DNS (*Domain Name System*)

Le DNS (*Domain Name System* ou système de noms de domaine) est un service permettant de traduire un nom de domaine en adresses IP de la machine portant ce nom (RFC 882/883 en 1983).

DNS utilise le protocole de transport **UDP** et le port **53**. La taille maximale des paquets utilisée est de 512 octets.

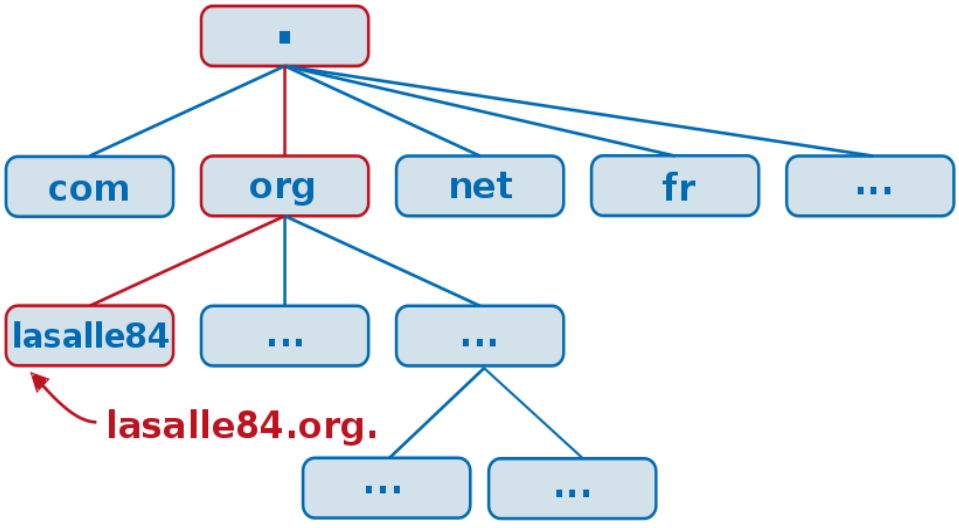
Le type d'enregistrement de ressource RR (*Resource Record*) est codé sur 16 bits. Les principaux enregistrements définis sont les suivants :

- **A** record (*Address record*) qui fait correspondre un nom d'hôte à une adresse IPv4 de 32 bits distribués sur quatre octets. AAAA pour IPv6.
- **CNAME** record (*Canonical Name record*) qui permet de faire d'un domaine un alias vers un autre. Cet alias hérite de tous les sous-domaines de l'original.
- **PTR** record (*PoinTer Record*) qui associe une adresse IP à un enregistrement de nom de domaine (aussi dit « reverse » car il fait le contraire du A record).

Hiérarchie du DNS (*Domain Name System*)

Le système des noms de domaines consiste en une hiérarchie dont le sommet est appelé la **racine** (représentée par un point). Dans un domaine, on peut créer un ou plusieurs sous-domaines ainsi qu'une délégation pour ceux-ci (les informations relatives à ce sous-domaine sont enregistrées sur un autre serveur).

Les domaines se trouvant immédiatement sous la racine sont appelés **domaine de premier niveau** (TLD : *Top Level Domain*). Les noms de domaines ne correspondant pas à une extension de pays sont appelés des **domaines génériques** (gTLD), par exemple **`.org`** ou **`.com`**. S'ils correspondent à des codes de pays (fr, be, ch...), on les appelle ccTLD (*country code* TLD).



On représente un nom de domaine en indiquant les domaines successifs séparés par un point, les noms de domaines supérieurs se trouvant à droite.

FQDN (*Fully qualified domain name*)

