LE SERVICE DNS (Domain Name System)

INTRODUCTION : « DNS » KESAKO ?

D.N.S. peut signifier plusieurs choses:

- Domain Name System : l'ensemble des organismes qui gèrent les noms de domaine.
  - Domain Name Service : le protocole qui permet d'échanger des informations à propos des domaines.
  - Domain Name Server : un ordinateur sur lequel fonctionne un logiciel serveur qui comprend le protocole DNS et qui peut répondre à des questions concernant un domaine.

  Sur Internet, une machine est identifiée de manière unique par son adresse IP :il est donc nécessaire d'utiliser un ANNUAIRE « Adresse IP / Nom ».

- Au début (1970-1984) : l'annuaire complet est dans un fichier texte (**/etc/hosts** sous Unix) : aujourd'hui ce fichier est encore utilisé pour l'annuaire local.
- 1984 : mise en place du DNS géré au niveau mondial par Network Information Center (http://www.nic.com)

En France, l'organisation gérante est l'Association Française pour le Nommage Internet en Coopération (http://www.afnic.fr)

LE SYSTEME DE RESOLUTION DE NOMS A BASE DE FICHIERS « hosts » : PRINCIPE DE FONCTIONNEMENT

```
hannibal@box:~$ cat /etc/hosts
127.0.0.1   localhost machine_Hannibal
127.0.1.1   box

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

hannibal@box:~$ ping -c 2 machine_Hannibal
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_req=1 ttl=64 time=0.027 ms
64 bytes from localhost (127.0.0.1): icmp_req=2 ttl=64 time=0.036 ms
--- localhost ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.027/0.031/0.036/0.007 ms
hannibal@box:~$
```

Depuis le début des réseaux IP, le principe de la résolution de noms est de faire correspondre un nom facile à mémoriser à une adresse IP, seule information réellement exploitable pour contacter une machine distante.

```
Nom-de-machine ↔  130.130.28.12
machine_Hannibal ↔ 127.0.0.1
```

Tant que les machines publiques sur Internet étaient peu nombreuses, toutes les résolutions se faisaient au moyen d'un fichier appelé **hosts** qu'on échangeait à intervalle régulier pour se tenir au courant des nouveautés.

Le DNS a été conçu pour pallier les limites du fichier hosts téléchargé, et devait répondre à certains impératifs de conception.

LE SYSTEME DE RESOLUTION DNS

- **Le DNS est dynamique :** les enregistrements doivent pouvoir être ajoutés de façon unique dans le système, et devenir rapidement disponibles pour tous.
- **Le DNS est répliqué :** on ne peut se permettre de dépendre d'un seul serveur, et les informations existent toujours en plusieurs exemplaires.
- **Le DNS est hiérarchisé** : les informations sont classées en une arborescence qui permet leur organisation. Chaque niveau de la hiérarchie est appelé « zone », et le sommet de cette hiérarchie est la zone « . ».
- **Le DNS est distribué :** les informations sont réparties en une multitude de « sous-bases » (les zones DNS), et l'ensemble de ces petites bases d'informations compose l'intégralité des enregistrements DNS. Ce fonctionnement a l'avantage de faciliter l'administration en répartissant la charge sur des milliers de serveurs.
- **Le DNS est sécurisé :** cet impératif est apparu plus tardivement, et n'est pas encore implémenté sur tous les serveurs DNS. On a

toutefois désormais la possibilité de sécuriser de bout en bout les opérations du DNS. Les services de sécurité disponibles sont l'authentification, le contrôle d'accès et le contrôle d'intégrité.

