

# DNS (Système de noms de domaine)

Septembre 2015

1. [Qu'appelle-t-on DNS ?](#)
2. [Noms d'hôtes](#)
3. [Introduction au Domain Name System](#)
4. [L'espace de noms](#)
5. [Les serveurs de noms](#)
6. [Résolution de noms de domaine](#)
7. [Types d'enregistrements](#)
8. [Domaines de haut niveau](#)
9. [Voir aussi...](#)

## 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 adresses FQDN) du type *[www.commentcamarche.net]*.

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*.

## Introduction au Domain Name System

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

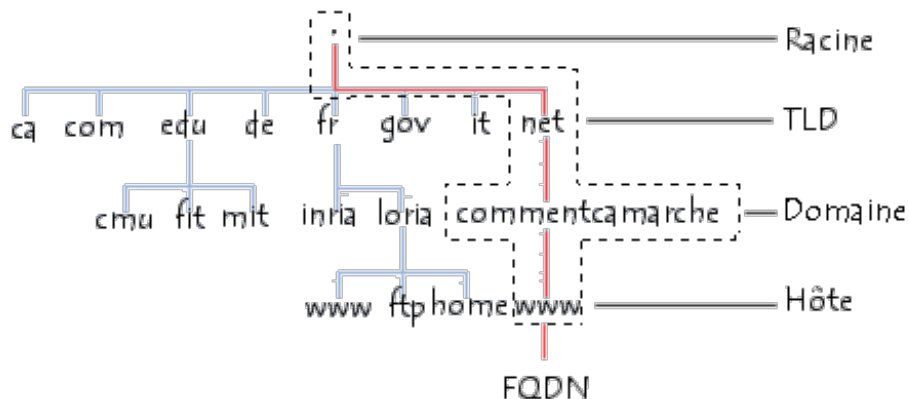
*Système de nom de domaine*, a été mis au point en novembre 1983 par Paul Mockapetris (RFC 882 et RFC 883), puis révisé en 1987 dans les RFCs 1034 et 1035. Le DNS a fait l'objet depuis de nombreuses RFCs.

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.

## L'espace de noms

La structuration du système DNS s'appuie sur une structure arborescente dans laquelle sont définis des domaines de niveau supérieurs (appelés **TLD**, pour *Top Level Domains*), rattachés à un noeud racine représenté par un point.



On appelle « **nom de domaine** » chaque noeud de l'arbre. Chaque noeud possède une étiquette (en anglais « *label* ») d'une longueur maximale de 63 caractères.

L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque noeud est séparé du suivant par un point (« . »).

L'extrémité d'une branche est appelée **hôte**, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine. A titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom *www*.

Le mot « **domaine** » correspond formellement au suffixe d'un nom de domaine, c'est-à-dire l'ensemble des étiquettes de noeuds d'une arborescence, à l'exception de l'hôte.

Le nom absolu correspondant à l'ensemble des étiquettes des noeuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé

**adresse FQDN** (*Fully Qualified Domain Name*, soit *Nom de Domaine Totalement Qualifié*). La profondeur maximale de l'arborescence est de 127 niveaux et la longueur maximale d'un nom FQDN est de 255 caractères. L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux. Ainsi *www.commentcamarche.net.* représente une adresse FQDN.

## 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 domain 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 ».

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*).

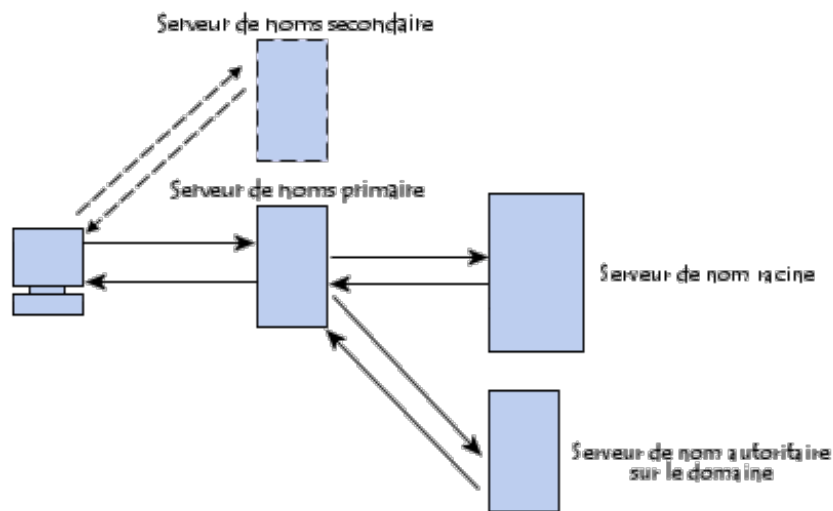
## Résolution de noms de domaine

Le mécanisme consistant 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* »).

