

RT 21

Administration des Services Réseaux



Chapitre III : Les services annuaires Le DNS (Domain Name System)

Dr. H. Zerrouki

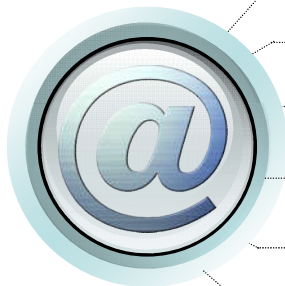
<zerrouki.hadj@gmail.com>

UDL-SBA, Faculté de Génie Electrique

DÉPARTEMENT
Télécommunications



Plan de cours



Les annuaires ?

Domain Name System (DNS)

Espace de noms de domaines

Recherche de ressources (Requêtes)

Format d'un message DNS

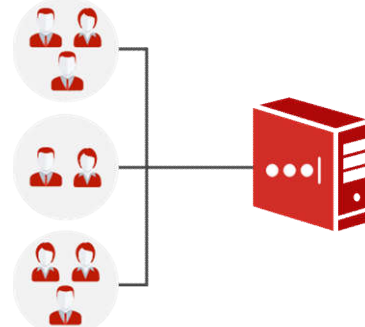
Les RR " Ressource Record"

Les annuaires

❑ Le service d'annuaire

- est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications.
- Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder.

Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur



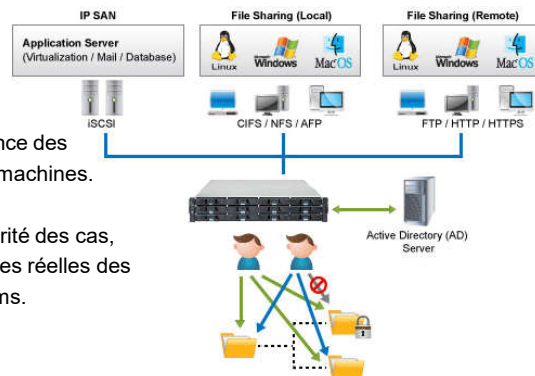
Dr. H. Zerrouki

Les annuaires

- Les particuliers et les entreprises ont de plus en plus recours aux réseaux pour accéder à des applications distribuées et à des ressources partagées (**sites web, serveurs d'applications, serveurs de fichiers**, etc.).
- Ces applications et ces ressources doivent interagir avec des ordinateurs situés dans le même **réseau local**, à travers l'intranet de l'**entreprise**, ou plus généralement au travers de l'**Internet**.

Cela nécessite la connaissance des adresses de ces différentes machines.

Or, dans la très grande majorité des cas, on n'utilise jamais les adresses réelles des machines ; on utilise des noms.



Dr. H. Zerrouki

Les annuaires

❑ Fonctionnement

Exemples simples :

1. L'accès à un **site web** se fera par l'intermédiaire d'un **nom** désignant le site.
2. L'accès à une **imprimante** se fera également par l'intermédiaire d'un **nom** désignant l'imprimante.



- Ces informations vont être gérées dans une base de données spéciale appelée **annuaire**.
- L'annuaire va permettre de transformer le nom du site ou le nom de l'imprimante en une adresse physique permettant aux protocoles de communication d'accéder aux équipements concernés.

Dr. H. Zerrouki

Les annuaires

❑ Qu'est-ce qu'un annuaire ?

- Un annuaire électronique peut être vu comme une **base de données spécialisée**, dont la fonction première est de retourner un ou plusieurs attributs d'un objet grâce à des fonctions de recherche multicritères.
- Un objet de l'annuaire peut représenter une **personne** et les attributs de cet objet seront alors son **nom**, son **prénom**, son **numéro de téléphone**.
- **Figure :** Les clients se connectent au service d'annuaire pour interroger la base de données du service

Un annuaire électronique va centraliser des informations et les rendre disponibles, via le réseau, à des applications, des systèmes d'exploitation ou des utilisateurs.



Dr. H. Zerrouki

Les annuaires

Un annuaire électronique va généralement s'appuyer sur les éléments suivants :

- **Un protocole** : échange des données proprement dit et indication des opérations à effectuer sur ces dernières.
- **Un modèle fonctionnel** : description de la nature des opérations que l'on peut effectuer, comme par exemple une recherche, ou une modification.
- **Un modèle de nommage** : identification des données ; organisation des différentes entrées de l'annuaire.
- **Un modèle d'information** : nature des données pouvant être enregistrées (des chaînes de caractères, des nombres, des numéros de téléphone...).
- **Un modèle de sécurité** : description des services de sécurité permettant d'assurer par exemple le chiffrement des données transférées ou bien l'authentification du client vis-à-vis du serveur.
- **Un modèle de distribution** : création et gestion de serveurs secondaires dans un but de sauvegarde ou de répartition de charge, création et gestion de liens spéciaux (*referrals*, méta-annuaires) pointant vers des annuaires responsables d'une partie des données de l'entreprise ou vers des annuaires complètement différents.

