I/ Introduction

Dans le monde de l'Internet, les machines du réseau sont identifiées par des adresses IP. Néanmoins, ces adresses ne sont pas très agréables à manipuler, c'est pourquoi, on utilise les noms. L'objectif a alors été de permettre la résolution des noms de domaines qui consiste à assurer la conversion entre les noms d'hôtes et les adresses IP. Cette solution est l'utilisation des DNS (Domain Name System : Système de noms de domaine).

II/ Historique du protocole DNS

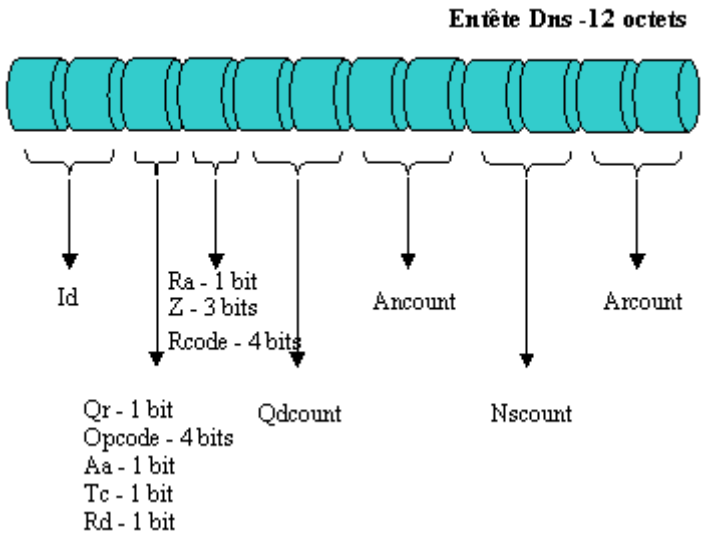
Jusqu'en 1984, la transcription de noms d'hôtes en adresses Internet s'appuyait sur une table de correspondance maintenue par le Network Information Center (NIC), et ce dans un fichier .txt, lequel était transmis par FTP à tous les hôtes. Il n'était à l'époque pas compliqué de stocker les adresses puisque le nombre de machines était très réduit.

En 1983-1984, Paul Mockapetris et John Postel ont proposé et développé une solution qui utilise des structures de base de données distribuée : les Domain Name System, RFCs 882 et 883 devenue obsolète par la RFC 1034. Les spécifications des DNS ont été établies en 1987.

III/ Les formats de l'entête DNS

1) L'entête DNS sur 12 octets

Voici la structure de l'entête DNS basée sur 12 octets.



Id

Codé sur 16 bits, doit être recopié lors de la réponse permettant à l'application de départ de pouvoir identifier le datagramme de retour.

Opcode

Sur 4 bits, ce champ perme de spécifier le type de requête :

Qr

Sur un 1 bit, ce champ permet d'indiquer s'il s'agit d'une requête (0) ou d'une réponse (1).

- 0 – Requête standard (Query)
- 1 – Requête inverse (Iquery)
- 2 – Statut d'une requête serveur (Statut)
- 3-15 – Réservé pour des utilisations futures

Aa

Le flag Aa, sur un bit, signifie « Authoritative Answer ». Il indique une réponse d'une entité autoritaire.

Tc

Le champ Tc, sur un bit, indique que ce message a été tronqué.

Rd

Le flag Rd, sur un bit, permet de demander la récursivité en le mettant à 1.

Ra

Le flag Ra, sur un bit, indique que la récursivité est autorisée.

Z

Le flag Z, sur trois bits, est réservé pour une utilisation future. Il doit être placé à 0 dans tous les cas. Désormais, cela est divisé en 3 bits : 1 bit pour Z, 1 bit pour AA (Authentificated Answer) qui indique si la réponse et authentifiée, et 1 bit NAD (Non-Authenticated Data) qui indique si les données sont non-authentifiées.

Rcode

Le champ Rcode, basé sur 4 bits, indique le type de réponse.