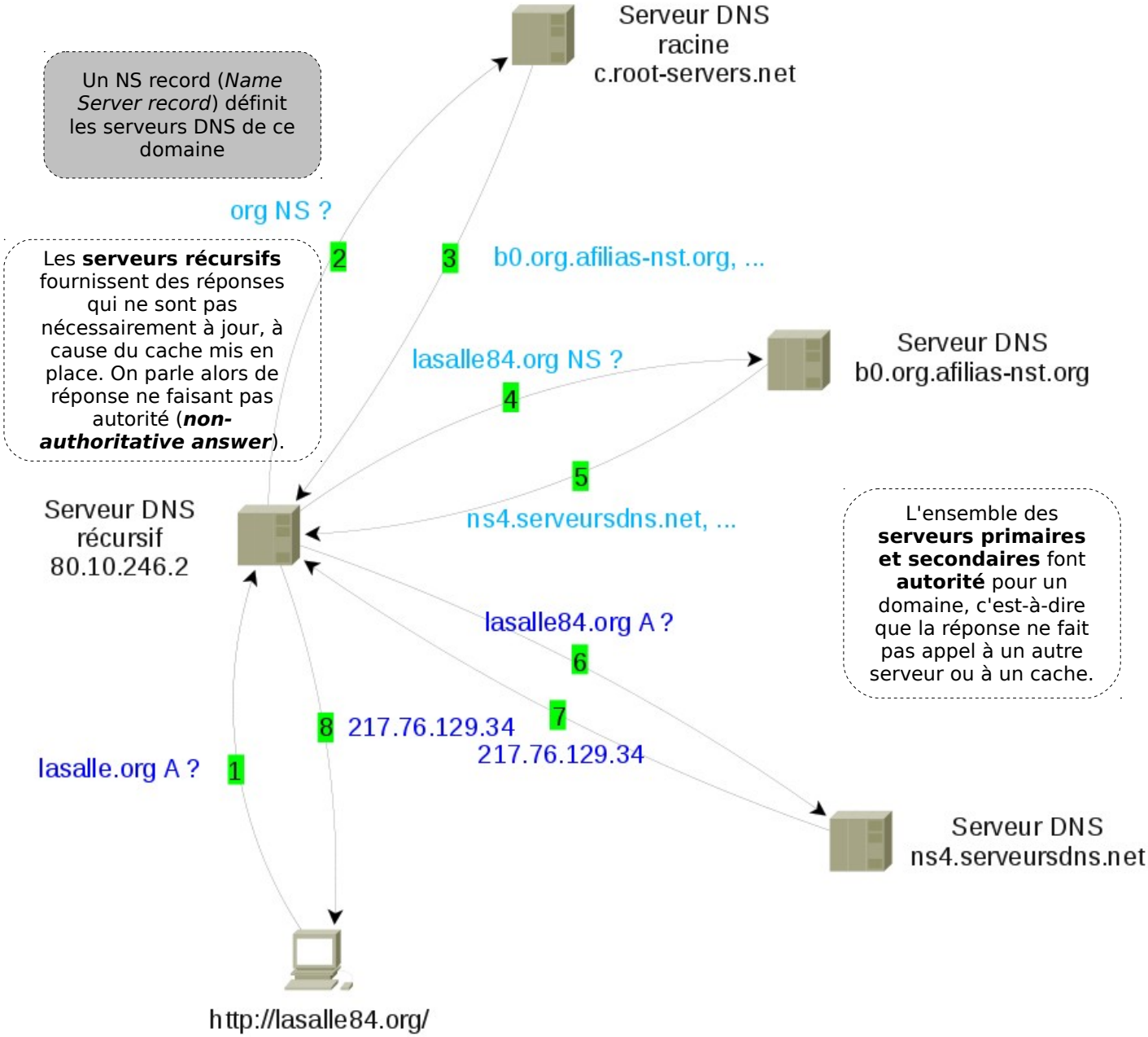
On entend par **FQDN** (Fully qualified domain name) ou **Nom de domaine pleinement qualifié** un nom de domaine écrit de façon absolue, y compris tous les domaines jusqu'au domaine de premier niveau (TLD), il est ponctué par un point final. Dans une réseau TCP/IP, une adresse FQDN sera l'association entre le nom de la machine et le domaine auquel elle appartient.

Remarque : la norme prévoit qu'un élément d'un nom de domaine (appelé label) ne peut dépasser 63 caractères, un FQDN ne pouvant dépasser 255 caractères.

Principe

Les hôtes n'ont qu'une connaissance limitée du système des noms de domaine. Quand ils doivent résoudre un nom, ils s'adressent à un ou plusieurs serveurs de noms dits **récursifs**, c'est-à-dire qui vont parcourir la hiérarchie DNS et faire suivre la requête à un ou plusieurs autres serveurs de noms pour fournir une réponse.

Quand un serveur DNS récursif doit trouver l'adresse IP de www.lasalle84.org, un **processus itératif** démarre pour consulter la hiérarchie DNS. Ce serveur demande aux serveurs DNS appelés **serveurs racine** quels serveurs peuvent lui répondre pour la zone org. Parmi ceux-ci, notre serveur va en choisir un pour savoir quels serveurs sont capables de lui répondre pour la zone lasalle84.org. C'est un de ces derniers qui pourra lui donner l'adresse IP de www.lasalle84.org. S'il se trouve qu'un serveur ne répond pas, un autre serveur de la liste sera consulté.



Les **serveurs "racine"** sont gérés par douze organisations différentes (2 européennes, 1 japonaise et 9 américaines). Sept de ces serveurs sont en réalité distribués dans le monde grâce à la technique ***anycast*** (plus de 200 serveurs répartis dans 50 pays du monde) et neuf disposent d'une adresse IPv64. Il existe 13 autorités de nom appelées de **a** à **`m.root-servers.net`**. Le serveur **k** reçoit par exemple de l'ordre de 20 000 requêtes par seconde.