QUELQUES REFLEXIONS ET PISTES DE RECHERCHE

Les serveurs DNS (notamment les serveurs racine) sont la cible de nombreuses attaques :

http://www.zdnet.fr/actualites/vers-un-blackout-de-l-internet-le-31-mars-non-car-le-systeme-dns-est-robuste-39768729.htm

Monitoring des serveurs DNS essentiels :

http://www.cymru.com/monitoring/dnssumm/index.html

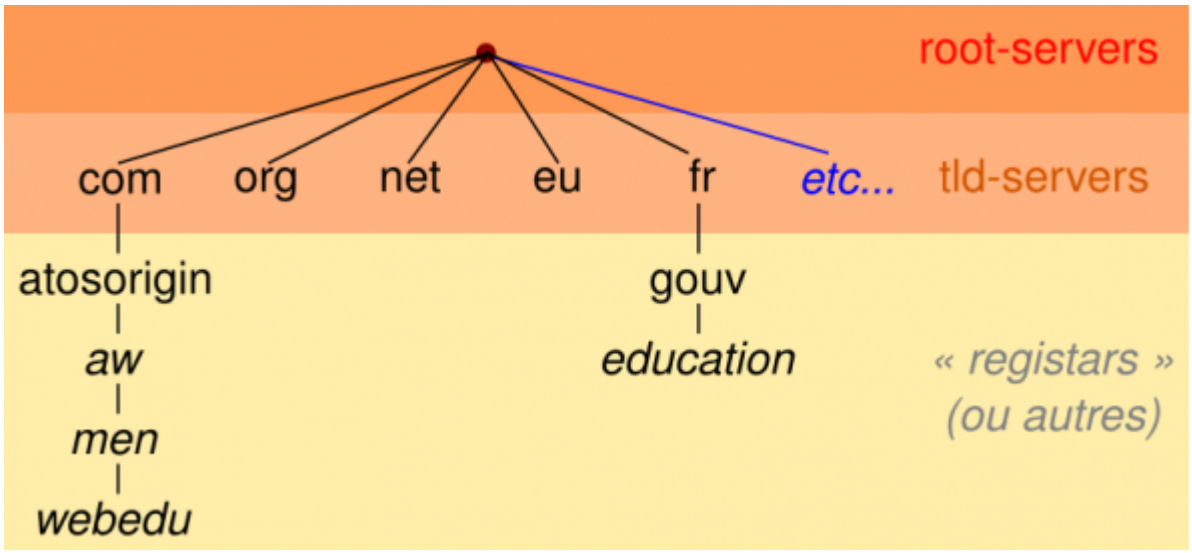
Les DNS : instruments potentiels de censure :

http://www.revoltenumerique.herbesfolles.org/2012/01/14/changer-de-serveur-dns-pour-contourner-la-censure

INFORMATIONS ACCESSIBLES GRÂCE AU DNS

- Adresse en fonction du nom,
- Nom en fonction de l'adresse IP : résolution inverse.
- Adresse de relais de messagerie.

STRUCTURATION DES NOMS DNS



HIERARCHIE PAR DOMAINE

www.education.gouv.fr.

machine **www** dans le domaine education, lui-même dans le domaine **gouv**, lui-même dans le domaine **fr.**

On omet en général la racine (le point=serveur racine) : www.education.gouv.fr**.**

Les majuscules ne sont pas significatives.

DNS EST UNE BASE DE DONNEES DISTRIBUEE

Une base de donnée est associée à chaque nœud.

- Un domaine est la partie de l'arborescence à partir du noeud portant son nom : Exemple : domaine **fr** : arborescence à partir du noeud **fr**
  - Dans un noeud, on trouve :
    1. les informations permettant de retrouver les noeuds fils
    2. les informations propre au noeud : liste des machines
  - La gestion de chaque noeud peut être effectuée par des entités différentes .

TERMINOLOGIE

ROOT-SERVERS

Nous avons au départ une série de 13 serveurs appelés **root-servers**. Nous en trouvons la liste et leur implantation dans le monde sur les sites

- http://root-servers.org
  - http://www.iana.org/domains/root/servers

Root Servers

The authoritative name servers that serve the DNS root zone, commonly known as the "root servers", are a network of hundreds of servers in many countries around the world. They are configured in the DNS root zone as 13 named authorities, as follows.

