# Documentation DNS

## Définitions

|  |  |
| --- | --- |
| Nom | Définition |
| SBELT | La structure « Safety Belt » a la meme forme que “SLIST”.  Liste les serveurs qui seront utilisés par le « resolver » lorsqu’il n’y a pas d’information dans le cache.  Serveurs racines |
| SLIST |  |

## Client

Le « resolver » permet de lancer des requêtes DNS pour la résolution de nom. Il existe 2 modes d’interrogation :

1. **Le mode récursif** : Le client envoie une requête au serveur DNS ; ce dernier renvoie une ***réponse complète*** au client qui est soit la correspondance recherchée soit un message d’erreur. Le serveur doit au besoin interroger d’autres serveurs de noms si le nom de domaine concerné par la requête n’est pas dans son cache et se trouve dans une zone pour laquelle il n’est pas ***autoritaire***.
2. **Le mode itératif :** Le client envoie une requête au serveur DNS ; ce dernier renvoie soit une ***réponse complète*** (s’il est autoritaire pour la zone concernée), soit une ***réponse partielle*** (adresse d’un autre serveur de noms qui va permettre au client d’avance dans le processus de résolution). Le client va alors lancer une autre requête vers le serveur spécifié dans la réponse précédente. Ce processus est répété autant de fois que nécessaire.

Le mode récursif est utilisé par les applications « clientes » et le mode itératif par les resolvers des serveurs de noms.

## Serveur de cache

Les serveurs de noms qui se chargent de traiter des requêtes récursives sont appelées des serveurs de noms récursifs. Afin d’améliorer leurs performances et éviter la surcharge du réseau, les serveurs récursifs utilisent un **cache** pour stocker les réponses des requêtes.

Pour des requêtes ultérieures des clients, un serveur cache consulte d’abord son cache pour voir si la requête a déjà été traitée, si c’est le cas les données correspondantes du cache sont fournies en réponse.

Le cache s’enrichit donc au fur à mesure du traitement des requêtes des clients. Ses données ont cependant une durée limitée qui est spécifiée dans le champ **TTL** (Time To Live).

La configuration minimale d’un serveur cache contient la liste des serveurs de la racine (**serveurs root**).

## Serveur forward

Un serveur cache ne peut pas procéder lui-même à la résolution complète d’une requête récursive ; si elle ne peut pas être satisfaite avec les données de son cache il peut faire suivre la requête à un autre serveur de noms.

Dans le cas où il fait suivre systématiquement les requêtes à d’autres serveurs, il est qualifié de serveur « **faire suivre** » ou esclave.

Le serveur auquel on fait suivre les requêtes est aussi appelé « **forwarder** ».

## Serveur autoritaire

**Exemple de résolution**

<https://tools.ietf.org/rfc/rfc1034.txt>

Supposons que le client envoie une requête de type MX pour le nom de domaine « ISI.EDU ».

1. Le « resolver » vérifie s’il existe une valeur dans le cache.
2. Le « resolver » a besoin de déterminer les meilleurs serveurs à interroger, il va rechercher « NS » pour les domaines « ISI.EDU », « EDU » et la racine.

Le « resolver » va exécuter une requête de ce type sur un des serveurs racines :

|  |  |
| --- | --- |
| OPCODE | SQUERY |
| QNAME | ISI.EDU. |
| QCLASS | IN |
| QTYPE | NX |

Si il y a un « timeout » alors le « resolver » va essayer une autre adresse.

Voici une réponse qui peut être reçue de « SRI-NIC.ARPA » :

|  |  |
| --- | --- |
| OPCODE | QUERY, RESPONSE |
| QNAME | ISI.EDU. |
| QCLASS | IN |
| QTYPE | MX |
| Authority | ISI.EDU. 172800 IN NS VAXA.ISI.EDU  A.ISI.EDU  VENERA.ISI.EDU |
| Additional | VAXA.ISI.EDU 172800 A 10.2.0.27  172800 A 128.9.0.33  VENERA.ISI.EDU 172800 A 10.1.0.52 |

Le « resolver » stocke la réponse dans le cache et met à jour sa « SLIST » avec les informations suivantes :

