DNS - DOMAIN NAME SYSTEM

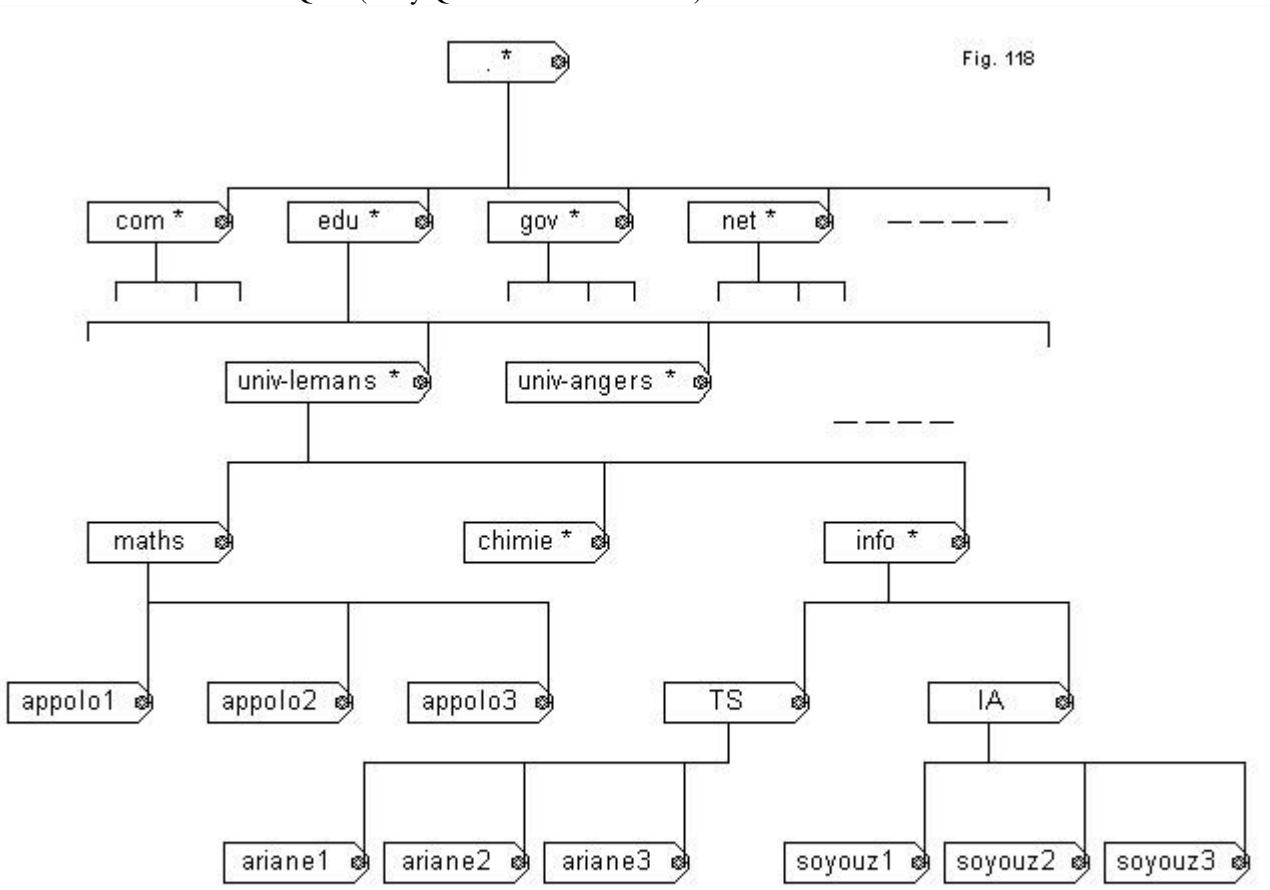
1 - Présentation

Le DNS est un protocole de résolution de noms donnant la correspondance entre les adresses IP sur 32 bits et noms de domaines et d'hôtes et réciproquement.
Une application fait appel aux primitives gethostbyname et gethostbyaddr pour résoudre les adresses dont elle se sert.
Ces commandes se trouvent dans la librairie C "libc" et sont connues sous le nom de "resolver".
Sur les réseaux de taille modeste, des tables de correspondances sont maintenues en statique.
Il s'agit du fichier texte "/etc/hosts".
En cas de mise à jour d'un nom symbolique ou d'une adresse IP, il faut modifier tous les fichiers hosts des machines du réseau.
Le NIS/YP (Network Information System/Yellow Pages) développé par Sun Microsystems, permet de centraliser sur un serveur la maintenance du fichier hosts.
Il est utilisé pour les réseaux de taille modeste.
A l'origine de l'Internet, ces informations étaient stockées dans un fichier HOSTS.TXT maintenu au Network Information Center (NIC).
Devant être téléchargé régulièrement par tous les hôtes présents sur l'Internet, ce système s'est vite avéré inefficace.
En 1984, fut introduit le DNS, développé par Paul Mockapetris.
L'utilisation des noms de domaine est préférable à l'utilisation des adresses IP, particulièrement dans les applications.
En effet, cela procure une couche d'isolation si l'on souhaite faire évoluer les adresses IP dans un réseau.
De plus, si un hôte possède plusieurs interfaces réseau, le DNS renverra toutes les adresses IP et la couche transport pourra sélectionner la plus performante.
Remarque : les noms de domaine ne jouent aucun rôle dans le routage des datagrammes de l'Internet.
Remarques sur la convention de nommage :

- un nom de domaine complet (avec sous-domaines et nom d'hôte) ne doit pas dépasser 255 caractères ;
- chaque partie séparée par un point ne doit pas avoir plus de 63 caractère ;
- le premier caractère d'un champ doit être une lettre de l'alphabet, minuscule ou majuscule ;
- tous les autres signes doivent être compris dans (a-z)|(A-Z)|(-) ;
- tous les autres signes, comme l'espace par exemple, sont interdits ;
- les lettres en majuscules ou minuscules ont la même signification (Univ-LeMans.FR=univ-lemans.fr).

