Le système de nommage d'Internet

Domain Name System

DNS

Introduction

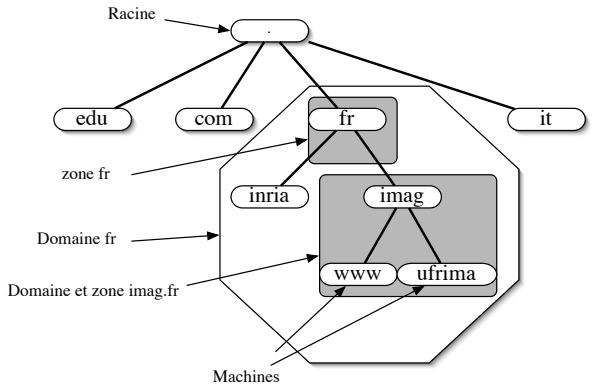
- Sur Internet une machine est identifiée de manière unique par une adresse IP (v4 ou/et v6)
- Annuaire Adresse IP / Nom
- Au début (1970-1984) : annuaire complet dans un fichier texte (*/etc/hosts* sous Unix):
  - Adresse Nom1 Nom2 Nom3
  - Cohérence des noms par diffusion du fichier
- Aujourd'hui ce fichier est encore utilisé pour l'annuaire local
- 1984 : mise en place du DNS
- Géré par **ICANN** : Internet Corporation for Assigned Names and Number
- En France **AFNIC**: Association Française pour le Nommage Internet en Coopération

Introduction

- Information accessible grâce au DNS
  - Adresse (V4 ou V6) en fonction du nom
  - Nom en fonction de l'adresse IP : résolution inverse
  - Adresse de relai de messagerie
- Système hiérarchique, redondant et distribué
  - Arborescence (comme un système de fichier)
  - Chaque site est maître de ses données
  - Dynamique: mise à jour automatique
- Bibliographie
  - DNS and BIND , Paul Albitz and Cricket Liu

Structuration des noms DNS

- Hiérarchique par domaine: ***www.imag.fr***
  - Machine ***www*** dans le domaine ***imag*** lui-même dans le domaine ***fr***
  - Analogie avec les noms de fichier/répertoire à l'envers avec le **.** à la place de **/**
  - On omet en général la racine (le point) : ***www.imag.fr.***
  - Les majuscules ne sont pas significatives



Une base de données distribuée

- Une base de donnée est associée à chaque noeud
- L'ensemble de ces bases de données constitue le DNS
- Dans un noeud, on trouve
  - Les informations permettant de retrouver les noeuds fils
  - Les informations propre au noeud : liste des machines
  - Comme dans un répertoire : des sous répertoires et des fichiers
- La gestion de chaque noeud peut être effectuée par des entités différentes

Terminologie

- **Domaine**
  - Un domaine est la partie de l'arborescence à partir du noeud portant son nom
  - Exemple: domaine ***fr***: arborescence à partir du noeud ***fr***
  - On parle de sous domaine pour un domaine inclus dans un autre
  - Exemple: ***imag.fr*** est un sous domaine du domaine ***fr***
- **Zone**
  - C'est la base de donnée associée à un noeud
- **Contenu des bases de donnée associées aux zones**
  - Noms/Adresses des serveurs de la zone
    - » Exemples:
      - Racine: liste des serveurs des domaines de premiers niveaux
      - **fr**: listes des adresses des serveurs des sous-domaines de ***fr***
  - Noms/Adresses des machines de ce domaine
- Terminologie de l'AFNIC: ***Domaine. Suffixe***

Domaines de plus haut niveau

- IANA (***Internet Assigned Numbers Authority)*** gère la zone racine
  - Assignation des domaines de plus haut niveau
- Composante de ICANN (Internet Corporation for Assigned Names and Numbers)
  - Organisation/société de droit Américaine à but non lucratif. Depuis 2016 est devenu une organisation internationale auto-régulée, indépendante et à but non lucratif
  - Attribution des noms de domaine mondialement
  - Depuis 2009 possibilité de nom de domaine en caractère non latin (arabe, chinois…)
- Suffixe ou Top Level Domain(TLD)
- Par pays (ou Country Code, ccTLD) en deux lettres :
  - **.fr**, **.us**, **.jp**, **.be**, ...

