

## TP DNS

Dans ce TP vous aurez à gérer des serveurs DNS (Domain Name System) sous Windows. Vous choisirez comme adresse IP pour votre ordinateur 192.168.114.X /24 où X est le numéro de votre disque dur.

### Interrogation en ligne

Dans un premier temps vous allez utiliser *nslookup* (les commandes équivalentes sous linux sont *dig* et *host*) pour interroger un serveur de nom. Le serveur de nom par défaut 192.168.114.254 étant peu bavard vous utiliserez celui de la salle : 192.168.107.200. Le serveur 192.168.107.200 est un serveur de nom gérant le domaine *pedago.src.* En vous aidant de l'aide, trouvez tous les enregistrements de la zone *pedago.src.* Vous penserez à indiquer à la commande *nslookup* d'utiliser le serveur DNS 192.168.107.200. A quoi correspond un enregistrement SOA, A, CNAME, NS, A, MX.

De même trouvez tous les enregistrements de la zone *168.192.in-addr.arpa.* A quoi correspond un enregistrement PTR.

Pour la suite vous configurez votre client DNS pour qu'il interroge votre propre serveur avec comme suffixe par défaut *faiX.com.* Les commandes *net stop "Client DNS"* et *net start "Client DNS"* peuvent vous être utiles pour arrêter et relancer le client DNS de Windows.

### Hosts

Avant l'apparition du système DNS les hôtes disposaient d'un fichier d'hôtes (*hosts*) réalisant la correspondance entre un nom d'hôte et une adresse IP (une résolution de nom d'hôte en adresse IP). Ce fichier était mis à jour par ftp depuis un serveur central. Ce fichier existe toujours pour la résolution de nom locale, vous le trouverez sous *c:\windows\system32\drivers\etc\* (la lettre du lecteur dépend de votre groupe).

Consultez ce fichier et ajoutez le nom *ma-machine* associé à votre adresse de boucle locale (127.0.0.1) ainsi que *machine-du-voisin* associé à son adresse IP. Testez ces deux noms d'hôtes avec la commande *ping* qui forcera une résolution de nom.

En imaginant le travail d'un administrateur réseaux devant gérer un parc de 100 machines et en vous interrogeant sur le moyen de diffusion du fichier *hosts*, expliquez pourquoi ce système simple a été abandonné ?

### Serveur autonomes

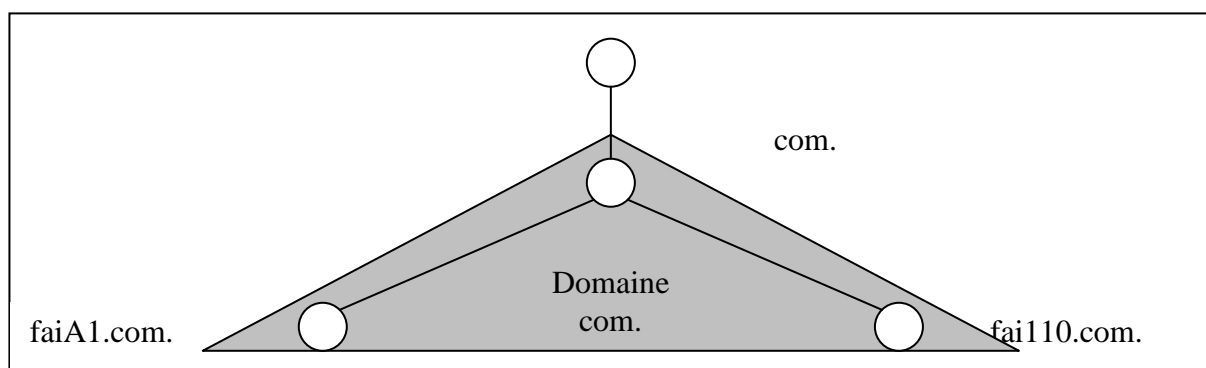


Figure 1 Espace de noms

Vous allez tous configurer votre machine en serveur de zone primaire. Vous allez gérer le domaine (et la zone), *faiX.com*.

Si le serveur DNS de votre machine n'est pas installé, faites le en utilisant l'assistant de gestion de serveur. Afin de pouvoir lire les fichiers de configurations, ne liez pas votre serveur à Active Directory et pour avoir un peu de travail sélectionnez l'option « configurer les indications de racine uniquement ».

