DNS: Domain Name Service

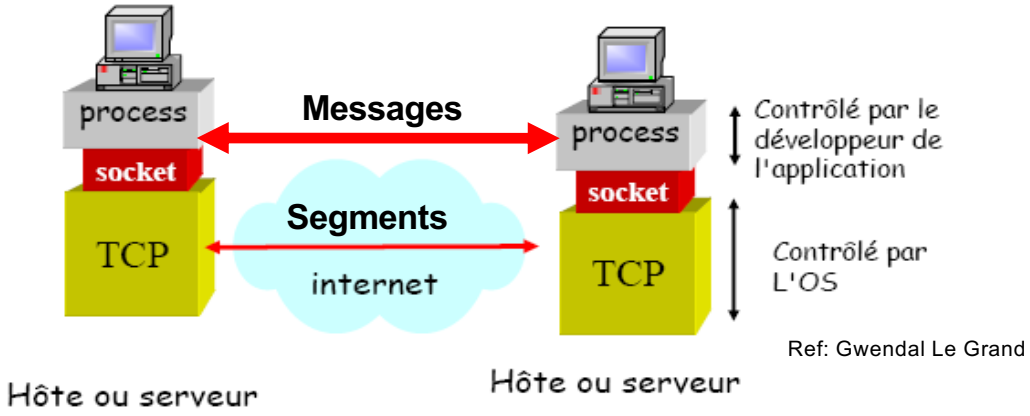
Jean-Louis Rougier
Département INFRES
Telecom Paris
rougier@telecom-paris.fr

APPLICATIONS

Préliminaires...

Applications et les Sockets

- Interface entre la couche application et la couche transport d'un hôte
- Permet la communication inter processus (IPC - Inter Process Communication) afin de permettre à divers processus de communiquer aussi bien sur une même machine qu'à travers un réseau TCP/IP
- Socket = Adresses IP + Numéros de Port (Source-Destination)
- Types: Datagram Socket (basé sur UDP) et Stream Socket (basé sur TCP)



Ref: Gwendal Le Grand

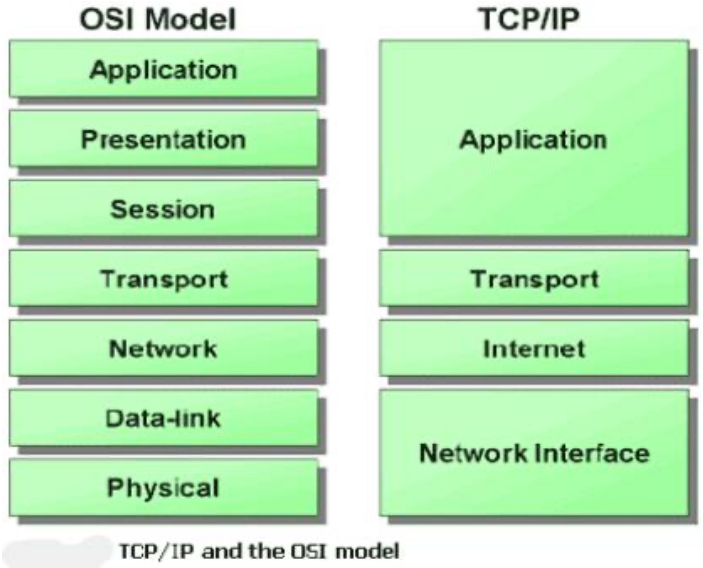
Applications – Ports et couche transport

Applications (Protocoles)	Numéros de Port	Protocole de Transport
DNS (Domain Name System)	53	TCP – UDP (UDP préférable)
HTTP (Hypertext Transfer Protocol)	80	TCP
HTTPS (Secure HTTP)	443	TCP
FTP (File Transfer Protocol)	21 (Control Connection) 20 (Data Connection)	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
POP3 (Post Office Protocol v3)	110	TCP
IMAP4 (Internet Message Access Protocol)	143	TCP - UDP

Modèle TCP/IP

Applications:

« Tout ce qui est au dessus de TCP/UDP »



TCP/IP and the OSI model

DNS

Introduction: Architecture

Définition du DNS

- **Le DNS (Domain Name System) est :**
  - Une base de données distribuée implémentée dans une hiérarchie de serveurs de noms
  - Un protocole applicatif
    Utilisé par d'autres protocoles applicatifs (usage général indépendant des types d'applications)
  - Un espace de nommage mondial, cohérent, indépendant des protocoles et des systèmes de communication
- **Le DNS permet (entre autre) d'associer une adresse IP à un nom de domaine et vice-versa.**

Historique

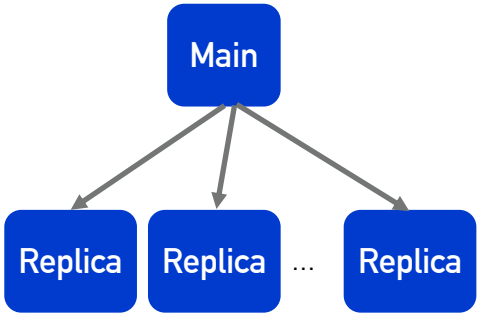
- **Problématique:**
  - **Connaitre les adresses IP du serveur recherché.**
  - **A l'origine:**
    - Localement: /etc/hosts
    - Globalement: Annuaire centralisé géré par le Network Information Center de **SRI** (non profit Science Research Institute, created by Stanford University)
    - Consultation par téléphone, email…
    - Problème: horaires de bureau. fermé le soir, les week-ends et pour Noël🎄 !!!
- **Projet initial:**
  - **Distribution/Synchronisation de l'annuaire vers d'autres sites.**
  - **Projet donné en particulier à Paul Mockapetris**
    - Qui n'obéit pas et construit son propre système (from scratch)
    - Architecture distribuée, « scalable » (anticipation de la croissance d'Internet)

https://www.internethalloffame.org/official-biography-paul-mockapetris

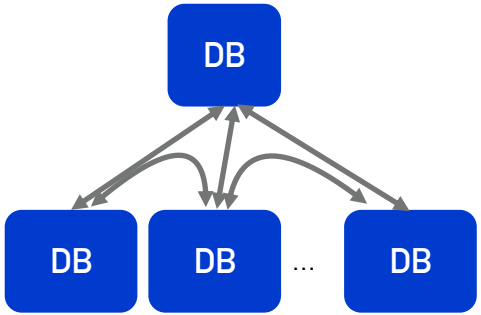
DNS = Base de donnée

- **BDD Distribuée (scalabilité, redondance)**

Master/Slave

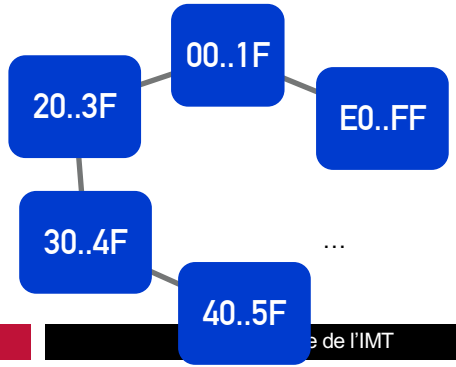


BdD Distribuée

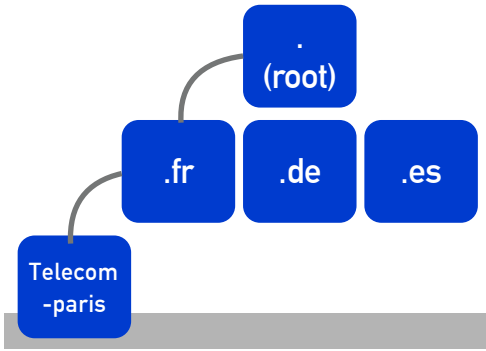


Problèmes potentiels:
- **Scalabilité**
- **Consistence**

Peer to Peer Structuré (Consistent Hashing)



BdD Structurée (Hiérarchie)



