

# DNS ET BIND

*Présenté par* **EDORH Hervé Séno**  
**INGÉNIEUR EN SYSTÈME D'INFORMATION**  
**ADMINISTRATEUR SYSTÈME LINUX/UNIX**

# INTRODUCTION AU DNS

DNS signifie DOMAIN NAME SYSTEM. Sa naissance est reliée à la naissance de l'internet. Il est plus aisé de retenir des noms que des numéros de carte d'identité ou de téléphone portable. Ainsi il est difficile de retenir les adresses IP des machines que le nom des machine car avec internet par exemple en 2005 avait plus de 50 millions de site internet. Le concept de « serveur de nom » est apparu dans le milieu des années 1970 et standardisé en 1987.

# INTRODUCTION AU DNS

Tout au début on utilisait une table de correspondances entre les noms de machines et leurs adresses ip, table qui était stockée dans un fichier « hosts » dans les système \*.NIX on les trouve dans le fichier **/etc/hosts**. Cette méthode s'est vu dépassée avec l'augmentation des ressources informatiques dans les réseaux

# INTRODUCTION AU DNS

Ensuite est apparu le **Network Information System (NIS)** développé par SUN MICROSYSTEMS. Il conserve le fichier hosts ainsi que certaines informations, dans une base de données sur une machine maître depuis laquelle les clients peuvent récupérer à tout moment ce dont ils ont besoin,

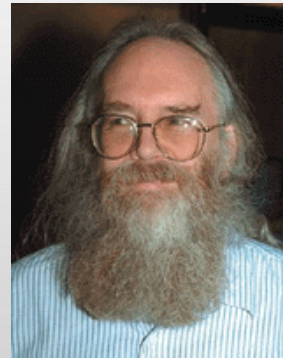
# INTRODUCTION AU DNS

Au fur et à mesure de l'augmentation des ressources les réseaux, il est apparu 3 problèmes :

1. Problème d'organisation: la base de données devenant de plus en plus lourdes, les requêtes vers cette dernière devenaient lentes ainsi donc, il fallait trouver une solution pour indexer et organiser les noms,
2. Problème de charge: dès que toutes les ressources du réseaux faisaient une requête vers le serveur de nom, la charge du serveur devenait de plus en plus lourde. Il fallait trouver une solution pour décharger et éparpiller la charge à travers le nombre de serveur de nom
3. Problème de gestion: Lorsque les administrateurs voulaient mettre à jour les enregistrements au même moment survenait des problèmes de gestion. Il fallait une méthode pour séparer l'administration (la délégation) des noms d'enregistrement (name records)

# INTRODUCTION AU DNS

En 1983-1984, une nouvelle méthode de résolution des noms fut adoptée. il s'agit du **DOMAIN NAME SYSTEM (DNS)**. Il fut l'oeuvre de **PAUL MOCKAPETRIS** et **JON POSTEL** qui règle simultanément les problèmes précédemment évoqués.



# INTRODUCTION AU DNS

Les standards **RFC (Request For Comment)** définissent la fonctionnalité DNS de base principalement le **RFC 1034** et **RFC 1035**. Tous deux ont été écrits vers les années 1987 par le **Dr Paul Mockapetris** au département **INFORMATION SCIENCES INSTITUTE OF THE UNIVERSITY OF SOUTHERN CALIFORNIA**. Bien que de nombreux RFC ultérieurs ont modifié certains comportements DNS, la fonctionnalité de base reste intacte. Ceci est en effet une réalisation remarquable

# INTRODUCTION AU DNS

Quand un serveur DNS est dans un réseau, toutes les machines (host) n'ont besoin que de connaître l'adresse physique du serveur du nom de la ressource (machine) qu'elle veulent accéder. Pour un site web par exemple ([www.exemple.com](http://www.exemple.com)), l'adresse entière de la ressource est retrouvée par requêtes envoyées au serveur de nom qui retrouve l'adresse du serveur où est hébergé le site web.

Un serveur de nom n'est autre qu'une base de données spéciale qui traduit les noms des ressources en adresse physique des machines.

# DOMAINE ET DÉLÉGATION

DNS (DOMAIN NAME SYSTEM) utilise un arbre de nom structuré. En haut de l'arbre « racine » (root) se trouve des nœuds: *Top-Level-Domains* (TLDs), le *Second-Levels-Domains* (SLD) et suivit par d'autres nœuds.

