Résolution de noms

(Z:\Polys\Internet_gestion_reseau\6.DNS.fm- 26 septembre 2008 12:17)

PLAN

- Introduction
- Noms et adresses
- Principe de la résolution de noms
- La résolution de noms sous Internet/Unix
- Conclusion

Bibliographie

- A.Fenyo, F.LeGuern, S.Tardieu, Se raccorder à Internet, Eyrolles, 1997
- L.Toutain, Internet et les réseaux locaux, Hermès, 1996.
- G.Hunt, TCP-IP network administration, O'Reilly, 1992.
- D.Comer, TCP/IP : Architectures, protocoles, et applic., InterEditions, 1998.

1. Introduction

On a besoin d'un service mondial d'annuaire pour Internet.

Service associant le nom d'une station à son adresse IP :

- Par exemple :

. pondichery.irisa.fr. ⇒ 131.254.61.13

Mais aussi, il faut un service associant un serveur de messagerie au nom d'un utilisateur.

. bcousin@ifsic.univ-rennes1.fr. ⇒mercure.univ-rennes-1.fr.

Il faut qu'il soit stable, fiable et performant.

2. Noms et adresses

2.1. Introduction

Les adresses IP sont adaptées à leurs tâches :

- identification dense (numérotation simple, sur 32 bits),
- aide à l'acheminement (netid + hostid)

Les êtres humains ont quelques difficultés à les utiliser :

- erreurs typographiques
- mémorisation difficile, etc.

La notation conventionnelle (décimale pointée) est insuffisante.

. on a besoin de noms symboliques:

. signifiants : <ma_machine>

. facile à administrer : <ma-machine.mon-entreprise.mon-pays.>

Remarque : problème similaire entre nom de fichier et référence interne au noyau du système du gestion des fichiers ("inode" /= ~mon-nom/mon-repertoire/mon-fichier).

Remarque : la distinction entre nom et adresse est artificielle, ils identifient tous les deux un objet. L'un est dit logique (ou de haut niveau), l'autre physique (de bas niveau).

2.2. Espace plat d'adresses

Initialement sous Internet l'espace des noms était plat.

2 fonctions distinctes :

- allocation/administration des noms : attribution unique d'une adresse à une station
- résolution de nom : une requête concernant une station permet de connaitre son adresse

Un organisme central administre l'espace des noms :

- vérifie l'unicité du nom
- mémorise l'association nom/adresse
  . NIC : "Internet Network Information Center"
- Avantages :
  . les noms peuvent être quelconques, aussi courts que voulu
  . la résolution d'adresse est triviale : consulter le fichier du site central
- Inconvénients
  . conflits de noms fréquents
  . la recherche peut être laborieuse
  . le site central surchargé par les demandes de créations de noms et de modifications d'associations

La résolution de noms est peu performante :

- soit la résolution est centralisée,
  . les liaisons menant au site sont surchargées
  . le site central est surchargé
- soit la résolution est répartie,
  . la distribution de la liste est extrêmement coûteuse
  . les copies ne sont pas à jour

2.3. Espace hiérarchique

On résout les problèmes précédents au moyen d'un espace hiérarchique de noms et de la délégation.

2.3.1 L'espace hiérarchiques des noms

. Présente une structure arborescente (similaire au système de fichiers, par ex.)
. Chaque noeud de l'arbre est identifié par un "label" :
  - d'au plus 63 caractères alpha-numériques,
  - majuscules et minuscules étant identiques
. Un noeud spécial, la racine, est identifié par une chaine de caractères vide.
. Le nom d'un noeud de l'arbre est identifié par la suite de labels rencontrés en partant de ce noeud et en allant vers la racine, chaque label étant séparé par un point.
  - un nom est unique, mais
  - plusieurs noms peuvent partager le même label
  - et un même nom peut avoir plusieurs labels identiques

Par exemple :
  - ma-station.ifsic.univ-rennes1.fr.

Dénomination relative ou absolue :

. Un nom absolu possède (est terminé par) un point [convention dépendant de l'implémentation]

par ex : ma-station.ifsic.univ-rennes1.fr.

. Un nom relatif doit être complété localement par un suffixe, celui du domaine local

par ex : ma-station(.ifsic.univ-rennes1.fr.)

nota : cette complémentation est définie par des règles purement locales

Remarque : ne pas confondre sous-domaine (de noms) et sous-réseau (IP).