- 0 – Pas d'erreur
- 1 – Erreur de format dans la requête
- 2 – Problème sur serveur
- 3 – Le nom n'existe pas
- 4 – Non implémenté
- 5 – Refus
- 6-15 – Réservés

Qdcount

Codé sur 16 bits, il spécifie le nombre d'entrée dans la section « Question ».

Ancount

Codé sur 16 bits, il spécifie le nombre d'entrée dans la section « Réponse ».

Nscount

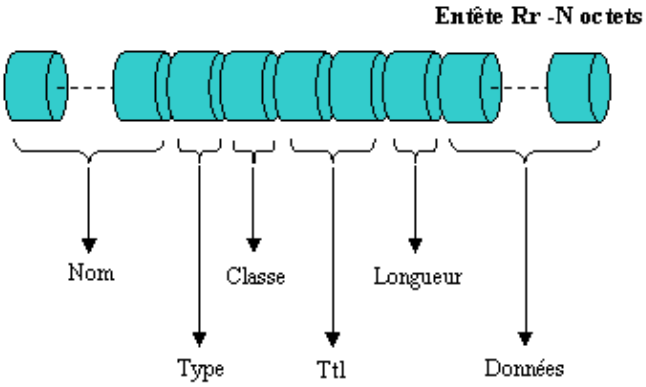
Codé sur 16 bits, il spécifie le nombre d'entrée dans la section « Autorité ».

Arcount

Codé sur 16 bits, il spécifie le nombre d'entrée dans la section « Additionnel ».

2) Les RR

La base de données des serveurs de noms (fichiers de domaine et fichiers de résolution inverse) est constituée « d'enregistrements de ressources », « Ressource Records » (RRs). Ces enregistrements sont répartis en classes. La seule classe d'enregistrement usuellement employée est la classe Internet (IN). L'ensemble d'informations de ressources associées à un nom particulier est composé de quatre enregistrements de ressources séparés (RR).



Nom

Nom du domaine où se trouve le RR. Ce champ est implicite lorsqu'un RR est en dessous d'un autre, auquel cas le champ owner est le même que celui de la ligne précédente.

Type

Ce champ type, codé sur 16 bits, spécifie quel type de donnée est utilisé dans le RR. Voici les différents types disponibles :

- Entrée=A et Valeur=01 : Adresse de l'hôte
- Entrée=ns et Valeur=02 : Nom du serveur de noms pour ce domaine
- Entrée=MD et Valeur=03 : Messagerie (obsolète par l'entrée MX)
- Entrée=MF et Valeur=04 : Messagerie (obsolète par l'entrée MX)
- Entrée=CNAME et Valeur=05 : Nom canonique (Nom pointant sur un autre nom)
- Entrée=SOA et Valeur=06 : Début d'une zone d'autorité (informations générales sur la zone)
- Entrée=MB et Valeur=07 : Une boite à lettre du nom de domaine (expérimentale)
- Entrée=MG et Valeur=08 : Membre d'un groupe de mail (expérimentale)
- Entrée=MR et Valeur=09 : Alias pour un site (expérimentale)
- Entrée=NULL et Valeur=10 : Enregistrement à 0 (expérimentale)
- Entrée=WKS et Valeur=11 : Services Internet connus sur la machine
- Entrée=PTR et Valeur=12 : Pointeur vers un autre espace du domaine (résolution inverse)
- Entrée=HINFO et Valeur=13 : Description de la machine
- Entrée=MINFO et Valeur=14 : Groupe de boite à lettres
- Entrée=MX et Valeur=15 : Mail exchange (Indique le serveur de messagerie. Voir [RFC-974] pour plus de détails
- Entrée=TXT et Valeur=16 : Chaîne de caractère

Classe
Une valeur encodée sur 16 bits identifiant une famille de protocoles ou une instance d'un protocole. Voici les classes de protocole possible :

- Entrée=In et Valeur=01 : Internet
- Entrée=Cs et Valeur=02 : Class Csnet (obsolète)
- Entrée=Ch et Valeur=03 : Chaos (chaosnet est un ancien réseau qui historiquement a eu une grosse influence sur le développement de l'Internet, on peut considérer à l'heure actuelle qu'il n'est plus utilisé)
- Entrée=Hs et Valeur=04 : Hesiod

TTL
C'est la durée de vie des RRs (32 bits, en secondes), utilisée par les solveurs de noms lorsqu'ils ont un cache des RRs pour connaître la durée de validité des informations du cache.