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	192.228.79.201	University of Southern California (ISI)
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	128.8.10.90, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	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	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	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, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Ces serveurs savent dire quels serveurs sont spécialisés dans les divers TLD (voir plus loin).

SERVEURS TLD (TOP LEVEL DOMAIN)

Ces serveurs savent dire quels sont les serveurs qui gèrent un domaine appartenant à ce TLD.

C'est à ce niveau que le registar intervient techniquement. Une fois le nom de domaine enregistré, le demandeur doit fournir l'adresse d'au moins un serveur qui saura résoudre les noms dans le domaine en question.

TLD (Top Level Domain)

- **TLD PAR PAYS** : ccTLD (country code TLD)

.fr .ru .eu .be ...

- **TLD INTERNATIONAUX** : gTLD (generic internationaux TLD)

.com (entreprise multinationale), .org (organisation), .edu (Université)

```
   .net (fournisseur d'accès), .pro (profession libérale)
```

.aero, .biz, .coop, .info, .museum, .name, .pro

L' **ICANN** (http://www.icann.org) est un organisme qui gère la liste des Top Level Domain (TLD): .com, .net, .org, .fr, .uk...

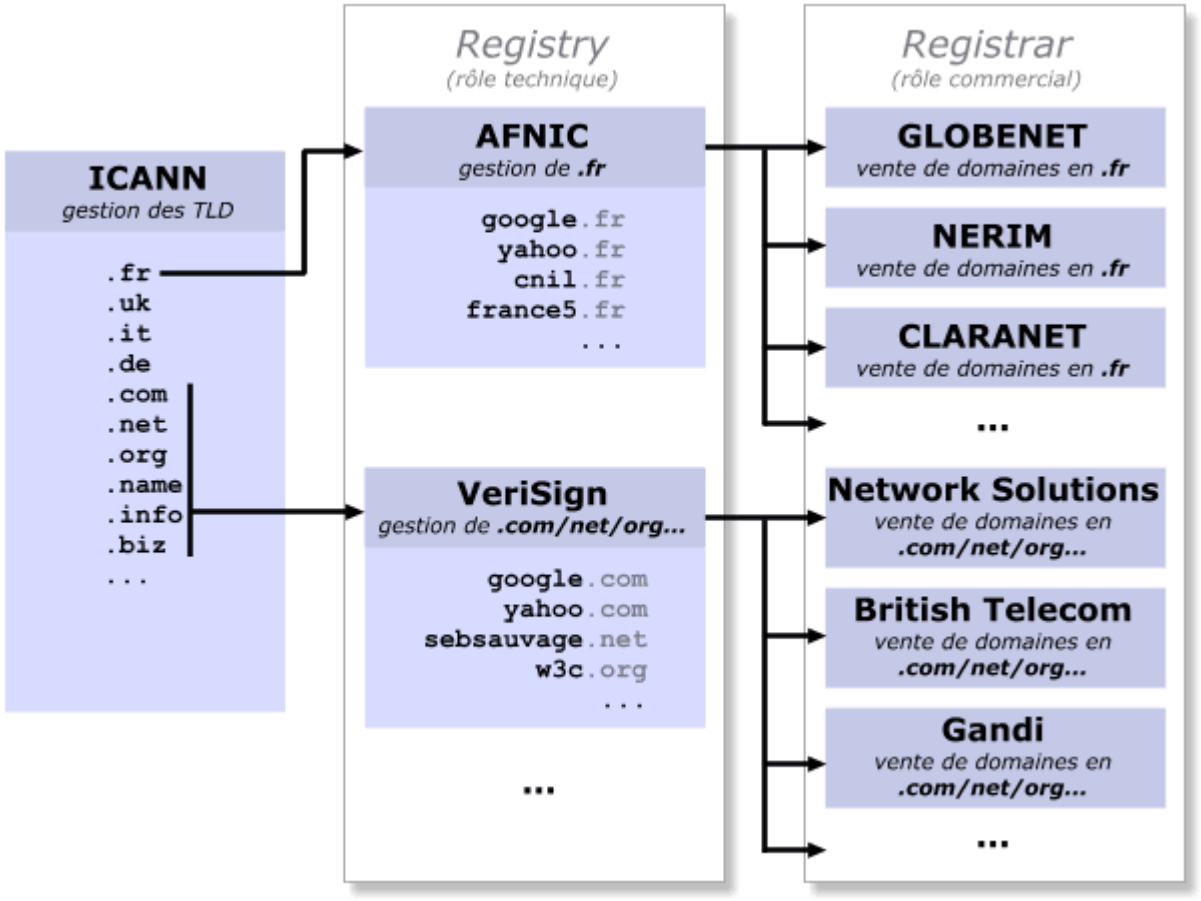
Il existe **une TLD par pays** (**.fr** pour France, **.it** pour Italie, **.de** pour l'Allemagne, etc.), ainsi que quelques TLD générales (**.com**, **.net**, **.org**,

