programmatic functions: `gethostbyname()`, `getaddrinfo()`[2]

[2] https://linux.die.net/man/3/gethostbyname

dns-types

DNS Types

A DNS name can carry **multiple records**, of different **types**:

- A : IPv4 address
- AAAA : IPv6 address[3]
- NS : Name Server
- CNAME : Canonical Name (Alias)
- MX : Mail Exchanger, ie what mail server to use for this @domain
- . . .

The following example has 2 A records, one AAAA, and one MX:

```
dstan@flan:~$ host epita.fr
epita.fr has address 104.26.6.225
epita.fr has address 104.26.7.225
epita.fr has IPv6 address 2606:4700:20::ac43:4796
epita.fr mail is handled by 0 epita—fr.mail.protection.outlook.com
```

[3] IPv4=32b=A hence IPv6=$32 \times 4 = 128$b=AAAA

Example: Query by type

Try it for yourself:

```
host -t CNAME www.lre.epita.fr

dig -t CNAME www.lre.epita.fr

host -t TXT lre.epita.fr

dig -t TXT lre.epita.fr

dig -t MX outlook.com
```

Name Server type

```
dig -t NS ml.lre.epita.fr
# Nothing but:
dig -t NS lre.epita.fr
# lre.epita.fr name server ns.lre.epita.fr.
```

A Name Server (NS) server for *lre.epita.fr* is a DNS server **specifically** answering for the domain, but **nothing else**:

```
host intra.lre.epita.fr ns.lre.epita.fr
# intra.lre.epita.fr is an alias for rp.lre.epita.fr.
# rp.lre.epita.fr has address 91.243.117.236
# but:
host ionis-group.com ns.lre.epita.fr
# Host ionis-group.com not found: 5(REFUSED)
```

Authoritative vs “Know-All”

- “*Know-All*” servers:
  - No matter what you ask them, they will answer.
  - Use them in your `/etc/resolv.conf`.
  - They’re anonymous: their IP won’t appear in NS answer query.
  - We will call them: **Resolver** or **Recursive Servers**
- **Authoritative** for a domain:
  - Everyone **knows**[4] they are authoritative for **this** domain (public knowledge).
  - If you ask them anything for another domain, they’ll **deny** you.

How to implement a recursive server?

[4] the domain name has a record of type NS to this authoritative server

Recursive Resolution

dns-recursive

Recursive Resolution: An Example

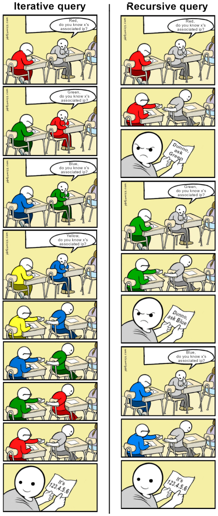
Let's resolve *fleet.pie.cri.epita.fr* by querying the DNS server **198.97.190.53**

```
dig —t A fleet.pie.cri.epita.fr @198.97.190.53

# No answer for what I'm looking for, but ...
#      .fr is managed by d.nic.fr
# We also have an additional section:
# (ADDITIONNAL SECTION) d.nic.fr IN A 194.0.9.1


dig —t A fleet.pie.cri.epita.fr @194.0.9.1

# Still no answer, but now:
#                  —> epita.fr has NS donna.ns.cloudflare.com:

dig —t A fleet.pie.cri.epita.fr @donna.ns.cloudflare.com

# Still no answer, but now:
#                  —> cri.epita.fr ah NS ns.cri.epita.fr

dig —t A fleet.pie.cri.epita.fr @ns.cri.epita.fr

# An answer
# fleet.pie.cri.epita.fr is:
#    a CNAME to ingress.prod—1.k8s.cri.epita.fr.
#    which has IP 91.243.117.180
```

NB: NS entries answers have to be translated to IP addresses themselves!

- Initial server **198.97.190.53** was nice to us (ADDITIONNAL SECTION) and gave us the IP of the NS: **glue record**.
- *d.nic.fr* was not so nice, we had to do a **second recursion** to resolve donna.ns.cloudflare.com to an IP (**173.245.58.151**).
- *donna.ns.cloudflare* was not so nice, we had to resolve again *ns.cri.epita.fr* to an IP (**91.243.117.210**).