* A.ISI.EDU
* VAXA.ISI.EDU
* VENERA.ISI.EDU

## Réponses

### CNAME RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| CNAME | A <domain-name> which specifies the canonical or primary name for the owner |

### HINFO RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| CPU | A <character-string> which specifies the CPU type |
| OS | A <character-string> which specifies the operating system type. |

### MB RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| MADNAME | A <domain name> which specifies a host which has the specified mailbox |

### MG RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| MGMNAME | A <domain name> which specifies a mailbox which is a member of the mail group specified by the domain name. |

### MINFO RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| RMAILBX | A <domain-name> which specifies a mailbox which is responsible for the mailing list or mailbox. If this domain name names the root, the owner of the MINFO RR is responsible for itself. Note that many existing mailing lists use a mailbox X-request for the RMAILBX field of mailing list X, e.g., Msgroup-request for Msgroup. This field provides a more general mechanism. |
| EMAILBX | A <domain-name> which specifies a mailbox which is to receive error messages related to the mailing list or mailbox specified by the owner of the MINFO RR (similar to the ERRORS-TO: field which has been proposed). If this domain name names the root, errors should be returned to the sender of the message. |

### MR RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| NEWNAME | A <domain-name> which specifies a mailbox which is the proper rename of the specified mailbox. |

### MX RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| PREFERENCE | A 16 bit integer which specifies the preference given to this RR among others at the same owner. Lower values are preferred. |
| EXCHANGE | A <domain-name> which specifies a host willing to act as a mail exchange for the owner name. |

### NS RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| NSDNAME | A <domain-name> which specifies a host which should be authoritative for the specified class and domain. |

### PTR RDATA format

Permet de convertir une adresse IP vers un nom de domaine :

* **Requête « forward »** : Nom de domaine vers une adresse IP.
* **Requête « reverse »** : adresse IP vers nom de domaine.

L’enregistrement « PTR » est utilisé pour faire un « reverse » DNS. Par exemple une adresse IP « 1.2.3.4 » va être stockée de cette façon « 1.2.3.4.in-addr.arpa ».

|  |  |
| --- | --- |
| Champ | Description |
| PTRDNAME | A <domain-name> which points to some location in the domain name space |

### SOA RDATA format

SOA (Start Of Authority) : On doit assigner à chaque zone un SOA (Start Of Authority). Cet enregistrement donne des informations et indique si le serveur qui est interrogé a bel et bien la charge de cette zone.

|  |  |
| --- | --- |
| Champ | Description |
| MNAME | The <domain-name> of the name server that was the original or primary source of data for this zone. |
| RNAME | A <domain-name> which specifies the mailbox of the person responsible for this zone. |
| SERIAL | The unsigned 32 bit version number of the original copy of the zone. Zone transfers preserve this value. This value wraps and should be compared using sequence space arithmetic. |
| REFRESH | A 32 bit time interval before the zone should be refreshed. |
| RETRY | A 32 bit time interval that should elapse before a failed refresh should be retried. |
| EXPIRE | A 32 bit time value that specifies the upper limit on the time interval that can elapse before the zone is no longer authoritative. |
| MINIMUM | The unsigned 32 bit minimum TTL field that should be exported with any RR from this zone. |

### TXT RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| TXT-Data | One or more <character string>s |

### A RDATA format

|  |  |
| --- | --- |
| Champ | Description |
| ADDRESS | A 32 bit Internet address |

### Erreurs retournées par le serveur DNS

Voici la liste des erreurs qui peuvent être retournées par un serveur DNS dans le champ « RCODE » de la réponse :

|  |  |
| --- | --- |
| Code | Description |
| 0 | No error condition |
| 1 | Format error – the name server was unable to interpret the query |
| 2 | Server failure – the name server was unable to process this query due to a problem with the name server |
| 3 | Name error – meaningful only for responses from an authoritative name server, this code signifies that the domain name referenced in the query does not exist. |
| 4 | Not implemented – the name server does not support the requested kind of query |
| 5 | Refused : the name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to a particular requester, or a name server may not wish to perform a particular operation for particular data. |

<https://www.sciencedirect.com/topics/computer-science/reverse-lookup-zone>