**www.google.com.**

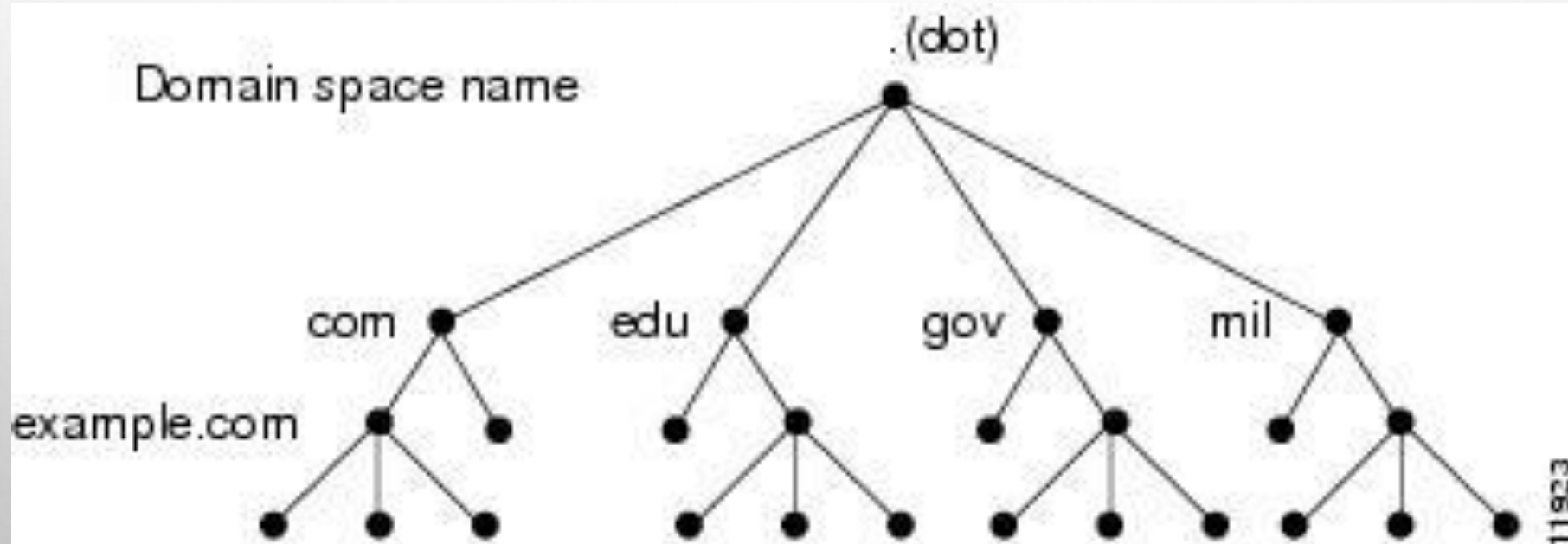
**.com ⇔ TLD**

**google ⇔ SLD**

**www ⇔ autre nœud**

donc un nom de domaine est sous la forme SLD.TLD

# DOMAINE ET DÉLÉGATION



# TLD

Il existe deux sortes de TLD

1. Generic Top Level Domains (gTLD): .com, .edu, .net, .org, .mil
2. Country Code Top-Level Domains (ccTLD): .us, .ca, .tv, .uk

# DOMAIN AUTHORITY ET DELEGATION

Le concept d'**authority** (autorité) et de **delegation** (délégation) viennent principalement de la hiérarchie des DNS et de leur organisation. A chaque nœud d'un nom de domaine est assigné à une autorité (authority). C'est une organisation responsable de la gestion du nœud. On parle d'administrer un nœud autoritairement (authoritatively).

L'autorité du domaine root est gérée par l'ICANN (Internet Corporation for Assigned Numbers and Names). Depuis 1998 l'ICANN assume cette responsabilité qui lui a été confié par l'United States Department of Commerce

# ICANN

Le but principal de l'ICANN est la gestion commercial des noms des domaines hiérarchiques. Pour faciliter cette compétition il a créé le concept de « accredited registrar » ou registrar accrédité. Les registrar sont des organisations à qui l'ICANN délègue des responsabilités limités dans la vente et l'administration des noms des domaines hiérarchiques.

Les gTLD sont autoritairement géré par l'ICANN et délégué à des registrar accrédités. Les ccTLD sont délégués par l'ICANN au pays pour leur administration

# ICANN

Dans les cas des ccTLDs, certains pays comme les Etats Unis (.us) et le Canada (.ca) ont décidé d'administrer leur nœud national et l'on délégué à chaque Etat en utilisant deux caractères état/province.

