Réseau - Protocole DNS

Difficulté : Novice

Résumé :

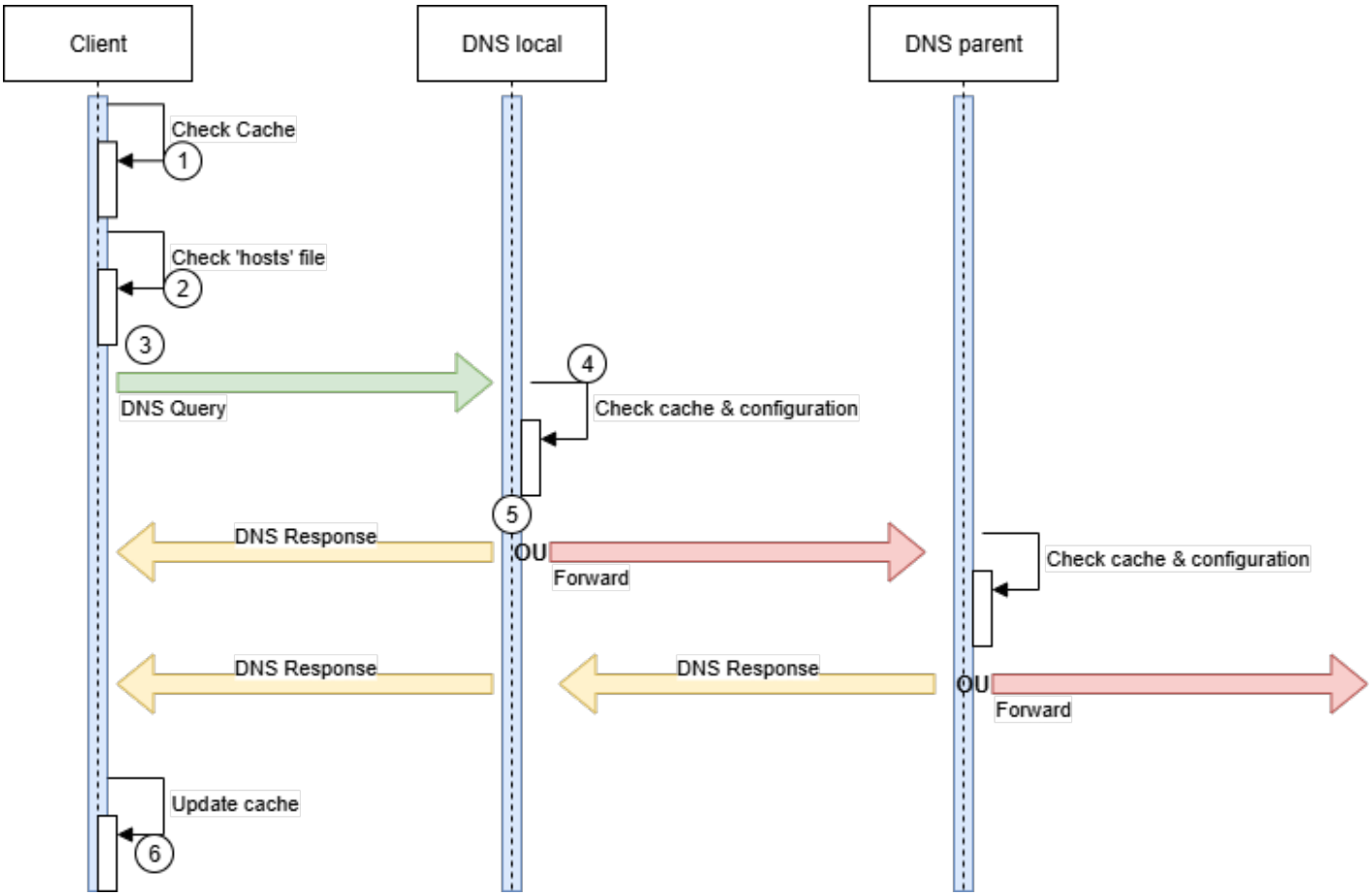
- **OSI** : couche 4, 6 & 7
- **Type** : UDP (parfois TCP)
- **Port** : 53 (853 DNSsec)