Dr. H. Zerrouki

Domain Name System (DNS)

- 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 (faciles à mémoriser par les humains).
- Les ordinateurs peuvent être déplacés entre réseaux, dans ce cas leurs adresses IP changent
- 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.
- La solution actuelle est l'utilisation des **DNS** (Domain Name System).

Dr. H. Zerrouki

Système de nom de domaine (DNS)

Historique

- Jusqu'en 1984, sur la suite des protocoles TCP/IP, la transcription de noms d'hôtes en adresses Internet s'appuyait sur une table de correspondance.
- Fichier HOSTS (ou HOSTS.TXT)
 - mise à jour manuelle
 - téléchargement dans tous les hôtes

209.206.202.64	www.scrimtech.com	scrimtech.com	# serveur web
199.45.92.97	sparky.leanrix.ca	leanrix.ca	# serveur leanrix
127.0.0.1	localhost		

Cette rubrique existe encore : /etc/hosts [Unix]

- avec la croissance exponentielle d'Internet il a fallu trouver une autre solution, car les problèmes se sont multipliés :
 - La mise à jour des fichiers** : En effet il fallait retransmettre le fichier de mise à jour à tous les hôtes, ce qui encombrait fortement la bande passante
 - L'autonomie des organismes** : Avec l'évolution de l'Internet, les organismes locaux ont eu la possibilité de créer leur propres noms et adresses, et ils étaient alors obligés d'attendre la mise à jours avant que les sites ne puissent être visibles par tous sur Internet.

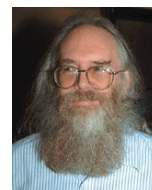
Système de nom de domaine (DNS)

Historique

- Ces problèmes ont fait émerger des idées sur l'espace des noms et sa gestion.
- Les propositions ont été diverses, mais l'une des tendances émergentes a été celle d'un espace de noms hiérarchisé,
- les noms utiliseraient le caractère "." pour marquer la frontière entre deux niveaux hiérarchiques.
- En **1983-1984**, **Paul Mockapetris** et **John Postel** proposent développent une solution qui utilise des structures de **base de données distribuée** : les *Domain Name System* devenue obsolète.
- Les spécifications des DNS ont été établies en **1987**.

base de données distribuée

- Partage l'administration
- Partage la charge



Système de nom de domaine (DNS)

Fonction de DNS

- Un ordinateur client (Client DNS) interroge un serveur DNS pour lui demander l'adresse IP d'un Troisième ordinateur configuré pour utiliser le nom de domaine DNS www.univ-sba.dz.
- Le serveur DNS étant en mesure de répondre à cette requête en interrogeant sa base de données locale, il renvoie une réponse qui fournit l'information demandée, c'est-à-dire un enregistrement de ressource A (Adresse d'hôte) contenant l'adresse IP correspondant à **www.univ-sba.dz**.



Dr. H. Zerrouki

Espace de noms de domaines

Noms de domaines DNS

Les éléments communs à toutes les implémentations des logiciels DNS sont :

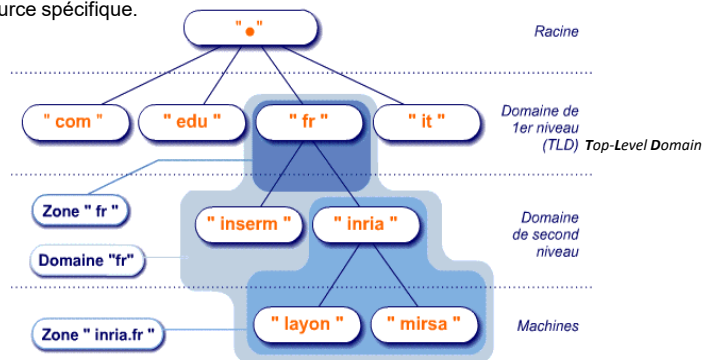
- **Un espace de noms de domaines DNS**, qui définit une structure hiérarchique des domaines permettant d'organiser les noms.
- **Des enregistrements de ressources**, qui mappent les noms de domaines DNS sur un type spécifique d'informations de ressources (**RR**) et sont utilisés lorsque le nom est inscrit ou résolu dans l'espace de noms.
- **Des serveurs DNS**, qui stockent les requêtes de noms portant sur des enregistrements de ressources et y répondent.
- **Des clients DNS**, également appelés solveurs, qui demandent aux serveurs de rechercher et de convertir les noms en un type d'enregistrement de ressource spécifié dans la requête. ex. **Chrom, Mozilla, IE, Microsoft Edge, etc..**