**.ny = New York, .qc = Quebec**

Ainsi **exemple.us** est le nom de domaine de « exemple » qui était délégué au « US national ccTLD administration » et **exemple.ny.us** est le nom de domaine « exemple » qui a été délégué à l'état de New York au Etat Unis

# ICANN

En résumé le nom de domaine:

[www.example.com](http://www.example.com)

est constitué de `www` et de `example.com`. Le nom de domaine « `example.com` » a été **délégué** à un gTLD registrar qui a son tour lui a été **délégué** par l'ICANN. Le propriétaire du « `www` » devient l'**autorité de délégation** du nom de domaine `example.com`. Le « `www` » est le hostname (le nom host) d'une ressource du réseau. Il faut garder en tête que ce n'est que par convention que les sites web, ont le `www` comme nom host

# ICANN

Considérons le nom:

[www.us.example.com](http://www.us.example.com)

La parti « us » est le sous domaine donc l'autorité de « exemple.com ». L'autorité de délégation de « exemple.com » a décidé de subdivisé ses noms de domaine en « country-based subdomain » (sous domaine basé sur les pays). Pour finir, l'autorité de délégation peut déléguer n'importe comment son nom de domaine et le propriétaire délégué est aussi responsable de l'administration de la délégation

# FQDN

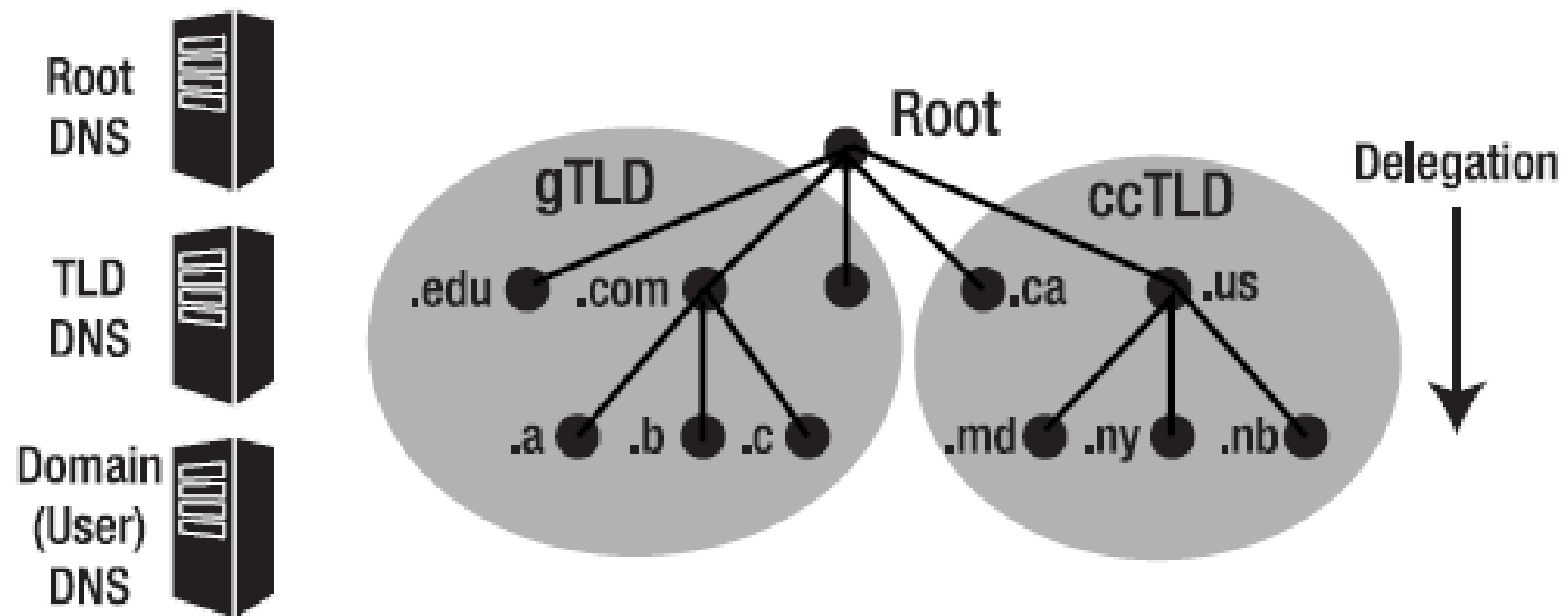
FULLY QUALIFIED DOMAIN NAMES (FQDN) définit un nom de domaine du « root » et donc doit se terminer par un « . »

[www.exemple.com](http://www.exemple.com) n'est pas un FQDN. Mais [www.exemple.com.](http://www.exemple.com) En est un