I. Introduction

Le protocole DNS (**D**omain **N**ame **S**ystem) permet de traduire les noms de domaine lisibles par l'homme (comme `www.example.com`) en adresses IP compréhensibles par les machines (`192.0.2.1`). Il joue un rôle fondamental dans la navigation sur Internet et dans la résolution de noms au sein des réseaux locaux.

Les échanges DNS se situent entre les couches 5 à 7 du modèle OSI, bien qu'ils reposent sur des mécanismes de transport en UDP ou TCP selon le contexte.

II. Diagramme



1 - Vérification locale (cache)

Lorsqu'une résolution est nécessaire ; effectuée par l'utilisateur ou le système ; la machine va dans un premier temps consulter son cache local.

- Si l'enregistrement s'y trouve, il va utiliser celui-ci.
- Si l'enregistrement ne s'y trouve pas :

2 - Vérification locale (fichier)

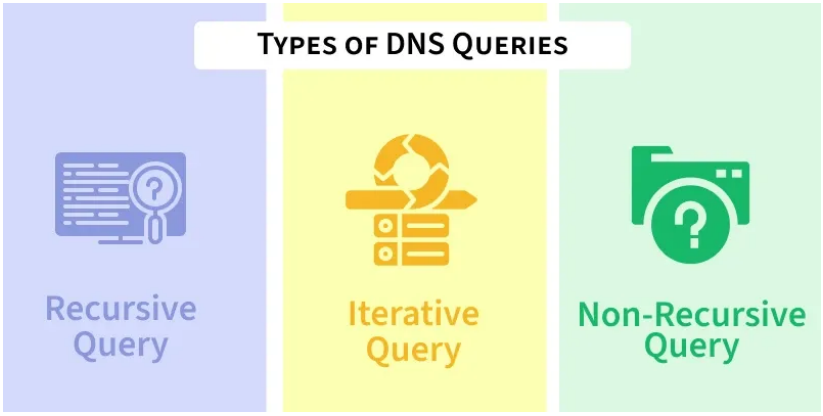
Le client va vérifier si ses fichiers 'Hosts' contiennent l'enregistrement.

- Si oui, il sera lu et mis en cache puis l'utiliser.
- Si non :

3 - DNS Query

Le client va interroger le(s) serveur(s) déclarés dans sa configuration réseau.

Il existe 3 types de requêtes :



Source : geeksforgeeks

- **Requête récursive** : Si le resolver (client) ne trouve pas l'enregistrement il va interroger le(s) DNS paramétré(s) et attends une réponse complète.
  - Le serveur va alors interroger ses forwarder et ainsi de suite jusqu'à ce qu'une réponse revienne au client.

- **Requête Itérative** : Si le resolver (client) ne trouve pas l'enregistrement, il va interroger le(s) DNS paramétré(s) et attend une réponse au moins partielle.
  - Le serveur va alors chercher un autre serveur qui a une information plus complète et renvoyer son adresse au client, qui pourra alors lui adresser sa requête, ainsi de suite jusqu'à résolution complète.

- **Requête non récursive** : Si le resolver (client) ne trouve pas l'enregistrement il va interroger le(s) DNS paramétré(s) et demande de consulter le cache.
  - Le serveur regarde dans son cache, soit il a l'information et la transmet au client, soit il n'a pas l'information et renvoie qu'il ne l'a pas. La recherche s'arrête là.

Dans tous les cas, si un serveur ne dispose pas de la réponse, il vérifiera si l'un de ses forwarder ou si les serveurs racine ont la réponse et soit fera la recherche pour le client (Récursive) soit lui donnera l'adresse d'un forwarder ou serveur racine (itérative).

