Le système de nom de domaine (Domain Name system ou DNS)

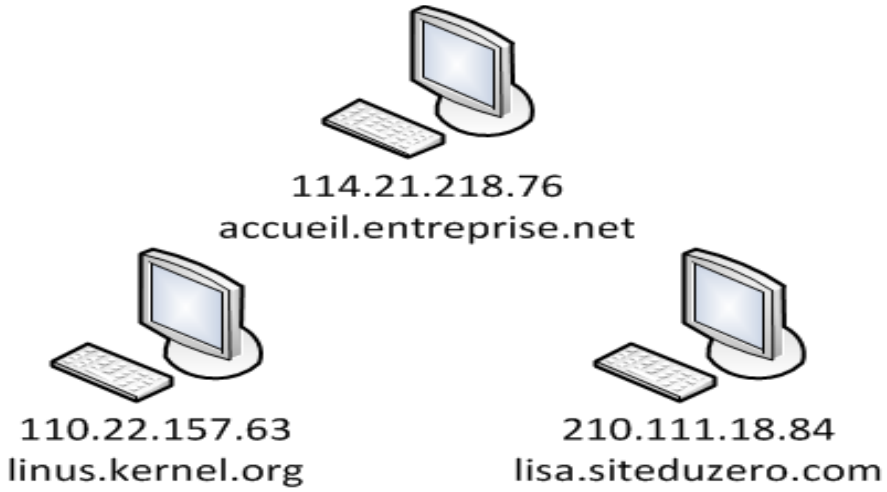
1.Introduction :

Les IP jouent un rôle fondamental dans l'identification des ordinateurs sur Internet, qui sont ainsi capables de se retrouver et de communiquer entre eux. Toutefois, pour un humain retenir une IP n'est pas facile (c'est déjà délicat pour 124.217.229.14, alors imaginez pour les nouvelles IP comme 1703:01b8:43c4:85a3:0000:0000:a213:bba7 !).

Pour résoudre ce problème, il serait possible d'associer un nom d'hôte à chaque machine, qui serait *équivalent* à écrire l'adresse IP. Ce nom d'hôte peut-être n'importe quel texte (comme `monordinateur`) mais il a le plus souvent la forme `accueil.entreprise.net`. Chaque ordinateur est identifiable soit par l'IP soit par le nom d'hôte :

2. Les noms d'hôte :

Les ordinateurs utilisent les adresses IP pour se repérer .Le nom d'hôte est seulement un *alias* qui revient à écrire l'IP.



Mais comment un ordinateur traduit-il un nom d'hôte que lui donne un humain en une adresse IP qu'il peut utiliser ?

La traduction *nom d'hôte => IP* est appelé **résolution d'hôte**.
L'opération inverse est aussi possible : *IP => nom d'hôte*. On parle de **résolution inverse**.

Pour traduire un nom d'hôte comme `lisa.siteduzero.com` en une IP comme 210.111.18.84, l'ordinateur a besoin d'une "table" qui contient toutes les équivalences.

3. Associer les IP et les noms d'hôtes :

Au début, cette fameuse table est crée sur chaque ordinateur dans un fichier appelé `hosts` (*hôtes* en anglais). Ce fichier existe toujours mais est très peu utilisé en pratique.

Si vous êtes sous Windows, vous pouvez le trouver dans C:\Windows\system32\drivers\etc\hosts (vous pouvez l'ouvrir avec Bloc-Notes).