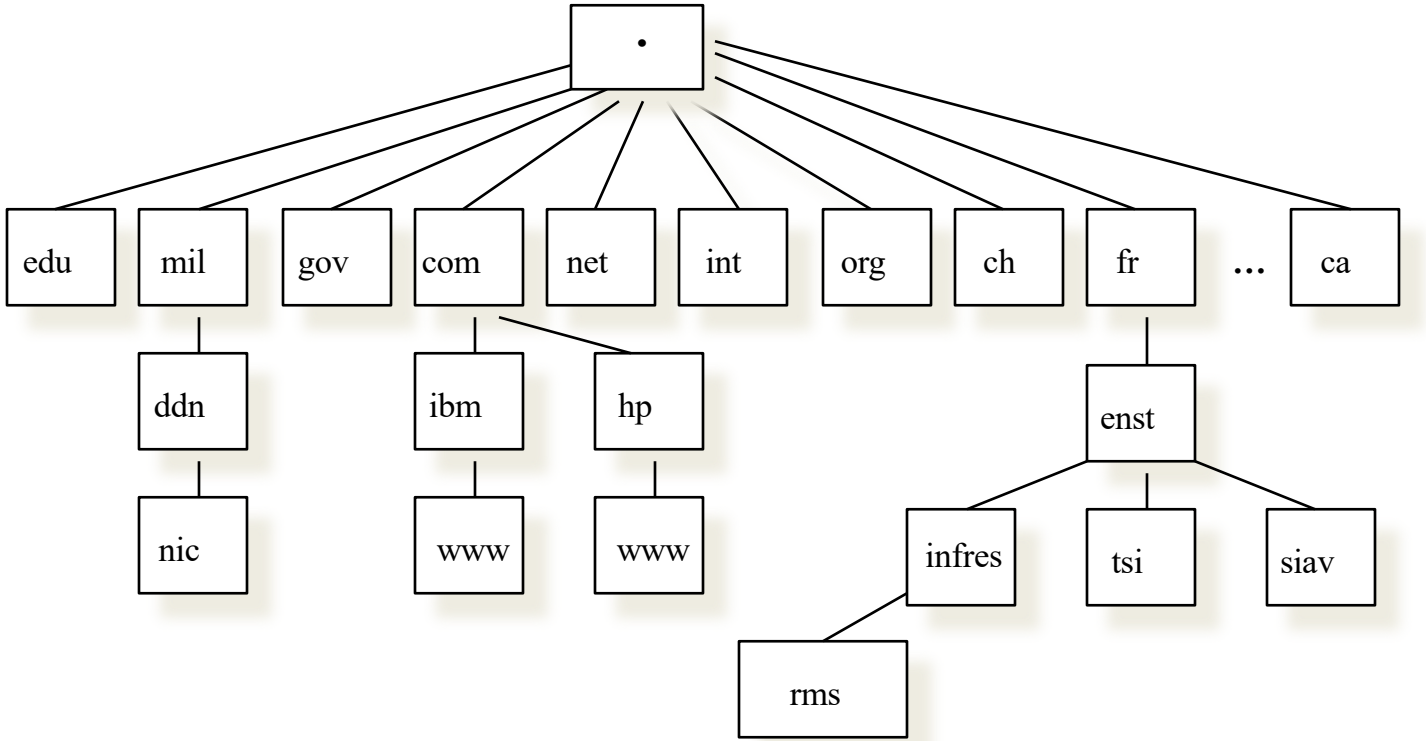
Problèmes:
- Latence de recherche
- Nombre de messages

DNS: Un Système distribué

- **Distribution des associations sur de multiples serveurs**
  - **Chaque serveur responsable d'une « zone »**
  - **Organisation hiérarchique pour passer d'une zone à une autre**

Nom de domaine

L’espace de nommage



L'espace de nommage

- **FQDN (Fully Qualified Domain Name)**
  - **doit être unique dans le réseau**
  - **concaténation des labels sur un chemin donné d'une feuille de l'arbre à la racine**
    - séparé par des dots « . » du point de vue des êtres humains
    - suite de pair (longueur, label) du point de vue des messages du réseau
    - le nom se termine par un point, mais ce dernier est souvent omis (représente le Root): www.enst.fr.
    - ex: www.enst.fr. <=> 3www4enst2frØ
      Le Ø signifie qu'après il y a le root (longueur du label est 0)
  - **le choix des noms est libre, mais souvent lié aux besoins des usages,**
    - exemple: www.telecom-paris.fr (*www* permet de retrouver intuitivement le nom d'un serveur web à telecom)
  - **la taille d'un nom de domaine est au maximum de 255 carac. (y compris les points), 255 octets**
    - la profondeur de l'arbre est limitée par cette taille, c.à.d. $255/(63+1_{point}) = 4$ labels

L’espace de nommage

- **Les TLD (Top-Level Domain) :**
  - **Domaines de premier niveau décris dans le RFC1591**
    - Connaissent tous les root server
  - **ccTLD: country code TLD** (ex. fr, us, ca, lb, …)
    - **http://www.icann.org/cctld/cctld.html**
  - **gTLD: generic TLD** (ex. com, org, net, …+ 7 nouveaux biz, aero, name, pro, musuem, info et coop et encore récemment .mobi)
    - **http://www.icann.org/gtld/gtld.html**
  - **Plus que 100 TLD dans le monde.**

L’espace de Nommage

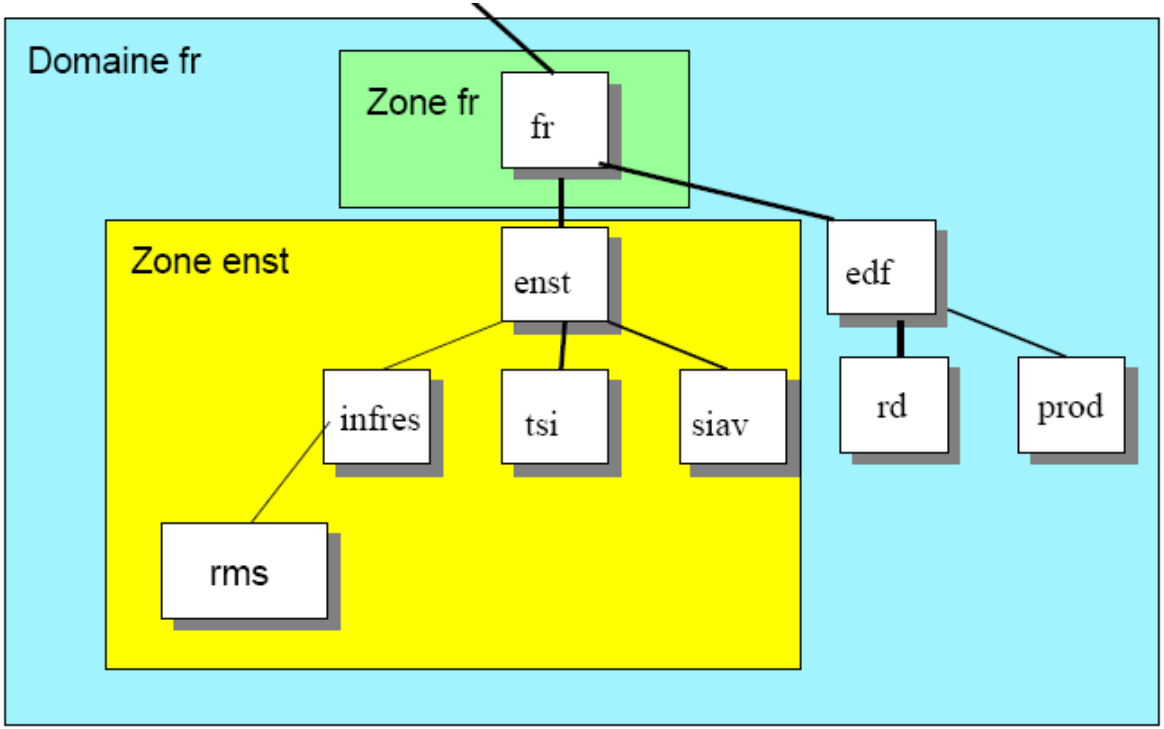
- La délégation:
  - Un nœud père délègue la gestion à un nœud fils
    → intérêt de la distribution de bases dans DNS
  - Le nœud père doit être en possession des adresses où se trouvent la base d’information de son fils

L’espace de nommage

Zone :