Dr. H. Zerrouki

Espace de noms de domaines

Présentation de l'espace de noms de domaines DNS

- Repose sur le concept d'arborescence des domaines nommés.
- Chaque niveau de l'arborescence représente une branche ou une feuille de cet arbre.
- **Une branche** est un niveau dans lequel plusieurs noms sont utilisés pour identifier un ensemble de ressources nommées.
- **Une feuille** représente un nom unique utilisé une seule fois à ce niveau pour identifier une ressource spécifique.



Dr. H. Zerrouki

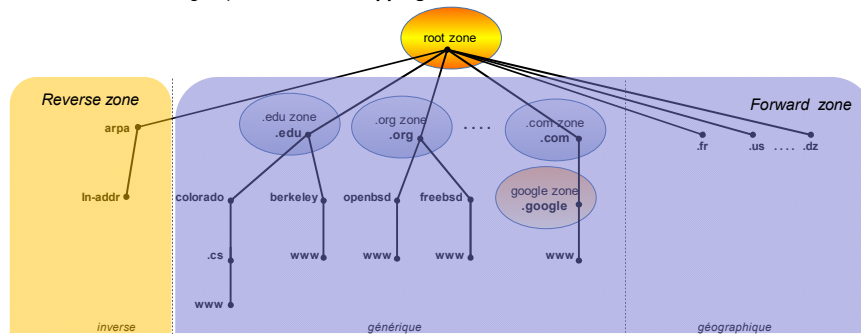
Espace de noms de domaines

Structure arborescente de l'espace de noms

- La racine de cet arbre est noté « . », nommé **dot**.
- Les nœuds situés à la profondeur 1 (**1^{er} niveau**) de l'arbre sont appelés les domaines **Top-Level Domain** (ou **root-level**) : les **TLDs**.

On distingue à ce niveau deux groupes :

- un groupe dit de **forward mapping** : noms d'hôtes → les adresses IP.
- un groupe de **reverse mapping** : adresses IP → noms de machine.



Dr. H. Zerrouki

Espace de noms de domaines

Structure arborescente de l'espace de noms

On distingue deux domaines pour le classement des noms.

❑ Le domaine directe

▪ Les domaines géographiques

sont directement maintenus par des organismes nationaux, l'AFNIC pour :
par exemple : USA (**us**), Royaume Uni (**uk**), la France (**fr**), Chine (**cn**) et l'Algérie (**dz**)

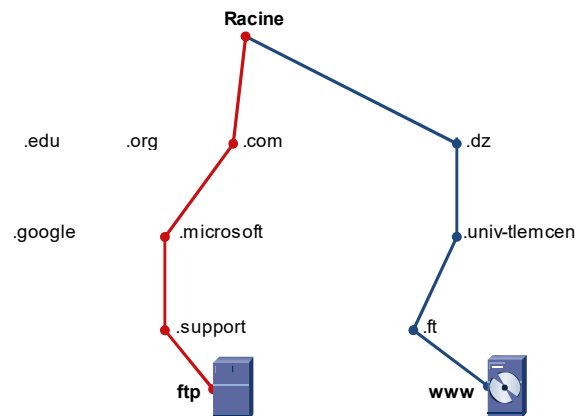
▪ Les domaines génériques

.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

❑ Le domaine inverse

.arpa - Transition ARPANet -> Internet + traduction inverse

Espace de noms de domaines



Nom complet (**FQDN Fully Qualified Domain Name**) constitué de segments séparés par des points (« . »). (**www.ft.univ-tlemcen.dz.**)

Espace de noms de domaines

Différents domaines DNS

La racine du domaine

- Il s'agit de la cime de l'arborescence, représentant un niveau non nommé. Elle est parfois affichée sous la forme de deux guillemets vides (" "), indiquant une valeur nulle. Lorsqu'elle est utilisée dans un nom de domaine DNS, elle est indiquée par un point à droite (.) nommé **dot**, pour indiquer que le nom est situé à la racine ou niveau supérieur de la hiérarchie du domaine.

