Généralités

Le système DNS est le support de nombreuses fonctionnalités sur Internet allant de la navigation à l'envoi de courriers électroniques. Sa bonne configuration est essentielle dans le cadre d'un réseau local, et primordiale sur Internet.

1. Les débuts de la résolution de noms et l'apparition du DNS

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

Tant que les machines publiques sur Internet étaient peu nombreuses, toutes les résolutions se faisaient au moyen d'un fichier appelé **hosts** qu'on téléchargeait 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 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.

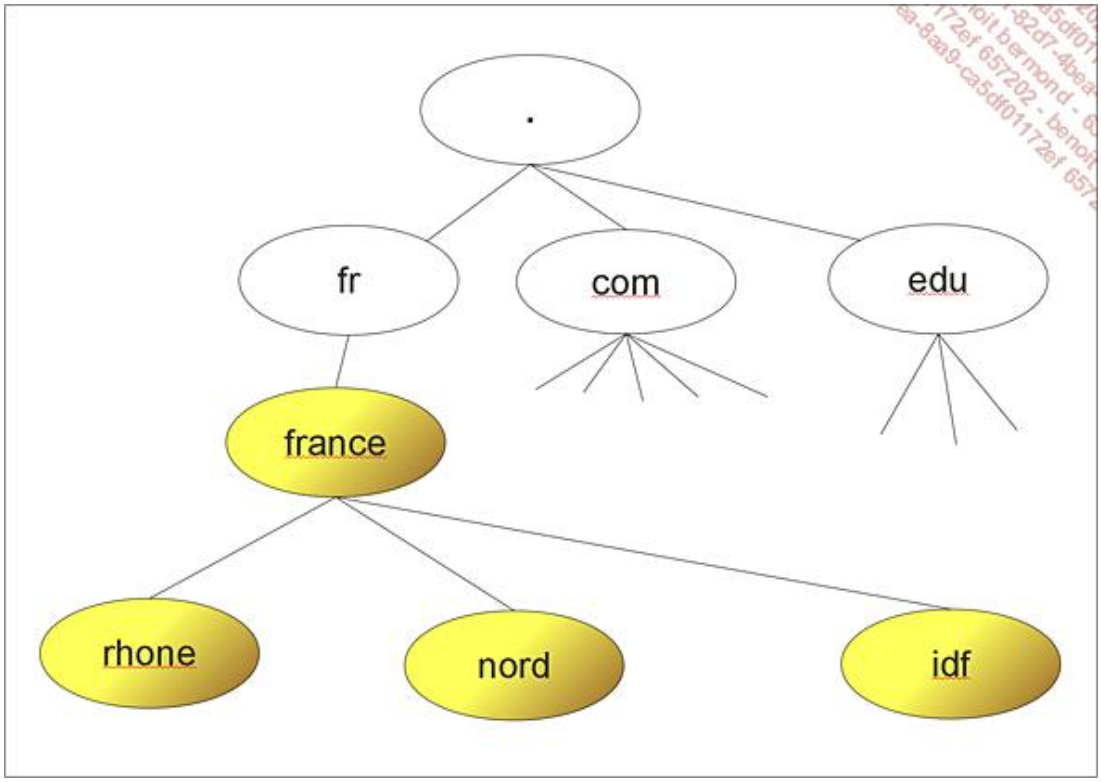
Le DNS est sécurisé

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.

2. Concept de zones DNS

Le nombre pléthorique d'enregistrements DNS ne permettrait pas leur gestion sans aucune forme d'organisation (cela reviendrait à avoir un fichier **hosts** contenant des millions de lignes). Leur organisation hiérarchique était donc indispensable, et c'est la raison d'être des zones DNS. Chaque niveau de la hiérarchie est une zone. Chaque arborescence est un domaine.

On a arbitrairement créé une zone appelée « . » (point), qui est à la racine de la hiérarchie, et qui contient tous les **tld** : **top level domain** (*domaine de niveau supérieur*). Les **tld** sont les extensions bien connues telles que **com**, **fr**, **net**, **be**, etc. Tous les domaines que nous connaissons et utilisons sont des sous-arborescences des **tld**.