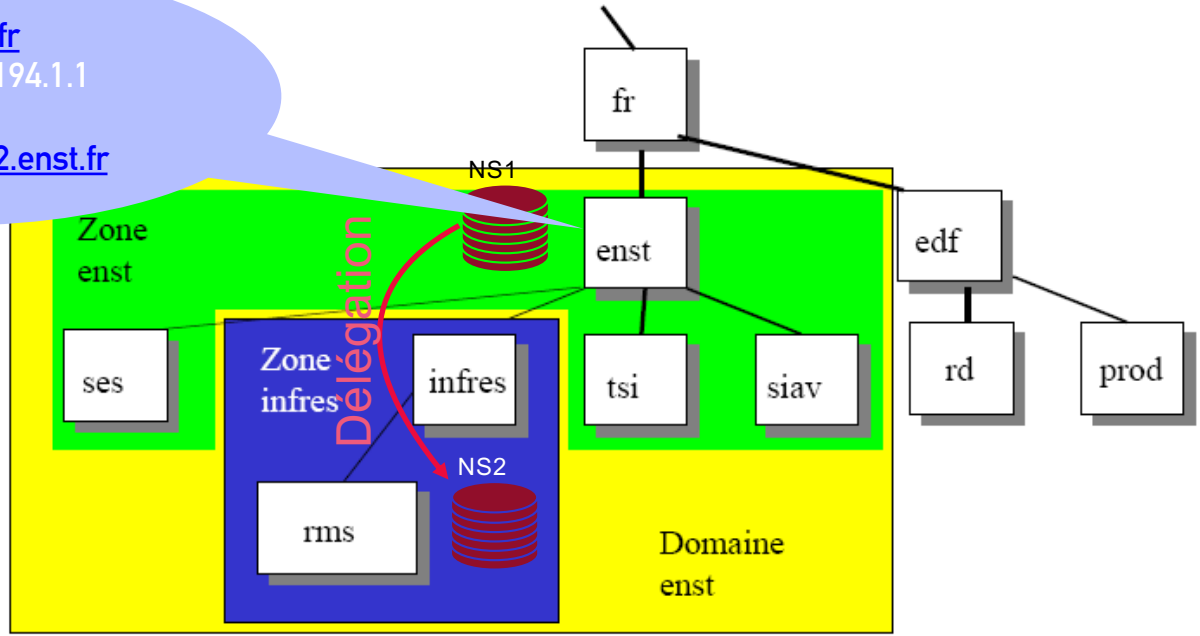
- Sous arbre (branche de l'arbre) qui est administré séparément.
- Contient une base avec toutes des informations associées à ses nœuds.
- Peut être subdivisée à nouveau en plusieurs zones.
- Pour une zone on a obligatoirement:
  - un serveur principal et un serveur secondaire.
  - Le serveur secondaire prend copie de la base d’information du principal.
- À chaque fois qu'une zone est créé, l'administrateur alloue un nom à cette zone, précise l’adresse IP du serveur principal et les noms des machines dans sa zone.

L’espace de nommage



L'espace de nommage

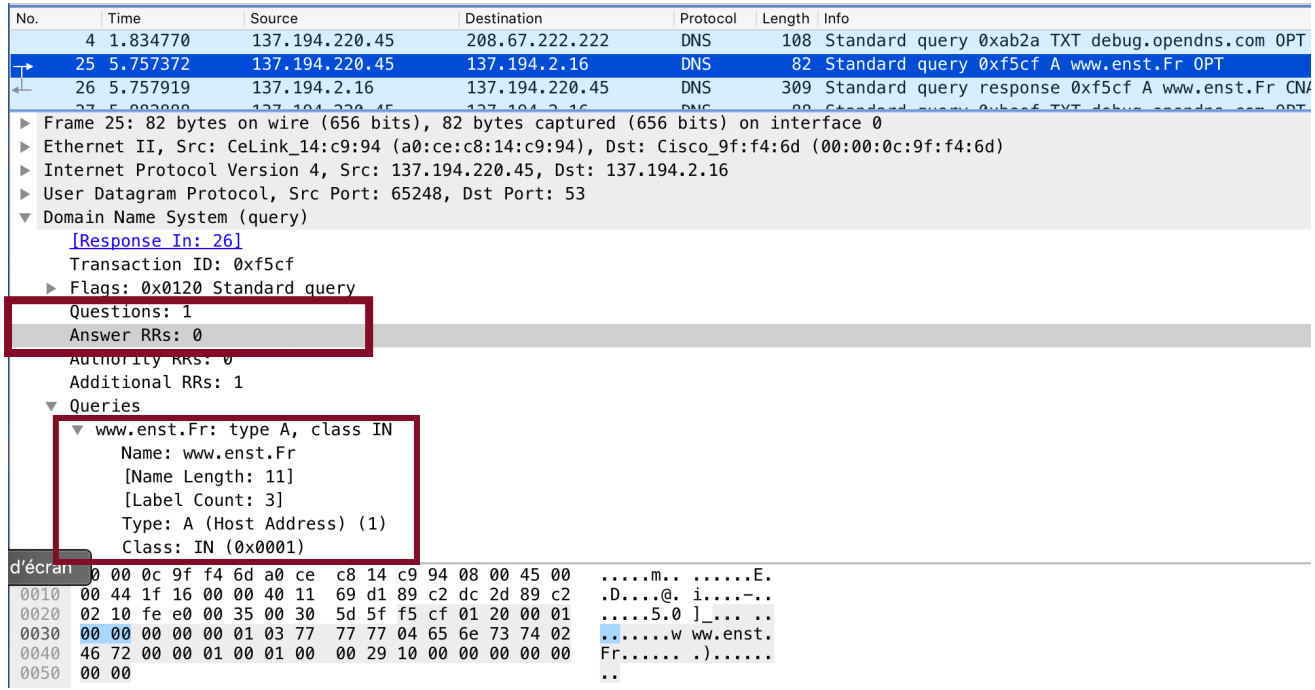
enst.fr -> ns1.enst.fr
www.enst.fr = 137.194.1.1
(…)
infres.enst.fr -> ns2.enst.fr



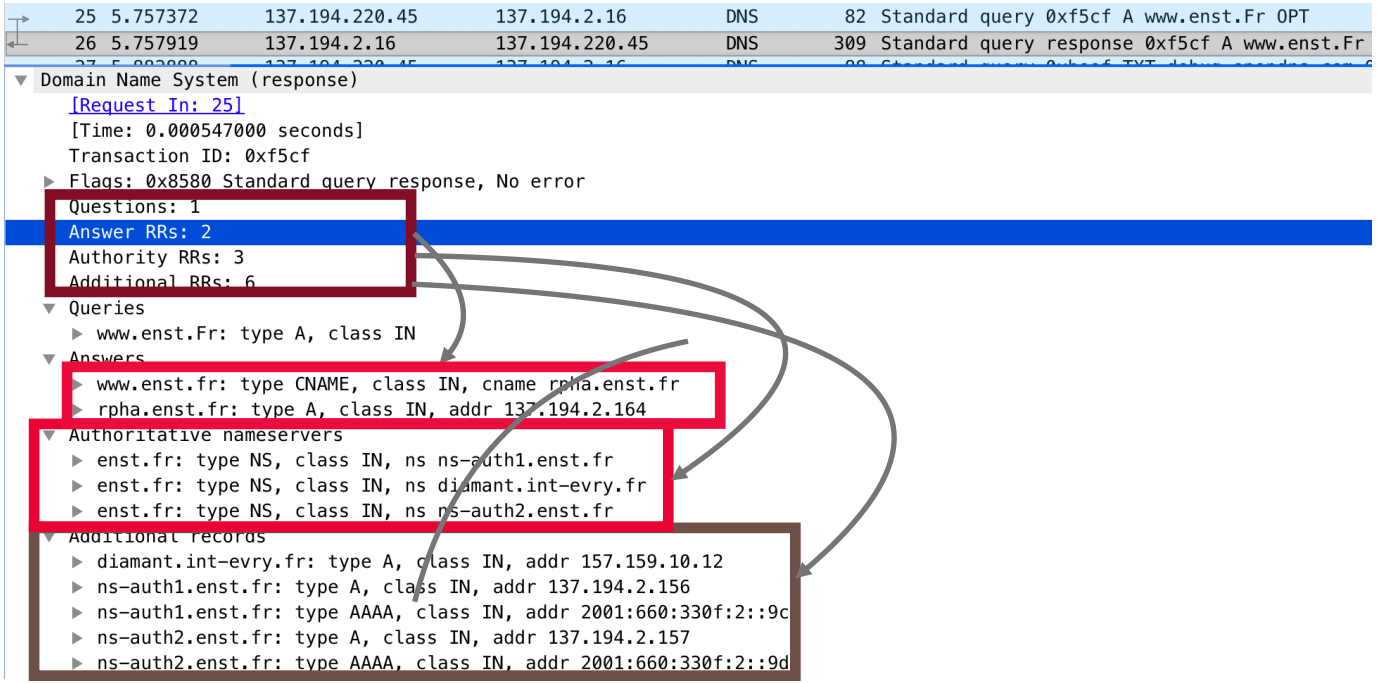
Une zone est sous la responsabilité d'un serveur (plus serveurs secondaires)
Ex: NS1 pour enst.fr, NS2 pour infres.enst.fr
Domaine = Toutes les machines dans « enst.fr »:
Zone enst.fr + Délégations (sous-zone infres.enst.fr)