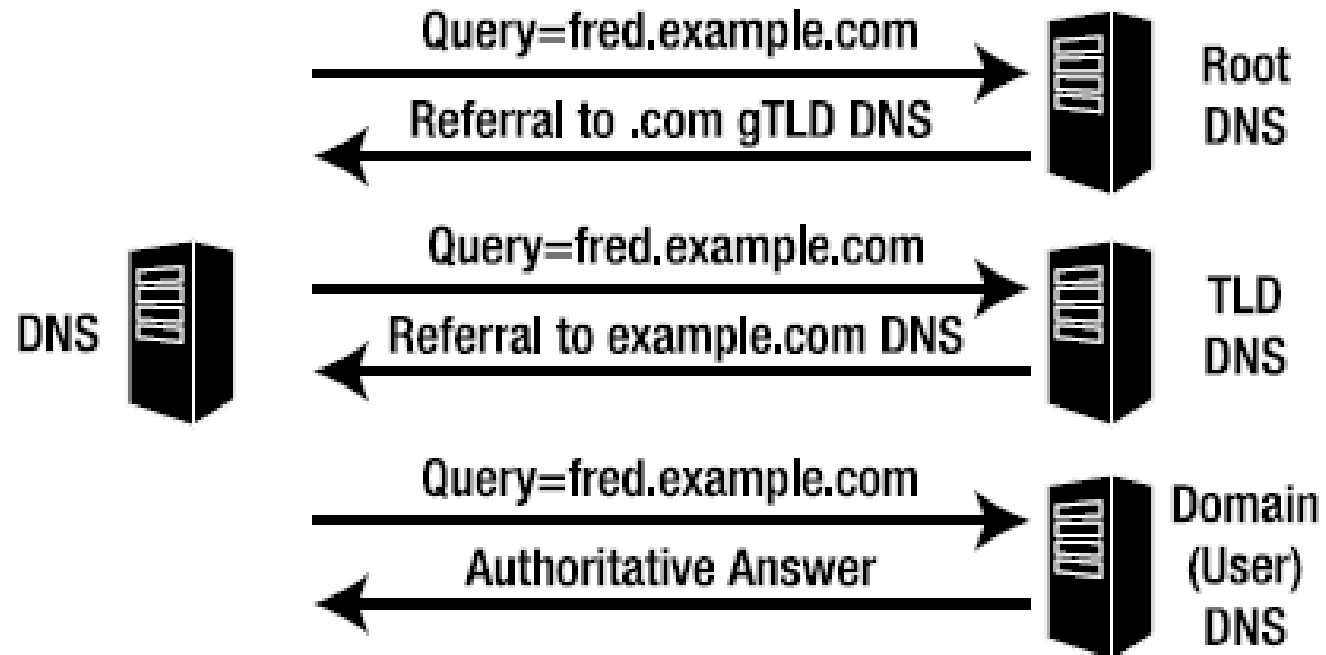
# DNS IMPLEMENTATION ET INTERNET

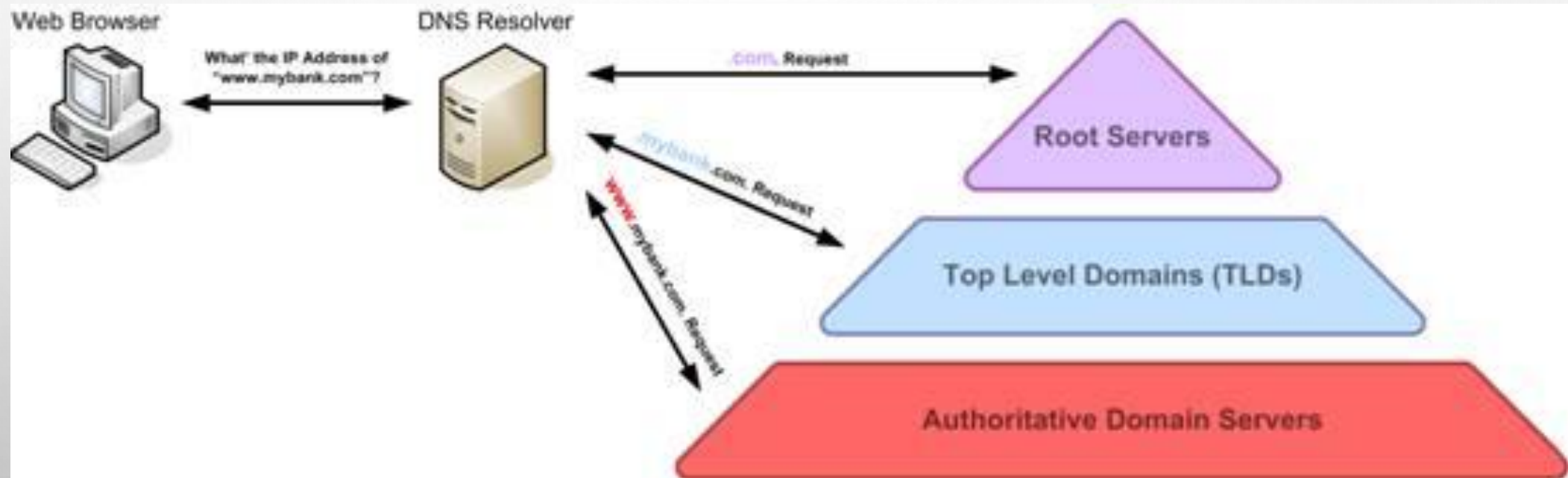
La mise en œuvre des **DNS de l'Internet** mappe la structure de délégation de nom de domaine que l'on vient de voir précédemment.

Il existe des serveurs de nom à chaque niveau de hiérarchie de délégation. Et la responsabilité de l'exécution des serveurs de nom hérite du contrôle d'autorité à chaque level.