Dans l'exemple ci-dessus, la zone france contient les sous-zones rhone, nord et idf. Mais on peut aussi dire que la zone « . » contient les sous-zones fr, com et edu. Les zones situées hiérarchiquement sous une zone sont appelées zones "enfant".

L'intérêt de cette organisation est de dédier un serveur (en fait au moins deux pour des raisons de tolérance de pannes) à la gestion d'une zone. Et comme la hiérarchie DNS est virtuellement illimitée, en largeur comme en profondeur, un serveur DNS ne gère en fait qu'une petite portion de l'espace de nom. Toujours dans notre exemple, si un serveur DNS héberge les données de la zone france, il est consulté pour toute résolution de nom se terminant par « france.fr », mais il n'héberge pas nécessairement les données des zones rhone, nord et idf, et peut se contenter de rediriger la requête vers le serveur de la zone enfant. On parle alors de **délégation** dans le sens où on délègue la gestion d'une zone enfant à un autre serveur.

Pour des raisons de tolérance de panne, les données de chaque zone DNS doivent être répliquées au moins une fois, c'est-à-dire exister à au moins deux exemplaires. Un serveur aura autorité sur la zone et sera responsable des mises à jour. On dit qu'il est **SOA** : **Start Of Authority**. Les zones hébergées sur ce serveur sont de type **master**, et ceux qui hébergent une réplique de la zone sont configurés en tant que **slave**.

3. Mécanisme de la résolution de nom

Quand une application d'une machine doit faire une résolution de nom, elle s'adresse au composant **resolver** de son système d'exploitation. Le **resolver** va alors envoyer une requête de résolution de nom au serveur DNS référencé sur cette machine. Les requêtes de client à serveur se font sur le port 53 et sont transportées par le protocole UDP.

Si le serveur interrogé dispose localement de l'information, il répond directement. On dit qu'il fait une réponse **authoritative** (autoritaire).

Si le serveur interrogé ne dispose pas de l'information, il va consulter la seule zone qu'il connaît, la zone « . », qui lui donnera l'adresse d'un des 13 serveurs racines de l'Internet. Le serveur interrogera alors ce serveur racine pour connaître l'adresse d'un serveur de la zone du **tld** : **top level domain** (domaine de premier niveau). Lequel serveur sera interrogé à son tour pour connaître l'adresse d'un serveur de nom gérant la zone directement sous le tld. Enfin, ce serveur sera interrogé pour savoir s'il dispose de l'enregistrement voulu dans ce domaine.