2 - Organisation

Dans le DNS, les noms d'hôtes sont organisés de façon hiérarchique dans des domaines.
Un domaine est un ensemble de sites informatiques qui ont un certain degré de relation entre eux.
C'est le cas pour une université par exemple : univ-lemans.fr.
Ou pour un ISP (Internet Service Provider) : cybercable.fr.
Les universités américaines sont toutes en ".edu" avec un nom de sous-domaine pour chacune d'elles : ".berkeley.edu".
Il est possible de gérer de façon hiérarchique les organisations, jusqu'au nom de l'hôte "appolo1.maths.univ-lemans.fr".
Les noms utilisés sont des FQDN (Fully Qualified Domain Name).



DNS - Exemple d'organisation d'un espace de nommage

Le haut de l'arbre, représenté par un point, correspond à la racine et est appelée le "root domain".
En fonction de sa position, un domaine peut être de premier niveau (top-level), de second niveau ou de troisième niveau.
Les top-level domains les plus fréquents sont les suivants :

.edu	sites liés à l'éduction ;
.com	entreprises commerciales ;
.org	organisations privées non commerciales ;
.net	passerelles et machines administratives de réseau ;
.mil	institutions militaires américaines ;

.gov	institutions gouvernementales américaines.

Les top-levels mil et gov sont exclusivement américains, mais les autres se trouvent partout.
En dehors des USA, chaque état peut utiliser un domaine de premier niveau qui lui est propre et défini par la norme ISO-3166.
La liste des codes de pays est récupérable sur de nombreux sites en faisant une recherche sur ISO3166.
Il faut noter le cas des îles Tuvalu qui ont vendu leur extension .tv à une firme américaine désireuse de commercialiser l'extension aux chaînes de télévision.
L'Australie utilise en plus, des domaines de second niveau tels que : com.au, edu.au, etc.
Dans chaque pays, il y a un NIC gérant ces extensions.
Une machine avec un nom en .fr, ne se trouve pas obligatoirement en France.
En 1993 de nouvelles conventions de nommage ont été proposées par l'IAHC (International Ad Hoc Commitee) quant à l'utilisation des gTLD (generic Top-Level Domains).
De nouveaux gTLD permettront d'"offrir" de nouvelles possibilités de nommage :

.firm	sociétés, activités commerciales ;
.store	magasins proposant des marchandises à la vente ;
.web	activités touchant au Web ;
.arts	activités culturelles et artistiques ;
.rec	détente, divertissements ;
.info	fournisseurs de services d'informations ;
.nom	définitions quelconques.

Il n'est pas possible de tirer de conclusion géographique à partir du nom de domaine.
Cette organisation hiérarchique de nommage permet l'unicité des noms d'hôtes.
L'hôte Ariane2 peut exister plusieurs fois, mais dans des domaines différents.
Le DNS permet de déléguer l'autorité des sous-domaines vers des administrateurs.
A l'intérieur d'un sous-domaine, le choix des noms est indépendant et incombe au responsable de ce sous-domaine.
L'espace de nommage est séparé en zones partant de domaines (les astérisques de la figure précédente représentent les zones).
Les zones correspondent à la surface couverte par un administrateur de domaine.
A l'origine, une demande de nom de domaine à l'InterNIC était gratuite.
Sous l'effet de la croissance rapide de l'Internet, l'InterNIC a décidé de faire payer l'attribution des noms de domaine.
L'InterNIC étant une organisation publique, il fut décidé de lancer un appel d'offres et d'octroyer à une société de droit privé, la possibilité de gérer l'attribution des noms de domaines.
C'est ainsi que la société américaine Network Solutions fut retenue en 1993 et qu'un contrat public fut signé.
A l'heure actuelle, la demande, l'installation et la maintenance pour 2 ans d'un nom de domaine coûte 100$.
Puis 50$ par an à partir de la 3ème année.
Il faut noter que 70% de cette somme est acquise à Network Solutions et 30% à l'InterNIC pour ses développements futurs.
Pour Network Solutions ces sommes représentent une manne financière énorme : 10 000 demandes par semaine, plus de 400 000 depuis sa création, 15 millions de $ acquis !!! A eux.

3 - Recherche de noms

Le DNS correspond à une énorme base de données réparties.
Le DNS est installé sur des machines, très souvent dédiées, que l'on appelle des serveurs de noms.
Pour chaque zone, il doit y avoir au moins deux serveurs de noms nommés serveur primaire et serveur secondaire.
Sur ces serveurs, toutes les données relatives aux noms et aux adresses IP des machines, seront référencées.
Le serveur DNS reçoit les requêtes des différents hôtes qui souhaitent faire référence à une machine mais qui n'en connaissent que le nom symbolique et pas l'adresse IP.
Les recherches se font de manière itérative.
En effet, si un hôte recherche une adresse IP d'une machine située sur un serveur à l'étranger, il ne trouvera pas l'information sur un DNS local.
Après avoir reçu la requête, le serveur de noms local va interroger le serveur de noms du domaine de plus haut niveau par exemple ".edu".
Le serveur de noms de ".edu" va lui transmettre tous les serveurs de noms relatifs au sous-domaine, par exemple le DNS de "berkeley.edu".
Le DNS local de l'hôte appelant va procéder ainsi jusqu'à arriver au serveur de noms gérant la zone où l'hôte de destination se trouve et dont l'adresse IP était recherchée.
Une fois que l'adresse IP de l'hôte destination est reçue sur le serveur de noms local, celle-ci est transmise à la station qui souhaitait communiquer avec cet hôte.
Le trafic généré peut sembler important mais il le sera toujours beaucoup moins que celui généré par le fichier HOSTS.TXT.
La technique du DNS a été améliorée en stockant dans les caches locaux des serveurs DNS, le résultat des requêtes déjà traitées.
A la prochaine demande, le serveur de noms commencera par analyser son cache avant d'interroger les autres DNS.
Les informations contenues dans le cache sont purgées à intervalles réguliers, définis dans le paramétrage du DNS.

