



*Configuration et gestion
d'un serveur*

Chapitre 7 : La résolution de nom

Objectifs :

Comprendre le mécanisme de résolution de nom DNS sur Internet.
Connaitre les notions d'arborescence DNS, de serveur Racine et de FQDN

Plan :

1. Le système de résolution de noms DNS.
2. Le mécanisme DNS.
 - 2.1. La requête DNS d'un client.
 - 2.2. Quelques serveurs DNS plus ou moins connus.
3. La résolution de nom DNS.
 - 3.1. Organisation de la recherche.
 - 3.2. Les serveurs Racine.

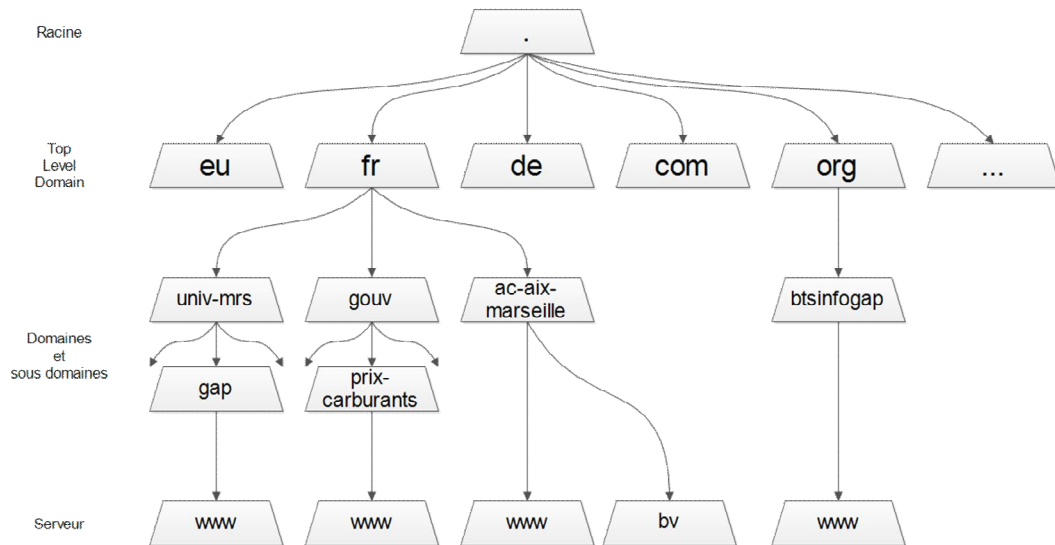
Ressources :

<http://www.localiser-ip.com>
<https://testdns.fr>
<https://www.youtube.com/watch?v=dcIrB8qRCbA>

1. Le système de résolution de noms DNS.

Le système DNS est donc fondé sur une arborescence.

Arborescence des noms de domaine sur Internet :



Il existe des serveurs DNS à tous les étages de l'arborescence, y compris au niveau des serveurs.

C'est l'ICANN qui délègue les droits de commercialisation des domaines de premier niveau (TLD), et assure leur bon fonctionnement.

ICANN : Internet Corporation for Assigned Names and Numbers (en français, la Société pour l'attribution des noms de domaine et des numéros sur Internet) est une autorité de régulation de l'Internet, basée en Californie, d'autorité mondiale.

Un nom de domaine complet, également appelé FQDN pour Full Quality Domain Name s'écrit ainsi :

`www.gap.univ-mrs.fr.`

`bv.ac-aix-marseille.fr.`

A noter que le point final est en théorie obligatoire pour indiquer la zone racine, mais a disparu des écritures.

2. Le mécanisme DNS.

2.1. La requête DNS d'un client.

Le protocole DNS est un protocole de la couche Application.

Il permet de consulter le serveur DNS configuré, pour trouver l'adresse IP qui correspond à une URL.

Un client fait la demande au serveur DNS qu'il retrouve dans sa configuration.