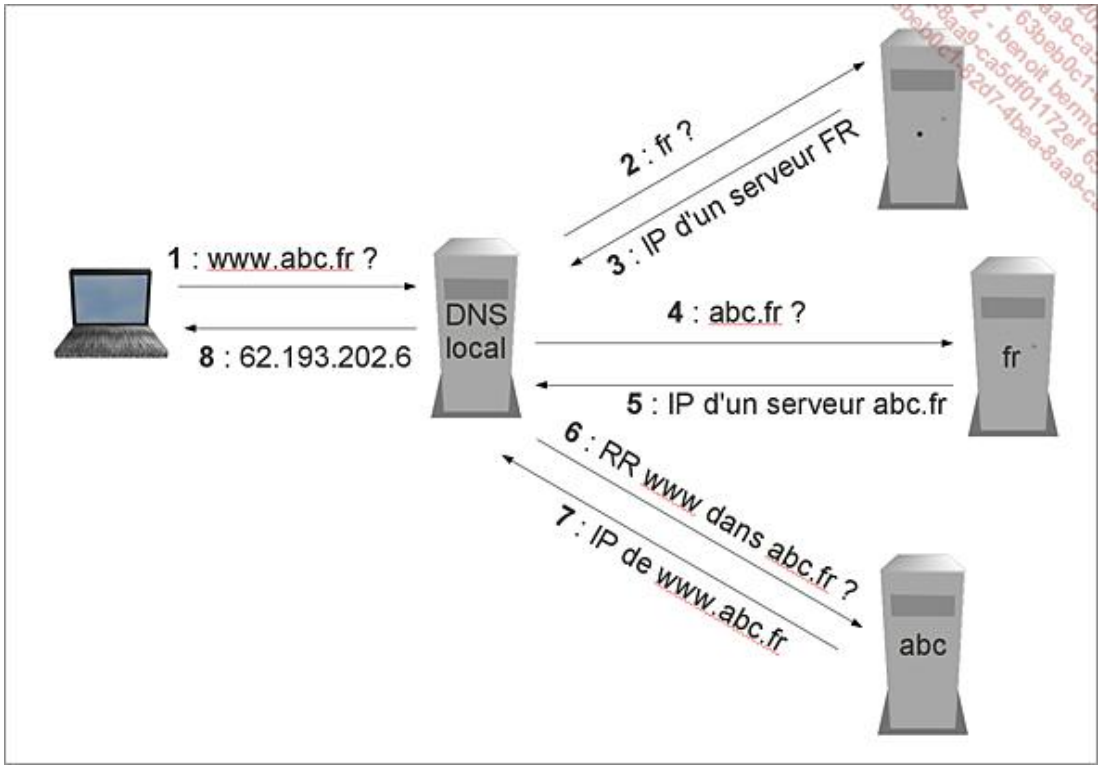


Schéma simplifié de la résolution de nom :

1. Le client à son serveur de référence (fournisseur d'accès ou serveur local) : quelle est l'adresse pour le nom **www.abc.fr** ?

2. Le serveur local à un serveur racine : donne-moi l'adresse d'un serveur connaissant la zone **fr**.

3. Tiens, le serveur à l'adresse **193.176.144.6** pourra te renseigner. Il possède les informations de la zone **fr**.

4. Le serveur local au serveur de la zone **fr** : donne-moi l'adresse d'un serveur connaissant la zone **abc.fr**.

5. Tiens : le serveur à l'adresse **213.41.120.195** pourra te renseigner.

6. Le serveur local au serveur de la zone **abc.fr** : possèdes-tu un enregistrement **www** dans ton domaine **abc.fr** ?

7. Oui, voici son adresse IP : **62.193.202.6**.

8. Le serveur local à la station cliente : tu m'as demandé **www.abc.fr** et son adresse IP est **62.193.202.6**.

4. Les enregistrements

Les zones n'ayant qu'un rôle structurant, il faudra pour assurer les résolutions de nom créer des enregistrements qui feront correspondre un nom à une adresse IP ou à une autre information. Ces enregistrements sont appelés **Ressources Records** (enregistrement de ressources), souvent notés **RR** et constituent les informations fondamentales du DNS.

Le **FQDN**, **Fully Qualified Domain Name** (*Nom de Domaine Pleinement Qualifié*) représente le nom d'hôte, avec toute son arborescence parente, jusqu'à la zone « . » . Par exemple, **www.saintmarcelin.fr** représente l'enregistrement **www** dans la zone **saintmarcelin.fr**, **fr** étant la dernière zone avant la zone point. Quand on ne veut aucune ambiguïté quant à la nature d'un nom DNS, on représente le **FQDN** avec la zone point matérialisée, c'est-à-dire qu'on écrit un point comme dernier caractère du **FQDN**. On obtient donc « **www.saintmarcelin.fr**. ». Cette notation est courante, voire indispensable dans les fichiers de configuration du serveur DNS.

Le système DNS a pour vocation première d'assurer un service de résolution de nom. C'est-à-dire de faire correspondre à un nom d'hôte une adresse IP. Ses créateurs ont toutefois prévu que le système DNS serait capable d'assurer la résolution pour différents types de noms et d'améliorer ainsi la finesse du service.

a. Enregistrement de type A

Le plus facile à appréhender et le plus courant. C'est l'enregistrement qui fait correspondre une adresse IP à un nom. Par exemple quand on tape http://www.site.fr, www est un enregistrement de type A dans la zone site.fr. Il correspond à une adresse IP qui est celle du serveur web hébergeant le site en question.

Résolutions dans la zone domaine.fr

www → 82.25.120.5

support → 125.12.43.2

vpn → 82.25.120.6

b. Enregistrement de type AAAA

Récent mais de plus en plus fréquent. Cet enregistrement fait correspondre à un nom une adresse IPv6.

