Le DNS

Domain name server

Table des matières

Qu'appelle-t-on DNS ?

Chaque ordinateur directement connecté à internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec un nom de domaine ou des adresses plus explicites (appelées addresses FQDN) du type www.google.com.

FQDN signifie Fully Qualified Domain Name, en français « nom de domaine complètement qualifié » (ou : « nom de domaine complet »). Le FQDN est l'adresse absolue d'un site Internet.

Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System).

On appelle résolution de noms de domaines (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.

Noms d'hôtes

Aux origines de TCP/IP, étant donné que les réseaux étaient très peu étendus ou autrement dit que le nombre d'ordinateurs connectés à un même réseau était faible, les administrateurs réseau créaient des fichiers appelés tables de conversion manuelle.

Ces tables de conversion manuelle étaient des fichiers séquentiels, généralement nommés hosts ou hosts.txt, associant sur chaque ligne l'adresse IP de la machine et le nom littéral associé, appelé nom d'hôte.

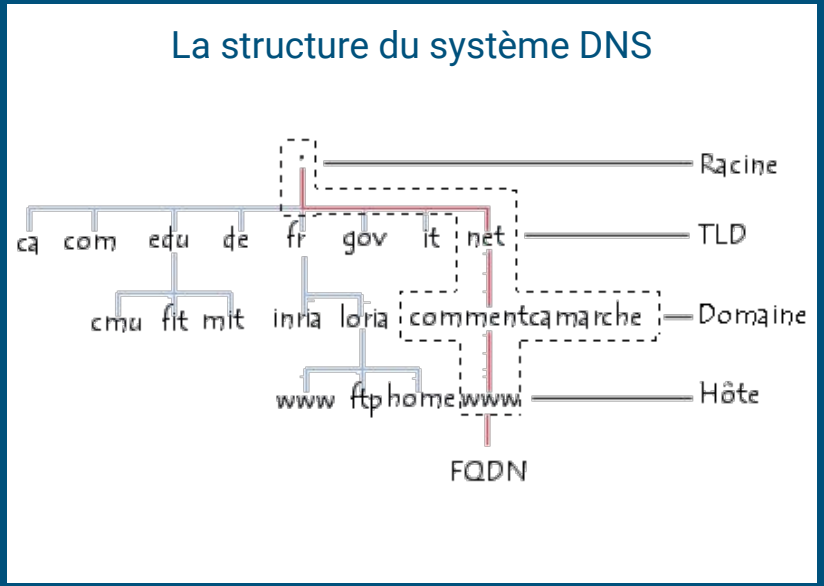
Le système précédent de tables de conversion nécessitait néanmoins la mise à jour manuelle des tables de tous les ordinateurs en cas d'ajout ou de modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallu mettre en place un système de gestion des noms hiérarchisé et plus facilement administrable. Le système nommé Domain Name System (DNS), traduisez Système de nom de domaine, a été mis au point en novembre 1983 par Paul Mockapetris (RFC 882 et RFC 883), puis révisé en 1987 dans les RFCs 1034 et 1035. Le DNS a fait l'objet depuis de nombreuses RFCs.

L'espace de noms

Ce système propose

- un espace de noms hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente, à la manière des systèmes de fichiers d'Unix.
- un système de serveurs distribués permettant de rendre disponible l'espace de noms.
- un système de clients permettant de « résoudre » les noms de domaines, c'est-à-dire interroger les serveurs afin de connaître l'adresse IP correspondant à un nom.

Nom de domaine



Les serveurs de noms

Les machines appelées serveurs de nom de domaine permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.

Chaque domaine possède un serveur de noms de domaines, appelé « serveur de noms primaire » (primary domain name server), ainsi qu'un serveur de noms secondaire (secondary domaine name server), permettant de prendre le relais du serveur de noms primaire en cas d'indisponibilité.

Chaque serveur de nom est déclaré dans à un serveur de nom de domaine de niveau immédiatement supérieur, ce qui permet implicitement une délégation d'autorité sur les domaines. Le système de nom est une architecture distribuée, où chaque entité est responsable de la gestion de son nom de domaine. Il n'existe donc pas d'organisme ayant à charge la gestion de l'ensemble des noms de domaines.

Les serveurs correspondant aux domaines de plus haut niveau (TLD) sont appelés « serveurs de noms racine ». Il en existe treize, répartis sur la planète, possédant les noms « a.root-servers.net » à « m.root-servers.net ».

Les serveurs de noms > (suite)

Un serveur de noms définit une zone, c'est-à-dire un ensemble de domaines sur lequel le serveur a autorité. Le système de noms de domaine est transparent pour l'utilisateur, néanmoins il ne faut pas oublier les points suivants :

Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server. Pas de panique: lorsque vous vous connectez à internet, le fournisseur d'accès va automatiquement modifier vos paramètres réseau pour vous mettre à disposition ces serveurs de noms.