Protocole DNS

PROTOCOLE DNS



PROTOCOLE DNS(2)



Resource RECORDS

- Les RRs principaux:
  - A: IPv4 Address
  - AAAA: IPv6 Address
  - NS: Name Server
  - CNAME: Canonical Name (Alias)
    Ex: www.telecom-paris.fr -> rpha-tp.enst.fr

```
#dig www.telecom-paris.fr
(…)
;www.telecom-paris.fr.    INA
;; ANSWER SECTION:
www.telecom-paris.fr.     86400 INCNAME rpha.telecom-paris.fr.
rpha.telecom-paris.fr.  86400 INCNAME rpha-tp.enst.fr.
rpha-tp.enst.fr.          86400 INA     137.194.2.166
;; AUTHORITY SECTION:
enst.fr.    86400 INNSdiamant.int-evry.fr.
enst.fr.    86400 INNSns-auth2.enst.fr.
enst.fr.    86400 INNSns-auth1.enst.fr.
;; ADDITIONAL SECTION:
diamant.int-evry.fr.140938  INA     157.159.10.12
ns-auth1.enst.fr.    86400     INA     137.194.2.156
ns-auth1.enst.fr.    86400INAAAA2001:660:330f:2::9c
ns-auth2.enst.fr.    86400INA     137.194.2.157
ns-auth2.enst.fr.    86400INAAAA2001:660:330f:2::9d
;; Query time: 34 msec
```

RR (MX)

- MX: Mail Exchange. Example:

```
% dig telecom-paris.fr MX
(…)
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3,
ADDITIONAL: 10
(…)
;; QUESTION SECTION:
;telecom-paris.fr.      INMX
;; ANSWER SECTION:
telecom-paris.fr.  86400 INMX20 mx2.enst.fr.
telecom-paris.fr.  86400 INMX10 mx1.enst.fr.
;; AUTHORITY SECTION:
telecom-paris.fr.  86400 INNSns-auth1.enst.fr.
telecom-paris.fr.  86400 INNSns-auth2.enst.fr.
telecom-paris.fr.  86400 INNSdiamant.int-evry.fr.
;; ADDITIONAL SECTION:
mx1.enst.fr.   86400 INA 137.194.2.137
mx1.enst.fr.   86400 INAAAA2001:660:330f:2::89
mx2.enst.fr.   86400 INA 137.194.2.136
mx2.enst.fr.   86400 INAAAA2001:660:330f:2::88
diamant.int-evry.fr. 129669INA 137.159.10.12
ns-auth1.enst.fr.  86400 INA 137.194.2.156
ns-auth1.enst.fr.  86400 INAAAA2001:660:330f:2::9c
ns-auth2.enst.fr.  86400 INA 137.194.2.157
ns-auth2.enst.fr.  86400 INAAAA2001:660:330f:2::9d
```

RR (suite)

- **Autres services:**
  - **Web n'existait pas lorsque DNS a été créé. MX existe donc mais il n'y a pas d'équivalent pour serveur HTTP.**
    - D'où la résolution de nom www.telecom-paristech.fr
    - Idem avec ldap.enst.fr, sip.r2.enst.fr, …
  - **Approche plus générique: découverte de service avec SRV**
    - **Syntaxe: SRV _ldap._tcp**.enst.fr


```
[centos@ns ~]$ dig _ldap._tcp.enst.fr SRV
;; QUESTION SECTION:
;_ldap._tcp.enst.fr.            IN        SRV

;; ANSWER SECTION:
_ldap._tcp.enst.fr.  21599     IN        SRV       0 0 389 ldap.enst.fr.
```

RR (suite)

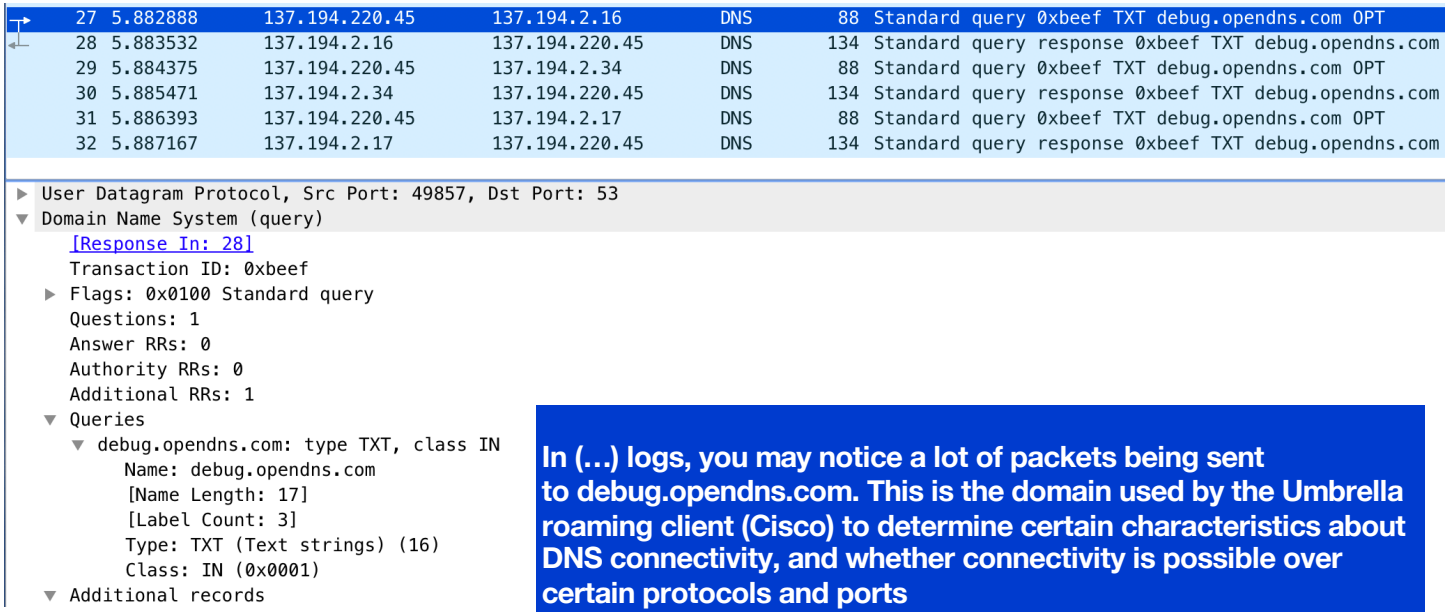
- **PTR:**
  - **Utilisé pour le service de inverse DNS**

```
[centos@ns ~]$ dig -x 137.194.208.23

;; QUESTION SECTION:
;23.208.194.137.in-addr.arpa.  IN        PTR

;; ANSWER SECTION:
23.208.194.137.in-addr.arpa. 21599 IN    PTR
        controller.r2.enst.fr.
```

À noter la syntaxe à « l'envers »

RR TXT: ExAMPLE « EXOTIQUE »

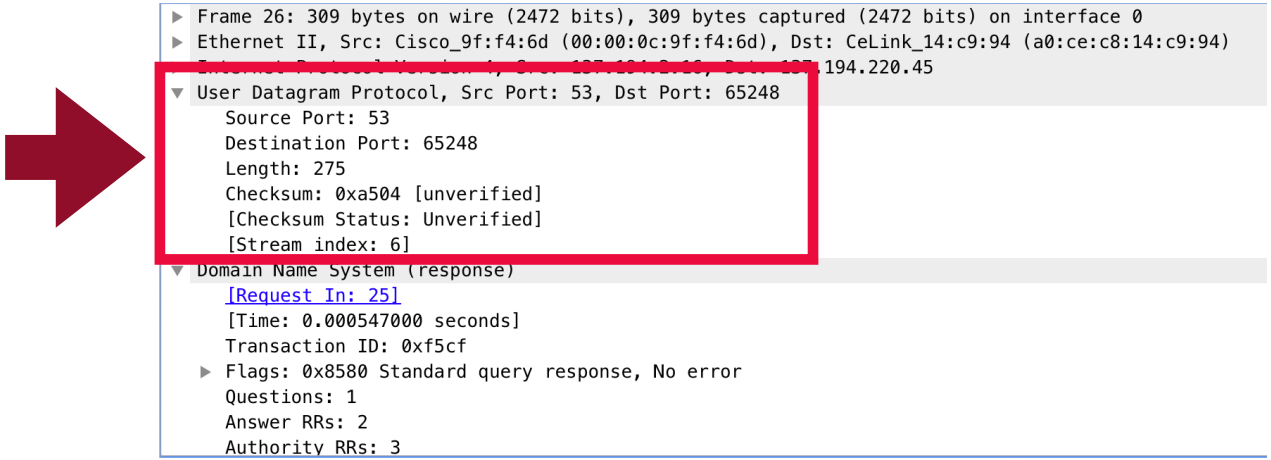
- **TXT:**
  - **Utilisé pour donner toute indication supplémentaire concernant une zone, une machine, …**
  - **Ex: email d'un administrateur, …**