.mil, **.biz**...).

Fin 2013, l'Internet a connu une nouvelle transformation importante. À l'initiative de l'Icann, l'organisme qui régule l'attribution des noms de domaine, des centaines de nouvelles extensions vont en effet voir le jour.

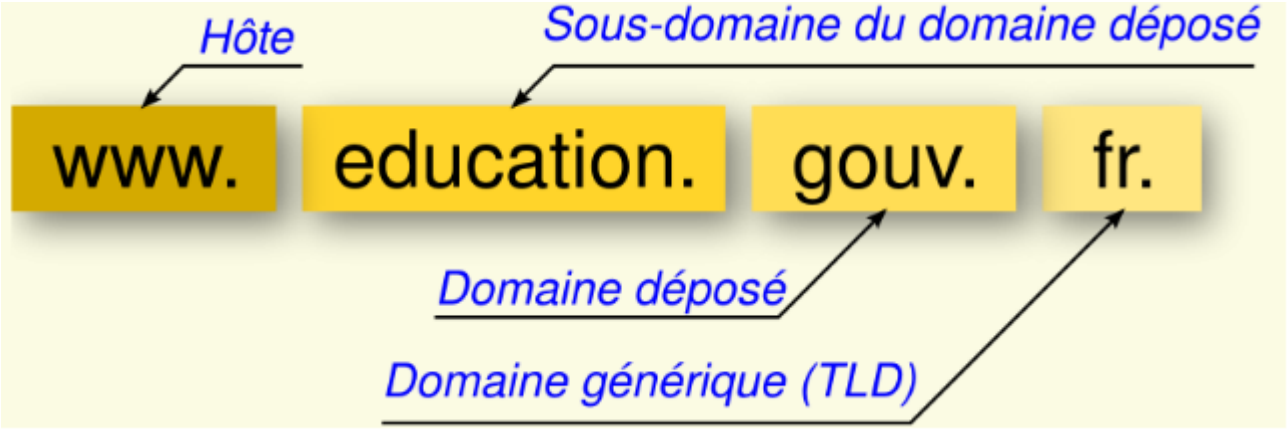
Aux emblématiques .com, .net et .org **s'ajouteront une multitude d'extensions génériques** (.cloud, .restaurant, .taxi...), **géographiques** (.alsace, .corsica, .tokyo...) **ou relatives à des marques** (.apple, .ferrari, .sony...).

L'ICANN délègue la gestion de chaque TLD à un organisme (appelé registry).



FQDN (Full Qualified Domain Name)

www.education.gouv.fr est un FDQN. En toute rigueur, il serait plus correct d'écrire www.education.gouv.fr**.** (**avec un point final**, subtile différence).



- la partie la plus à gauche représente toujours un hôte (une machine) ; (ici **www**)
- la partie la plus à droite représente toujours un domaine générique () ; (ici **fr.**)
- entre les deux, les éventuels sous-domaines et le domaine déposé de l'entité concernée. (ici un sous-domaine **education** et un domaine **gouv**)

Nous avons donc une structure arborescente dont l'origine est le fameux point final, que l'on omet généralement, mais qui existe bel et bien et qui représente la racine de l'arbre.