4 - Serveurs de noms

Les serveurs de noms contenant toutes les informations relatives aux hôtes d'une zone particulière sont dits "ayant autorité" sur cette zone.
On les appelle des "serveurs de noms autoritatifs" (barbarisme pour Authoritative Name Server).
Il doit y avoir un serveur maître ou serveur primaire par zone et des serveurs secondaires qui vont récupérer à intervalles réguliers les informations du serveur primaire.
Posséder plusieurs serveurs de noms permet de distribuer la charge induite par les requêtes et donne une certaine tolérance aux pannes.
Il est enfin possible de mettre en place un serveur de noms n'ayant autorité sur aucun domaine.
C'est le cas quand on souhaite mettre en place un serveur de noms sur un réseau local.
Ce type de serveur s'appelle un "caching only server".

5 - La base de données DNS

La base de données DNS ne contient pas uniquement des noms logiques et des adresses IP.
Elle contient également des informations sur d'autres DNS ainsi que d'autres types d'entrées.
Chaque entrée dans la base de données DNS, ou chaque information élémentaire s'appelle un "Resource Record" ou RR.
Chaque enregistrement est associé à une classe spécifiant le type de réseau auquel il s'applique et à un type décrivant le genre de données.
La classe peut être IN (Internet) pour des adresses IP ou parfois Hesiod correspondant à un protocole utilisé par le MIT ou d'autres encore.
Le RR le plus courant est de type A et correspond à une association d'un domaine qualifié et d'adresse IP.
Exemple :

```
ariane2   IN   A   149.76.12.2
```

Syntaxe du RR A :

```
<HOST> [<TTL>] [<CLASS>] A <ADDRESS>
```

HOST	Nom de l'hôte. Le nom d'hôte est donné sans nom de domaine car celui-ci est donné en début de zone
TTL	Time To Live en secondes pour ce Resource Record
CLASS	Toujours IN
ADDRESS	Adresse IP du serveur de l'hôte

Exemple :

```
; Hôtes dans le domaine XL.
PRIMARYDNS   A     151.87.0.23      ; adresse IP de PRIMARYDNS.XL
             A     165.160.10.10    ; l'hôte est Multihomed
DNS2         A     151.87.0.54      ; adresse IP de DNS2.XL
DNS3         A     151.87.0.55      ; adresse IP de DNS3.XL
SECONDARYDNS CNAME         DNS2    ; DNS2 peut être identifié
                           ; comme SECONDARYDNS
```

Il est possible qu'un hôte possède plusieurs noms.
Un seul de ces noms est déclaré comme nom officiel ou nom canonique (Canonic NAME).
Tandis que le nom canonique est associé à A, les autres ne sont que des alias.
Exemple :

```
ariane2     IN    A        149.76.12.2
hote2Signal IN    CNAME    ariane2
```

Le fichier contenant ces informations s'appelle "named.hosts".
Syntaxe du RR CNAME :

```
<NICKNAME> [<TTL>] [<CLASS>] CNAME <HOST>
```

NICKNAME	Nom d'alias de l'hôte. S'il n'y a que le nom de l'hôte, celui-ci fait partie du domaine de départ de la zone
TTL	Time To Live en secondes pour ce Resource Record
CLASS	Toujours IN
HOST	Nom de l'hôte avec le nom de domaine absolu quand il ne fait pas partie du domaine de départ de la zone

Au début de ce fichier on trouve un enregistrement sur plusieurs lignes et dont le type est SOA (Start Of Authority).
Cet enregistrement contient les informations générales sur la zone pour laquelle le serveur a autorité.

Cet enregistrement comprend, entre autre, la durée par défaut en secondes pendant laquelle les enregistrements doivent être conservés.
En général entre 86 400 (1 jour) et 604 800 (1 semaine).
Exemple extrait du fichier named.hosts pour le département info :

```
;
; Informations ayant autorité pour info.univ-lemans.fr
@   IN   SOA  soyouz1.ia.info.univ-lemans.fr admin.info.univ-lemans.fr (
       991208    ; numéro de série
       360000    ; mise à jour
       3600      ; tentative après échec
       3600000   ; délai d'expiration
       86 400    ; ttl par défaut (time to live)
    )
```

Le nom spécial @ correspond au propre nom du domaine.
Syntaxe du RR SOA :

```
<NAME> [<TTL>] [<CLASS>] SOA <PRIMESERVER> <MAILPERSON> <SERIAL> <REFRESH> <RETRY> <EXPIRE>
<MINIMUM>
```

NAME	Nom du domaine (ou de la zone) avec lequel démarre la zone
TTL	Time to Live de ce Resource Record (en secondes)
CLASS	Toujours IN
PRIMESERVER	Noms du serveur et du domaine du DNS primaire du domaine concerné
MAILPERSON	Adresse électronique de la personne à contacter pour la zone dans laquelle un point remplace le @
SERIAL	Numérotation continue de la version de ce Zone File. Il doit être incrémenté à chaque mise à jour
REFRESH	Nombre de secondes après qu'un Name Server secondaire doit se mettre en relation avec le Name Server primaire pour vérifier la validité des RR stockés. Une valeur de 3600 (1 heure) est recommandée.
RETRY	Nombre de secondes qu'un Name Server secondaire doit attendre après un échec de contact avec le Name Server primaire, pour recommencer l'opération. La valeur recommandée est 600 (10 minutes)
EXPIRE	Nombre de secondes après lesquelles un Name Server secondaire doit déclarer non valables, ses RR pour la zone concernée si aucune mise à jour n'a eu lieu dans l'intervalle. En général 2 600 000 secondes (1 mois)
MINIMUM	Une indication en secondes qui est utilisée comme valeur par défaut de paramètre TTL dans d'autres RR si l'information pour ce paramètre n'a pas été donnée

Exemple :

```
;
;Début de la Zone
XL.   IN   SOA   PRIMARYDNS.XL DNS-MASTER.XLNIC.NET (
              282374   ; numéro courant
              1800     ; actualisation toutes les 30 minutes
              600      ; en cas d'erreur, essai toutes les 10 minutes
              604800   ; s'arrête après une semaine
              86400    ; default TTL, un jour
          )
```

Les serveurs de noms de domaines doivent connaître les zones d'autorité de niveau inférieur.