In (…) logs, you may notice a lot of packets being sent to debug.opendns.com. This is the domain used by the Umbrella roaming client (Cisco) to determine certain characteristics about DNS connectivity, and whether connectivity is possible over certain protocols and ports

UDP versus TCP

- UDP/TCP port for DNS: 53
- UDP preferred
  - transaction courte, query/response
  - (max packet size: 512 octets)



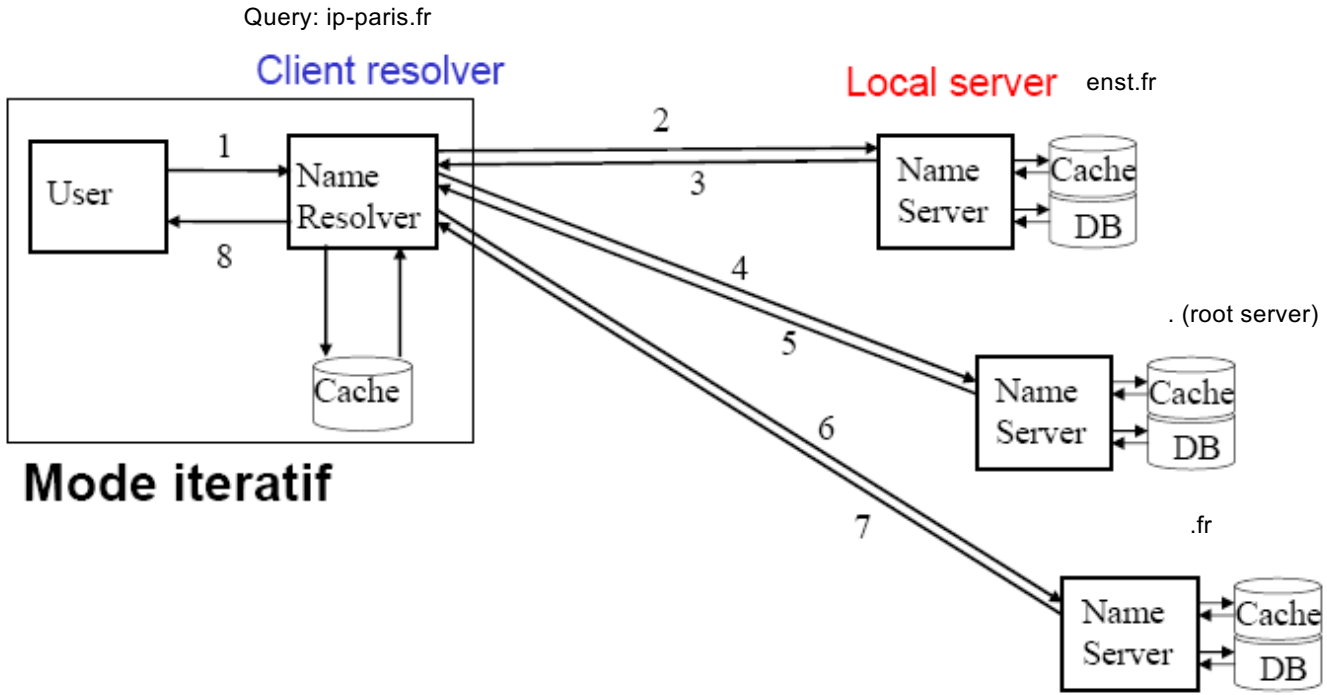
OUTILS DNS (Linux)

- **Nslookup**
  - **Affichage compact**
- **Dig**
  - **Plus verbeux (+ de détails) par défaut**
  - **Option « trace » intéressante pour comprendre DNS (cf. plus loin)**

Parcours de l’arborescence

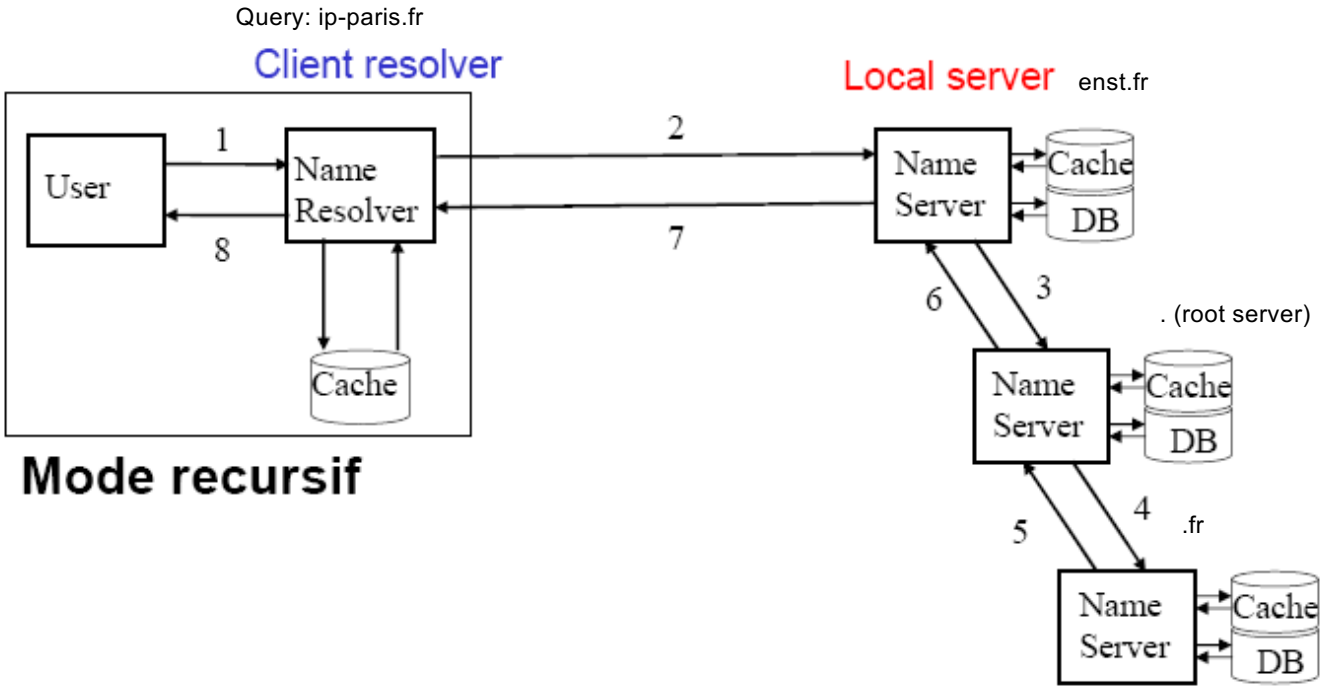
- **Authoritative**
  - **Serveur responsable de sa zone.**
- **Non Authoritative**
  - **Serveur disposant de l’information mais non responsable de la zone en question.**
- **Itératif versus Récursif (voir transparents suivants)**