Lorsqu'une application souhaite se connecter à un hôte connu par son nom de domaine (par exemple « *www.commentcamarche.net* »), celle-ci va interroger un serveur de noms défini dans sa configuration réseau. Chaque machine connectée au réseau possède en effet dans sa configuration les adresses IP de deux serveurs de noms de son fournisseur d'accès.

Une requête est ainsi envoyée au premier serveur de noms (appelé « serveur de nom primaire »). Si celui-ci possède l'enregistrement dans son cache, il l'envoie à l'application, dans le cas contraire il interroge un serveur racine (dans notre cas un serveur racine correspondant au TLD « .net »). Le serveur de nom racine renvoie une liste de serveurs de noms faisant autorité sur le domaine (dans le cas présent les adresses IP des serveurs de noms primaire et secondaire de *commentcamarche.net*).

Le serveur de noms primaire faisant autorité sur le domaine va alors être interrogé et retourner l'enregistrement correspondant à l'hôte sur le domaine (dans notre cas *www*).



## 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 révéifier.

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 :

- **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.</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 la liste des ccTLD.

Code	Pays
AC	Ile de l'Ascension
AD	Andorre
AE	Emirats Arabes Unis
AF	Afghanistan
AG	Antigua et Barbuda
AI	Anguilla
AL	Albanie
AM	Arménie
AN	Antilles Néerlandaises
AO	Angola
AQ	Antarctique
AR	Argentine
AS	Samoa Américaines
AT	Autriche
AU	Australie
AW	Aruba
AZ	Azerbaïdjan
BA	Bosnie-Herzégovine
BB	Barbade

BD	Bangladesh
BE	Belgique
BF	Burkina Faso
BG	Bulgarie
BH	Bahreïn
BI	Burundi
BJ	Bénin
BM	Bermudes
BN	Brunei
BO	Bolivie
BR	Brésil
BS	Bahamas
BT	Bhoutan
BV	Ile Bouvet
BW	Botswana
BY	Biélorussie
BZ	Belize
CA	Canada
CC	Iles Cocos
CD	République démocratique du Congo
CF	République Centrafricaine
CG	Congo
CH	Suisse
CI	Côte d'Ivoire
CK	Iles Cook
CL	Chili
CM	Cameroun
CN	Chine
CO	Colombie
COM	Organisme à but commercial
CR	Costa Rica

CU	Cuba
CV	Cap Vert
CX	Ile Christmas
CY	Chypre
CZ	République Tchèque
DE	Allemagne
DJ	Djibouti
DK	Danemark
DM	Dominique
DO	République Dominicaine
DZ	Algérie
EC	Equateur
EDU	Organisme ayant un rapport avec l'éducation
EE	Estonie
EG	Egypte
EH	Sahara Occidental
ER	Erythrée
ES	Espagne
ET	Ethiopie
EU	Europe
FI	Finlande
FJ	Fidji
FK	Iles Falkland (Malouines)
FM	Micronésie
FO	Iles Féroé
FR	France
FX	France (Territoire Européen)
GA	Gabon
GB	Grande-Bretagne
GD	Grenade
GE	Géorgie



GF	Guyane Française
GG	Guernesey
GH	Ghana
GI	Gibraltar
GL	Groenland
GM	Gambie
GN	Guinée
GOV	Organisme gouvernemental
GP	Guadeloupe
GQ	Guinée Equatoriale
GR	Grèce
GS	Géorgie du Sud
GT	Guatemala
GU	Guam (USA)
GW	Guinée-Bissau
GY	Guyana
HK	Hong Kong
HM	Iles Heard and McDonald
HN	Honduras
HR	Croatie
HT	Haïti
HU	Hongrie
ID	Indonésie
IE	Irlande
IL	Israël
IM	Ile de Man
IN	Inde
IO	Territoires Britanniques de l'océan Indien
IQ	Irak
IR	Iran
IS	Islande