**fred.example.com.**





# OPERATION DES « ROOT DNS »

Les serveurs de nom root (serveurs racines) sont la responsabilité de l'ICANN. Il existe 13 « serveurs root » dans le monde. Ils occupent un nom de domaine réservé: **root-servers.net**.

Chaque serveur racine comprend typiquement plus d'un serveur physique, mais partage une adresse ip commune. Les serveurs racines sont nommés à partir

**a.root-servers.net** jusqu'à **m.root-servers.net**

Server	Operator	Locations	IP Address
A	VeriSign Global Registry Services	Dulles, VA	198.41.0.4
B	Information Sciences Institute	Marina del Rey, CA	IPv4: 192.228.79.201, IPv6: 2001:478:65::53
C	Cogent Communications	Chicago; Herndon, VA; Los Angeles; New York City	IPv4: 192.33.4.12
D	University of Maryland	College Park, MD	IPv4: 128.8.10.90
E	NASA Ames Research Center	Mountain View, CA	IPv4: 192.203.230.10
F	Internet Systems Consortium, Inc. (ISC)	Auckland, Beijing, Brisbane, Dubai, Hong Kong, Jakarta, Johannesburg, Lisbon, Los Angeles, Madrid, Monterrey, Moscow, Munich, New York City, Osaka, Ottawa, Palo Alto, Paris, Prague, Rome, San Fran- cisco, San Jose, Sao Paulo, Seoul, Singapore, Taipei, Tel Aviv, Toronto	IPv4: 192.5.5.241, IPv6: 2001:500::1035
G	US DOD Network Information Center	Vienna, VA	IPv4: 192.112.36.4

H	US Army Research Lab	Aberdeen, MD	IPv4: 128.63.2.53, IPv6: 2001:500:1::803f:235
I	Autonomica/NORDUnet	Amsterdam, Ankara, Bangkok, Brussels, Bucharest, Chicago, Geneva, Frankfurt, Helsinki, Hong Kong, Kuala Lumpur, London, Milan, Oslo, Stockholm, Tokyo, Washington DC	IPv4: 192.36.148.17
J	VeriSign Global Registry Services	Amsterdam; Atlanta; Dulles, VA (2 locations); London; Los Ange- les; Miami; Mountain View, CA; Seattle; Seoul; Singapore; Ster- ling, VA; Stockholm; Tokyo	IPv4: 192.58.128.30
K	Réseaux IP Européens Network Coordination Centre (RIPE)	Amsterdam, Athens, Doha, Frank- furt, London, Milan	IPv4: 193.0.14.129, IPv6: 2001:7fd::1
L	Internet Corporation for Assigned Names and Numbers (ICANN)	Los Angeles	IPv4: 198.32.64.12
M	WIDE Project	Paris, Seoul, Tokyo	IPv4: 12.27.33, IPv6: 2001:dc3::35

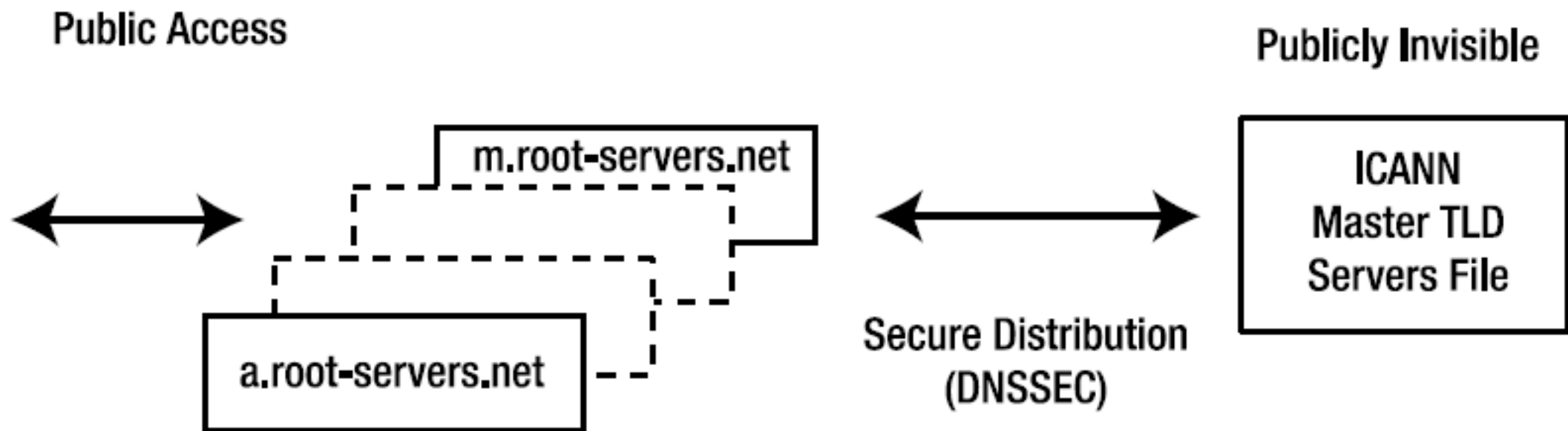
# OPERATION DES « ROOT DNS »

Les serveurs racines fournissent les serveurs TLD nécessaires (gTLD ou ccTLD). par exemple, si un utilisateur demande des informations sur **fred.example.com**, les serveurs racines vont fournir une liste des serveurs de noms d'autorité des tld.com.