2.3.2 Délégation / domaine de noms

Chaque organisation a la responsabilité de l'administration de son espace de noms (appelé "name domain").

Le responsable d'un domaine de noms peut décider de déléguer à un sous-responsable l'administration d'une partie du domaine des noms dont il a la charge.

Une arborescence de domaines et sous-domaines est ainsi créée.

Les sous-domaines d'un domaine de noms forment une partition du domaine.

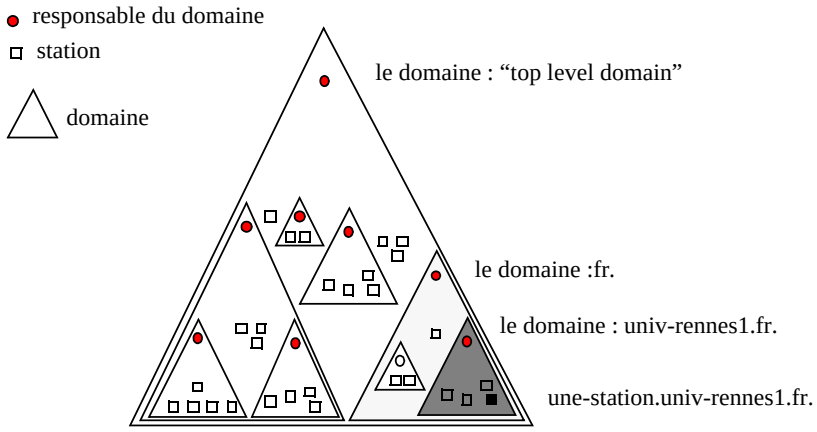
Le nom d'un domaine de noms est formé par la suite des labels identifiant la branche associée au domaine de noms.

Remarque : The NIC ("Network Information Center") à la responsabilité d'administrer le domaine de niveau le plus élevé.

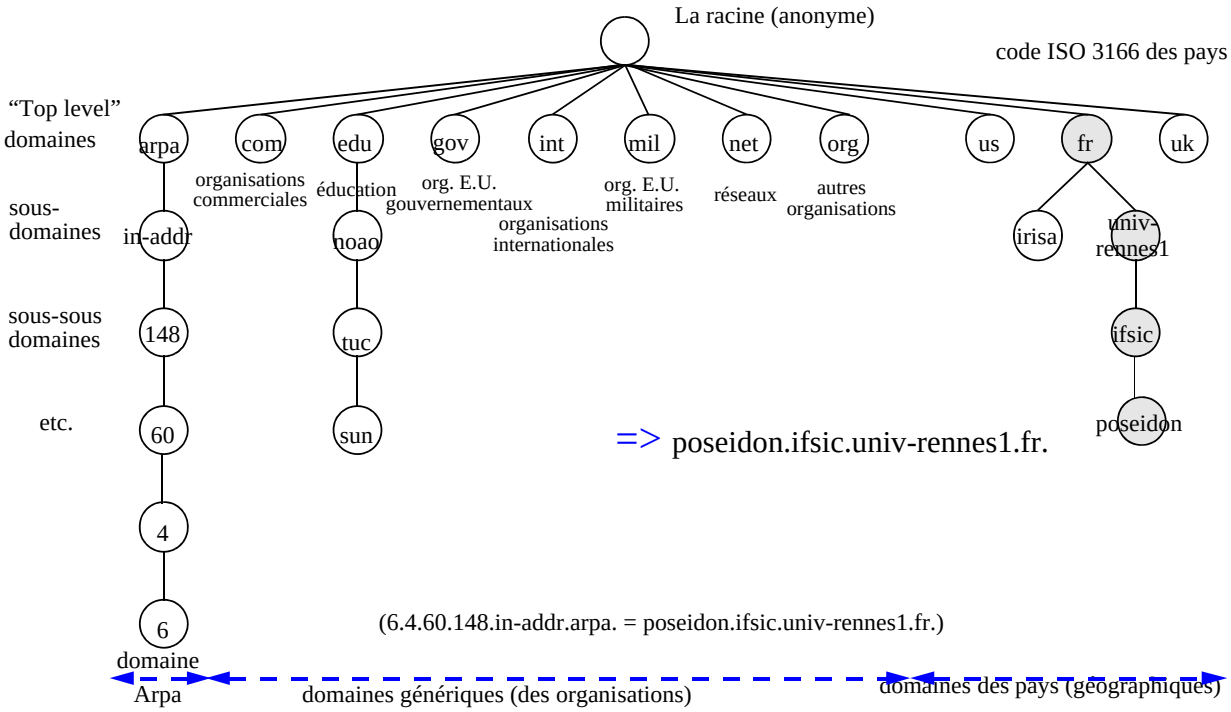
Remarque : chaque domaine gère de manière autonome ses noms.