Domaine de premier niveau

- Nom de deux ou trois lettres utilisé pour indiquer un pays/une région ou le type d'organisation utilisant un nom. « **.dz** », qui indique un nom inscrit au nom d'une organisme (entreprise) nationale Algérienne sur Internet.

Domaine de second niveau

- Noms de longueur variable inscrits au nom d'un individu ou d'une organisation pour une utilisation sur Internet. Ces noms sont toujours associés à un domaine de premier niveau approprié, selon le type d'organisation ou l'emplacement géographique dans lequel un nom est utilisé. « **univ-tlemcen.dz** », qui est le nom de domaine de second niveau inscrit au nom de univ-tlemcen par le Registre des noms de domaines DNS d'Internet.

Espace de noms de domaines

Différents domaines DNS

Sous-domaine

- Noms supplémentaires pouvant être créés par une organisation et associés au nom de domaine de second niveau inscrit. Ils comprennent les noms ajoutés pour développer l'arborescence DNS des noms dans une organisation et la diviser en services ou en emplacements géographiques.
- « **ft.univ-tlemcen.dz** », qui est un sous-domaine fictif défini par univ-tlemcen pour être utilisé dans un exemple de nom de la faculté de Technologie.

Nom d'hôte ou de ressource

- Noms qui représentent une feuille de l'arborescence DNS des noms et identifient une ressource spécifique. Généralement, l'étiquette la plus à gauche d'un nom de domaine DNS identifie un ordinateur spécifique du réseau.
- « **www.ft.univ-tlemcen.dz** », où la première étiquette (« **www** ») est le nom d'hôte DNS d'un ordinateur spécifique du réseau de la faculté de Technologie de l'université de Tlemcen.

Espace de noms de domaines

Type de serveurs et autorités

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

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.

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 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

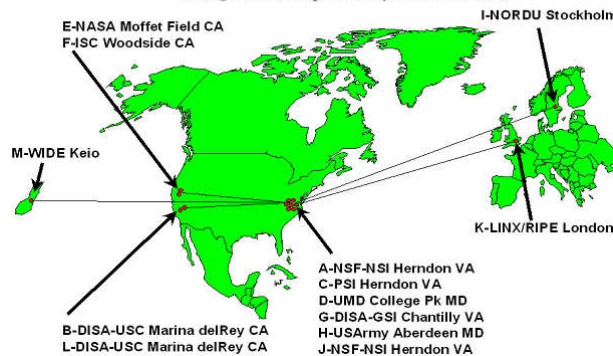
Espace de noms de domaines

Le serveur racine

- Les serveurs racine connaissent les serveurs de nom 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.) actuellement jusqu'à 13 éparpillés sur la planète .

DNS Root Servers

Designation, Responsibility, and Locations



Recherche de ressources

Les Résolveurs

- Les "résolveurs" sont des programmes qui interfacent les applications utilisateur aux serveurs de noms de domaines. Ce n'est pas l'utilisateur qui effectue les requêtes directement.
- Dans le cas le plus simple, un résolveur reçoit une requête provenant d'une application (**ex.**, Applications HTTP, Courrier électronique, Telnet, FTP) sous la forme d'un appel d'une fonction de bibliothèque, d'un appel système etc., et renvoie une information sous une forme compatible avec la représentation locale de données du système.
- Le résolveur est situé sur la même machine que l'application recourant à ses services, mais devra par contre consulter des serveurs de noms de domaines sur d'autres hôtes.
- Comme un résolveur peut avoir besoin de contacter plusieurs serveurs de noms, ou obtenir les informations directement à partir de son cache local, le temps de réponse d'un résolveur peut varier selon de grandes proportions, depuis quelques millisecondes à plusieurs secondes.

Dr. H. Zerrouki

Recherche de ressources

Les Requêtes DNS

- La principale activité d'un serveur de noms est de répondre aux requêtes standards.
- La requête et sa réponse sont toutes deux véhiculées par un message standardisé.
- La requête contient des champs **QTYPE**, **QCLASS**, et **QNAME**, qui décrivent le(s) type(s) et les classes de l'information souhaitée, et quel nom de domaine cette information concerne.
- Les requêtes sont des messages envoyés aux serveurs de noms en vue de consulter les données stockées par le serveur.
- On peut utiliser bien **UDP** que **TCP** pour envoyer ces requêtes sur le port **53**.