Les entrées correspondant à ce genre d'informations sont notées NS.
L'entrée NS donne le nom qualifié du serveur et une entrée A donnera l'adresse IP correspondante.
Ces entrées qui servent à lier la hiérarchie sont souvent appelées "glue records".
Exemple extrait du fichier named.hosts pour le univ-lemans.fr :

```
; Informations ayant autorité pour univ-lemans.fr
.........
; Glue records pour la zone info.univ-lemans.fr
info            IN    NS   soyouz1.ia.info.univ-lemans.fr.
                IN    NS   ariane1.ts.info.univ-lemans.fr
soyouz1.ia.info   IN    A    149.76.12.1
ariane1.ts.info   IN    A    149.76.5.1
.........
```

Syntaxe du RR NS :

```
<DOMAIN> [<TTL>] [<CLASS>] NS <SERVER>
```

DOMAIN	Nom du domaine pour lequel le Name Server est responsable. Le signe @ se réfère au domaine actuel pour lequel le Zone File actuel a été chargé dans le Name Server
TTL	Time To Live en secondes pour ce Resource Record
CLASS	Toujours IN
SERVER	Nom du serveur désigné comme responsable pour ce domaine

Exemple :

```
XL.   NS    DNS2.XL.        ; second Name Server dans le domaine .XL
      NS    DNS3.XL.        ; troisième
      NS    SUN2.QUNET.NET.  ; et un de l'autre côté de l'océan Atlantique
```

Le Name Server secondaire peut être hébergé à n'importe quel endroit du réseau.
Les autres RR (Resource Records) existants sont :

```
MX      Mail eXchanger   Serveur qui sert de boîte aux lettres pour le courrier entrant
HINFO   Host INFO        Informations sur le matériel et le SE de l'hôte
PTR     PoinTeR          Crée un alias qui renvoie à d'autres éléments du DNS
```

La redirection du mail fait partie intégrante du DNS qui renverra l'adresse du serveur sur lequel le protocole de courrier est implémenté.
Syntaxe du RR MX :

```
<NAME> [<TTL>] [<CLASS>] MX <PREFERENCE> <HOST>
```

NAME	Nom de l'hôte, ou avec le domaine
TTL	Time To Live en secondes pour ce Resource Record
CLASS	Toujours IN
PREFERENCE	Pour chaque hôte plusieurs RR peuvent être fournis. Le champ Preference détermine l'ordre de priorité. Le serveur possédant la plus petite préférence (0) sera sollicité en premier ; puis l'hôte dont la préférence est juste supérieure
HOST	Nom de l'hôte sur lequel le protocole de courrier est installé

Exemple :

```
*.RZ.ILE-UNI     MX   1    SERVER.RZ.ILE-UNI   ; tous les mails au serveur
                                    ; du centre informatique
SERVER.GESTION.ILE-UNI  A  199.65.0.15   ; hôte SERVER.GESTION.ILE-UNI .XL
                MX   1    SERVER.GESTION.ILE-UNI
```

Syntaxe du RR HINFO :

```
<HOST> [<TTL>] [<CLASS>] HINFO <HARDWARE> <SOFTWARE>
```

HOST	Nom de l'hôte, ou avec le domaine
TTL	Time To Live en secondes pour ce Resource Record
CLASS	Toujours IN
HARDWARE	Nom du système informatique sur lequel l'hôte fonctionne (sans espaces)
SOFTWARE	Nom du système d'exploitation 'sans espaces)

Exemple :

```
; Hôtes et domaines pour de petites sociétés et institutions, sans Name Server
www.WebCom   A   216.173.18.1                ; hôte www.WebCom.XL
          MX  1            www.WebCorn     ; mail au même hôte
          HINFO  PC WINNT
```

L'IANA (Internet Assigned Number Authorithy a défini les désignations des matériels et systèmes d'exploitation. Ces définitions sont accessibles à la [RFC1700].

Exemple d'un Zone File du domaine XL des îles Xanadu (source : La Bible Internet Micro-Application) :

```
;
;Début de la Zone
XL.    IN    SOA    PRIMARYDNS.XL DNS-MASTER.XLNIC.NET (
                282374      ; numéro courant
                1800        ; actua1isation toutes les 30 min
                600         ; en cas d'erreur, essai toutes les 10 min
                604800      ; s'arrête après une semaine
                86400       ; default TTL, un jour
                )
XL.    NS    DNS2.XL.           ; second Name Server dans le domaine .XL
      NS    DNS3.XL.           ; troisième
      NS    SUN2.QUNET.NET.    ; et un de l'autre côté de l'Atlantique
; Hôtes dans le domaine XL.
PRIMARYDNS   A      151.87.0.23   ; adresse IP de PRIMARYDNS.XL
          A      165.160.10.10 ; l'hôte est Multihomed
DNS2         A      151.87.0.54   ; adresse IP de DNS2.XL
DNS3         A      151.87.0.55   ; adresse IP de DNS3.XL
SECONDARYDNS        CNAME  DNS2   ; DNS2  peut être identifié
                          ; comme SECONDARYDNS
; Hôtes et domaines pour de petites sociétés, sans Name Server
www.WebCom   A      216.173.18.1  ; hôte www.WebCom.XL
          MX     1 www.WebCorn ; mail au même hôte
          HINFOPC WINNT
SERVER.RZ.ILE-UNI  A   199.65.0.10  ; hôte SERVER.RZ.ILE-UNI.XL
PLUTO.RZ.ILE-UNI   A   199.65.0.11  ; hôte PLUTO.RZ.ILE-UNI.XL
*.RZ.ILE-UNI       MX  1   SERVER.RZ.ILE-UNI  ; tous les mails au serveur
                                   ; du centre informatique
SERVER.GESTION.ILE-UNI  A   199.65.0.15  ; hôte SERVER.GESTION.ILE-UNI .XL
                    MX  1     SERVER.GESTION.ILE-UNI
; Hôtes et domaines pour des entreprises sur d'autres Name Server
UNITED-BANANAS    NS   DNS2.XL.     ; *.UNITED-BANANAS.XL
                           ; sur DNS2.XL
OEPNV             NS   DNS.OEPNV.XL ; propre Name Server
DNS.OEPNV         A    194.42.127.3 ; glue-record
```

```
CAPITALE        NS   SUN1.XLSERVICEPROVIDER.NET.    ; sur le DNS du provider
```

