DNS

IUT 1 – Université de Lyon

DNS

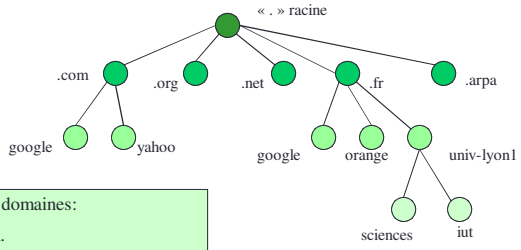
- Questions:
  - Connaissez vous des noms de PCs ou de serveurs (web, mail, etc.) ?
  - Connaissez vous des adresses IP de PCs ou de serveurs (web, mail, etc.) ?

Le DNS

- A quoi cela sert?
  - Correspondance entre un nom de machine et une adresse IP
  - C'est l'adresse IP qui est utilisée pour joindre une machine et non son nom

Le DNS

- Les machines ne sont pas nommées n'importe comment
- Association d'un parc informatique à un nom de domaine (entreprise, université, etc.)
- Association administrative (il faut enregistrer son nom de domaine!)
- Le nom de domaine fait partie de **l'arbre de nommage**:



Nom complet des domaines:

google.com.

iut.univ-lyon1.fr.

sciences.univ-lyon1.fr.

Le DNS

- Un domaine peut contenir un nombre arbitraire de machines

Pour le domaine univ-lyon1.fr:
machine1.univ-lyon1.fr.
machine2.univ-lyon1.fr.
www.univ-lyon1.fr.
ftp.univ-lyon1.fr.

- Il peut aussi contenir des sous-domaines

Pour le domaine iut.univ-lyon1.fr:
machine1.iut.univ-lyon1.fr.
machine2.iut.univ-lyon1.fr.
www.iut.univ-lyon1.fr.
ftp.iut.univ-lyon1.fr.

Le DNS: le problème

- Base de données de plusieurs milliards d'entrée.
- Approche centralisée: un seul serveur
  - Mise à jour permanente
  - Problème de sécurité (contrôle d'accès)
  - Problème de charge
  - Ingérable
- Approche décentralisée
  - Chaque domaine gère ses noms de machines
- Comment fait-on pour obtenir une adresse IP d'un autre domaine?

Le DNS: le principe (résolution itérative)

- Un ou plusieurs serveurs sont responsable d'un domaine
- A chaque nœud de l'arbre correspond au moins un serveur
- Un serveur responsable d'un domaine doit:
  - Gérer toutes les machines de son domaine (association nom – adresse IP)
  - Connaître l'adresse des serveurs responsables des sous domaines (dans l'arbre de nommage)
  - Connaître l'adresse du serveur root.

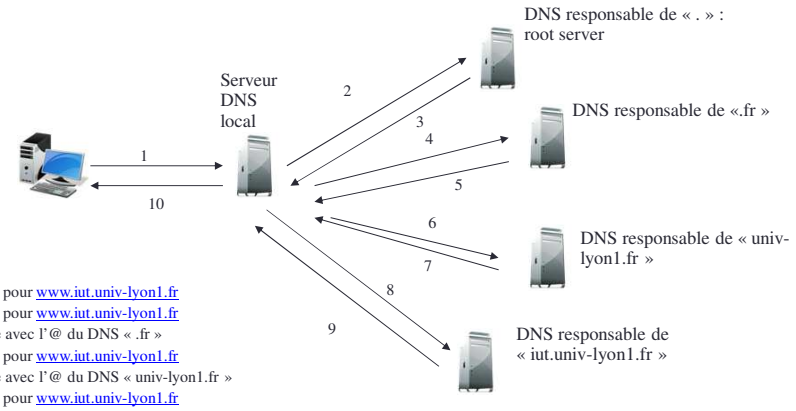
DNS

- Un serveur DNS n'est pas forcément responsable d'un domaine
- Peut-être utilisé uniquement pour résoudre les requêtes des clients
- Un client a forcément un serveur DNS configuré pour résoudre ses requêtes (qui peut être responsable d'un domaine ou non)
  - Manuellement
  - Automatiquement

Questions

- Avec ces hypothèses:
  - Un serveur DNS ne connaît que les adresses de son propre domaine
- Comment fait il pour trouver les autres adresses?