Structure des requêtes

- Parmi les champs fixes on trouve 4 bits très importants appelé code d'opération (**OPCODE**).
- Le code d'opération permet de donner des informations sur la nature du message (requête, réponse, ...). Les quatre possibilités sont :

Dr. H. Zerrouki

Recherche de ressources

Structure des requêtes

- **Question**, Contient la question (nom d'hôte ou de domaine sur lequel on cherche des renseignements et type de renseignements recherchés).
- **Answer**, Contient les RRs (Ressource Records) qui répondent à la question.
- **Authority**, Contient des RRs qui indiquent des serveurs ayant une connaissance complète de cette partie du réseau.
- **Additional**, Contient des RRs supplémentaires pouvant être utiles pour exploiter les informations contenues dans les autres sections.

Voici un exemple de requête où l'on souhaite connaître le nom du serveur de courrier s'occupant de frameip.com.

Header	OPCODE=QUERY
Question	QNAME=ISI.EDU., QCLASS=IN, QTYPE=MX
Answer	vide
Authotity	vide
Additional	vide

Dr. H. Zerrouki

Recherche de ressources

Structure des requêtes

```

Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
0000 00 00 0c 8a 6b 30 00 00 00 00 00 01 08 00 45 00 ....k0.. .....E.
0010 00 39 d8 03 00 00 80 11 c0 9c 0a 0a 65 01 c3 07 .9..... ..e...
0020 70 01 13 10 00 35 00 25 75 d9 00 03 01 00 00 01 p....5.% u.....
0030 00 00 00 00 00 00 07 66 72 61 6d 65 69 70 03 63 .....f rameip.c
0040 6f 6d 00 00 0f 00 01 om.....
  
```

La réponse obtenue est :

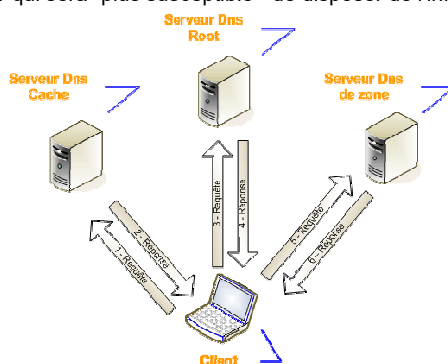
Header	OPCODE=QUERY, RESPONSE, AA			
Question	QNAME=ISI.EDU., QCLASS=IN, QTYPE=MX			
Answer	ISI.EDU	MX 10	VENERA.ISI.EDU	
		MX 20	VAXA.ISI.EDU	
Authority	Vide			
Additional	VENERA.ISI.EDU	86400	A	10.1.0.52
		86400	A	128.9.0.32
	VAXA.ISI.EDU	86400	A	10.2.0.27
		86400	A	128.9.0.33

Dr. H. Zerrouki

Recherche de ressources

a) Le mode Itératif

- Ce mode est le plus simple du point de vue du serveur.
- Les serveurs répondent directement à la requête sur la base seule de ses informations locales.
- La réponse peut contenir la réponse demandée, ou bien donne la référence d'un autre serveur qui sera "plus susceptible" de disposer de l'information demandée.

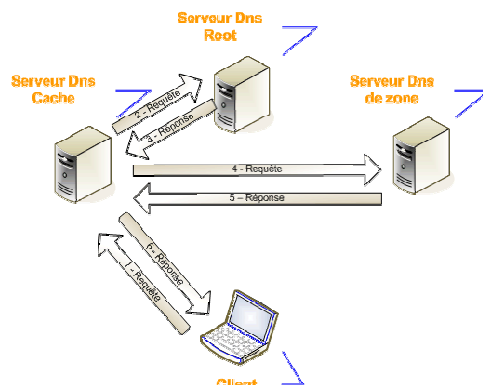


Dr. H. Zerrouki

Recherche de ressources

a) Le mode Récursif

- Le mode récursif une fois est plus simple du point de vue du client.
- Dans ce mode, le premier serveur prend le rôle de **résolveur** (redirectionneur).