4-5 - Vérification du cache

Tout comme le client effectue de son côté une vérification de son cache et de ses fichiers locaux aux étapes 1 et 2, les serveurs relais vont effectuer la même opération. Cela permettra une réponse plus rapide.

6 - Mise à jour du cache

Une fois la réponse obtenue, le cache local du resolver est mis à jour.

Ces enregistrements resterons mis en cache pour la durée du TTL.

III. Principes de bases

3.1 Le cache DNS

Chaque enregistrement DNS dispose d'un TTL (Time To Live). Lorsqu'un enregistrement est mis en cache, il périmera à l'expiration du TTL. Celui-ci sera alors supprimé du cache et rajouté à nouveau lors d'une prochaine requête.

> **Astuce** : Tous les systèmes disposent de commandes pour vider manuellement ce cache.

> **Info** : C'est cette mécanique qui est utilisée lors des attaques par empoisonnement de cache DNS (DNS poisoning).

3.2 La hiérarchie des serveurs DNS

L’architecture DNS se compose d’un système de résolution de nom hiérarchique et décentralisé pour les ordinateurs, les services ou toute autre ressource connectée à Internet ou à un réseau privé. Il stocke les différentes informations associées des noms de domaine attribués à chacune des ressources.

La hiérarchie DNS repose sur plusieurs niveaux qui peuvent intervenir lors d’une résolution DNS :

- Tout en haut : **Les serveurs DNS racines**
  - Ceux qui gèrent les domaines de niveaux supérieurs.
- Puis en dessous **les serveurs de domaine de premier niveau**
  - Les domaines nationaux par exemple .fr, .eu, etc... (ou encore d'autres comme .com, .net, etc...).
- Au niveau intermédiaire **les serveurs DNS d'autorité**
  - Les serveurs faisant autorité pour les domaines complets comme mfrstegreve.fr ou labs404.com (souvent ceux du registar)
- Puis **les DNS récursifs et itératives**
  - Ce sont les serveurs enregistrés dans les paramètres de la connexion (souvent ceux du FAI ou les DNS locaux).

Liste des serveurs racines

Actuellement, il existe 13 serveurs DNS racines dont une grande majorité se trouvent aux USA.

Serveurs DNS racines	Adresse IPv4	Adresse IPv6	Opérateur

A	198.41.0.4	2001:503:ba3e::2:30	VeriSign
B	192.228.79.201	2001:478:65::53	USC-ISI
C	192.33.4.12	2001:500:2::c	Cogent Communications
D	199.7.91.13	2001:500:2d::d	University of Maryland
E	192.203.230.10		NASA
F	192.5.5.241	2001:500:2f::f	ISC
G	192.112.36.4		U.S. DoD NIC
H	128.63.2.53	2001:500:1::803f:235	US Army Research Lab
I	192.36.148.17	2001:7FE::53	Autonomica
J	192.58.128.30	2001:503:c27::2:30	VeriSign
K	193.0.14.129	2001:7fd::1	RIPE NCC
L	199.7.83.42	2001:500:3::42	ICANN
M	202.12.27.33	2001:dc3::35	WIDE Project

3.3 Les types de domaines

Il en existe 3 types :

- **Les domaines Génériques** : Des domaines sans rattachements géographiques mais mondialement reconnus et utilisés.
  - .org, .com, .net, ...
- **Les domaines Nationaux ou Coutry Code Domain** : Domaines attachés à une origine géographique.
  - .fr, .uk, .au, .ru, .us, ...
- **Les domaines inverses** : Utilisé pour les 'Reverse lookup'. Les recherches inversées. Notamment utilisés pour vérifier qu'une IP est bien dans le domaine recherché.
  - .arpa

IV. Types d'enregistrements DNS

Les enregistrements DNS sont des parties importantes de la Système de nom de domaine (DNS). Il existe plus de 30 types d'enregistrements, chacun servant de saisie de base de données qui fournit des informations spécifiques sur un domaine, y compris son adresse IP, ses serveurs de messagerie et sa sécurité. Ces enregistrements sont stockés dans des fichiers DNS Zone et gérés par les serveurs DNS.