Remarque : l'arbre des domaines de noms n'a aucun besoin d'être équilibré.

Exemple :



2.4. L’arborescence des domaines de noms sous Internet



2.5. Obtention d'un domaine en France

L'Afnic est le gestionnaire du domaine .fr.

==> http://www.nic.fr. !

3. La résolution de noms

3.1. La "Host table"

3.1.1 Présentation

Solution triviale au problème de traduction :

- chaque système contient un fichier des associations nom/adresse

Sous Unix : /etc/hosts (sous Windows : Windows\host)

- Exemple : le fichier /etc/hosts de la station "poseidon" :

```
#
# Internet host table
#
127.0.0.1 localhost
148.60.4.20 poseidon.ifsic.univ-rennes1.fr. poseidon
```

- La première entrée :
  - . 127.0.0.1 = "local loopback address"
  - . "localhost" = nom générique de la station elle-même
    - . les accès locaux ou distants peuvent être codés de manière identique
- La seconde entrée :
  - . l'adresse de la station : 148.60.4.20
  - . le nom officiel et les alias de la station

3.1.2 Conclusion

Cette technique n'est pas "scalable" :

- le réseau mondial contient des millions de stations
  - . le fichier local devrait contenir une entrée pour toutes les stations
- le réseau mondial est modifié en permanence (pannes, adjouts, suppressions, etc.)
  - . l'administration serait très difficile : mise-à-jour multiples, lenteur, risque d'incohérence, etc.

Il faut une technique offrant :

- un contrôle centralisé par domaine
- une dissémination automatique des associations : nom/adresse

=> Système réparti de serveurs de noms : DNS ("Domain Name System")

Cependant, cette technique locale est utilisée :

- lors du démarrage du système (lors du "boot"),
- sur les petits sites isolés du reste du réseau,
- sur les vieilles stations ne disposant de DNS.

3.2. Résolution des noms par serveurs

3.2.1 Les serveurs

"Domain Name System" : un système réparti de serveurs de noms.

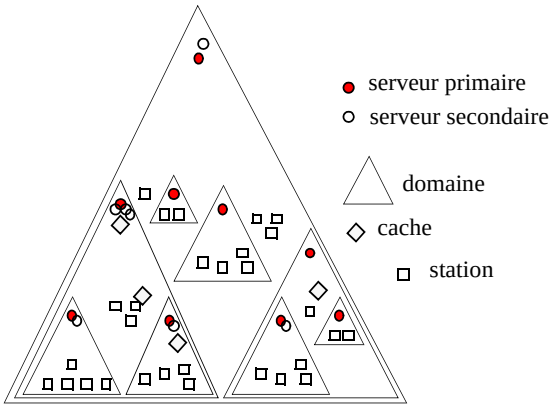
A chaque domaine de noms est associé au moins un serveur primaire.

- c'est le serveur responsable du domaine ("authoritative server")
  - . les administrateurs ont un point central de gestion
- ce serveur contient les informations relatives au domaine
  - . niveau supérieur : le serveur du domaine racine ("root server")
  - . niveau inférieur : les serveurs de chacun de ses sous-domaines
  - . les règles de répartition des noms dans les sous-domaines
  - . les noms qu'il gère directement

Ce serveur primaire peut être flanqué de serveurs secondaires (aucun ou plusieurs)

- ils assurent la permanence du service : redondance
- ils échangent automatiquement une copie des infos détenues par le primaire
  - . les informations obtenues à partir de ces serveurs sont à jour ("authoritative").
  - . les serveurs secondaires doivent ne pas être localisés dans le domaine pour garantir la disponibilité de leur service

Exemple :