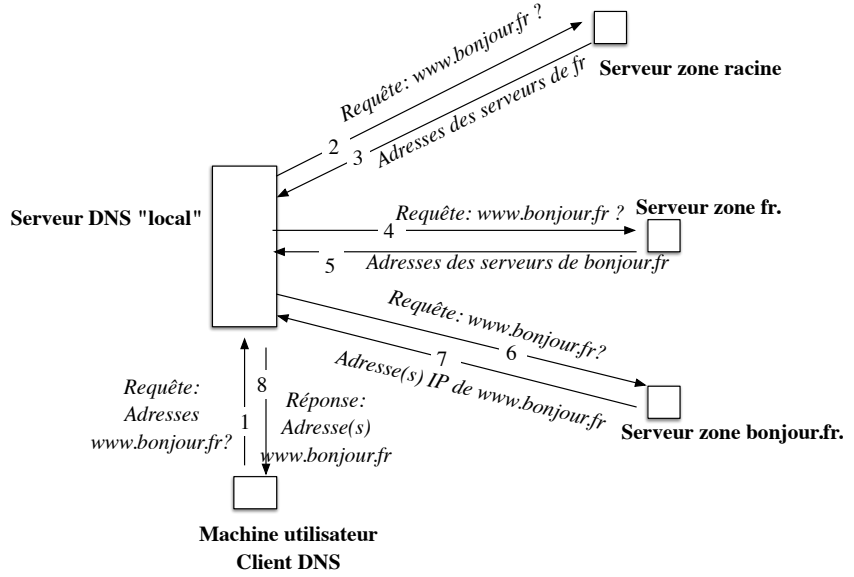
Domaines existants

- Suffixe ou Top Level Domain(TLD)
  - Génériques internationaux (gTLD) en trois lettres
  - voir **http://fr.wikipedia.org/wiki/Domaine_de_premier_niveau#Sur_Internet**
  - Exemples créés à l'origine en 1985
    - » **.com** (entreprise multinationale),
    - » **.org** (organisation à but non commercial),
    - » **.info** (Service d'informations)
    - » **.net** (fournisseur d'accès),
  - d'autres
    - » **.biz** (business)
    - » .**name** (individu)
    - » .**pro** (professionnels)

Principe de fonctionnement

- Application client/serveur
- **Serveur DNS**
  - Gère la base de données contenant
    - nom/adresse IP des machines du domaine
    - nom/adresse IP des serveurs d'un sous-domaine
  - Système robuste par redondance: plusieurs serveurs possèdent la base de donnée d'un domaine
- **Client DNS**
  - Resolver: permet l'interrogation d'un serveur
  - Référence à un serveur DNS par défaut "local"
- Interrogation client vers le serveur local
  - Récursive
  - Le client attend la réponse finale
- Interrogations serveur à serveur
  - Souvent itératives (mais peuvent aussi être récursives)

Exemple d'une interrogation DNS



Interrogations et découpage des zones

- Les requêtes successives sur les serveurs sont des requêtes sur le **nom complet**
  - Le serveur répond
    - » soit par l'adresse IP du nom complet demandé
    - » soit par la liste des serveurs pouvant y répondre si il ne connait pas l'adresse du nom complet demandé
- Ceci pour deux raisons
  - Les serveurs gérant des zones de «haut niveau» peuvent faire des statistiques, recherches... sur les requêtes complètes
  - Le découpage des zones n'est pas connu par les serveurs DNS
    - » Par exemple la zone de ***truc.fr*** est peut être géré par les serveurs de ***.fr***

Interrogation DNS

- Pour une zone : une liste d'adresse de serveurs
  - Répartition des interrogations
  - Requêtes successives si défaillance d'un serveur ou du réseau
  - Importance de la répartition géographique des serveurs d'une même zone
- Mécanisme de cache dans le serveur "local" pour limiter le nombre d'interrogations
  - Evite la surcharge du réseau
  - Diminue les délais de réponse
  - Baisse la charge des serveurs de haut niveau
- Remplissage du cache lors des requêtes des clients
- Durée de vie limitée dans le cache
  - TTL(Time To Live) spécifié dans les réponses

Serveurs «racine»

- Gérés par 2 organisations européennes, une japonaise et 9 américaines
- Racine : 13 «autorités» de nom répartis dans le monde (appelés de A à M)
  - Connaissent tous les serveurs de premier niveau (TLD): .fr, .com, ...
  - SERVEUR "ORIGINE" (ou primaire, ou maitre) géré par IANA/ICANN
    - » ***A.ROOT-SERVERS.NET***
  - SERVEURS MIROIRS (ou secondaire, ou esclave)
    - » de ***B.ROOT-SERVERS.NET*** à ***M.ROOT-SERVERS.NET***
- En fait grappe de serveurs pour chaque entité: ~200 serveurs répartis dans le monde
- De l'ordre de 50 000 requêtes par seconde sur un serveur en 2016