En 2004, l'ICANN a pris la responsabilité de l'entretien des « root servers » donc des fichiers **maître tld**. Ce sont des fichiers qui répertorient les serveurs faisant autorité pour chaque tld.

# OPERATION DES « ROOT DNS »

La distribution de ce fichier (**maître tld**) pour chacun des serveurs racines opérationnels est effectuée en utilisant des transactions sécurisées. Ce ne sont pas des serveurs publiquement visibles.



# GENERIC TOP LEVEL DOMAINS gTLD

Les gTDL sont contrôlés par l'ICANN. Lorsque la concurrence de commerce de noms de domaine a été introduite dans l'enregistrement de noms de domaine, l'ICANN a établi deux entités distinctes:

- REGISTRY OPERATOR ou OPERATEUR DE REGISTRE
- REGISTAR

# GENERIC TOP LEVEL DOMAINS gTLD

REGISTRY OPERATOR ou OPERATEUR DE REGISTRE possède un contrat « opérateur de registre » avec l'ICANN pour faire fonctionner les serveurs d'autorité DNS gTLD.

Il y a un opérateur de registre unique pour chacun des gTLD, par exemple, le centre de département américain de la défense et de l'information (the US Department of Defense, Network Information Center), est l'opérateur de registre pour le gTLD .mil, mais chaque opérateur de registre peuvent faire fonctionner plusieurs serveurs de noms

# GENERIC TOP LEVEL DOMAINS gTLD

## Fonctionnement:

Par exemple, si la requête lancée pour **exemple.net**, les serveurs racines (root) vont fournir la liste des gTLD « .net » vers les serveurs d'autorité dns des opérateurs de registre. Le public n'a aucun contact avec l'opérateur de registre. Cependant, un certain nombre d'opérateur de registre sont également des REGISTAR. Par exemple, **Verisign inc.** est l'opérateur de registre pour le gTLD **.com**, mais est également un registrar bien connu.



WIKIPÉDIA  
L'encyclopédie libre

[Accueil](#)  
[Portails thématiques](#)  
[Article au hasard](#)  
[Contact](#)

[Contribuer](#)

[Débuter sur  
Wikipédia](#)

[Aide](#)

[Communauté](#)

[Modifications  
récentes](#)

[Faire un don](#)

[Imprimer / exporter](#)

[Créer un compte](#) [Se connecter](#)

Article [Discussion](#)

Lire

[Modifier](#)

[Modifier le code](#)

[Historique](#)



## Verisign

**VeriSign, Inc** (NASDAQ : **VRSN** ) est une société américaine établie à [Reston](#), dans l'État de [Virginie](#). La société exploite une vaste infrastructure réseau comprenant notamment deux des treize [serveurs racines du DNS](#). Elle gère également le registre officiel pour les domaines de premier niveau génériques [.com](#), [.net](#) et [.name](#), les domaines de premier niveau géographiques [.cc](#) et [.tv](#), et les systèmes back-end pour les domaines de premier niveau [.jobs](#) et [.edu](#). Verisign propose également plusieurs services de sécurité comme le [DNS géré](#), la limitation des attaques par [dénî de service distribué \(DDoS\)](#) et la création de rapports sur les cybermenaces.

En 2010, Verisign revend son activité Authentification à [Symantec](#) pour 1,28 milliard de dollars. L'authentification englobait les services [SSL \(Secure Socket Layer\)](#), les services d'[infrastructure à clés publiques](#) (PKI, Public Key Infrastructure), le sceau Verisign Trust (Verisign Trust Seal) et les services de protection des identités (VIP, Verisign Identity Protection)<sup>3</sup>.

En août de la même année, l'ancien directeur financier de Verisign, Brian Robins, annonce le transfert de la société de son site historique de [Mountain View](#), en [Californie](#), à Dulles, en Virginie du Nord, à compter de 2011. Une décision justifiée par le fait que la société réalise 95 % de son activité sur la côte est des [États-Unis](#)<sup>4</sup>.