Longueur
Sur 16 bits, ce champ indique la longueur des données suivantes.

Données
Données identifiant la ressource, ce que l'on met dans ce champ dépend évidemment du type de ressources que l'on décrit.

- A : Pour la classe IN, une adresse IP sur 32 bits. Pour la classe CH, un nom de domaine suivi d'une adresse octale Chaotique sur 16 bits.
- Cname : un nom de domaine.
- Mx : une valeur de préférence sur 16 bits (la plus basse possible) suivie d'un nom d'hôte souhaitant servir d'échangeur de courrier pour son propore domaine.
- Ptr : Une adresse IP sous forme d'un nom.
- Ns : Un nom d'hôte.
- Soa : Plusieurs champs.

IV/ Les zones

Structure arborescente de l'espace de noms
Le service DNS utilise la gestion hiérarchique des noms. On distingue deux domaines pour le classement des noms.

- Les domaines géographiques (Codes ISO 3166)
- Les domaines génériques
  - .com – Commerciaux
  - .edu – Organismes d'éducation américaine
  - .net – Organismes de gestion de réseaux
  - .org – Organismes non-commerciaux
  - .int – Organismes internationaux
  - .gov – Organismes gouvernementaux USA
  - .mil – Organismes militaires USA
  - .arpa – Transition ARPAnet-> Internet + traduction inverse

L'arborescence des noms de domaine est constituée :

- d'une racine
- de nœuds identifiés par des labels dont les informations sont stockées dans une base de données

V/ Type de serveurs et autorités

Par le découpage en zone on a donc trois types de serveurs de noms.

1) Le serveur primaire

Le serveur primaire est serveur d'autorité sur sa zone : il tient à jour un fichier appelé « fichier de zone », qui établit les correspondances entre les noms et les adresses IP des hosts de sa zone. Chaque domaine possède un et un seul serveur primaire.

2) Le serveur secondaire

Un serveur de nom secondaire obtient les données de zone via le réseau, à partir d'un autre serveur de nom qui détient l'autorité pour la zone considérée. L'obtention des informations de zone via le réseau est appelé transfert de zone. Il est capable de répondre aux requêtes de noms IP (partage de charge), et de secourir le serveur primaire en cas de panne. Le nombre de serveurs secondaires par zone n'est pas limité. Ainsi il y a une redondance de l'information. Le minimum imposé est un serveur secondaire.

Un serveur qui effectue un transfert de zone vers un autre serveur est appelé serveur maître. Un serveur maître peut être un serveur primaire ou un serveur secondaire. Un serveur secondaire peut disposer d'une liste de serveurs maîtres (jusqu'à dix

serveurs maîtres). Le serveur secondaire contacte successivement les serveurs de cette liste, jusqu'à ce qu'il ait pu réaliser son transfert de zone.

3) Le serveur cache

Le serveur cache ne constitue sa base d'information qu'à partir des réponses des serveurs de noms. Il inscrit les correspondances nom / adresse IP dans un cache avec une durée de validité limitée (TTL) ; il n'a aucune autorité sur le domaine : il n'est pas responsable de la mise à jour des informations contenues dans son cache, mais il est capable de répondre aux requêtes des clients DNS.

De plus on peut distinguer les serveurs racine : ils connaissent les serveurs de noms ayant autorité sur tous les domaines racine. Les serveurs racine connaissent au moins les serveurs de noms pouvant résoudre le premier niveau (.com, .edu, .fr, etc.).

Un serveur de nom, en terme physique, peux très bien jouer le rôle de plusieurs de ces fonctions. On trouvera par exemple, beaucoup d'entreprise qui héberge leurs domaines sur le serveur DNS primaire servant aussi de cache pour les requêtes sortantes des utilisateurs internes.