Si le serveur DNS connaît la réponse, il l'indique.

S'il ne la connaît pas, il transmet la demande à son serveur DNS référent.

Au sein des réseaux locaux d'entreprise, le serveur DNS est souvent privé, le serveur DNS référent est généralement celui du FAI ou un serveur DNS public connu (voir ci-après).

Chez les particuliers, la box sert de relai DNS, vers le DNS du FAI.

2.2. Quelques serveurs DNS plus ou moins connus.

8.8.8.8 : serveur DNS de Google. L'objectif de Google est de collecter encore plus de données sur vos habitudes internet.

1.1.1.1 : serveur DNS de cloudFlare, respectueux à priori de la vie privée, en ne conservant les log que 24h et en s'engageant à ne pas les revendre. Jusqu'au prochain changement de politique.

9.9.9.9 : serveur DNS de Quad9, également respectueux de la vie privée, et qui intègre un filtre contre les sites de mauvaise réputation.

L'inconvénient de ces 3 services DNS est qu'ils sont aux USA ou en Australie. L'engagement (ou pas) de respect de la vie privé est subordonné à la non modification des changement de politique des entreprises, et les trames DNS parcourent le monde, générant une consommation d'énergie supérieure à une recherche nationale.

A noter quelques adresses de services DNS français :

Orange : 80.10.246.2

SFR : 109.0.66.10

OVH : 91.121.161.184, 91.121.164.227, 188.165.197.144

(Localisations validées avec les services de <http://www.localiser-ip.com>)

3. La résolution de nom DNS.

3.1. Organisation de la recherche.

Prenons comme exemple la recherche de l'adresse IP du serveur `www.gap.univ-mrs.fr`

La requête du client est transmise à son serveur DNS référent.

Celui va alors organiser la recherche.

Il interroge le serveur Racine le plus proche, qui lui indique l'adresse du serveur de premier niveau à contacter : un serveur TLD qui gère le domaine `.fr`

Le serveur DNS référent interroge alors le serveur TLD pour obtenir l'adresse l'adresse IP correspondant à `univ-mrs.fr`

Si l'adresse recherchée avait été `www.univ-mrs.fr`, le travail de résolution DNS serait terminé, le client informé, la requête HTTP prête à partir.

Mais le lien recherche un sous domaine.

Le serveur DNS référent consulte alors le DNS de `univ-mrs.fr` pour obtenir l'adresse du serveur.

Le serveur DNS référent donne alors l'information au client qui peut compléter sa requête HTTP.

Ce site permet de faire des recherches DNS : <https://testdns.fr>

Cette vidéo retrace les étapes : <https://www.youtube.com/watch?v=dcIrB8qRCbA>

3.2. Les serveurs Racine.

Une requête est envoyée à un **serveur racine**. Il en existe en fait 13 répartis tout autour de la Terre.

	Adresse IPv4	Adresse IPv6	Opérateurs
A	198.41.0.4	2001:503:ba3e::2:30	VeriSign
B	192.228.79.201	2001:478:65::53	USC-ISI
C	192.33.4.12	2001:500:2::c	Cogent Communications
D	199.7.91.13	2001:500:2d::d	University of Maryland
E	192.203.230.10		NASA
F	192.5.5.241	2001:500:2f::f	ISC
G	192.112.36.4		U.S. DoD NIC
H	128.63.2.53	2001:500:1::803f:235	US Army Research Lab
I	192.36.148.17	2001:7FE::53	Autonomica
J	192.58.128.30	2001:503:c27::2:30	VeriSign
K	193.0.14.129	2001:7fd::1	RIPE NCC
L	199.7.83.42	2001:500:3::42	ICANN
M	202.12.27.33	2001:dc3::35	WIDE Project

Derrière ces adresses se situent en fait plusieurs serveurs, montés en clustering.

En réalité, il n'existe pas 13 mais plus de 370 serveurs racine physiques répartis pour répondre au plus vite aux requêtes des clients.