4.1 Terminologie DNS

Avant de voir les types de dossiers DNS spécifiques, il est utile de comprendre une terminologie DNS de base.

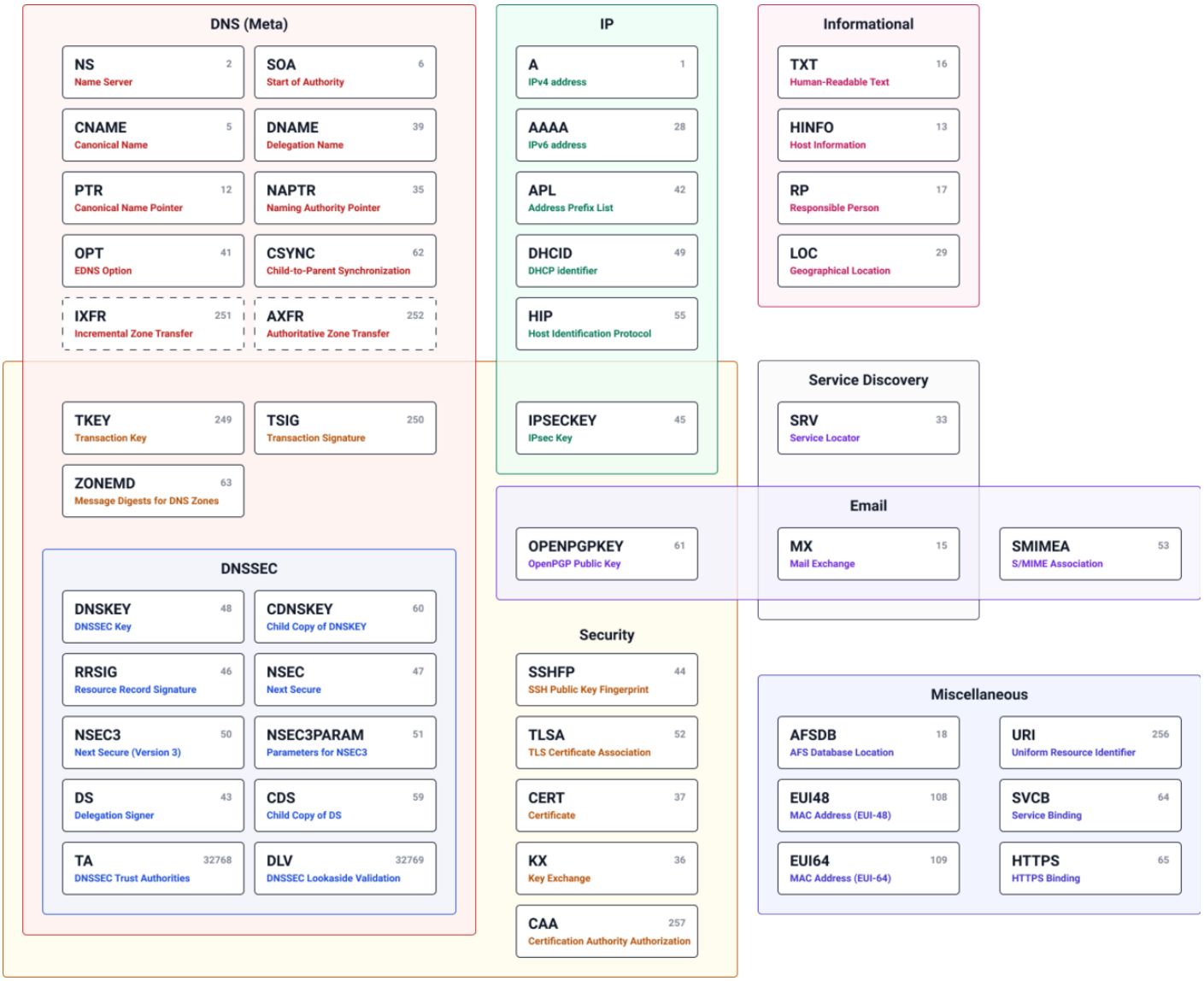
Voici quelques termes clés utiles dans la compréhension de DNS Records.