Ce fichier a la forme suivante :

```
127.0.0.1       localhost
127.0.1.1       mateo21-desktop

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

On y trouve une équivalence IP / nom d'hôte par ligne.
Ainsi, on y lit qu'écrire 127.0.0.1 ou écrire localhost est équivalent. On y trouve par ailleurs des adresses IPv6 raccourcies (fe00::0 est une IPv6).

Ce système a quand même un défaut : pour que chaque ordinateur connaisse toutes les équivalences entre les IP et les noms d'hôtes, il faut recopier ce fichier sur tous les ordinateurs !

Et quand on ajoute un ordinateur sur le réseau, il faut rajouter une ligne dans chaque fichier hosts de chaque ordinateur pour qu'il connaisse le nouveau nom d'hôte !
Cette technique était viable à l'époque où les réseaux étaient encore très petits, mais aujourd'hui avec environ 4 milliards d'ordinateurs sur Internet (et il s'en rajoute chaque jour) c'est impossible à maintenir !

Pour résoudre ce problème, ils ont inventé un système intelligent et un peu complexe : les DNS.

4.Le système de nom de domaine (Domain Name system ou DNS) :

Devant la multiplication des ordinateurs sur le réseau, et donc des noms d'hôtes, Paul Mockapetris a inventé en 1983 les noms de domaine (Domain Name System, ou DNS).

Il s'agit d'un système hiérarchique qui permet de "découper" le réseau en un ensemble de domaines, eux-mêmes composés de sous-domaines, éventuellement composés de sous-sous-domaines, etc. Il y a donc plusieurs niveaux de domaines possibles.

4. 1 Les différents niveaux de domaine :

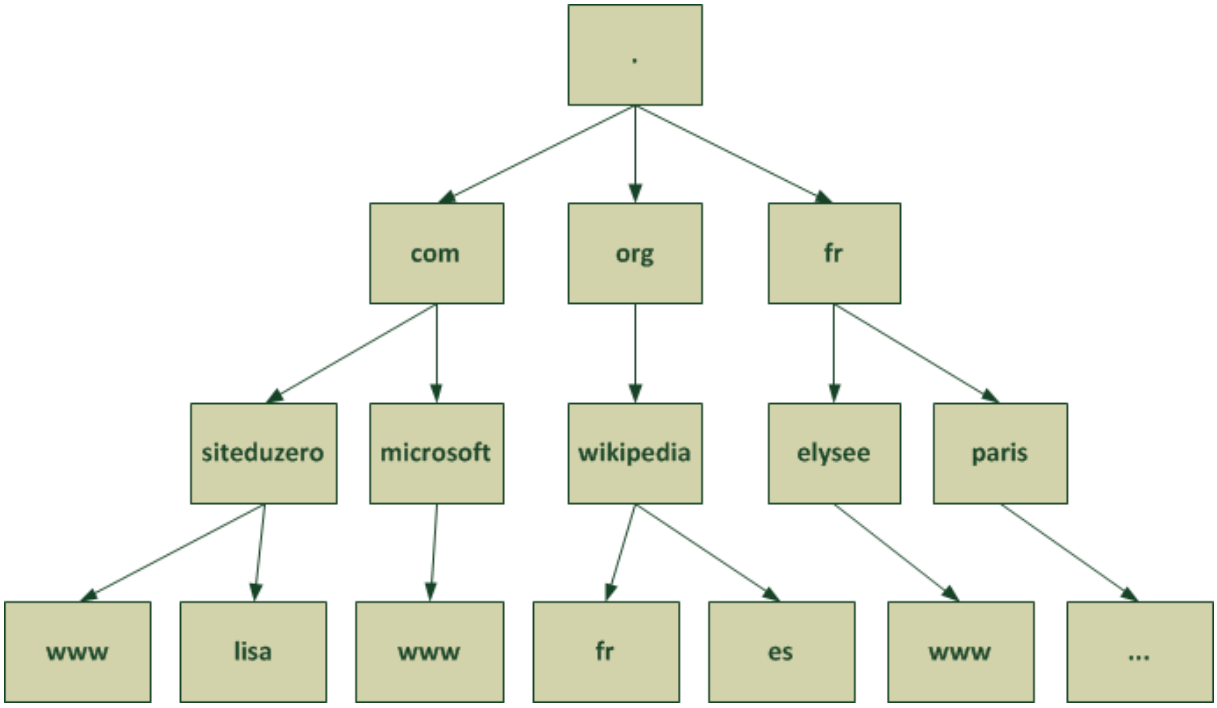
Prenons un nom de domaine que vous connaissez bien :

www.siteduzero.com

Il est composé de 3 niveaux de domaines, que l'on lit de droite à gauche :

1. **com** : c'est le domaine de premier niveau. On parle de "Top level domain", ou TLD.
2. **siteduzero** : en-dessous, il existe de très nombreux domaines de second niveau : **siteduzero**.com, **microsoft**.com, **apple**.com, **dell**.com...
3. **www** : chacun de ces domaines peut avoir des sous-domaines, le plus couramment utilisé sur le web étant "www". On a donc www.siteduzero.com, www.microsoft.com... Cela étant, ce n'est pas une obligation, et on peut imbriquer plusieurs sous-domaines.

Les domaines sont organisés **hiérarchiquement** entre eux comme ceci :



Comme vous le voyez, les domaines de premier niveau ("fr", "org", "com"...) dépendent d'un sommet appelé **racine** : c'est le point tout en haut du schéma.

Il peut y avoir jusqu'à 127 niveaux de domaines (aa.bb.cc.dd.ee.ff.[...].com). Chacun de ces niveaux est appelé label, constitué de 63 caractères maximum.
Le nom de domaine complet, appelé "Fully Qualified Domain Name" (FQDN) est constitué de tous les sous-domaines et inclut le point final représentant le serveur racine (**www.siteduzero.com.**). Il peut comprendre jusqu'à 253 caractères.