Type de requêtes

- **Adresse de machines**
  - Dénoté ***a*** pour IPV4
  - Possibilités de plusieurs machines pour un même nom
    - » Réponses "circulaires" pour répartir la charge
  - Dénoté ***aaaa*** pour IPV6
- **Nom canonique et alias**
  - Plusieurs noms possibles pour une adresse IP
  - Un nom canonique et des alias
  - dénoté ***cname*** (Canonical Name)
- **Serveurs d'une zone ?**
  - Liste des serveurs d'un domaine
  - Dénoté ***ns***

Type de requêtes

- **Serveur de messagerie**
  - Indique les serveurs SMTP à contacter pour envoyer un courriel à un utilisateur d'un domaine donné
  - Dénoté ***mx*** (Mail eXchange)
- **Interrogation inverse**
  - Permet de faire une requête inverse : un nom à partir d'une adresse
  - Dénoté ***ptr***
- ***Serveur maître d'un domaine***
  - Permet de connaître des informations sur le serveur maître d'un domaine
  - Dénoté ***soa*** (Start Of Autority)

Implémentation

- JEEVES : première implémentation du DNS (1984)
- BIND (The Berkeley Internet Name Domain) sur BSD Unix
- Interrogation en UDP ou TCP si la taille des paquets dépasse 512 octets
- Echange des bases de données en TCP
- Client
  - à travers les fonctions de programmation comme ***gethostbyname***, ***gethostbyaddr,*** remplacés aujourd'hui par ***getaddrinfo*** *(gestion des adresses IPV6)…*
  - outils associés (***host***, ***nslookup***...)
- Serveur processus particulier
  - Port 53 en TCP ou UDP
  - nom: ***named***

Outils DNS

- **nslookup**
  - ***nslookup www.google.fr***
  - Changement de serveur : ***server ns2.nic.fr***
  - mode debug: **set debug**
  - Serveurs d'une zone: ***set q=ns***
  - Adresses pour un nom: ***set q=a***
  - Serveurs de courrier: ***set q=mx***
  - Nom canonique: ***set q=cname***
  - Visualisation de la base de donnée: ***ls imag.fr***
- **host**
  - Mode debug : ***-d***
  - Type de requête: ***-t a*** , ***-t ns*** ...
- **dig**

Exemple

- **host -d -t a goedel.e.ujf-grenoble.fr**
  - *Trying "goedel.e.ujf-grenoble.fr"*
  - *;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37230*
  - *;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2*
  - *;; QUESTION SECTION:*
  - *;goedel.e.ujf-grenoble.fr. IN A*
  - *;; ANSWER SECTION:*
  - *goedel.e.ujf-grenoble.fr. 86255 IN A 195.220.82.132*
  - *;; AUTHORITY SECTION:*
  - *e.ujf-grenoble.fr. 913 IN NS cubango.ujf-grenoble.fr.*
  - *e.ujf-grenoble.fr. 913 IN NS colorado.ujf-grenoble.fr.*
  - *;; ADDITIONAL SECTION:*
  - *colorado.ujf-grenoble.fr. 26781 IN A 152.77.2.5*
  - *cubango.ujf-grenoble.fr. 23685 IN A 193.54.238.51*

Exemple

- **host -d -t ns imag.fr**
  - Trying "imag.fr"
  - ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53175
  - ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 6
  - ;; QUESTION SECTION:
  - ;imag.fr. IN NS
  - ;; ANSWER SECTION:
  - imag.fr. 86400 IN NS ns2.nic.fr.
  - imag.fr. 86400 IN NS dns.inria.fr.
  - imag.fr. 86400 IN NS isis.imag.fr.
  - imag.fr. 86400 IN NS imag.imag.fr.