Mode itératif



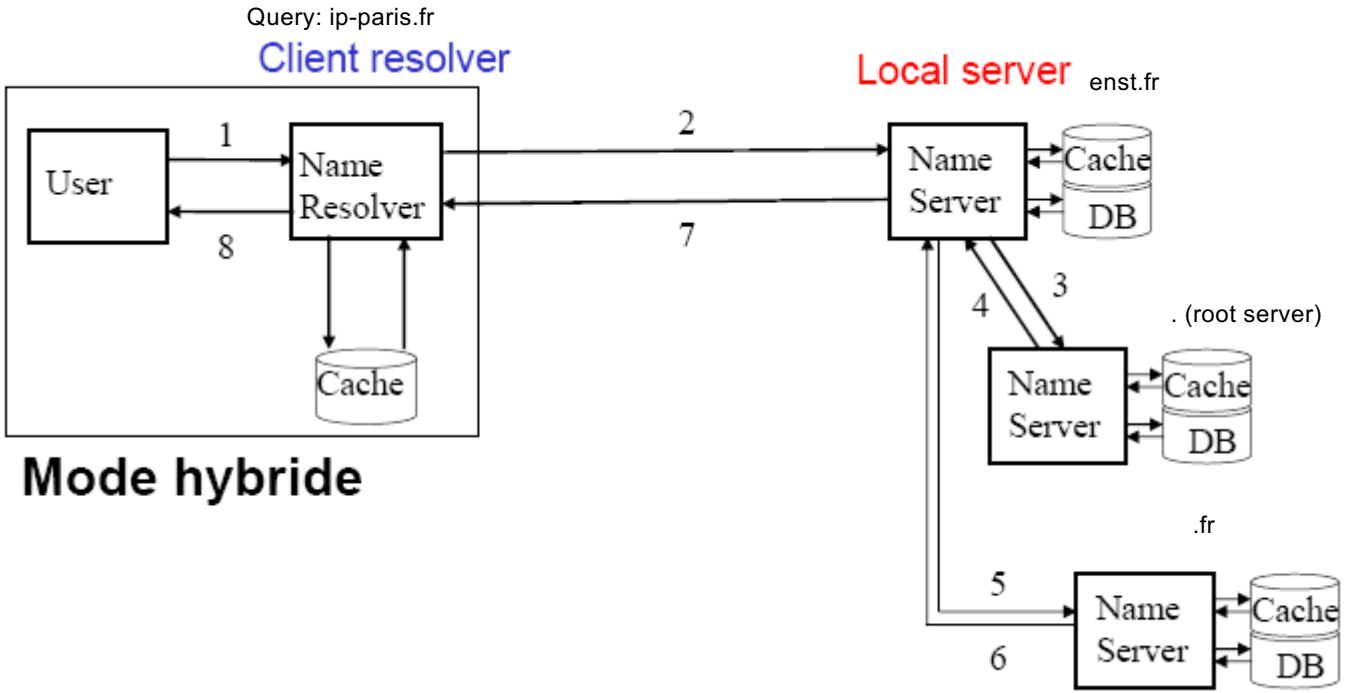
Ref: Dario Rossi

Mode Récursif



Ref: Dario Rossi

Mode Hybride



Ref: Dario Rossi

EXAMPLE DE PARCOURS DANS l'arborescence (Etape 1)

Dig « trace » (Etape 1: « . », racine)

```
 <<>> DiG 9.11.4-P2-RedHat-9.11.4-9.P2.el7 <<>> +trace cs.ucla.edu
;; global options: +cmd
.               74904   IN      NS      a.root-servers.net.
.               74904   IN      NS      h.root-servers.net.
.               74904   IN      NS      e.root-servers.net.
.               74904   IN      NS      l.root-servers.net.
.               74904   IN      NS      c.root-servers.net.
.               74904   IN      NS      f.root-servers.net.
.               74904   IN      NS      j.root-servers.net.
.               74904   IN      NS      d.root-servers.net.
.               74904   IN      NS      g.root-servers.net.
.               74904   IN      NS      i.root-servers.net.
.               74904   IN      NS      b.root-servers.net.
.               74904   IN      NS      k.root-servers.net.
.               74904   IN      NS      m.root-servers.net.
.               74904   IN      RRSIG   NS 8 0 518400 20191213170000 20191130160000 22545 .
gGZBrktIkbjNA4wid3KNGdKGTzJmQZVsUjOy9/Itndl7kOXJbr+0iFy1
2IP85x69mlNuvmVBvSEMRxZK6L54hqiW90W6NJ8S7KoughDBayvxcmVq
L9v2kRc6JE/cNruyKH1oC+Nm8S1V+ocfOifpm6epGP7B3W3StNSinVvQ
+i8h0AziAUpzUcgWqBf9pxx7II199HAkb440poK3BbiBwWJ+F0GGKoFz
f+POa3W/jJg1ZYcbQNtDtNxuvv2GBXAPPOkNpFM5+fJdlkYrqcky4hen
9XNjzFXe9/SPMt6FAMt2QPv1oszpFRa3vmlxahrJWRtA75kd5SNP2Ejr UavrOg==
;; Received 525 bytes from 8.8.4.4#53(8.8.4.4) in 2 ms
```

EXAMPLE DE PARCOURS DANS l'arborescence (Etape 2)

Dig « trace » (Etape 2 « edu. »)

```
edu.            172800  IN      NS      g.edu-servers.net.
edu.            172800  IN      NS      m.edu-servers.net.
edu.            172800  IN      NS      c.edu-servers.net.
edu.            172800  IN      NS      b.edu-servers.net.
edu.            172800  IN      NS      a.edu-servers.net.
edu.            172800  IN      NS      i.edu-servers.net.
edu.            172800  IN      NS      d.edu-servers.net.
edu.            172800  IN      NS      k.edu-servers.net.
edu.            172800  IN      NS      l.edu-servers.net.
edu.            172800  IN      NS      j.edu-servers.net.
edu.            172800  IN      NS      e.edu-servers.net.
edu.            172800  IN      NS      f.edu-servers.net.
edu.            172800  IN      NS      h.edu-servers.net.
edu.            86400   IN      DS      28065 8 2
4172496CDE85534E51129040355BD04B1FCFEBAE996DFDDE652006F6 F8B2CE76
edu.            86400   IN      RRSIG   DS 8 1 86400 20191214050000 20191201040000 22545 .
Di8W3cfRS6gJwZLFlkXlhWfrXzNSPQwA8/JHL0WBa62X4CQbU85rOzPR
iMvoxF0ks/Y+A/rj2PIAdYfGO7e2JNWtP124gXcTL9gT3O8Ew/w6L1PQ
KeO8irHsxFsMLDMuWiKEOTJXJ6VD8qVTIjSEw6SJMClKlM/Fs20CW57d
shFJ13nsqKGNo1NRl1qlXP0K3dTzdCfJpbDh4wRqb+5flrIyFOP8GYdg
PDGHVGvVZ2+3EjjL4h9aFVB+yXX7eFnGCppJNhXx3K4/Z7aZSp4dnC8M
1cEdemxxsL+e9Y97RMo0kJBVwBwmclkedPXymiqM264tYyIQXEmfXQLa ZA1A0g==
;; Received 1170 bytes from 192.36.148.17#53(i.root-servers.net) in 20 ms
```

EXAMPLE DE PARCOURS DANS l'arborescence (Etape 3)

- **Dig « trace » (Etape 3. « ucla.edu.»)**

```
ucla.edu.          172800  IN      NS      ns1.dns.ucla.edu.
ucla.edu.          172800  IN      NS      ns2.dns.ucla.edu.
ucla.edu.          172800  IN      NS      ns3.dns.ucla.edu.
ucla.edu.          172800  IN      NS      ns4.dns.ucla.edu.
9DHS4EP5G85PF9NUFK06HEK0O48QGK77.edu. 86400 IN NSEC3 1 1 0 -
9V5L4LUB1VNJ9EQQLIHEQCBREACL25O0 NS SOA RRSIG DNSKEY NSEC3PARAM
9DHS4EP5G85PF9NUFK06HEK0O48QGK77.edu. 86400 IN RRSIG NSEC3 8 2 86400 20191208101043
20191201090043 47252 edu. HAtj388G/njp0PX/lbKeuIvGiR9ehU0ZkFwhpyHB1E1pxccjDBS3O1AE
qqubO5sbJO2ahm2ZjnpCSLDhzgm1YjNuGRzP4HZRPgP3e9TAIvtMb3y7
P01jFhIGka58NpJCUiIK4IRVGlGthcPMvEDc5qdboPbJbaRwBPYB2j+Y
Qs4wt4nDA0fV9HxGgu+n0a5jGhnX2Sk7WJnh8D0Xjg7KDA==
S0GBH2DA0BHLGIVARV8IP5PDT48TMKSL.edu. 86400 IN NSEC3 1 1 0 -
S31H6N28EA1T4CUQRJ3OTBVTFM3EU37F NS DS RRSIG
S0GBH2DA0BHLGIVARV8IP5PDT48TMKSL.edu. 86400 IN RRSIG NSEC3 8 2 86400 20191208091523
20191201080523 47252 edu. w6YLMi5QZVFPyom0F3WcGGO/bgv83XTYdPV92s4iwJtRkXdCVWYvUkxQ
RrP3UW0pHaJQpvBl+/Ajvf6DUS0Ahm4HtZ1pQ0GIKHyUeP78YNhUhzWz
WyvFwnALc+gKB6ra5kGMF9LdJo+mW/oSvAoCVIe2UvTy6wq/KYw4YRU4
FFHgTQAU85YkjXp+Owfjhf75teSUK/r5bKWBWTi2Gtzm6A==
;; Received 841 bytes from 192.31.80.30#53(d.edu-servers.net) in 19 ms
```