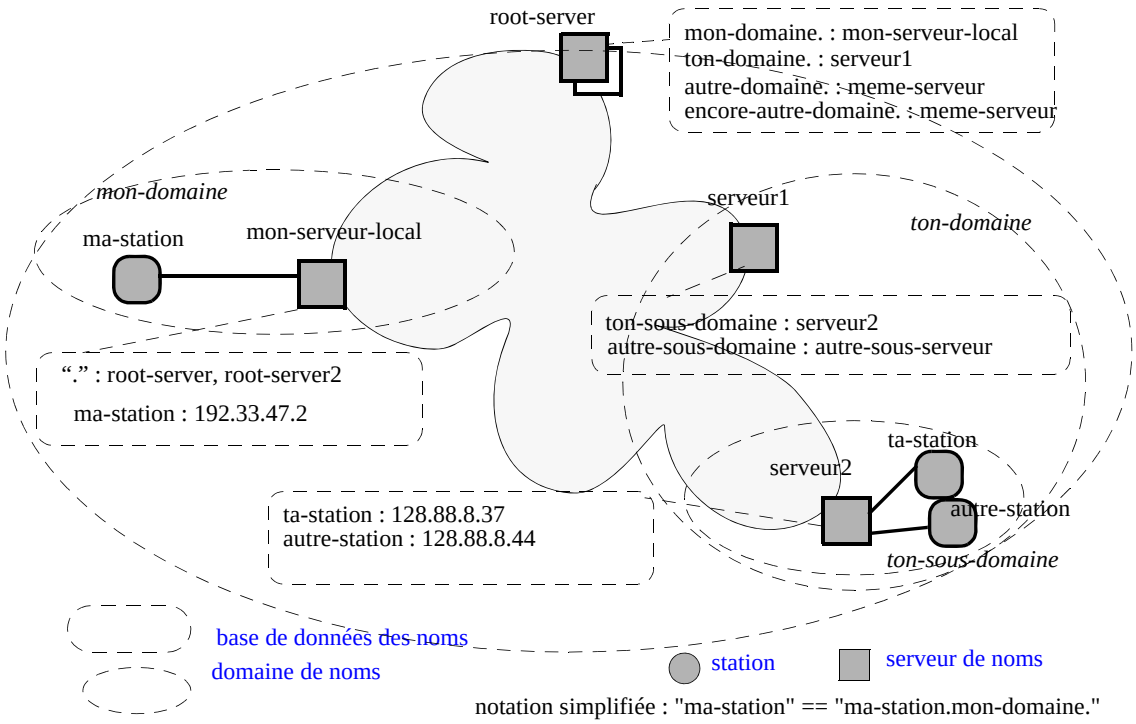
Des caches peuvent être mis en oeuvre afin d'accélérer la résolution des noms :

- la dissémination des infos est effectuée en fonction de l'utilisation réelle.
- les serveurs gérant ces caches stockent des infos qui peuvent ne pas concerner le domaine local.
- les information obtenues peuvent être incorrectes ou incomplètes. Le serveur primaire associe à chaque information une durée de vie.

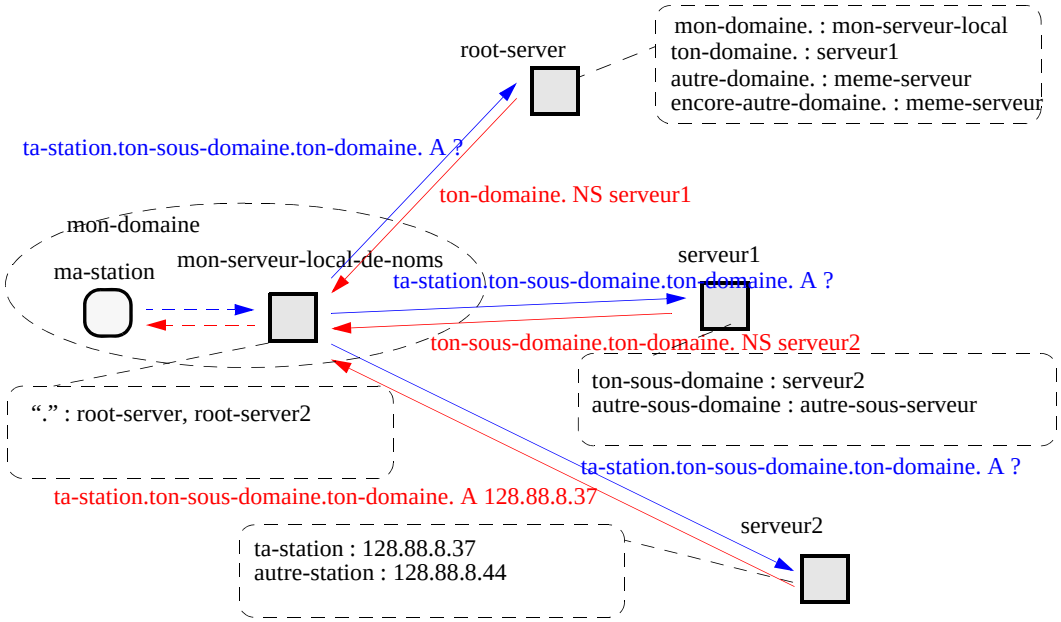
Remarque : un même machine peut supporter plusieurs serveurs de domaines de noms, et avec plusieurs rôles. Les serveurs primaires peuvent ne pas être localisés dans la zone dont ils ont la charge.