- **Enregistrement des ressources:** L'élément de données de base dans le DNS. Chaque enregistrement spécifie des informations sur un domaine.
- **Nom:** Le nom de domaine auquel l'enregistrement s'applique.
- **TTL (temps de vie):** La durée pour laquelle le dossier est mis en cache par les DNS Resolvers.

- **Classe:** Spécifie la famille du protocole. Dans (Internet) est le plus courant.
- **Taper:** Le type d'enregistrement DNS (par exemple, a, aaaa, cname).
- **Donnés:** Les données spécifiques de l'enregistrement, telles qu'une adresse IP.
- **Fichiers de zone:** Fichiers contenant des mappages entre les noms de domaine et les adresses IP.
- **Nom du serveur:** Un serveur qui gère les enregistrements DNS pour un domaine.

4.2 Types d'enregistrements DNS les plus courants

Chaque type d'enregistrement DNS a une fonction spécifique, ce qui aide à gérer les noms de domaine et à garantir un approvisionnement approprié du trafic Internet.



source : Wikipedia

4.3 Champs spécifiques

Certains protocoles se basent sur l'utilisation de champs spécifiques. La plupart du temps, il s'agit de champs TXT devant être formatés de manière très précise.

C'est le cas par exemple pour la vérification des serveurs de messageries qui peuvent utiliser les champs **DMARK** et **SPF**.

Ou la VoIP.

V. Principes avancés

5.1 Recherche inversée

Tout comme il est possible avec le DNS de savoir quelle adresse IP corresponds à quel nom d'hôte, il est également possible d'effectuer une recherche inversée pour avoir les noms attachés à une adresse IP.

Cela sert dans le cadre de vérification ou de diagnostic.

Cette recherche s'appuie sur une zone de recherche inversée contenant les champs en **.arpa**.

5.2 DNSsec

Le DNSSEC (**D**omain **N**ame **S**ystem **SEC**urity extensions) est une extension du protocole DNS qui ajoute une couche de sécurité en garantissant l'authenticité des réponses DNS.

Chaque zone DNS est signée avec une clé privée.

La clé publique est placée dans l'un des champs de la zone et permet à un client qui ferai une requête de vérifier l'authenticité de la réponse.

Cela permet de se prémunir des attaques de type "DNS spoofing" ou de "cache poisoning".

> **Attention** : Cela permet de garantir l'authenticité de la réponse mais ne chiffre pas les échanges. De plus tous les équipements ne seront pas forcement compatible avec ce protocole.

Les enregistrements spécifiques utilisés sont :

- **RRSIG** : contiens la signature cryptographique d'un enregistrement DNS.
- **DNSKEY** : contient la clé publique utilisée pour vérifier les signatures.
- **DS** : sert à déléguer la vérification entre zones.

5.3 DoH / DoT

Le DoH (**D**ns **O**ver **H**ttps), vise à faire passer les requêtes DNS par le biais d'un canal chiffré par HTTPS. Rendant son interception et sa modification plus difficile.

Si aujourd'hui beaucoup de navigateurs l'intègre nativement, il est très peu présent sur les équipements réseaux.

Le DoT (**D**ns **O**ver **T**ls) vise à faire passer les requêtes DNS par le biais d'un canal chiffré par TLS. Les avantages sont les mêmes qu'avec le DoH. Mais il utilise un port à part (853), permettant de le différencier du trafic HTTPS, mais également de faire un filtrage plus fin sur les pare-feu.

Revision #2
Created 2026-07-17 20:31:38 UTC by Olivier
Updated 2026-07-17 20:37:08 UTC by Olivier