Exemple

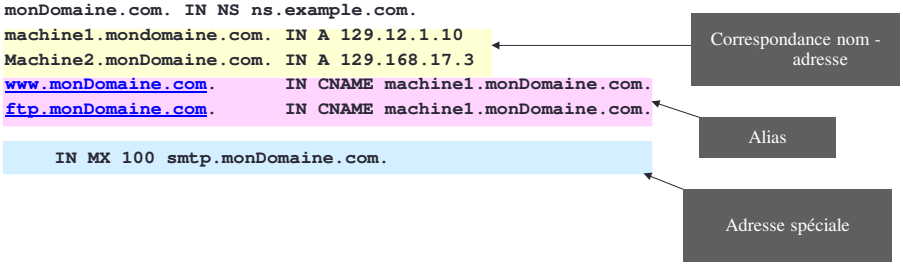


1. Requête pour www.iut.univ-lyon1.fr
2. Requête pour www.iut.univ-lyon1.fr
3. Réponse avec l'@ du DNS « .fr »
4. Requête pour www.iut.univ-lyon1.fr
5. Réponse avec l'@ du DNS « univ-lyon1.fr »
6. Requête pour www.iut.univ-lyon1.fr
7. Réponse avec l'@ du DNS de «iut.univ-lyon1.fr »
8. Requête pour www.iut.univ-lyon1.fr
9. Réponse avec l'adresse de la machine demandé (www….)
10. Réponse avec l'adresse de la machine demandée

Exemple de fichiers de configuration du DNS (bind sous Linux)

```
$TTL 604800
@ IN SOA monDomaine.com. root.monDomaine.com. (
     1 ; Serial
     604800 ; Refresh
     86400 ; Retry
     2419200 ; Expire
     604800 ) ; Negative Cache TTL
;
monDomaine.com. IN NS ns.example.com.
machine1.mondomaine.com. IN A 129.12.1.10
Machine2.monDomaine.com. IN A 129.168.17.3
www.monDomaine.com.      IN CNAME machine1.monDomaine.com.
ftp.monDomaine.com.      IN CNAME machine1.monDomaine.com.

     IN MX 100 smtp.monDomaine.com.
```



Exercice

- Un client effectue une requête à son DNS local pour le nom
  - ftp.g1S4.iut.univ-paris5.fr
  - Quels sont les étapes de la résolution?
- On suppose maintenant que le DNS garde en *cache* les résolutions qu'il a déjà effectué:
  - Quels sont les étapes de la résolution pour le nom:
    - www.google.com
    - machine1.univ-paris5.fr
- Quelles sont les informations minimales que doit conserver un serveur DNS responsable d'un domaine?

Maitre / esclave

- Un serveur DNS peut ne pas être suffisant pour un domaine donnée: problème de charges
- Utilisation d'un serveur maître et de serveurs esclaves
  - Le serveur esclave télécharge la base de données sur le serveur maître
  - Il répond aux requêtes de manière identique au serveur maître

Exemple de fichiers de configuration du DNS (le maître)

```
$TTL 604800
@ IN SOA monDomaine.com. root.monDomaine.com. (
     1 ; Serial
     604800 ; Refresh
     86400 ; Retry
     2419200 ; Expire
     604800 ) ; Negative Cache TTL
;
monDomaine.com. IN NS ns.example.com.
machine1.mondomaine.com. IN A 129.12.1.10
Machine2.monDomaine.com. IN A 129.168.17.3
www.monDomaine.com.      IN CNAME machine1.monDomaine.com.
ftp.monDomaine.com.      IN CNAME machine1.monDomaine.com.

     IN MX 100 smtp.monDomaine.com.
```

N° de série : incrémenté à chaque modification.

Période entre deux téléchargement de la base par le serveur esclave

Période entre deux essais (en cas d'échec) et temps avant expiration

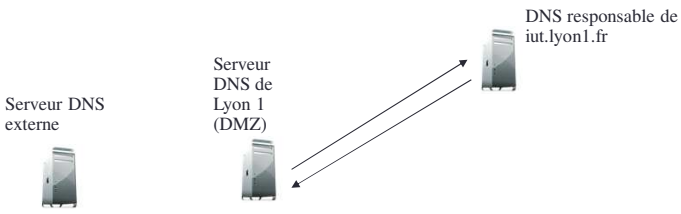
DNS inverse

```
$TTL 3600
1.168.192.in-addr.arpa. IN SOA ns1.example.org. admin.example.org. (
2006051501 ; Serial
10800 ; Refresh
3600 ; Retry
604800 ; Expire
3600 ) ; Minimum

    IN NS ns1.example.org.
  IN NS ns2.example.org.

1.1.168.192.in-addr.arpa. IN PTR example.org.
2.1.168.192.in-addr.arpa. IN PTR ns1.example.org.
3.1.168.192.in-addr.arpa. IN PTR ns2.example.org.
4.1.168.192.in-addr.arpa. IN PTR mx.example.org.
5.1.168.192.in-addr.arpa. IN PTR mail.example.org.
```

Exercice



- Comment sont configurés les clients?
- Quel doit être l'adresse IP des serveurs auxquels se connectent les client de l'université? De l'IUT?
- Comment faire pour que ce soit le DNS de la DMZ de Lyon 1 qui répondent aux requêtes?