Résolution inverse

- Trouver le nom à partir de l'adresse
- Même principe que pour les noms
- Chaque octet de l'adresse IP est vue comme un sous domaine
- Un domaine TLD particulier pour les adresses IPV4: ***arpa***
- Sous domaines
  - ***in-addr*** pour les adresses IPv4
  - ***ip6*** pour les adresses IPv6
- Exemple: ***229.38.88.129.in-addr.arpa***

Exemple de résolution inverse

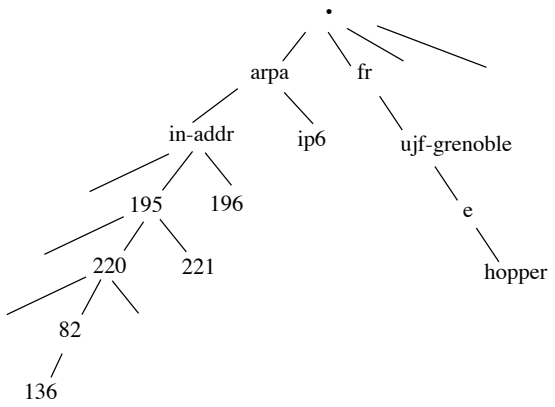
- **host -d 195.220.82.136**
  - Trying "136.82.220.195.in-addr.arpa"
  - ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32544
  - ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4
  - ;; QUESTION SECTION:
  - ;136.82.220.195.in-addr.arpa. IN PTR
  - ;; ANSWER SECTION:
  - 136.82.220.195.in-addr.arpa. 85913 IN PTR hopper.e.ujf-grenoble.fr.

  - ;; AUTHORITY SECTION:
  - 82.220.195.in-addr.arpa. 85913 IN NS cubango.ujf-grenoble.fr.
  - 82.220.195.in-addr.arpa. 85913 IN NS soleil.uvsq.fr.
  - 82.220.195.in-addr.arpa. 85913 IN NS colorado.ujf-grenoble.fr.
  - 82.220.195.in-addr.arpa. 85913 IN NS adminpg.inpg.fr.

  - ;; ADDITIONAL SECTION:
  - ....

Exemple de résolution inverse

- hopper.e.ujf-grenoble.fr
- 136.82.220.195.in-addr.arpa



Fichiers “système” de configuration DNS côté client

- Système à la Unix: Fichier ***/etc/resolv.conf***
  - Adresse du serveur et suffixe par défaut
    - » Exemple:
      - ***search imag.frimag.fr***
      - ***nameserver 195.221.224.1***
      - ***nameserver 129.88.30.1***

- Fichier permettant d’activer le client DNS
  - On peut activer ou non la résolution de nom par DNS ou /etc/hosts
  - FreeBSD: ***/etc/host.conf***
  - Unix/solaris: ***/etc/nsswitch.conf***

Fichiers “système” de configuration DNS côté serveur

- Configuration du processus serveur (Système à la Unix)
  - FreeBSD: ***/etc/namedb/named.conf***
  - Unix/solaris/Linux**:** ***/etc/named.conf***
  - **C**ontient la liste des zones gérées par le serveur
    - » Nom du domaine
    - » Nom du fichier “base de donnée”
    - » Type master/slave
  - Spécifie l’endroit où se trouve les fichiers “base de donnée”
  - Contient au moins la base de données des serveurs racines

Le fichier named.conf

```
options
{
directory "/var/spool/named";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "rev.127.0.0";
};

zone "imag.fr" {
        type slave;
        file "imag.fr.zone";
        masters { 129.88.30.1; };
};

zone "224.221.195.in-addr.arpa" {
        type slave;
        file "rev.195.221.224";
        masters { 129.88.30.1; };
};
zone "." {
        type hint;
        file "named.root";
};
```


Le fichier named.conf

- Directory des fichiers de base de donnée
  - `/var/spool/named`
- Zone imag.fr
  - Fichier *imag.fr.zone*
  - Type esclave
  - Adresse du maître: *129.88.30.1*
- Zone *224.221.195.in-addr.arpa*
  - Résolution inverse
- Zone *0.0.127.in-addr.arpa*
  - Inclus dans tous les serveurs DNS
- Zone racine "."
  - Zone indispensable pour effectuer la résolution de premier niveau
  - Fichier *named.root*
  - Peut être obtenu sur le site *www.internic.net*

Base de donnée des serveurs racine (root.cache)

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    October 20, 2016
;       related version of root zone:   2016102001
;
; formerly NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
; FORMERLY NS1.ISI.EDU
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:84::b
;
; FORMERLY C.PSI.NET
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c