L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) doit également être définie : le serveur de noms secondaire peut relayer le serveur de noms primaire en cas de dysfonctionnement.

Le serveur le plus répandu s'appelle BIND (Berkeley Internet Name Domain). Il s'agit d'un logiciel libre disponible sous les systèmes UNIX, développé initialement par l'université de Berkeley en Californie et désormais maintenu par l'ISC (Internet Systems Consortium).

Résolution de noms de domaine

Le mécanisme consiste à trouver l'adresse IP correspondant au nom d'un hôte est appelé « résolution de nom de domaine ». L'application permettant de réaliser cette opération (généralement intégrée au système d'exploitation) est appelée « résolveur » (en anglais « resolver »).

Outil windows et mac : nslookup

Ouvrir la console terminal

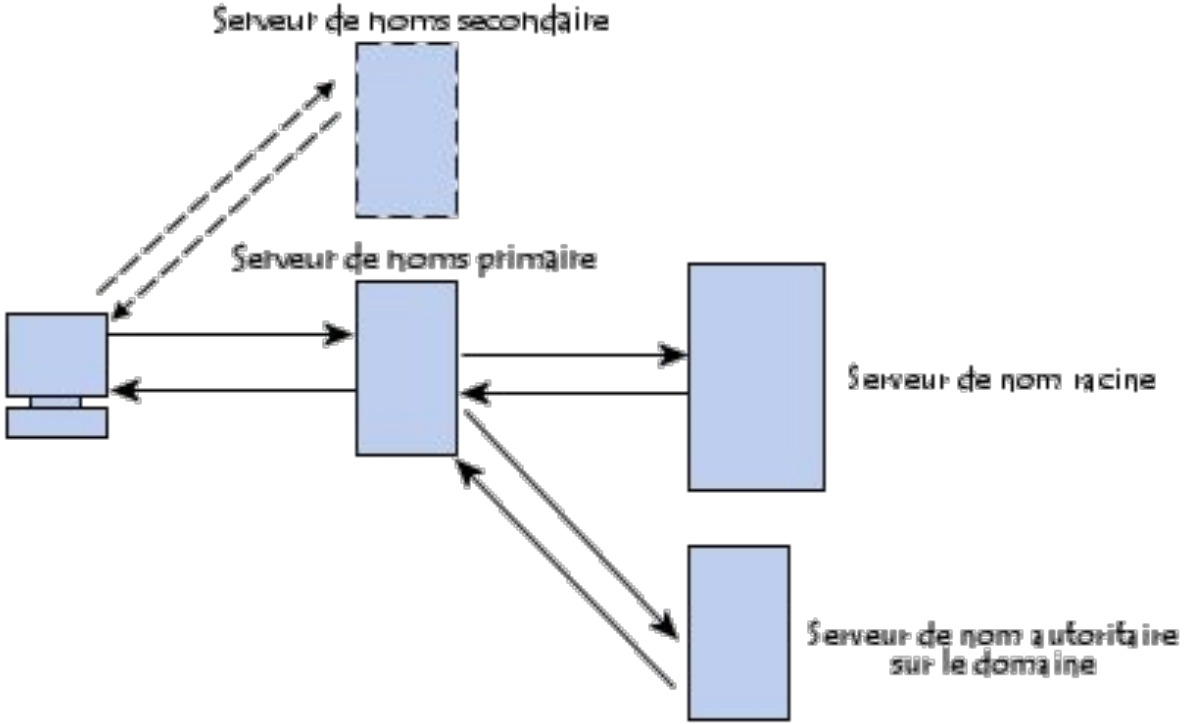
ou le command prompt sous windows

> nslookup

> set q=(voir tableau)

Set queries	Description
set q=a	To know the IP address
set q=any	To know all types of data
set q=CNAME	To know the Canonical name
set q=MB	To know the Mailbox domain name
set q=MX	To know about the mail exchange server
set q=SOA	To know about the Start-Of-Authority of a DNS Zone
set q=WKS	To know about the Well Known service

Résolution de noms de domaine > (suite)



Types d'enregistrements

Un DNS est une base de données répartie contenant des enregistrements, appelés **RR** (*Resource Records*), concernant les noms de domaines. Seules sont concernées par la lecture des informations ci-dessous les personnes responsables de l'administration d'un domaine, le fonctionnement des serveurs de noms étant totalement transparent pour les utilisateurs.

En raison du système de cache permettant au système DNS d'être réparti, les enregistrements de chaque domaine possèdent une durée de vie, appelée **TTL** (*Time To Live*, traduisez *espérance de vie*), permettant aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier.