**VeriSign, Inc.**



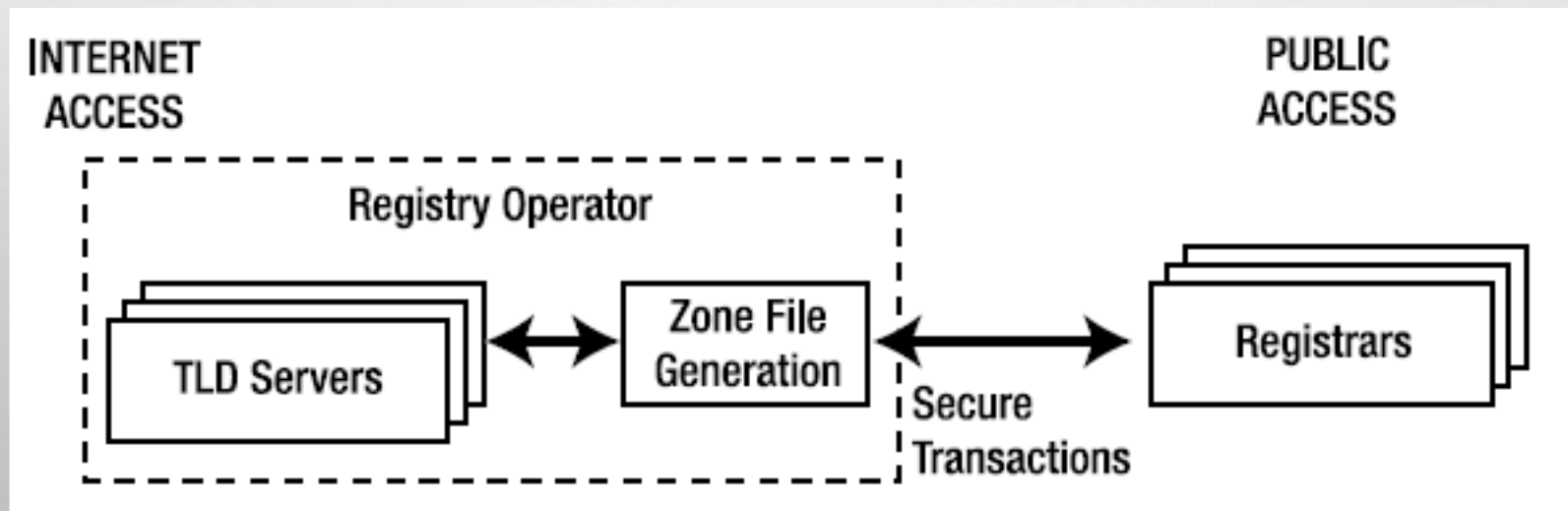
**VERISIGN™**

# GENERIC TOP LEVEL DOMAINS gTLD

Les REGISTAR sont accrédités par l'ICANN pour interagir avec le public pour l'achat et l'enregistrement d'un ou plusieurs **gTLD**. Lorsque vous achetez ou renouvelez un nom de domaine, vous traitez avec un REGISTAR. Le REGISTAR conserve tous les détails nécessaires, y compris le nom du propriétaire, le contact administratif, contact de facturation, le contact technique, les serveurs de noms faisant autorité pour le nom de domaine, etc... Le REGISTAR est responsable dans la fourniture d'information de la part de l'opérateur de registre pour les **gTLD** avec un extrait des données qui contient les **SLD** et avec le nom et les adresses ip des serveurs de nom d'autorité pour le domaine. Cette information est exclusivement utilisé pour répondre aux requêtes DNS.

# GENERIC TOP LEVEL DOMAINS gTLD

La séparation des rôles entre les operateurs de registre et les registrar permet aux organismes acteurs d'un domaine de se spécialiser dans les deux différents domaine chacun et de concentrer exclusivement leur travail dans la maintenance des serveurs qui leur ont été confié



**Table 1-2. gTLDs Available Prior to November 2000**

<b>gTLD</b>	<b>Use</b>	<b>Registry Operator</b>	<b>Registrars</b>
.arpa	Address and Routing Parameter Area (ARPA) reserved for use in Internet infrastructure	IANA ( <a href="http://www.iana.org/arpa-dom">www.iana.org/arpa-dom</a> )	Not available for registration
.com	Historically for abbreviation of company	VeriSign, Inc.	ICANN-Accredited Registrars
.edu	Special TLD reserved for use by certain US educational institutions	EDUCAUSE	EDUCAUSE ( <a href="http://www.educause.edu">www.educause.edu</a> )
.gov	Reserved exclusively for use by the US government	US General Services Administration	US General Services Administration (GSA)
.int	Reserved exclusively for use by organizations established by international treaty	IANA ( <a href="http://www.iana.org/int-dom">www.iana.org/int-dom</a> )	IANA
.mil	Reserved exclusively for use by the US military	US DOD Network Information Center	US DOD Network Information Center
.net	Historically for use by network operators	VeriSign, Inc. until June 2005	ICANN-accredited registrars
.org	Historically a nonprofit organization	Public Interest Registry ( <a href="http://www.pir.org">www.pir.org</a> ) DNS operated by Afilias Limited	ICANN-accredited registrars