Dr. H. Zerrouki

Recherche de ressources

Exemple

- Comment se fait le parcours de l'arborescence pour la résolution de noms ?
- On prend par exemple l'adresse suivante : **www.ft.univ-tlemcen.dz** Il faut alors :
 1. Interroger le serveur **DNS Cache**.
 2. Trouver le serveur DNS de la racine "."
 3. Interroger pour trouver le serveur DNS des **.dz**
 4. Interroger pour trouver le serveur DNS des **univ-tlemcen.dz**
 5. Poser la question finale au serveur DNS de **ft.univ-tlemcen.dz** qui identifiera l'entrée **www**
 6. Réponse **193.194.71.237**

Recherche de ressources

Les Requêtes inverses

- Dans le cas d'une requête inverse, le solveur envoie une demande à un serveur de noms afin que celui-ci renvoie le nom d'hôte associé à une adresse IP connue.
- Deux moyens existent pour convertir une adresse IP en nom d'hôte :
 - l'usage de requêtes DNS inversées (Au sens Opcode=Iquery où **IQuery = 1**)
 - les requêtes DNS de type PTR (Pointeur)(Classe **IN** et Opcode=**Query**).
- En effet, dans le premier cas, on envoie un message DNS contenant une réponse et on demande toutes les questions pouvant conduire à cette réponse,
- Les requêtes PTR posent la question de façon explicite : Qui est l'adresse **a.b.c.d** ?
- Une requête DNS inversée a la particularité d'avoir le champ Question vide, et de contenir une entrée dans le champ **Answer**.
- Pour que le serveur DNS comprenne le sens de la requête, le champ **Opcode** des en-têtes du message DNS doit être à la valeur **IQuery**.

Recherche de ressources

Les Requêtes inverses

- Voici une représentation :

Header	OPCODE=IQUERY, ID=997
Question	"EMPTY"
Answer	"ANYNAME" A IN 10.1.0.52
Authotity	"EMPTY"
Additionnal	"EMPTY"

- Pour répondre aux requêtes inverses en évitant des recherches exhaustives dans tous les domaines, un domaine spécial appelé **in-addr.arpa** a été créé pour associer les adresses IP aux noms d'hôte qui leur correspondent.

Exemple

- pour connaître le nom de la machine dont l'adresse est **193.194.71.237**, on envoie une requête dont la question contient **QNAME= 237.71.194.193.IN-ADDR.ARPA**.

Dr. H. Zerrouki

Recherche de ressources

Les Requêtes inverses

Exp. : Ligne de commande permettant d'établir la requête.

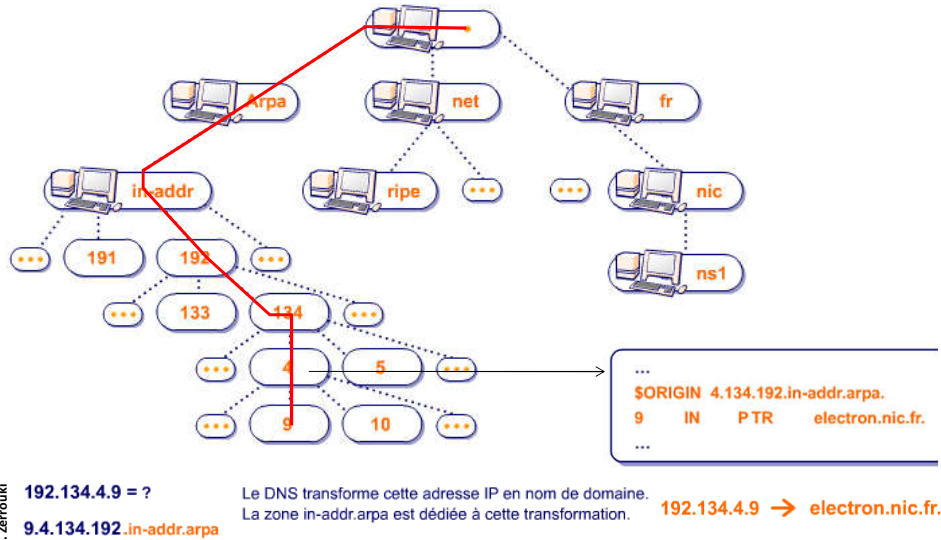
```
Administrateur : C:\Windows\system32\cmd.exe - nslookup
> nslookup
Serveur : UnKnown
Address: fe80::267f:3cff:fe93:6b10

DNS request timed out.
  timeout was 2 seconds.
*** Le délai de la requête sur UnKnown est dépassé.
> set type=ptr
Server: UnKnown
Address: fe80::267f:3cff:fe93:6b10

Réponse ne faisant pas autorité :
237.71.194.193.in-addr.arpa      name = vietud.univ-tlemcen.dz
237.71.194.193.in-addr.arpa      name = forum.univ-tlemcen.dz
>
```

Dr. H. Zerrouki

Comment fait le DNS pour retrouver un nom de machine
à partir d'une adresse IP ?