3.2.2 Exemple de résolution de noms

Les acteurs :

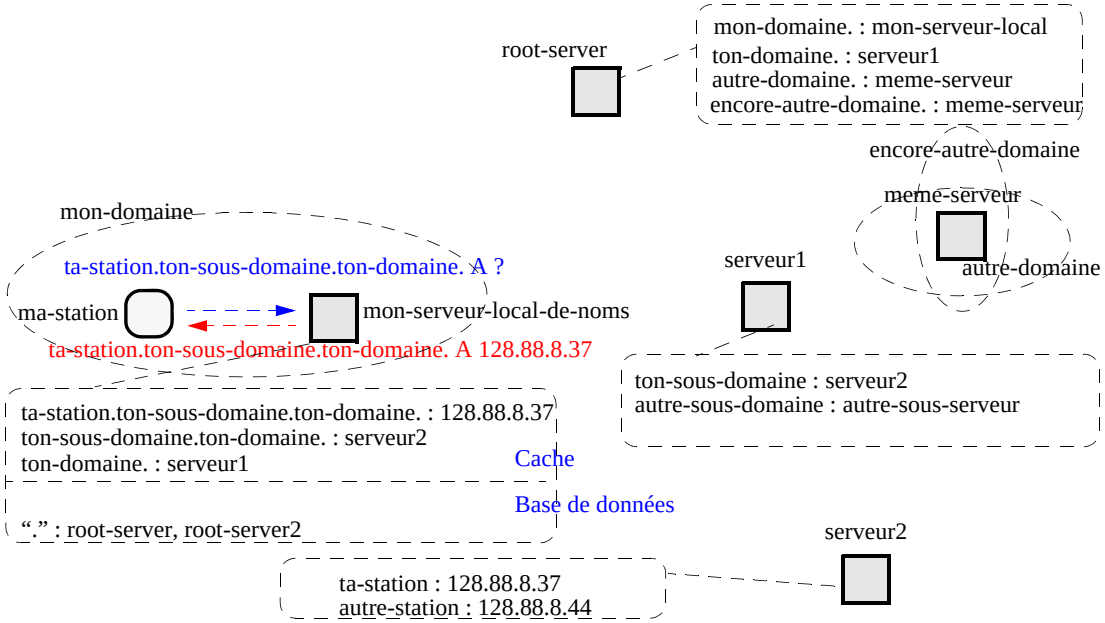


La résolution :



Cet enchainement est non-récursif. Dans le cas récursif, le serveur interrogé interroge d’autres serveurs distants, puis transmet la réponse au serveur local. Cela surcharge le serveur initial.

Le “cache”:



La réponse obtenue ne fait pas autorité : “non-authoritative”.

Remarque : “meme-serveur” supporte 2 domaines !

3.3. Caractéristiques

Différences avec d'autres systèmes de résolution de noms :

- les informations ne sont pas centralisées dans un seul fichier ou une station.
  . répartition de la charge
- les informations obtenues peuvent être détenues par d'autres serveurs.
  . souplesse, fiabilité
- les informations sont obtenues seulement quand on en a besoin.
  . minimisation
- le système gère un cache des informations obtenues précédemment.
  . optimisation

Le DNS peut s'adapter :

- à différents réseaux de communication (“Class”)
- à différents systèmes d'exploitation
- à différents objets et informations (“Type”) :
  . station, serveur de courrier, résolution inverse, informations diverses, etc.