...etc pour les 13 serveurs de la zone racine
```


Base de donnée de *imag.fr*

```
$ORIGIN .
$TTL 7200       ; 2 hours
imag.fr         IN SOA  imag.imag.fr. fr-imag-subdom-admin.imag.fr. (
                                2004040204 ; serial
                                21600      ; refresh (6 hours)
                                3600       ; retry (1 hour)
                                3600000    ; expire (5 weeks 6 days 16 hours)
                                86400      ; minimum (1 day)
                                )
                        NS      dns.inria.fr.
                        NS      ns2.nic.fr.
                        NS      imag.imag.fr.
                        NS      isis.imag.fr.
                        A       129.88.30.1
                        MX      10 imag.imag.fr.
                        MX      20 harmonie.imag.fr.
                        MX      50 mx-serv.inrialpes.fr.
TXT             "IMAG    BP  53     F-38041  GRENOBLE  Cedex  9  (France)"
TXT     "Institut d'Informatique et de Mathematiques Appliquees"
TXT     "or IMAG 46 Av. Felix Viallet  F-38031 GRENOBLE Cedex
```

Base de donnée de *imag.fr*

- ***$ORIGIN*:** spécifie le suffixe à ajouter aux noms qui suivent
- ***$TTL (Time to Live):*** durée de vie maximale dans le cache (en seconde) (souvent ~1 jour)
- Nom d'un domaine géré : ici ***imag.fr*.**

Base de donnée de *imag.fr*

- Information relative au domaine, permet de répondre aux interrogations de type *SOA*
- **SOA (*Start Of Authority*):** spécifie des informations relatives à l'administrateur du domaine
  - **N**om du serveur primaire **(ici *imag.imag.fr*)**
  - **A**dresse du mail de l'administrateur (où le caractère @ est remplacé par un .) Si il y a des points avant l'@, ils sont remplacés par \. (ex: Pascal\.sicard.imag.fr)
  - **Serial *(2004040204)* :** Numéro de version : (aammjjVV) qui permet au serveur secondaire de détecter des modifications
  - **Refresh *(21600)* :** (en seconde) période de rafraîchissement (entre deux interrogations des secondaires pour mise à jour)
  - **Retry *(3600)* :** durée minimale entre deux interrogations d'un secondaire suivant un échec
  - **Expire *(3600000)* :** durée maximale dans un serveur secondaire au-delà non garantie
  - M**inimum *(86400)* :** durée de conservation d'un enregistrement dans un cache name server

Base de donnée de *imag.fr* (suite)