PRINCIPE DE FONCTIONNEMENT (BASE SUR LE MODELE CLIENT-SERVEUR)

LES SERVEURS DNS

Ils gèrent une base de données contenant :

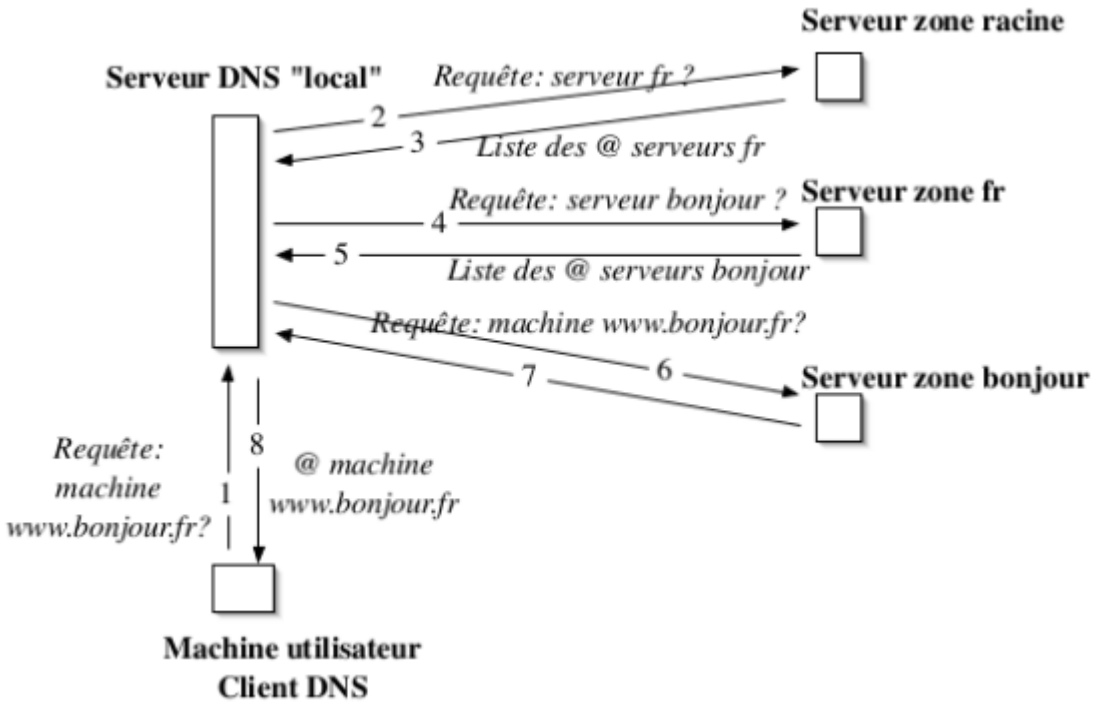
- nom/@IP des machines du domaine
    - nom/@IP des serveurs d'un sous-domaine

Le système DNS est un système robuste par redondance: plusieurs serveurs possèdent la base de données d'un domaine.

CLIENTS DNS

Un client DNS s'appuie sur un composant logiciel appelé « resolver » qui interroge un serveur DNS « de proximité » : serveur DNS local à l'entreprise, DNS FAI...

EXEMPLE D'UNE INTERROGATION DNS



VOUS VOULEZ ACHETER UN NOM DE DOMAINE ? PETIT GUIDE ANTI-ARNAQUE !

Il ne faut acheter un nom de domaine que chez un registrar agréé par l'ICANN.

La liste est là : registars autorisés

Cela vous évitera bien de mauvaises surprises. Et en cas de problème, l'ICANN possède un médiateur.

Pour savoir si vous êtes réellement propriétaire de votre domaine, faites un **whois.** Si vous n'apparaissez pas comme administrateur du domaine, vous vous êtes fait rouler !