6 - Requêtes inverses

Certaines applications cherchent à connaître le nom canonique de l'hôte à partir de l'adresse IP, c'est à dire le besoin contraire au DNS.
Cette opération est une "requête inverse" ou "reverse mapping".
Il peut être intéressant, pour des raisons de vérification de l'identité d'un client par exemple, de connaître son nom canonique.
Dans un réseau local, il est très aisé d'utiliser le fichier "/etc/hosts" pour mener à bien la requête inverse.
Il n'est pas possible de le faire avec le DNS.
C'est pour cette raison qu'un domaine spécial a été créé et qui se nomme "in-addr.arpa".
Ce domaine contient les adresses de toutes les machines en notation inversée.
Par exemple, l'adresse 149.76.12.2 correspondra au nom :

```
2.12.76.149.in-addr.arpa.
```

Le RR correspondant dans le fichier "named.rev" sera PTR.
Exemple extrait du fichier named.rec pour le sous-réseau 12 de info.univ-lemans.fr.

```
;
; le domaine 12.76.149.in-addr.arpa
.....
2    IN    PTR    soyouz2.ia.info.univ-lemans.fr
3    IN    PTR    soyouz3.ia.info.univ-lemans.fr
.....
```

Les divisions en zones ne correspondent pas aux divisions des sous-réseaux.
Par exemple pour le sous-réseau correspondant à ts.info.univ-lemans.fr il faudra créer "5.76.149.in-addr.arpa".
Une conséquence de ce système réside dans le fait que les sous-réseaux doivent faire appel à des masques à octets.
Il ne serait pas possible d'utiliser un masque de ce type : 149.76.12.192.

7 - La commande whois

Cette commande est généralement une commande Unix.
Elle permet d'obtenir tous les renseignement sur un nom de domaine.
Ceci est pratique si l'on souhaite savoir si un nom de domaine a déjà été attribué.
Il est également possible d'obtenir ces informations en allant sur le site de l'InterNIC :

```
http://rs.internic.net/whois.html
```

Exemple de requête whois sur pichereau.net :

```
Whois Search Results

Search again:

Whois Server Version 1.1
```

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to http://www.internic.net for detailed information.

```
Domain Name: PICHEREAU.NET
```

Registrar: ALABANZA, INC.

```
Whois Server: whois.alabanza.com

Referral URL: www.alabanza.com

Name Server: GOMEZ.CYBERCABLE.TM.FR

Name Server: TDR1.CYBERCABLE.TM.FR

>>> Last update of whois database: Sun, 2 Jan 00 02:00:00 EST <<<
```

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and Registrars.

8 - Le protocole DNS

Le Name Server peut recevoir des requêtes de la part de Resolvers (application cherchant à résoudre un nom de domaine) ou d'autres Name Servers.
La communication entre un client DNS et son Name Server peut être basée sur UDP ou sur TCP.
Dans les deux cas, il s'agira du port 53.
Les Name Server doivent être capable de supporter UDP ou TCP tandis que le client peut choisir l'un ou l'autre.
Le DNS échange des RR entre un Name Server et son client sous forme ASCII.
Le format global d'un message DNS est le suivant.

Fig. 120

Structure d'un message DNS

L'en tête est constitué de 6 mots de 16 bits.