IT	Italie
JM	Jamaïque
JO	Jordanie
JP	Japon
KE	Kenya
KG	Kirghizistan
KH	Cambodge
KI	Kiribati
KM	Comores
KN	Saint Kitts et Nevis
KP	Corée du Nord
KR	Corée du Sud
KW	Koweït
KY	Iles Caïmans
KZ	Kazakhstan
LA	Laos
LB	Liban
LC	Sainte-Lucie
LI	Liechtenstein
LK	Sri Lanka
LR	Libéria
LS	Lesotho
LT	Lituanie
LU	Luxembourg
LV	Lettonie
LY	Libye
MA	Maroc
MC	Monaco
MD	Moldavie
MG	Madagascar
MH	Iles Marshall

MK	Macédoine
ML	Mali
MIL	Organisme militaire
MM	Myanmar
MN	Mongolie
MO	Macao
MP	Iles Marianne du Nord
MQ	Martinique
MR	Mauritanie
MS	Montserrat
MU	Ile Maurice
MV	Maldives
MW	Malawi
MX	Mexique
MY	Malaisie
MZ	Mozambique
NA	Namibie
NC	Nouvelle-Calédonie
NE	Niger
NET	Organisme ayant un rapport avec Internet
NF	Iles Norfolk
NG	Nigeria
NI	Nicaragua
NL	Pays-Bas
NO	Norvège
NP	Népal
NR	Nauru
NT	Zone Neutre
NU	Niue
NZ	Nouvelle-Zélande
OM	Oman

ORG	Organisme non référencé
PA	Panamá
PE	Pérou
PF	Polynésie française
PG	Papouasie Nouvelle-Guinée
PH	Philippines
PK	Pakistan
PL	Pologne
PM	Saint-Pierre et Miquelon
PN	Pitcairn
PR	Porto Rico (USA)
PS	Territoires palestiniens
PT	Portugal
PY	Paraguay
PW	Palau
QA	Qatar
RE	Réunion
RO	Roumanie
RU	Fédération Russe
RW	Rwanda
SA	Arabie Saoudite
SB	Iles Salomon
SC	Seychelles
SD	Soudan
SE	Suède
SG	Singapour
SH	Sainte-Hélène
SI	Slovénie
SJ	Iles Svalbard et Jan Mayen
SK	République Slovaque
SL	Sierra Leone

SM	San Marin
SN	Sénégal
SO	Somalie
SR	Surinam
ST	Sao Tomé et Principe
SU	Union Soviétique
SV	Salvador
SY	Syrie
SZ	Swaziland
TC	Iles Turks et Caicos
TD	Tchad
TF	Territoire Austral Français
TG	Togo
TH	Thaïlande
TJ	Tadjikistan
TK	Tokelau
TM	Turkménistan
TN	Tunisie
TO	Tonga
TP	Timor Est
TR	Turquie
TT	Trinité et Tobago
TV	Tuvalu
TW	Taïwan
TZ	Tanzanie
UA	Ukraine
UG	Ouganda
UK	Royaume-Uni
UM	US Minor Outlying Islands
US	Etats-Unis
UY	Uruguay

UZ	Ouzbékistan
VA	Cité du Vatican
VC	Saint-Vincent et Grenadines
VE	Venezuela
VG	Iles Vierges Britanniques
VI	Iles Vierges Américaines
VN	Viêt Nam
VU	Vanuatu
WF	Wallis et Futuna
WS	Samoa de l'Ouest
YE	Yémen
YT	Mayotte
YU	Yougoslavie
ZA	Afrique du Sud
ZM	Zambie
ZR	Zaïre
ZW	Zimbabwe

## Voir aussi...

- [Les noms de domaine](#)

[◀ Précédent](#)

- [1](#)
- [2](#)
- [3](#)
- [4](#)
- [5](#)
- [6](#)
- [7](#)
- [8](#)
- [9](#)
- [10](#)

[Suivant ▶](#)



Réalisé sous la direction de Jean-François PILLOU,  
fondateur de CommentCaMarche.net.

Ce document intitulé « DNS (Système de noms de domaine) » issu de **CommentCaMarche** ([www.commentcamarche.net](http://www.commentcamarche.net)) est mis à disposition sous les termes de la licence Creative Commons. Vous pouvez copier, modifier des copies de cette page, dans les conditions fixées par la licence, tant que cette note apparaît clairement.