EXAMPLE DE PARCOURS DANS l'arborescence (Etape 4)

- **Dig « trace » (Etape 4. « cs.ucla.edu.»)**

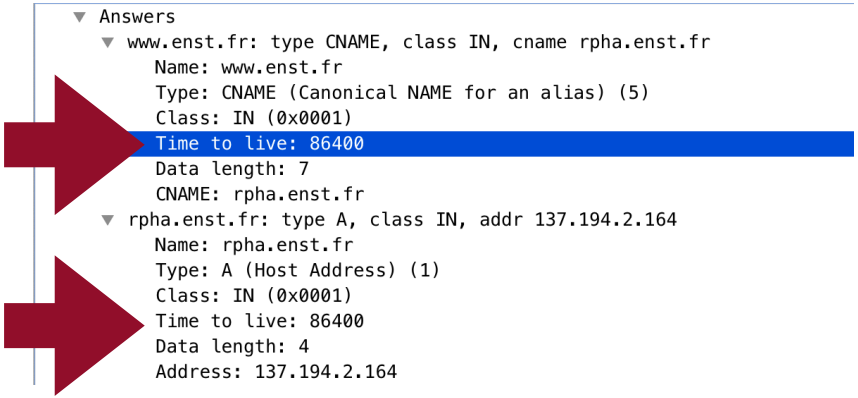
cs.ucla.edu.	14400	IN	A	164.67.100.181
cs.ucla.edu.	14400	IN	NS	NS3.DNS.UCLA.EDU.
cs.ucla.edu.	14400	IN	NS	NS0.CS.UCLA.EDU.
cs.ucla.edu.	14400	IN	NS	NS1.CS.UCLA.EDU.
cs.ucla.edu.	14400	IN	NS	NS3.CS.UCLA.EDU.
cs.ucla.edu.	14400	IN	NS	NS2.CS.UCLA.EDU.
cs.ucla.edu.	14400	IN	NS	NS1.DNS.UCLA.EDU.
cs.ucla.edu.	14400	IN	NS	NS2.DNS.UCLA.EDU.

;; Received 425 bytes from 192.35.225.7#53(ns1.dns.ucla.edu) in 144 ms

A REFAIRE AVEC WWW.CS.UCLA.EDU

CACHING

- **Pour plus de passage à l'échelle**
  - **Mémorisation des réponses pendant une certaine durée de temps**
    - configurable grâce au paramètre TTL):

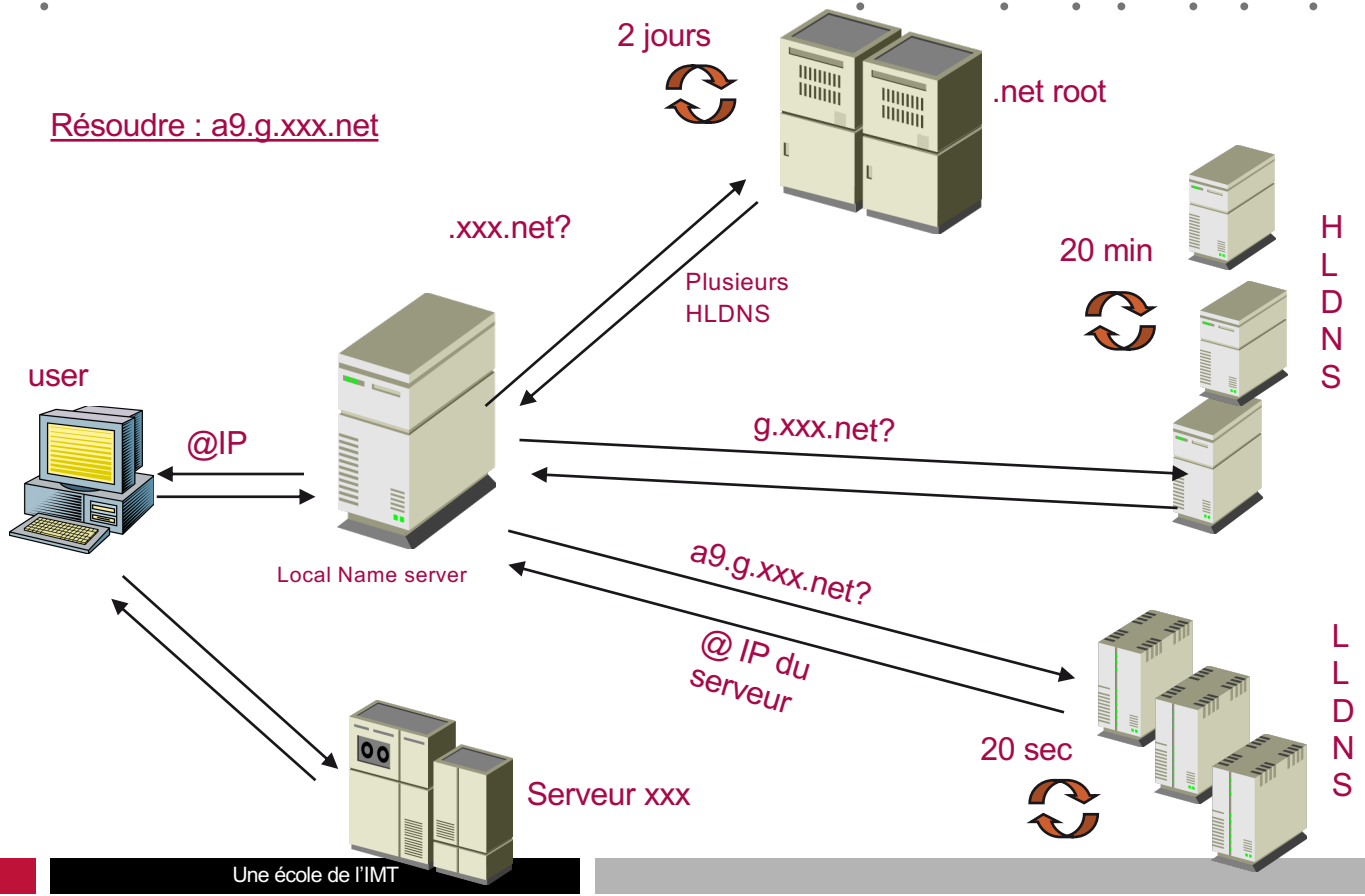


TTL

- **Exemple d'un site hébergé par un CDN**

```
jean-louis@Clibou ~ % dig www.tf1.fr
(…)
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
(…)
;; ANSWER SECTION:
www.tf1.fr.                    724 IN CNAME    d220140hrb0h87.cloudfront.net.
d220140hrb0h87.cloudfront.net. 60 IN A         13.35.198.26
d220140hrb0h87.cloudfront.net. 60 IN A         13.35.198.31
d220140hrb0h87.cloudfront.net. 60 IN A         13.35.198.95
d220140hrb0h87.cloudfront.net. 60 IN A         13.35.198.97
```

CDN : choix du meilleur serveur



Root Servers, TLDs, …

Le haut de la hiérarchie

Root DNS Servers

- **Root Servers**
  - Au plus haut de la hiérarchie
  - Se connaissent les uns les autres
  - Connaissent tous les TLDs
  - 13 serveurs qui sont présents dans l'ensemble des bases de données des serveurs de noms

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

L’espace de nommage

- **Les TLD (Top-Level Domain) :**
  - **Domaines de premier niveau décris dans le RFC1591**
  - **Connaissent tous les root server**
  - **ccTLD: country code TLD** (ex. fr, us, ca, lb, …)
    - **http://www.icann.org/cctld/cctld.html**
  - **gTLD: generic TLD** (ex. com, org, net, …+ 7 nouveaux biz, aero, name, pro, musuem, info et coop et encore récemment mobi)
    - **http://www.icann.org/gtld/gtld.html**
  - **Plus que 100 TLD dans le monde.**

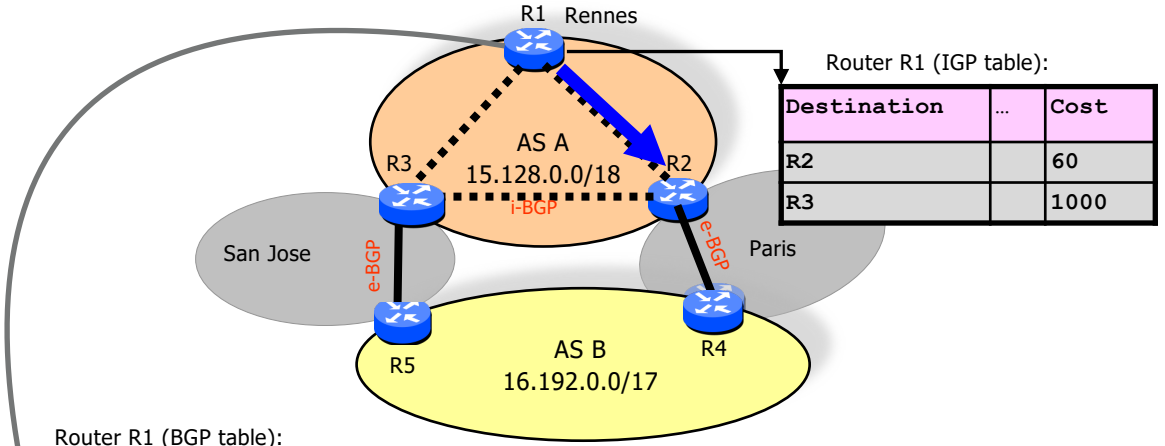
Appendix: Anycasting

Très utilisé pour des services DNS (entre autre)

How does ANYCAST WORK ?