Dr. H. Zerrouki

Format d'un message DNS

Le transport

Utilisation d'UDP

- Le port serveur utilisé pour l'envoi des datagrammes en UDP est **53**.
- Les datagrammes DNS en UDP sont limités à **512 octets** (valeur représentant les données sans l'entête UDP et IP).
- L'utilisation d'UDP n'est pas recommandée pour les transferts de zone, mais uniquement pour les requêtes standards.

Utilisation de TCP

- Le port serveur utilisé pour l'envoi des datagrammes en TCP est **53**.
- Le datagramme inclus alors un champ de deux octets nommé "**longueur**", il permet de spécifier la longueur totale des données indépendamment de la fragmentation.

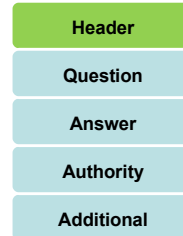
Dr. H. Zerrouki

Format d'un message DNS

Format d'un message DNS

- Une l'entête DNS basé sur 12 octets **Header**

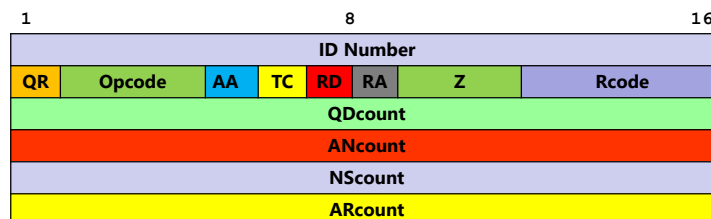
Les quatre sections suivantes ne contiennent pas nécessairement de données.



- Pour les requêtes seules la section **Question** en possède.
- Les réponses aux requêtes de type **A**, **PTR**, **CNAME** figurent dans la section **Answers**
- Les réponses aux requêtes de type **NS** figurent dans la section **Authority**
- Enfin, les autres informations sont dans la section **Additional**.

Format d'un message DNS

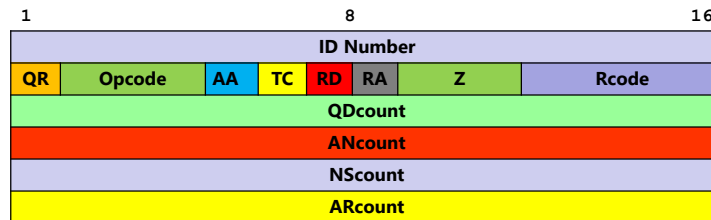
L'entête d'un message DNS



- **ID Number** : Codé sur **16 bits**, identifier le message : (requête, réponse) même ID
- **QR** : Sur un **1 bit**, permet d'indiquer s'il s'agit d'une requête (**0**) ou d'une réponse (**1**).
- **Opcode** : Sur **4 bits**, ce champ permet de spécifier le type de requête :
 - **0** - Requête standard (**Query**)
 - **1** - Requête inverse (**Iquery**)
 - **2** - Status d'une requête serveur (**Status**)
 - **3-15** - Réserve pour des utilisations futurs

Format d'un message DNS

L'entête d'un message DNS

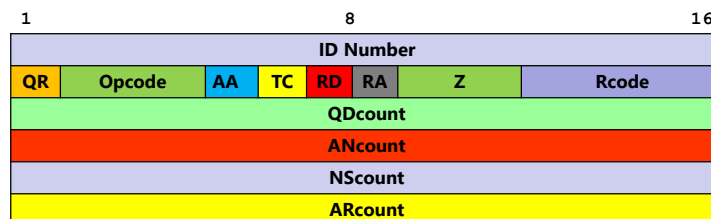


- **AA** : Le flag AA, sur **1 bit**, signifie "**Authoritative Answer**". Il indique une réponse d'une entité autoritaire.
- **TC** : Le champ TC, sur **1 bit**, indique que ce message a été tronqué à **0**.
- **RD** : Le flag RD, sur **1 bit**, permet de demander la récursivité en le mettant à **1**.
- **RA** : Le flag RA, sur **1 bit**, indique que la récursivité est autorisée à **1**.
- **Z** : Le flag Z, sur **3 bits**, est réservé pour une utilisation future.