Résolutions dans la zone domaine.fr

www → 2001:610:12:123a:28:15ff:fed9:97e6

support → 2001:610:12:123a:28:15ff:fed9:97e8

c. Enregistrement de type PTR

Pointer, le contraire de A. Si les enregistrements de type A font correspondre une adresse IP à un nom d'hôte, les PTR font exactement le contraire. Ils existent dans des zones un peu particulières nommées IN-ADDR.ARPA.

Le nom normalisé de la zone sera formé par les octets de la partie réseau de l'adresse IP ordonnés en sens inverse, suivi de la chaîne de caractères « .in-addr.arpa ».

Résolutions dans la zone 1.168.192.in-addr.arpa

10 → serveur1.entreprise.local (pour serveur1.entreprise.local → 192.168.1.10)

15 → printer1.entreprise.local (pour printer1.entreprise.local → 192.168.1.15)

Résolutions dans la zone 85.in-addr.arpa

25.8.92 → www.abc.fr (pour www.abc.fr → 85.92.8.25)

29.123.65 → www.def.net (pour www.def.net → 85.65.123.29)

d. Enregistrement de type CNAME

Canonical Name (alias ou surnom). Ce type d'enregistrement fait correspondre un nom à un autre nom. Par exemple si vous créez un serveur web pour les usages internes de votre entreprise sur un serveur existant qui s'appellerait « production1.maboite.com », vous pouvez créer un CNAME « intranet » plus intuitif pour les utilisateurs.

Résolutions dans la zone maboite.com

intranet → production1

imprimante1 → printer1

e. Enregistrement de type MX

Mail Exchanger (Indicateur de serveur de messagerie pour un domaine). Ce type d'enregistrement fait savoir à des agents de transfert de messagerie quel est le serveur destinataire final d'un courriel. L'exemple ci-dessous est à titre d'illustration et ne présage pas du format d'un enregistrement MX.

Résolution dans la zone domaine.fr

@domaine.fr → smtp.domaine.fr → 82.25.120.6

f. Enregistrement de type SOA

Start Of Authority (début d'autorité). Indique le serveur ayant la responsabilité de la zone. Toute zone fonctionnelle a un enregistrement SOA.

Résolution dans la zone domaine.fr

domaine.fr → ns.hebergeur.net

g. Enregistrement de type NS

Name Server (serveur de nom). Indique les serveurs de noms pour la zone. Toute zone fonctionnelle a au moins un enregistrement NS.

Résolution dans la zone domaine.fr

domaine.fr → ns.hebergeur.net

5. DNS sur Linux

a. Le serveur DNS

Les services DNS s'exécutant sur Linux sont presque exclusivement basés sur le logiciel **BIND** (*Berkeley Internet Name Domain*). Comme son nom l'indique, il a été conçu dans l'université de Berkeley en Californie. Les premiers développements datent des années 80 et son maintien est actuellement assuré par l'« Internet System Consortium » (*ISC*), une association à but non lucratif qui gère un certain nombre de logiciels structurants de l'Internet et des réseaux locaux.

b. Le client DNS

Les machines Linux disposent nativement d'un client DNS appelé **resolver**. Toute application fonctionnant sur Linux et ayant besoin de faire une requête DNS s'appuiera sur ce composant.

Il exploite le fichier de configuration simple **/etc/resolv.conf**.

Format simplifié du fichier /etc/resolv.conf

```
search domaine
domain domaine
nameserver A.B.C.D
```

Fichier /etc/resolv.conf : directives et variables utilisées	
search	Facultatif : indique le suffixe de recherche employé sur le poste Linux. Permet de ne pas taper l'intégralité du FQDN dans les applications. Le fichier /etc/resolv.conf admet plusieurs domaines de recherches précisés par search.
domain	Facultatif et obsolète : indique un suffixe de recherche unique employé sur le poste Linux.
domaine	Le FQDN du domaine constituant le suffixe de recherche.
nameserver	Indique l'adresse IP du serveur DNS qui assurera les résolutions. Le fichier /etc/resolv.conf admet plusieurs serveurs DNS précisés par nameserver.