4. Le résolution de noms sous Unix

4.1. Présentation

L’implémentation la plus courante sous Unix :

- BIND (“Berkeley Internet Name Domain”)
  . un “resolver” de noms
  . un serveur de résolution de noms
- Protocole normalisé :
  . RFC 1034 : concepts (1987)
  . RFC 1035: spécifications et implémentations

Le “resolver” de noms :

- code qui effectue la demande,
- sous la forme d’une bibliothèque de fonctions : gethostbyname(), gethostbyaddr()
- s’exécute sur la station locale,
- présent dans toutes les stations (accèdant au service DNS).
- utilise
  . soit des informations locales : /etc/hosts,

. soit des serveurs de noms distants : /etc/resolv.conf

```
domain ifsic.univ-rennes1.fr
search ifsic.univ-rennes1.fr irisa.fr univ-rennes1.fr
nameserver 148.60.4.1
nameserver 148.60.4.5
nameserver 131.254.254.2
```

nom du domaine par défaut
noms de domaines externes (utilisé pour compléter les noms)
adresse de serveur de noms
adresse de serveur de noms alternatifs
etc.

Le serveur de noms :

- répond aux demandes,
- procédé réparti de résolution des noms,
- s'exécute dans des stations distantes,
- un processus par serveur :
  . nommé : named = "name deamon", ou in.named,
  . associé au port n° 53 par TCP ou UDP,
  . présent sur tous les serveurs de noms (offrant le service DNS).

. La commande : nslookup

. La commande : dig

```
%nslookup jaihpur
Server:  dns-2.irisa.fr
Address:  131.254.5.2

Name:    jaihpur.irisa.fr
Address:  131.254.13.18
```


4.2. Exemples de fichiers de la base de données

Les fichiers contiennent des "DNS resource records".

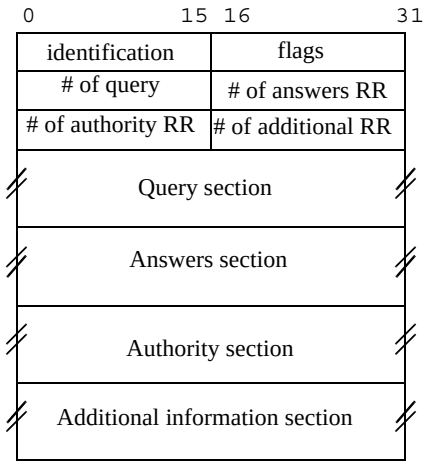
Le fichier du domaine de noms "mon-domaine" :

```
mon-domaine.            SOA mon-serveur.mon-domaine. admin-email.mon-domaine. (     ;; start of authority
      2002011200        ; numero de version (aaaammjjvv)
      10800             ; refresh (3h), fréquence à laquelle les serveurs secondaires tente de m-a-j
      3600              ; retry (1h), délais après lequel les serveurs secondaires retente une connexion
      604800            ; expire (1 sem.), délais après lequel les s. s. non m-a-j de répondront plus aux requêtes
      86400 )           ; TTL (1 jour), valeur par défaut du TTL
;
mon.domaine.            IN NS mon-serveur.mon-domaine.
                        IN NS mon-serveur-bis.mon-domaine.                    ; les serveur de noms du domaine
;
mon-serveur.mon-domaine. IN A 192.33.47.2
ma-station.mon-domaine.  IN A 192.33.47.102                                   ; adresse des stations
;
autre-nom-de-ma-station.mon-domaine. IN CNAME ma-station.mon-domaine.
```

Le fichier inverse :

```
47.33.192.in-addr.arpa. SOA mon-serveur.mon-domaine. admin-email.mon-domaine. ( ;; start of authority
      1                 ; serial
      10800             ; refresh (3h)
      3600              ; retry (1h)
      604800            ; expire (1 sem.)
      86400 )           ; min. TTL (1 jour)
;
47.33.192.in-addr.arpa. IN NS mon-serveur.mon-domaine.
                        IN NS mon-serveur-bis.mon-domaine.)                   ;serveur de noms
;
2.47.33.192.in-addr.arpa.           IN PTR mon-serveur.mon-domaine.
102.47.33.192.in-addr.arpa.         IN PTR ma-station.mon-domaine.
```

4.3. Format général des messages DNS

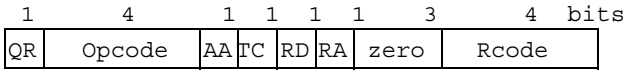


. Un entête de longueur fixe :
- 12 octets

. Identification :
- identifie le message : choisi par le demandeur, retourné par le répondeur.