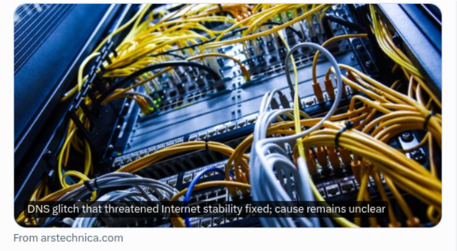
Recursive Resolution in a Nutshell


Iterative query
Red, do you know x's associated ip?
Green, do you know x's associated ip?
Blue, do you know x's associated ip?
Yellow, do you know x's associated ip?
It's 123.4.5.6
Recursive query
Red, do you know x's associated ip?
Dunno, ask Green
Green, do you know x's associated ip?
Dunno, ask Blue
Blue, do you know x's associated ip?
It's 123.4.5.6
pbfcomics.com

Where do we start ? Root servers

For example: **198.97.190.53**

- Root servers IP addresses are **hardcoded**, publicly known by everyone.
- Full list: `https://en.wikipedia.org/wiki/Root_name_server#Root_server_addresses`
- They are **Widespread**: Several continents, AS, Companies
- In reality, **multiple** servers behind one IP
- Crucial for the Internet stability.



DNS glitch that threatened Internet stability fixed; cause remains unclear

From arstechnica.com

`https://arstechnica.com/security/2024/05/dns-glitch-that-threatened-internet-stability-fixed-cause-remains-unclear/`

Exercise: Recursive Resolution

Start with *j.root-servers.net* and give the NS servers used in the resolution for the below FQDNs.
NB: more than one solution.

- *www.epita.fr*
- *mail.dgfip.finances.gouv.fr*
- *ftp.debian.org*
- ...

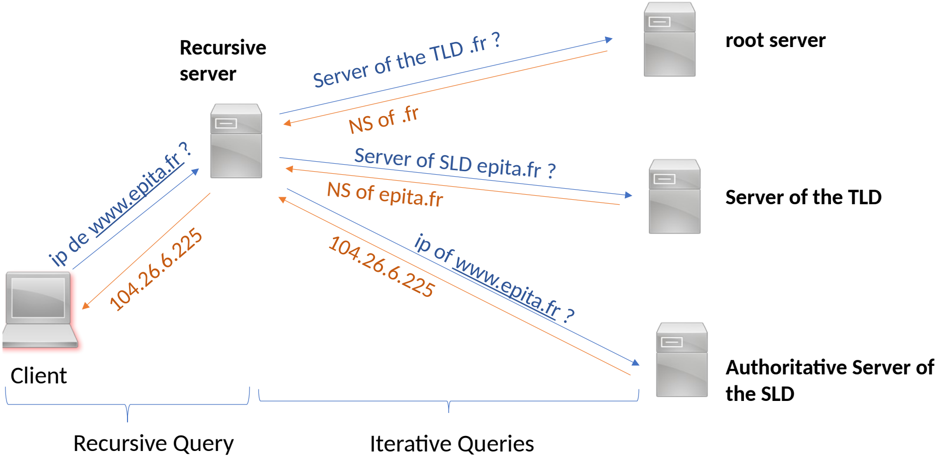
Resilience and Caching

Some domains may have more than one NS, some may crash. (ex: *dns2.finances.gouv.fr.* at time of writing this slide). It is the admin's job to **synchronize all** their servers so they provide the same answer: usually one **main** authoritatitve and several **secondary** authoritative servers copying main.

- Record of type SOA (Start of Authority for a zone): gives the delay before any refresh
- Every DNS answer comes with a **TTL** (time to live).
- Based on this TTL, recursive servers **cache** results.
- **Relieves** the NS servers, especially root servers.

⇝ editing DNS entries (to change IP) **needs to be planned** to avoid downtime.

The global picture



Remark: Recursive Server and Legal Implications

- DNS-blocking is the first technical measure to block a website in France, after a court order.
- ⇝ operating a resolver in France may have **legal consequences**, especially if you are an ISP.
- Some reference: `https://www.bortzmeyer.org/censure-francaise.html`
- Another (telegram accidental block in May 2023): `https://www.bortzmeyer.org/blocage-telegram-france.html`

```
# NB: 192.168.1.254 is my ISP modem
dstan@flan:~$ host www.palaceofchance.com 192.168.1.254

www.???ofchance.com is an alias for offre-illegale.anj.fr.
offre-illegale.anj.fr has address 145.239.225.117

dstan@flan:~$ host www.???ofchance.com 8.8.8.8

www.???ofchance.com has address 137.???.???.???
```

Summary

- The DNS is a giant global **database** storing key/values;
- Values can be of **many types** (A,AAAA,NS, ...)
- The keys are FQDNs, which are **hierachically delegated**: sub<SLD<TLD<"."
- Two kinds of DNS servers: **authoritative** and **recursive**
- Authoritative: answers for **one domain only**
- Exercise: perform **recursive resolution** by hand, from root to the final NS.
- Conclusion: **Distributed system**, **Vital** for the Internet.