- Based on BGP
- Same prefix is announced by different sites (at different locations). BGP will guide trafic towards « nearest » peering point… (for instance with « hot potato »)

Hot Potato: IGP distance is used to choose between i-BGP routes



Router R1 (IGP table):

Destination	…	Cost
R2		60
R3		1000

Router R1 (BGP table):

Network	Next HOP	AS Path
16.192.0.0/17	R3	B i(from iBGP) - IGP cost:1000
> 16.192.0.0/17	R2	B i(from iBGP) - IGP cost: 60

Anycasting (suite) - Lien avec RES201

- **Le fournisseur DNS peut également controller la diffusion des annonces BGP:**
  - ***Annonces sélectives:*** **Contrôle la portée des annonces BGP, grâce à des « communautés » BGP spécifiques.**

Ex: https://www.us.ntt.net/support/policy/routing.cfm

2914:1205 Paris,France 2914:1601 Sao Paulo, Brazil
2914:2204 fr (France) 2914:2601 br (Brazil)
2914:3200 Europe 2914:3600 South America
2914:4029 do not advertise to any peer in North America
2914:4229 do not advertise to any peer in Europe
2914:4429 do not advertise to any peer in Asia

Tata Corp:
6453:2000 – EU Region
6453:3000 – AP Region

Le client (DNS provider) peut attacher des communautés spécifiques (définies par son opérateur) aux routes annoncées. L'opérateur met en place des filtres qui prennent en compte ces communautés spécifiques. Cela permet d'annoncer ou pas une route à un voisin BGP donné, en fonction de la présence ou non d'une communauté (et des propriétés de ce voisin BGP)

Example (With a looking Glass)

- **Looking Glass: https://www.us.ntt.net/support/looking-glass/**

```
## Paris Router (for Google DNS server)
BGP routing table entry for 8.8.8.0/24
(…)
Paths: (21 available, best #21)
  (...)
  Path #20: Received by speaker 0
  Not advertised to any peer
  6453 15169
    209.58.116.21 (metric 26623) from 129.250.1.5 (129.250.1.5)
      Origin IGP, metric 4294967294, localpref 100, valid, confed-internal
      Received Path ID 0, Local Path ID 0, version 0
      Community: 2914:390 2914:1008 2914:2000 2914:3000 6453:1000 6453:1300 6453:1305 65504:6453
  Path #21: Received by speaker 0
  Advertised to update-groups (with more than one peer):
    0.11 0.19 0.20 0.21
  6453 15169
    129.250.8.2 from 129.250.8.2 (66.110.10.90)
      Origin IGP, localpref 100, valid, external, best, group-best
      Received Path ID 0, Local Path ID 0, version 425515913
      Community: 2914:390 2914:1205 2914:2204 2914:3200 6453:2000 6453:2200 6453:2202 65504:6453
      Origin-AS validity: not-found
```

Example (With a looking Glass)

- **Looking Glass: https://www.us.ntt.net/support/looking-glass/**

Sao Paolo Router (for Google DNS server)
Router: São Paulo - BR
Command: show bgp ipv4 unicast 8.8.8.8

BGP routing table entry for 8.8.8.0/24
(...)
Paths: (20 available, best #20)
(...)
Path #20: Received by speaker 0
  Advertised to update-groups (with more than one peer): 0.3 0.12 0.13 0.15
  Advertised to peers (in unique update groups): 200.194.64.36
  6453 15169
    129.250.8.178 from 129.250.8.178 (66.110.11.186)
      Origin IGP, localpref 100, valid, external, best, group-best
      Received Path ID 0, Local Path ID 0, version 546857265
      Community: 2914:390 2914:1601 2914:2601 2914:3600 6453:1000 6453:1100 (…)
      Origin-AS validity: not-found

DNSSEC

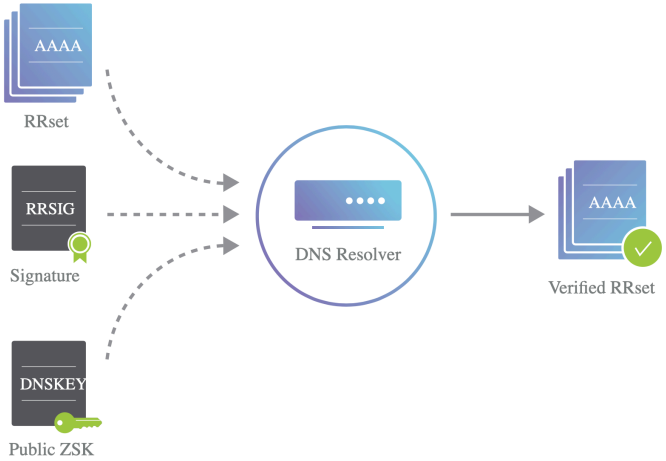
Sécurisation de l'infrastructure DNS

Probleme

- **Données transmises par DNS ne sont pas authentifiées**
  - **Possibilité d'injection de fausses informations, etc.**
    - Ex: Probable Cache Poisoning of Mail Handling Domains https://insights.sei.cmu.edu/cert/2014/09/-probable-cache-poisoning-of-mail-handling-domains.html
    - The Hitchhiker's Guide to DNS Cache Poisoning. https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf
  - A Brief History of DNS Hijackings - ICANN. By Google
  - …

BASIC IDEAS

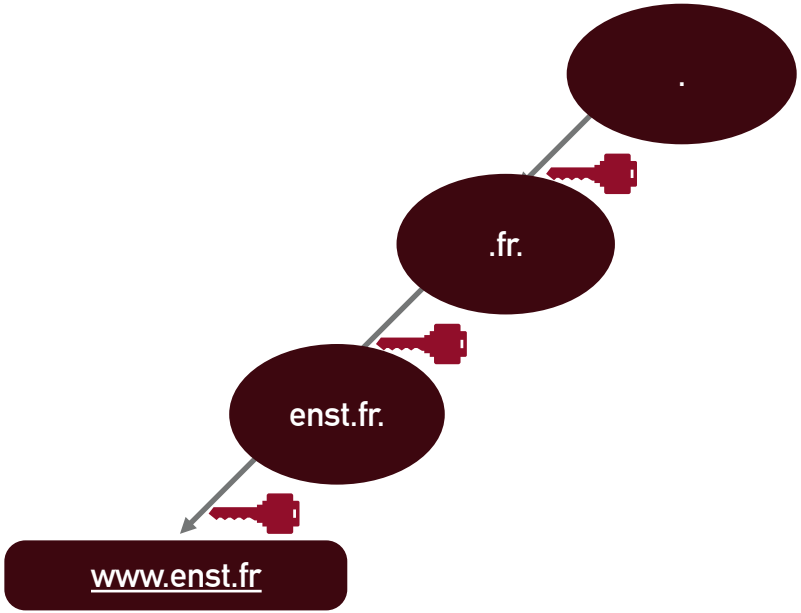
- **Protecting RRs**
  - **RR signed with authoritative private key**
  - **Public key included in ANSWER with DNSKEY**



- **Problem**
  - **How to verify the certificate ?**

Images from CloudFlare (https://www.cloudflare.com/dns/dnssec/how-dnssec-works/)

Chain of TRUST



- **Question: Can root servers be trusted ???**
  - **https://www.cloudflare.com/dns/dnssec/root-signing-ceremony/**