. # of query (resp. answers, authority, additional) : nombre d'enregistrements dans la section correspondante.
- dans chaque section il peut y avoir 0 ou plusieurs enregistrements
- chaque enregistrement donnent des informations sur une ressource (RR : “resource record”)

4.4. Le champ Flags



QR (1bit) [Query/Response] : 0 = demande; 1 = réponse

Opcode (4 bits) : 0 = recherche standard; 1 = recherche inverse (couteux); 2 = demande de statut du serveur

AA (1bit) [Authoritative answer] : le serveur de noms qui a répondu a autorité sur le domaine .

TC (1bit) [Truncated] : la réponse totale est plus longue (>512 octets) que celle contenue dans le message.

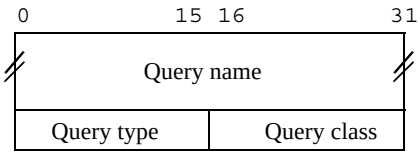
RD (1bit) [Recursion desired] : le demandeur demande au serveur de noms d'effectuer, si nécessaire, une recherche récursive. Ce serveur va s'occuper des recherches auprès d'autres serveurs. Sinon la recherche est itérative : le demandeur devra lui-même interroger les serveurs dont le nom figurera dans la réponse.

RA (1bit) [Recursion available] : le serveur indique au demandeur qu'il propose les services de recherche récursive.

Zero (3bits) : inutilisés.

Rcode (4 bits) : code de retour [0 = pas d'erreur, 1= erreur de format ; 2 = panne de serveur, 3 = le nom n'existe pas (fourni par un serveur ayant l'autorité), 4 = le serveur ne peut pas répondre, 5 = le serveur refuse de répondre].

4.5. Un enregistrement de la section Questions



Query name :
. le nom de la ressource sur laquelle on veut obtenir des informations
. ce champ est de longueur variable

Query type :
. type de l'information recherchée
. autres enregistrements de réponse (champ Type).

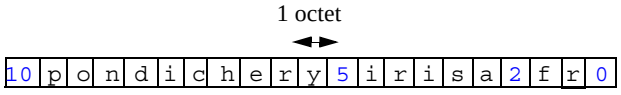
```
Type Code  Description
 A - 1  host address (nom → adresse IP)
 NS - 2  name server   (nom → nom du serveur)
CNAME - 5  canonical name (nom → alias)
 SOA - 6  start of authority (informations sur le domaine des noms)
 PTR  - 12  pointer (adresse IP → nom)
HINFO - 13  host info (nom → informations diverses sur la station)
 MX  - 15  mail exchanger (nom → serveur de messagerie)
AAAA  - 28  IPv6 address (nom → IPv6 address)
 ANY - 255  all records req
```

Query class :
. famille protocolaire employée : Internet =1
. généricité

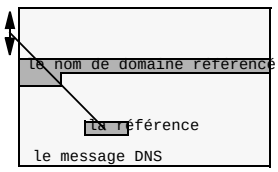
4.6. Le format des noms

Un nom : une suite de labels.
. chaque label étant une suite de caractères (codés en ASCII), suite préfixée par un octet indiquant la longueur de la chaine de caractères [1-63].
. terminé par un label nul (un octet à zéro) symbolisant la racine.
. peut ne pas se terminer en frontière de mots.

Par exemple : pondichery.irisa.fr.

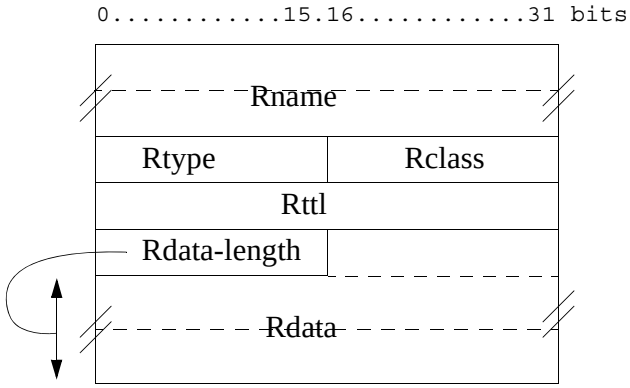


Autre exemple possible : 13.61.254.131.in-addr.arpa.