**Table 1-3.** *gTLDs Authorized by ICANN in November 2000*

<b>gTLD</b>	<b>Use</b>	<b>Registry Operator</b>
.aero	Reserved for use by the airline industry	Société Internationale de Télécommunications Aéronautiques (SITA— <a href="http://www.sita.aero">www.sita.aero</a> )
.biz	Generic business name domain	NeuLevel, Inc. ( <a href="http://www.neulevel.biz">www.neulevel.biz</a> )
.coop	Reserved for use by cooperatives	Dot Cooperation LLC ( <a href="http://www.cooperative.org">www.cooperative.org</a> )
.info	Generic information resources	Afilias Limited ( <a href="http://www.afilias.info">www.afilias.info</a> )
.museum	Reserved for use by museums	Museum Domain Management Association ( <a href="http://musedoma.museum">http://musedoma.museum</a> )
.name	For use by individuals—vanity domain names	Global Name Registry ( <a href="http://www.gnr.name">www.gnr.name</a> )
.pro	Professional organizations	RegistryPro ( <a href="http://www.nic.pro">www.nic.pro</a> )

**Table 1-4.** *sTLDs Authorized by ICANN in April 2005*

<b>TLD</b>	<b>Use</b>	<b>Registry Operator</b>
.jobs	Reserved for use by employment companies and human resources organizations	Employ Media LLC ( <a href="http://www.employmedia.com">www.employmedia.com</a> )
.travel	Reserved for use by the travel industry	Tralliance Corporation ( <a href="http://www.tralliance.info">www.tralliance.info</a> )

# CONTRY CODE TOP LEVEL DOMAINS

COUNTRY CODE TOP LEVEL DOMAINS (ccTLD) est géré par l'ICANN et délégué au pays. La relation entre l'ICANN et les autorités responsables des codes de pays est compliquée par la souveraineté des états et la sensibilité culturelle. Le travail de l'ICANN est principalement consultatif plutôt que contractuelle.

L'INTERNET ASSIGNED NUMBERS AUTHORITY (IANA) est un département de l'icann maintient une liste à jour des codes de pays.

[www.iana.org/cctld/cctld-whois.htm](http://www.iana.org/cctld/cctld-whois.htm) au nom de l'ICANN

# WHOIS

WHOIS est un service par lequel n'importe qui peut obtenir des informations et détails sur les noms de domaines ou les adresses ip

Exemple: [www.allwhois.com](http://www.allwhois.com)

# COMPOSANT D'UN SYSTÈME DNS

1. Fichiers de données décrivant les nom de domaine appelés des « fichier de zone »
2. Programme ou logiciel DNS
3. Un resolver

# COMPOSANT D'UN SYSTÈME DNS

Un serveur de noms peut gérer un ou plusieurs domaines à l'aide des fichiers de zone. Les fichiers de zone décrivent les propriétés globales du domaine et machines (host) ou des services fournies par ce domaine. Ces propriétés et services sont définis sous la forme de documents textuels **RESOURCES RECORDS** (RR) organisés dans la « fiche de zone ». Le format des fichiers de zone et leurs **RESOURCES RECORDS** sont normalisés dans la norme RFC1035 afin de permettre leur portabilité sur les différents les logiciels dns standard

# COMPOSANT D'UN SYSTÈME DNS

Le logiciel DNS fait essentiellement 3 choses

1. Il lit les fichiers de zone duquel il est responsable
2. Il lit les fichiers de configuration
3. Il répond aux questions ou queries venant des clients

# COMPOSANT D'UN SYSTÈME DNS

Le « resolver » est installé sur chaque machine fourni une traduction entre la requête de l'utilisateur ex: [www.exemple.net](http://www.exemple.net) en question (ou questions) vers les logiciels DNS utilisant souvent le protocole UDP. Un « resolver » est un programme complexe mais les standard les plus simple sont appelé « stub resolver » (comme sur les système WINDOWS et \*NIX).

Un navigateur par exemple utilise un « stub resolver » pour traduire une URL vers les adresse IP des serveurs DNS de FAI

# BIND

BERKELEY INTERNET NAME DOMAIN plus connu sous le nom de BIND est un programme open source et actuellement développé par l'INTERNET SYSTEM CONSORTIUM INC. ([www.isc.org](http://www.isc.org)) et est probablement le plus connu et le plus déployé des implémentations DNS.

Historiquement tous les serveurs racines utilisaient BIND. Mais afin d'encourager la diversité certains serveurs racine aujourd'hui tournent sur NSD DNS ([www.nlnetlabs.nl/nsd](http://www.nlnetlabs.nl/nsd))

# ATELIER: DYNAMIC DNS

- INSTALLATION DE BIND ET DE ISC DHCP SERVER
- CONFIGURATION DE BIND
- DYNAMIC DNS