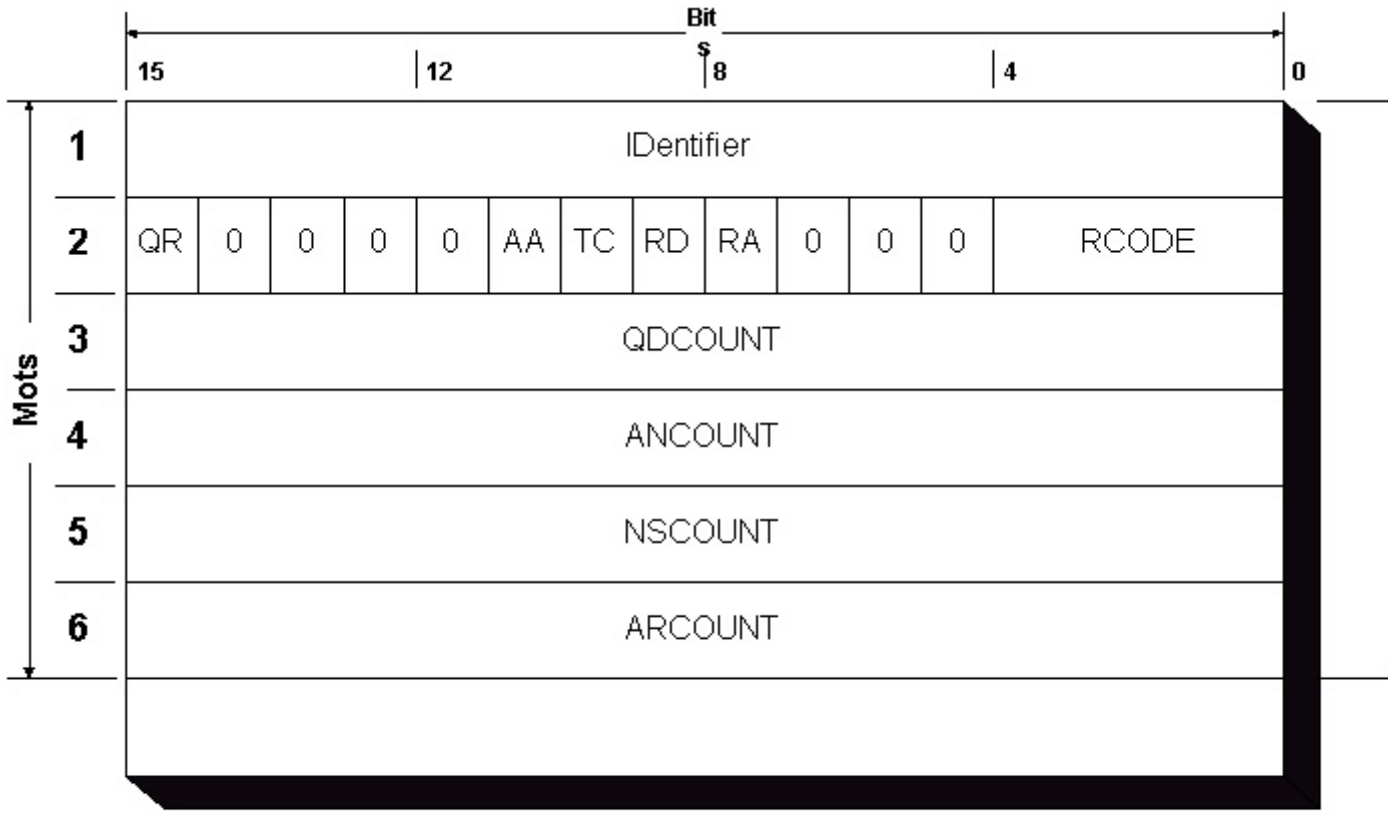


Fig. 119

Format de l'en-tête d'un message DNS

IDentifier.
Ce champ permet d'établir une connexion entre la demande à un serveur DNS et la réponse qui lui sera fournie. Une valeur quelconque unique est attribuée à ce champ de 16 bits lors de la requête. La réponse renverra la même valeur.
Les flags décrivent le statut et le type de messages DNS.
QR (Query Response).
Ce bit est à 0 lors d'une requête DNS et à 1 lors de la réponse.
AA (Authoritive Anwser).
Quand ce bit vaut 1 cela signifie que le Name Server est compétent pour le domaine interrogé.
TC (Truncation).
Quand TC vaut 1, cela signifie que la réponse à une demande est trop longue (>512 octets). Dans le cas de TCP, ce bit n'a aucune importance.
RD (Recursion Desired).
Si RD est positionné à 1, le Name Server interrogé peut alors renvoyer sa demande à d'autres Name Servers si lui-même n'a pas de réponse à fournir au client.
RA (Recursion Available).
Lors d'une réponse à une demande, RA vaut 1 si le Name Server est capable d'interroger un autre Name Server, à 0 sinon.
RCODE (Response Code).
Message de contrôle de la réponse :

0	OK -aucune erreur
1	Erreur de format -le NS n'a pas pu interpréter la demande
2	Erreur de serveur - le NS n'a pas pu répondre à la demande en raison d'une erreur dans le NS
3	Erreur de domaine - le domaine indiqué est inconnu du NS compétent - il n'existe pas
4	Non implémenté - le NS n'est pas en mesure de satisfaire la demande

5	Refused - Le NS rejette la demande

QDCOUNT.
Nombre des demandes dans la section Question (valeur client).
ANCOUNT.
Nombre des Resources Records dans la section Answer (valeur NS).
NSCOUNT.
Nombre des Resources Records dans la section Authority (valeur NS).
ARCOUNT.
Nombre des Resources Records dans la section Additional (valeur NS).

9 - Structure d'une requête

Le client qui effectue une demande devra renseigner les champs de l'en-tête ainsi que la section Question.
En général la question portant sur un nom de domaine, le champ QDCOUNT vaut 1.