D'une manière générale, un enregistrement DNS comporte les informations suivantes :

Nom de domaine (FQDN)	TTL	Type	Classe	RData
www.commentcamarche.net.	3600	A	IN	163.5.255.85

- **Nom de domaine** : le nom de domaine doit être un nom FQDN, c'est-à-dire être terminé par un point. Si le point est omis, le nom de domaine est relatif, c'est-à-dire que le nom de domaine principal suffixera le domaine saisi ;
- **Type** : une valeur sur 16 bits spécifiant le type de ressource décrit par l'enregistrement. Le type de ressource peut être un des suivants :
  - **A** : il s'agit du type de base établissant la correspondance entre un nom canonique et une adresse IP. Par ailleurs il peut exister plusieurs enregistrements A, correspondant aux différentes machines du réseau (serveurs).
  - **CNAME** (*Canonical Name*) : il permet de faire correspondre un alias au nom canonique. Il est particulièrement utile pour fournir des noms alternatifs correspondant aux différents services d'une même machine.
  - **HINFO** : il s'agit d'un champ uniquement descriptif permettant de décrire notamment le matériel (CPU) et le système d'exploitation (OS) d'un hôte. Il est généralement conseillé de ne pas le renseigner afin de ne pas fournir d'éléments d'informations pouvant se révéler utiles pour des pirates informatiques.
  - **MX** (*Mail eXchange*) : correspond au serveur de gestion du courrier. Lorsqu'un utilisateur envoie un courrier électronique à une adresse (utilisateur@domaine), le serveur de courrier sortant interroge le serveur de nom ayant autorité sur le domaine afin d'obtenir l'enregistrement MX. Il peut exister plusieurs MX par domaine, afin de fournir une redondance en cas de panne du serveur de messagerie principal. Ainsi l'enregistrement MX permet de définir une priorité avec une valeur pouvant aller de 0 à 65 535 :

    ```
    www.commentcamarche.net.                IN MX 10 mail.commentcamarche.net.
    ```

  - **NS** : correspond au serveur de noms ayant autorité sur le domaine.
  - **PTR** : un pointeur vers une autre partie de l'espace de noms de domaines.
  - **SOA** (*Start Of Authority*) : le champ SOA permet de décrire le serveur de nom ayant autorité sur la zone, ainsi que l'adresse électronique du contact technique (dont le caractère « @ » est remplacé par un point).
- **Classe** : la classe peut être soit **IN** (correspondant aux protocoles d'internet, il s'agit donc du système utilisé dans notre cas), soit **CH** (pour le système chaotique) ;
- **RDATA** : il s'agit des données correspondant à l'enregistrement. Voici les informations attendues selon le type d'enregistrement :
  - A : une adresse IP sur 32 bits ;
  - CNAME : un nom de domaine ;
  - MX : une valeur de priorité sur 16 bits, suivi d'un nom d'hôte ;
  - NS : un nom d'hôte ;
  - PTR : un nom de domaine ;
  - SOA : plusieurs champs.

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.
  - 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.
  - 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 la liste des ccTLD.

Qu'est-ce qu'un nom de domaine ?

Un site internet est défini par son URL. Ainsi, un site hébergé par un hébergeur gratuit (par exemple un fournisseur d'accès à internet) possède généralement une adresse du type :

`http://www.votre-fournisseur.com/votrenom`

Ce type d'adresse est assez difficile à mémoriser, ainsi une adresse telle que la suivante est préférable :

`http://www.votrenom.com`

Utilité du nom de domaine

Un site internet possèdant son propre nom de domaine, est beaucoup plus facile à mémoriser. Ainsi, un visiteur reviendra plus facilement sur un site dont le nom est facile à retenir que sur un site dont le nom est extrêmement compliqué.

De plus, un nom de domaine bien choisi favorisera le bouche à oreille et permettra au site de gagner plus vite en popularité.

Enfin, un nom de domaine donne généralement une touche de professionnalisme et de crédibilité à un site internet, et provoque chez l'internaute un sentiment de confiance plus fort.

Choix du nom de domaine

Etant donné que le nom de domaine doit être facile à diffuser, il est indispensable de le choisir le plus simple possible. Il est évident qu'un nom de domaine n'est pas qu'une liste complexe de caractères, il doit être choisi à bon escient en évitant les écueils suivants :

- choisir des noms compliqués
- choisir des noms trop longs (www.commentcamarche.net est déjà limite)
- mettre des caractères spéciaux tels que sous-tirets (_) (il sera plus aisé de dire «comment ça marche point net tout attaché » que « comment tiret du haut ça tiret du haut marche point net »)

De plus le nom de domaine doit :

- être prononçable ;
- avoir dans la mesure du possible une signification ;
- être disponible.

Vérifier la disponibilité d'un nom

Il existe des outils (fournis par les organisations en charge des noms de domaine), appelés Whois, permettant de vérifier la disponbibilité d'un nom de domaine, voire d'en connaître son propriétaire.

Références

Livre : DNS and BIND by Paul Albiz & Cricket Liu, O'REILLY
Web :
https://web.maths.unsw.edu.au/~lafaye/CCM/internet/dns.htm
https://web.maths.unsw.edu.au/~lafaye/CCM/web/webdomain.htm

Démo

Gérer le DNS dans CPanel