4.2 Les serveurs DNS :

Pour gérer ces très nombreux noms de domaines, et leurs sous-domaines, ils ont inventé un système de serveurs capables de gérer chacun un ou plusieurs niveaux de domaine. Ce sont les **serveurs DNS**.

Pourquoi créer plusieurs serveurs DNS ? Un seul serveur central ne suffirait pas ?

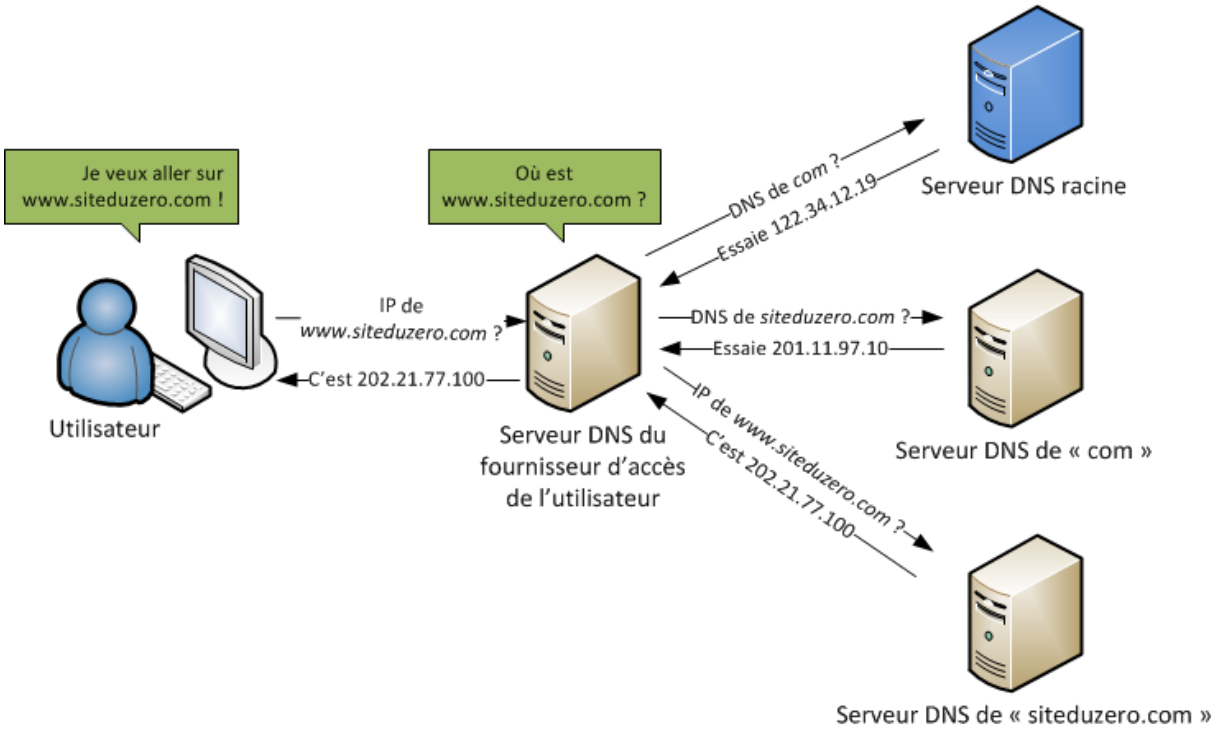
Non, car il serait trop fréquemment demandé. Imaginez que tous les ordinateurs du monde dépendent d'un seul serveur DNS pour connaître toutes les IP ! Si celui-ci venait à tomber en panne, Internet ne fonctionnerait tout simplement plus (et de toute façon un seul serveur ne peut pas supporter autant de requêtes).

Il y a plusieurs niveaux de serveurs :

- **Les serveurs racine** : au nombre de 13, nommés de a.root-servers.net à m.root-servers.net, ils contiennent l'adresse des serveurs DNS de chaque domaine de premier niveau (com, net, org, fr...).
- **Les serveurs DNS de premier niveau** : il y en a plusieurs par domaine ("com", "net", "fr"...). Ils connaissent l'adresse des serveurs DNS de chacun des sous-niveaux. Ainsi, les serveurs DNS du domaine "com" connaissent l'adresse des serveurs DNS qui gèrent siteduzero.com, microsoft.com, apple.com...
- **Les serveurs DNS de second niveau** : très nombreux, ce sont eux le plus souvent qui contiennent les équivalences nom de domaine / IP. Ainsi, le serveur DNS de siteduzero.com connaît tous les sous-domaines (www.siteduzero.com, lisa.siteduzero.com, scratchy.siteduzero.com, etc.) et connaît l'adresse IP de la machine qui gère chacun de ces domaines.

En plus de ces serveurs, chaque fournisseur d'accès à Internet (FAI) propose un serveur DNS qui fait office d'intermédiaire entre les internautes et les "vrais" serveurs DNS.

Alors, que se passe-t-il lorsqu'un visiteur demande à visiter un site web ? Voici comment cela fonctionne, résumé dans les grandes lignes dans un schéma :



Les serveurs qui connaissent réellement l'adresse IP associée à www.siteduzero.com sont appelés *serveurs DNS ayant autorité*. Sur ce schéma ci-dessus, il s'agit du serveur en bas à droite de l'image.

En pratique, il y a plusieurs serveurs à chaque fois :

- Il y a 13 serveurs racine, mais grâce à des fonctionnalités avancées de routage (appelées *anycast*), plusieurs centaines de serveurs peuvent se partager une même adresse IP. Il y a donc physiquement des centaines de serveurs qui gèrent la racine, mais "seulement" 13 IP différentes.
- Il y a plusieurs serveurs de premier niveau à chaque fois pour chaque domaine...
- Il y a aussi plusieurs serveurs DNS pour un domaine comme siteduzero.com (au moins 2) ce qui permet au système de continuer à fonctionner en cas de panne de l'un d'eux. Il y a donc toujours au moins un serveur DNS principal (primaire) et un serveur secondaire contacté en cas de panne du premier.