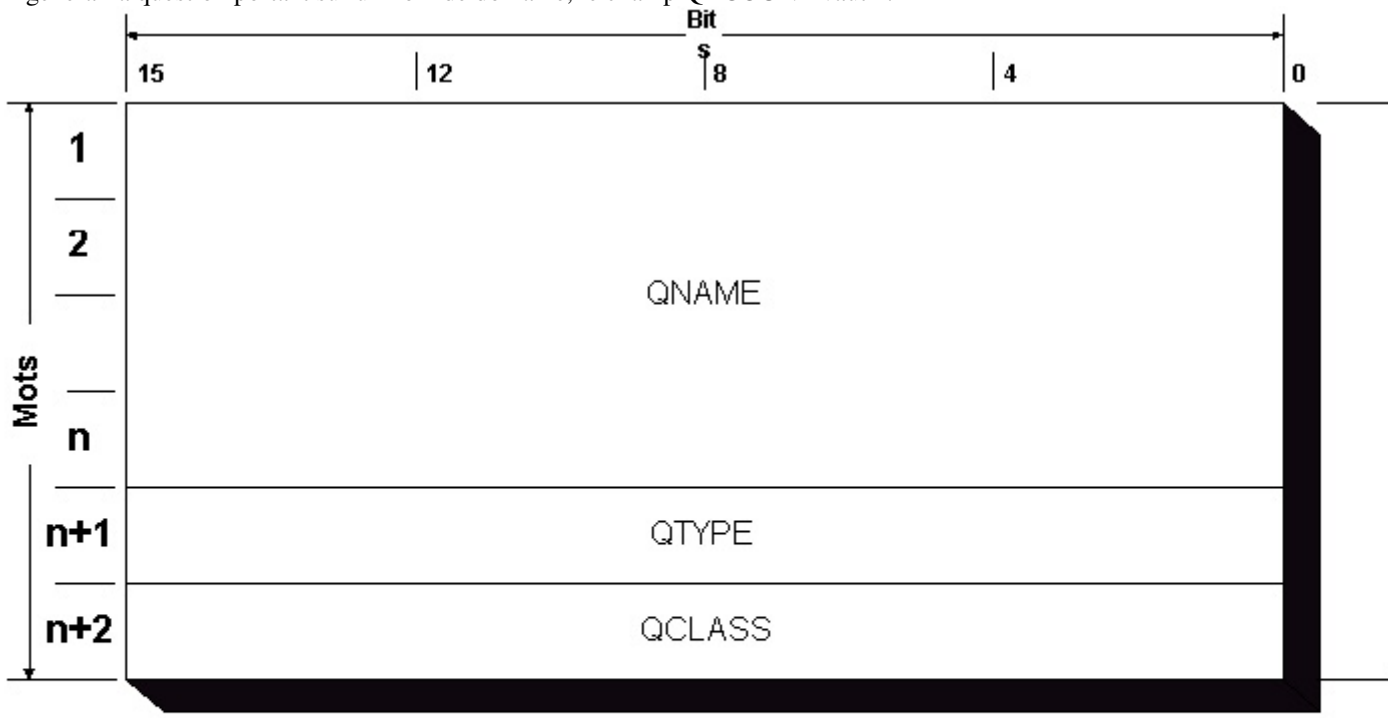


Fig. 121

Format de la section Question d'une demande

QNAME.
Dans ce champ est indiqué le nom du domaine/hôte recherché. Le nom est décomposé en ses domaine, sous-domaines et hôte et les points séparateurs sont ôtés. Le codage se fait par chaîne avec un premier octet de longueur de chaîne puis les octets de la chaîne. Ceci pour chaque chaîne jusqu'à la dernière qui sera suivie d'un octet à 0. Cet octet à 0 délimite le champ QTYPE.
QTYPE.
Le champ QTYPE, sur 16 bits, décrit le type d'information (RR) que le client souhaite obtenir.

Code	Resource Record	Tâche
1	A	Communique l'adresse IP d'un hôte donné
2	NS	Fournit le nom d'un NS compétent pour un domaine donné
5	CNAME	Fournit le ou les noms d'alias pour un hôte donné
6	SOA	Fournit les informations du SOA RR pour un domaine donné
12	PTR	Fournit les informations concernant l'élément sur lequel pointe le nom indiqué
13	HINFO	Fournit les informations sur le matériel et le SE d'un hôte donné
15	MX	Signale les hôtes auxquels doit être transmis le courrier électronique pour l'hôte donné

252	(AFXR)	Délivre tous les RR pour une zone donnée sur son domaine de départ
255	(*)	Retourne tous les RR à l'hôte ou au domaine donné

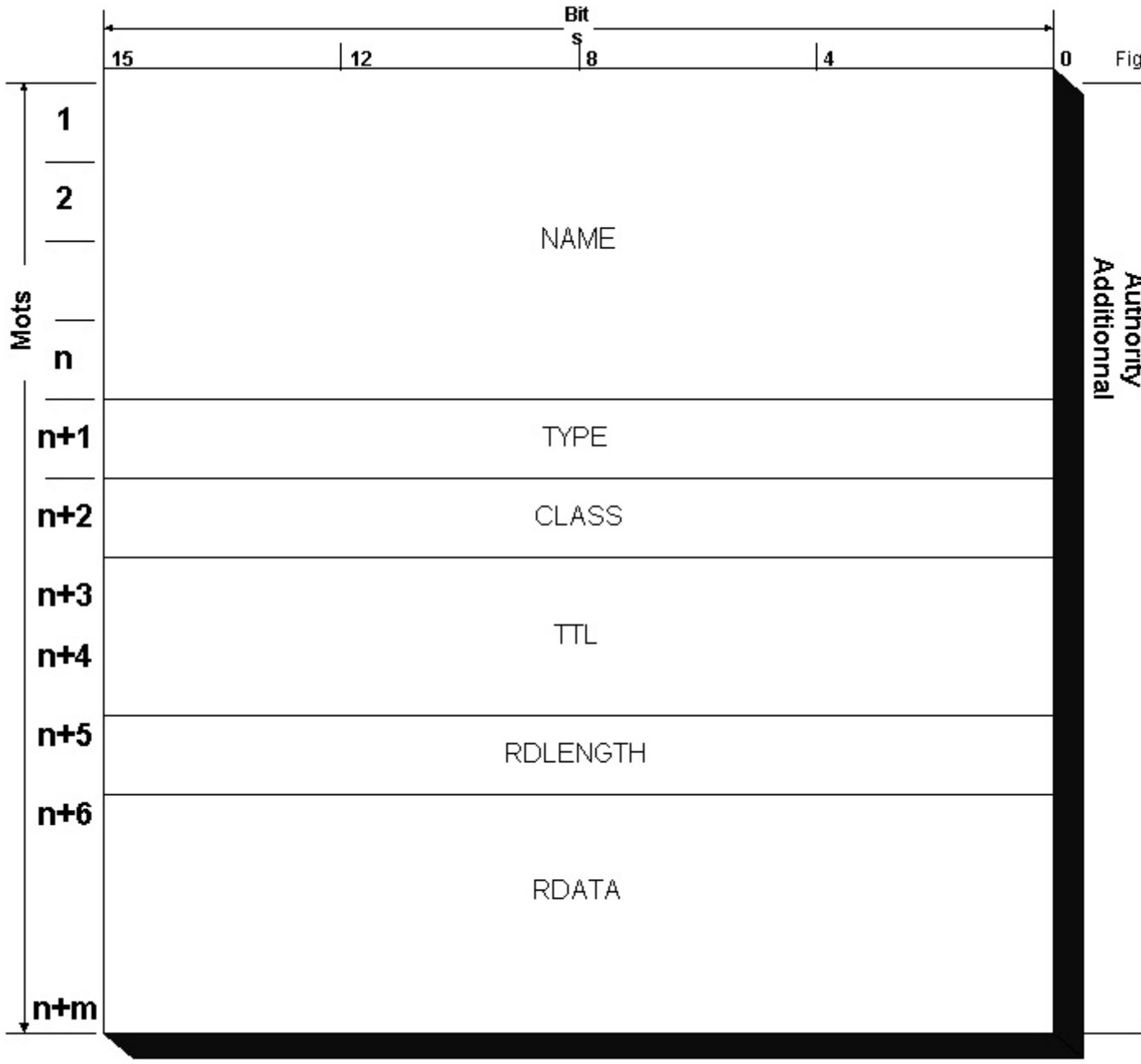
Le code qui apparaît le plus souvent est le 1 correspondant à la communication d'une adresse IP.
QCLASS.
Entier sur 16 bits qui spécifie la classe dans laquelle les informations sont obtenues. Aujourd'hui, seule la classe INTERNET dont la valeur est 1, est utilisée.