```
$ORIGIN imag.fr.
abricot                 A       152.77.201.179
                        MX      10 imag
                        MX      20 harmonie
                        MX      50 mx-serv.inrialpes.fr.
abricotier              CNAME   abricotier.inrialpes.fr.
abyssin                 A       129.88.33.45
                        MX      10 imag
                        MX      20 harmonie
                        MX      50 mx-serv.inrialpes.fr.
acacia2                 CNAME   acacia2.inrialpes.fr.
acajou                  CNAME   acajou.inrialpes.fr.
achab                   A       129.88.33.38
                        MX      10 imag
                        MX      20 harmonie
                        MX      50 mx-serv.inrialpes.fr.
$ORIGIN ad.imag.fr.
sv-fede                 A       129.88.28.100
$ORIGIN imag.fr.
adagio                  A       129.88.103.23
                        MX      10 imag
                        MX      20 harmonie
                        MX      50 mx-serv.inrialpes.fr.
```


Base de donnée DNS

- Les champs ont le même nom que les types des requêtes
- ***NS*** indique les serveurs de la zone
  - Le serveur répondra avec ces informations à une requête *ns*
- ***MX*** indique les serveurs de courriers (protocole SMTP)
  - 1ère colonne : Poids indiquant la priorité dans le cas de plusieurs serveurs de mail (poids faible -> plus grande priorité)
- ***A*** indique pour un nom, l'adresse correspondante
- ***TXT*** donne des indications textuelles comme l'adresse postale
- ***CNAME*** donne le nom canonique

Type de serveurs

- Serveur maître, principal
  - Sur lequel sont faites les modifications par l'administrateur
  - Il a l'origine de l'autorité sur une zone (Start Of Autority: SOA)
- Serveur esclave, secondaire
  - Interroge et récupère régulièrement les bases de données depuis le serveur maître
  - Peut posséder un cache pour minimiser les requêtes (Non authoritative Reponse)
- Une réponse à une interrogation peut être faite par un serveur primaire ou secondaire
- Un serveur peut être secondaire pour certaines zones et primaire pour d'autres

Echange des bases de données

- Echange classique
  - Un serveur secondaire d'une zone interroge régulièrement le serveur primaire de cette zone (à l'initiative du secondaire)
  - La fréquence de mise à jour est indiqué par la valeur ***REFRESH*** dans le SOA
  - Mise à jour possible de serveur secondaire à primaire mais aussi de secondaire à secondaire
  - La version d'une zone est identifiée par son numéro de série (***SERIAL***). A chaque modification elle est augmentée
  - Le serveur secondaire transfert d'abord le SOA de la zone et vérifie le numéro de série
    - » Si c'est le cas il demande le transfert soit de la base de donnée complète, soit seulement des modifications (transfert incrémental)
  - La récupération de la base de donnée se fait au dessus de TCP
- Echange sur modification
  - Pour accélérer la mise à jour des bases de données, un serveur primaire peut notifier aux serveurs secondaires une modification

DNS menteur

- Un serveur DNS peut être configuré pour renvoyer à une requête DNS, une adresse IP différente de celle apparaissant dans les bases de données DNS
- Loi Anti-terroriste de novembre 2014 autorise les FAI à bloquer l'accès aux sites terroristes
- Peut être fait via un DNS menteur
- Utilisé aussi pour les accès à des noms DNS non existant, redirection vers des publicités ou autres
- Utilisé aussi pour les accès à des sites ne respectant pas les droits d'auteurs. Interdiction de l'accès.
- Il suffit de changer l'adresse du serveur DNS à interroger

Sécurité pour le DNS

- **DNS central dans le réseau; Gros potentiel d'attaque : redirection de trafic ...**
- **Attaque importante détectée pendant l'été 2008 aux USA**
  - » **Capture d'ID de requête**
    - Le pirate capture des paquets de requête DNS (connait donc l'ID des requêtes)
    - Envoie la réponse fausse avant le vrai serveur DNS et redirige vers un site d'hameçonnage
  - » **Empoisonnement de Cache**
    - Remplissage du cache d'un serveur par de fausses informations (Nom/IP)
    - Exemple
      - Envoie par le pirate d'une requête à un serveur DNS X sur un nom de machine *www.google.fr*
      - Le pirate prépare des réponses pour répondre à la place du serveur DNS de Google.fr au serveur DNS X
      - Le serveur DNS X remplit son cache avec une fausse adresse IP

Sécurité pour le DNS

- Quelques points de sécurité possibles aujourd'hui:
  - On peut limiter l'envoi des réponses aux requêtes DNS à une liste d'adresses IP (celles des machines du domaine par exemple)
  - On peut limiter l'envoi des bases de donnée à une liste d'adresses IP (serveurs secondaires)
  - On peut utiliser des techniques de chiffrement et/ou authentification

DNSSEC

- Authentification des serveurs DNS par signature à base de clé privée/publique
- Normalisé en 2005
- Permet d'éviter l'empoisonnement de cache
- Principe:
  - » Une clé privée est rajoutée aux enregistrements et permet de signer les réponses
  - » Une clé publique est disponible et vérifiable par chaîne de confiance auprès des serveurs de niveau supérieur
  - » Exemple: La clé publique de imag.fr est signée par la clé privée de la zone fr, elle même signée par la clé privée de la zone racine
- Authentification Signature de la zone racine en 2010
- N'assure pas la confidentialité des données

Chiffrement des requêtes/réponses

- DNS over HTTPS (DOH)
  - » Requête DNS client/serveur à travers HTTPS
  - » Possible entre Firefox et google depuis 2018
  - » Permet de passer outre le filtrage DNS
- DNS over TLS (DOT)
  - » Utilise la couche transport sécurisé
  - » Bind 9 implémente DNS over TLS
- Utilisables aujourd'hui dans la plupart des OS à travers une application dédiée ou l'utilisation d'un serveur DNS local
- Permet de passer outre les filtrages DNS (par proxy) et DNS menteur

Serveurs DNS « public » et sécurisé

- CloudFlare
- OpenDNS
- Google
- Neustar
- OpenNIC
- Quad9
- FreeDNS
- …
- https://dnslookup.fr/blog/quel-resolveur-dns-public-choisir/

Le DNS dans la pratique

- Le serveur
  - Fichiers de configuration
    - » Unix/linux: ***/etc/named.conf***
    - » Free BSD: ***/etc/namedb/named.conf***
  - Base de données
    - » Spécifié dans le fichier de configuration
  - Lancement du serveur
    - » Unix/linux: ***/etc/rc.d/init/named restart***
    - » Free BSD: ***named -b /etc/namedb/named.conf***
- Le client
  - Fichier de spécification du serveur DNS: **/etc/resolv.conf**
  - Fichier de spécification de la résolution de nom:
    - » Unix/linux: ***/etc/nsswitch.conf***
    - » Free BSD: ***/etc/host.conf***