Une représentation par référence, sur 2 octets, existe :
- permet de ne pas représenter plusieurs fois la même suite de labels
- le premier octet de la référence possède les 2 bits de poids fort à 1
- les bits de poids faibles indiquent l'emplacement de la suite de labels (son déplacement par rapport au début du message DNS)
- utilisé lorsqu'un message DNS utilise plusieurs noms ayant même suffixe

4.7. Le format général des autres enregistrements des autres Sections

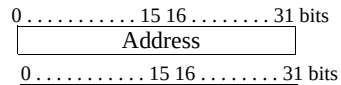


- Rname : le nom de la ressource dont on a obtenu l'enregistrement (cf. Qname)
- Rtype : le type de la ressource (cf. Qtype)
- Rclass : la classe protocolaire (cf. Qclass)
- Rttl : la durée de conservation de l'enregistrement dans le cache
- Rdata-length : la longueur (en octets) du champ Rdata
- Rdata : la valeur de la ressource (dépend du type)

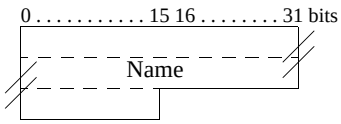
4.8. Différents types de ressources

Chaque type de ressource a un format particulier pour son champ Rdata :

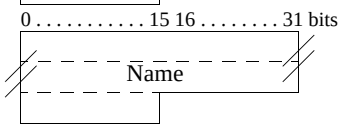
Type A [1] : adresse de la station de nom Rname
. sous Internet : adresse IP 32 bits



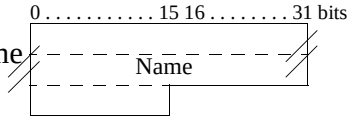
Type NS [2] : nom du serveur du domaine Rname



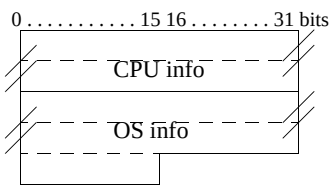
Type CNAME [5] : autre nom de la station Rname



Type PTR [12] : nom de la station dont l'adresse est Rname

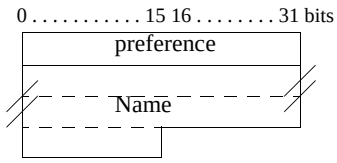


Type HINFO[13] : informations sur l'équipement Rname

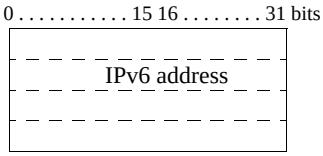


Type MX [15] : nom du serveur de messagerie pour le domaine Rname

. preference : s'il y a plusieurs serveurs disponibles ce champ permet d'indiquer celui qu'il faut favoriser



Type AAAA[28] : adresse de la station de nom Rname
. pour IPv6 (16 octets)



Type * [255] : toutes les informations disponibles sur Rname

4.9. Exemple

Tableau 1 : un message DNS

0	ce75	8180	0001	0002	0001	0000	0366	7470
16	0561	7070	6c65	0363	6f6d	0000	0100	01c0
32	0c00	0500	0100	0185	b900	170b	6272	6963
48	2d61	2d62	7261	6305	6170	706c	6503	636f
64	6d00	c02b	0001	0001	0001	85b9	0004	822b
80	0203	c037	0002	0001	0000	37ae	0012	0352
96	5330	0849	4e54	4552	4e49	4303	4e45	5400

- Entête du message DNS
  - . Identificateur du message : 0xce75,
  - . Flags : "response", recherche standard, réponse d'un cache, message entier, récursion autorisée, récursion disponible, pas d'erreur (0x8180)
  - . 1 question (0x0001), 2 réponses (0x0002), 1 serveur (0x0001), 0 information additionnelle (0x0000)
- Le premier et seul enregistrement de la "Query section"
  - . nom de la machine : Qname = "ftp.apple.com."
  - . type de la ressource : Qtype = A (0x0001) $\Rightarrow$ adresse IP ?
  - . classe protocolaire : Qclass = Internet (0x0001)

5. Conclusion

Service de résolution de noms :

- mais pas uniquement de noms: inverse, serveur de messagerie, infos, etc.
- pour Unix et Internet mais pas uniquement.

Fiable, stable, facile à administrer et performant

On distingue les fonctions :

- administration des noms, délégation
- résolution des noms

Une arborescence de domaines, les noms sont une suite de labels.

Le procédé de résolution :

- locale
- par serveurs (primaire, secondaire, cache)

DNS : “Domain Name System”, BIND, “resolver”/”name server”