Le schéma précédent est volontairement simplifié. Plusieurs serveurs peuvent répondre à chacune des questions. C'est d'ailleurs pour cela que les serveurs disent "*Essaie* cette IP" : si l'IP ne répond pas il sera toujours possible de contacter d'autres serveurs qui possèdent la même information.

4.3 Les catégories de Domaines de haut niveau :

Il existe deux catégories de **TLD** (*Top Level Domain*, soit *domaines de plus haut niveau*) :

- Les domaines dits « génériques », appelés **gTLD** (*generic TLD*). Les gTLD sont des noms de domaines génériques de niveau supérieur proposant une classification selon le secteur d'activité. Ainsi chaque gTLD possède ses propres règles d'accès :
    - gTLD historiques :
        - **.arpa** correspond aux machines issues du réseau originel ;

        - **.com** correspondait initialement aux entreprises à vocation commerciale. Désormais ce TLD est devenu le « TLD par défaut » et l'acquisition de domaines possédant cette extension est possible, y compris par des particuliers.
        - **.edu** correspond aux organismes éducatifs ;
        - **.gov** correspond aux organismes gouvernementaux ;
        - **.int** correspond aux organisations internationales ;
        - **.mil** correspond aux organismes militaires ;
        - **.net** correspondait initialement aux organismes ayant trait aux réseaux. Ce TLD est devenu depuis quelques années un TLD courant. L'acquisition de domaines possédant cette extension est possible, y compris par des particuliers.
        - **.org** correspond habituellement aux entreprises à but non lucratif.</gras>
    - nouveaux gTLD introduits en novembre 2000 par l'ICANN :
        - **.aero** correspond à l'industrie aéronautique ;
        - **.biz** (*business*) correspondant aux entreprises commerciales ;
        - **.museum** correspond aux musées ;
        - **.name** correspond aux noms de personnes ou aux noms de personnages imaginaires ;
        - **.info** correspond aux organisations ayant trait à l'information ;
        - **.coop** correspondant aux coopératives ;
        - **.pro** correspondant aux professions libérales.</gras>
    - gTLD spéciaux :
        - **.arpa** correspond aux infrastructures de gestion du réseau. Le gTLD arpa sert ainsi à la résolution inverse des machines du réseau, permettant de trouver le nom correspondant à une adresse IP.
- Les domaines dits «nationaux », appelés **ccTLD** (country code TLD). Les ccTLD correspondent aux différents pays et leurs noms correspondent aux abréviations des noms de pays définies par la norme ISO 3166. Le tableau ci-dessous récapitule quelques ccTLDs.

Code	Pays
AE	Emirats Arabes Unis
AF	Afghanistan
AL	Albanie
AM	Arménie
AR	Argentine
BD	Bangladesh
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BH	Bahreïn
BI	Burundi
BJ	Bénin
BR	Brésil
CI	Côte d'Ivoire
CL	Chili
CM	Cameroun
DZ	Algérie
EG	Egypte
ES	Espagne
ET	Ethiopie