Dr. H. Zerrouki

Format d'un message DNS

L'entête d'un message DNS



- **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** : sur **16 bits**, il spécifie le nombre d'entrée dans la section "**Question**".
- **ANcount** : sur **16 bits**, il spécifie le nombre d'entrée dans la section "**Réponse**".
- **NScount** : sur **16 bits**, il spécifie le nombre d'entrée dans la section "**Autorité**".
- **ARcount** : sur **16 bits**, il spécifie le nombre d'entrée dans la section "**Additionnel**".

Dr. H. Zerrouki

Les RR " Ressource Record"

- La base de données des serveurs de noms (fichier 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 associé à un nom particulier est composé de quatre enregistrements de ressources séparés (**RR**).

Format de l'entête RR (N octets)

1	8	16
Nom		
Type		
Classe		
TTL		
Longueur		
Données		

Dr. H. Zerrouki

Les RR " Ressource Record"

- **Nom** : identifie l'entité, **un hôte** ou bien **un domaine**, que l'enregistrement décrit.
- **Type** : Ce champ type, codé sur **16 bits**, spécifie quels types de données sont utilisés dans le RR. Ils sont cependant classifiables en **4** groupes :
 - **Zone** : identification du/des domaine(s) et NS (Noms de Serveur) associés.
 - **Basic** : les correspondances noms/adresses et routage de mail.
 - **Security** : ajout de l'authentification et signature des fichiers de zone.
 - **Option** : informations supplémentaires sur les hôtes et les domaines.
- **Classe** : Une valeur encodée sur **16 bits** identifiant une famille de protocoles ou une instance d'un protocole. Voici les classes de protocole possible :
 - **IN 01** Internet
 - **CS 02** Class Csnnet (obsolète)
 - **CH 03** Chaos (chaosnet est un ancien réseau, il n'est plus utilisé)
 - **HS 04** Hesiod
- **TTL** : C'est la durée de vie des RR (**32 bits**, en secondes), utilisée par les solveurs de noms lorsqu'ils ont un cache des RR pour connaître la durée de validité des informations du cache.
- **Longueur** : Sur **16 bits**, ce champ indique la longueur des données suivantes.

Dr. H. Zerrouki

Les RR " Ressource Record"

- **Données** : Données identifiant la ressource, ce que l'on met dans ce champ dépend évidemment du type de ressources que l'on décrit.
 - **A** : (**Address**) fait correspondre un nom d'hôte à une adresse IPv4 ;
 - **AAAA** : (**Address IPv6**) fait correspondre un nom d'hôte à une adresse IPv6 ;
 - **CNAME** : (**Canonical Name**) permet de créer un alias pointant sur un autre nom d'hôte ;
 - **NS** : (**Name Server**) définit le ou les serveurs DNS du domaine ;
 - **MX** : (**Mail Exchanger**) définit le ou les serveurs de mail du domaine ;
 - **PTR** : (**Pointer**) fait correspondre une IP à un nom d'hôte. Il n'est utilisé que dans le cas d'une zone inverse, que nous verrons plus loin ;
 - **SOA** : (**Start of Authority**) donne les infos de la zone, comme le serveur DNS principal, l'adresse mail de l'administrateur de la zone, le numéro de série de la zone et des durées que nous détaillerons.
- **Exemple**

```

■ Answers
■ www.frameip.com: type A, class inet, addr 195.7.102.13
  Name: www.frameip.com
  Type: Host address
  Class: inet
  Time to live: 1 hour
  Data length: 4
  Addr: 195.7.102.13
    
```

Dr. H. Zerrouki

Exemple : Configuration d'une zone DNS

```

$ORIGIN example.com.
$TTL 86400
@      IN      SOA      dns1.example.com.  hostmaster.example.com. (
                                2001062501 ; serial
                                21600      ; refresh after 6 hours
                                3600       ; retry after 1 hour
                                604800    ; expire after 1 week
                                86400     ; minimum TTL of 1 day

                                IN      NS      dns1.example.com.
                                IN      NS      dns2.example.com.

                                IN      MX      10      mail.example.com.
                                IN      MX      20      mail2.example.com.

                                IN      A       10.0.1.5

server1 IN      A       10.0.1.5
server2 IN      A       10.0.1.7
dns1    IN      A       10.0.1.2
dns2    IN      A       10.0.1.3

ftp     IN      CNAME   server1
mail    IN      CNAME   server1
mail2   IN      CNAME   server2
www     IN      CNAME   server2
    
```

Dr. H. Zerrouki