Méfiance avec les noms de domaine gratuits. Généralement, ils ne peuvent pas être gratuits, il doit y avoir une contrepartie (souscription à un autre service payant, gratuité provisoire, superposition de publicités, etc.).

Acheter volontairement un nom de domaine (soit seul, soit avec un service d'hébergement web) est généralement plus sûr (pas de mauvaise surprise, comme avec les domaines “gratuits” en .tk).

Quand vous utilisez des redirecteurs gratuits comme Ulimit, V3, go.to ou Bigfoot, vous n'êtes pas propriétaire du domaine ! Vous êtes à la merci du propriétaire du domaine: il peut bloquer l'adresse, la rediriger vers ce qu'il veut ou vous couper l'accès.

Acheter un nom de domaine vous protège contre ce genre de mauvaise surprise. Et même en cas de litige avec votre registrar, les règles de l'ICANN vous permettent de changer de registrar sans perdre votre nom de domaine.

Dans les URL visibles dans votre navigateur, le nom de domaine est le mot qui précède immédiatement le TLD (.com, .net, .org...) avant le premier slash (/). Ne vous faites pas abuser ! http://www.sebsauvage.net : le nom de domaine est sebsauvage.net. http://kikoo.go.to/my_home.html , le nom de domaine est go.to, et non pas kikoo . http://kikoo.multimania.com/www.microsoft.com : le nom de domaine est multimania.com , pas microsoft.com ! http://www.microsoft.com:msdn@kikoo.multimania.com/show.html : le nom de domaine est multimania.com , pas microsoft.com !

Les domaines ne sont pas attribués à vie. Ce ne sont que des locations, à renouveler. Certains louent des noms de domaine à l'année, d'autres pour 10 ans. Si vous avez un nom de domaine, n'oubliez pas de le renouveler ! (Votre registrar est censé vous le rappeler avant la date d'expiration.) Ce genre de mésaventure est arrivé à Hotmail.com : Microsoft avait oublié de renouveler le nom de domaine. Il a été racheté par un particulier qui l'a gracieusement rendu à Microsoft.

Si votre site web est important commercialement, n'hésitez pas à acheter plusieurs noms de domaine proches.

METTRE EN PLACE SON SITE WEB AVEC SON PROPRE NOM DE DOMAINE

Vous avez besoin de 4 choses:

1. Acheter un nom de domaine: Il vous suffit de choisir un registrar (accrédité par l'ICANN) qui vend des noms de domaines dans la TLD qui vous intéresse (com/net/org/...) et de voir les conditions à remplir pour en obtenir un.

1. Faire héberger ses DNS: Une fois votre domaine acheté, vous devrez fournir à votre registrar l'adresse IP de 2 serveurs DNS qui répondront aux requêtes concernant votre domaine. Vous avez plusieurs possibilités pour faire héberger vos DNS:

   * Chez votre registrar: Beaucoup de registrars proposent d'héberger (à titre payant ou gracieux) vos DNS. C'est souvent la solution la plus rapide à mettre en place. * Chez votre hébergeur HTTP: Certains hébergeurs HTTP proposent également d'héberger aussi vos DNS, mais c'est rarement le cas des hébergeurs gratuits. * Chez un hébergeur de DNS. On peut trouver de nombreux hébergeurs spécialisés DNS dont certains sont gratuits, comme http://www.mydomain.com. * Chez vous, à condition d'avoir au minimum 2 serveurs DNS avec adresses IP fixes connectés en permanence.

2. Faire héberger son site web (HTTP). * Chez un hébergeur HTTP, gratuit ou payant. * Chez vous (entreprise ou particulier), si vous avez une connexion permanente à l'Internet et une adresse IP fixe. Si vous avez une adresse IP dynamique, c'est faisable également (il y a des astuces - voir plus loin).
3. Mettre en place la redirection afin que qcelui qui tape www.votredomaine.com arrive bien sur votre site web (là où il est hébergé).