10 - Structure de la réponse

Bien qu'il y ait un identifiant, la Question est retournée dans le message de réponse.
Le nombre de RR retournés se trouve dans les champs correspondants de l'en-tête de message DNS.
Si en retour, la section Answer est vide, deux cas peuvent se présenter :

- L'élément recherché se trouve réellement dans la zone de compétence du NS auquel la requête a été adressée, mais le ZONE FILE est mal renseigné, ou l'hôte a changé de nom ou il a été supprimé. Le champ RCODE indiquera le type d'erreur rencontrée ;
- L'élément recherché ne se trouve pas dans le domaine de compétence du NS interrogé et le bit RD n'a pas été positionné à 1. Dans ce cas, le NS n'interroge pas d'autres NS;

Dans ce second cas de figure, avec le bit RD=0, si le NS connaît d'autres NS à interroger, il communiquera ces informations au client, dans la section Authority.
La section Additional contient des informations supplémentaires, par exemple, des RR de type A avec les adresses IP de NS dont les noms ont été cités dans Authority.
Structure des champs Answer, Authority et Additionnal.



Format des sections de réponses à une demande DNS

NAME.
Nom de l'élément concerné par la recherche. La notation est la même qua dans la section Question.
TYPE.
Type des RR retournés sous la forme d'entiers de 16 bits. Les mêmes codes que pour la section Question sont utilisés.
TTL (Time To Live).
Durée en secondes sous la forme d'un entier sur 32 bits, qui restent au RR avant d'être vidé du cache client. Si cette valeur vaut 0, la réponse n'est valide que pour la requête en question.
RDLENGTH.
Champ sur 16 bits donnant au travers d'un entier, la longueur du champ RDATA.
RDATA.
Le contenu du RR en fonction de son type (adresse IP ou nom d'un Name Server, par exemple) :

- Dans le cas d'un RR A, l'adresse IP de l'hôte courant se trouve dans RDATA sous la forme 32 bits ;
- Dans le cas d'un RR NS, le nom de l'hôte NS du domaine recherché, est donné dans le RDATA, avec comme convention de codage, la même que citée précédemment ;

- Dans le cas d'un RR HINFO, les noms du matériel et du SE dans le RDATA sous la forme de chaînes.

11 - Technique de compression

Les DNS sont capables d'utiliser des algorithmes de compression de données afin d'économiser la bande passante et d'améliorer les temps de réponse.
La technique de compression est utilisée pour les messages en retour.
L'algorithme est basé sur le fait que les chaînes de caractères représentant des noms de domaines apparaissent de façon fréquente dans un même message.
Lorsque l'option de compression sera choisie, une deuxième occurrence d'une chaîne de caractères sera représentée par un pointer de 14 bits, représentant un offset par rapport au début du message et pointant vers la première occurrence de la chaîne de caractères.
Par définition, chaque chaîne représentant un domaine, possède au maximum 63 caractères donc codable sur 6 bits.
Les 2 bits restants sont utilisés pour informer le DNS que la compression est mise en œuvre.
Donc, quand la compression est demandée, les 6 bits de cet octet plus les 8 du suivant, soit au total 14 bits, sont utilisés pour donner l'offset dans le message.
Ce système est utilisé même si les noms de domaine ne sont que partiellement identiques.

12 - Spécifications DNS dans les RFC

[rfc1032]	Domain Administrators Guide, M. Sthal, 1987	décrit la politique d'attribution des noms de domaine, les institutions compétentes et la tâche des administrateurs de domaine.
[rfc1033]	Domain Administrators Operations Guide, M. Lottor, 1987	manuel pour les administrateurs de domaine, comportant un point sur l'édition et la maintenance de Zone Files pour Name Server.
[rfc1034]	Domain Names - Concepts and Facilities, P. Mockapetris, 1987	document de référence décrivant la constitution de l'espace symbolique du DNS, le rôle des divers logiciels et leur interaction.
[rfc1035]	Domain Names - Implementation and Specifications, P.Mockapetris, 1987	définit le protocole DNS pour la communication entre des Name Servers et des clients DNS et fournit des conseils pour la réalisation concrète de Name Servers et de Resolvers.
[rfc1296]	Internet Growth (1981-1991), M. Lottor, 1992	belle étude sur la croissance de I'Internet, avec l'exemple du DNS.
[rfc1480]	The US Domain, A. Cooper & J. Postel, 1993	décrit la constitution du domaine américain et les règles d'installation de nouveaux sous-domaines pour des institutions d'état, des écoles et des autorités à l'intérieur de ce domaine. Bel exemple de structuration hiérarchique des grands réseaux par les sous-domaines.
[rfc1591]	Domain Name System Structure and Delegation, J. Postel, 1994	définit encore une fois les règles pour la transmission de l'autorité aux sous-domaines à l'intérieur du DNS et ce qui est exigé des administrateurs du DNS.