## **Zone de recherche directe**

Créer une zone de recherche directe contenant :

- *dns.faiX.com* comme serveur de nom et comme serveur faisant autorité sur la zone *faiX.com*,
- *www.faiX.com* , *www2.faiX.com*., *smtp.faiX.com* comme alias vers la machine précédente,
- *turing-X.faiX.com* vers la machine de la salle turing (192.168.114.X+96) de même numéro de poste si vous êtes dans la salle *postel* et *postel-X.faiX.com* vers la machine de la salle *postel* (192.168.114.X) de même numéro de poste si vous êtes dans la salle *turing*.
- *smtp.faiX.com* comme serveur de mail de votre domaine avec une priorité de 10.

Tester votre domaine avec des *ping* et *nslookup* pour l'enregistrement MX.

Consulter le fichier de zone dans *c:\windows\system32\dns*.

Pouvez-vous résoudre des noms d'hôtes du domaine géré par votre voisin, pourquoi ?

Pouvez-vous réaliser une résolution inverse, à savoir résoudre une adresse IP en un nom d'hôte ?

## **Zone de recherche inverse**

Créer deux zones de recherche inverse pour les machines que vous gérez.

Tester vos zones avec *nslookup*.

Consulter le fichier *c:\windows\system32\dns\114.168.192.in-addr.arpa.dns*

## **Redirecteurs**

Un serveur de DNS si il ne peut répondre à une requête, i.e. ne peut trouver de correspondance dans ces fichiers de zone, peut utiliser des redirecteurs pour relayer la requête vers d'autres serveurs.

Définissez deux redirecteurs, un premier vers le serveur de domaine de votre voisin et un deuxième vers le serveur DNS de l'IUT (192.168.114.254)<sup>1</sup>.

Tester la résolution pour une machine du domaine SRC et pour une machine gérée par le serveur de noms de votre voisin.

## **Délégation**

Les redirecteurs correspondent à une approche locale, un serveur utilisé sur un intranet peut gérer un domaine fantaisiste comme le domaine maison et rediriger les requêtes non résolues vers le serveur de DNS du FAI.

---

<sup>1</sup> Sous Windows une alternative aux redirecteurs est l'utilisation des indications de racine.

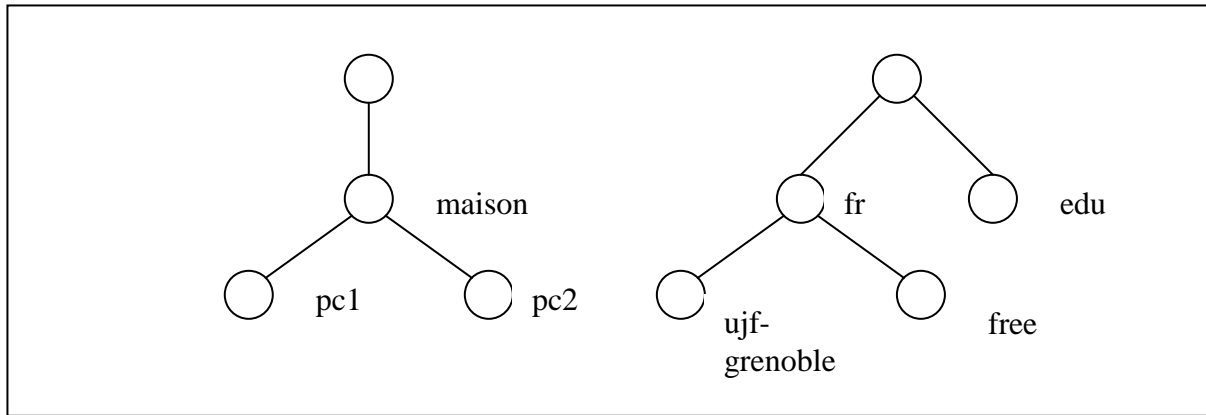


Figure 2 Redirection

Sur Internet une autre solution est utilisée, les serveurs peuvent déléguer leur autorité. *Postel-15* (192.168.114.15) ou *turing-15* (192.168.114.11) selon votre salle vont gérer le domaine *.com*. et va pour chaque sous-domaine déléguer son autorité vers vos serveurs de DNS.

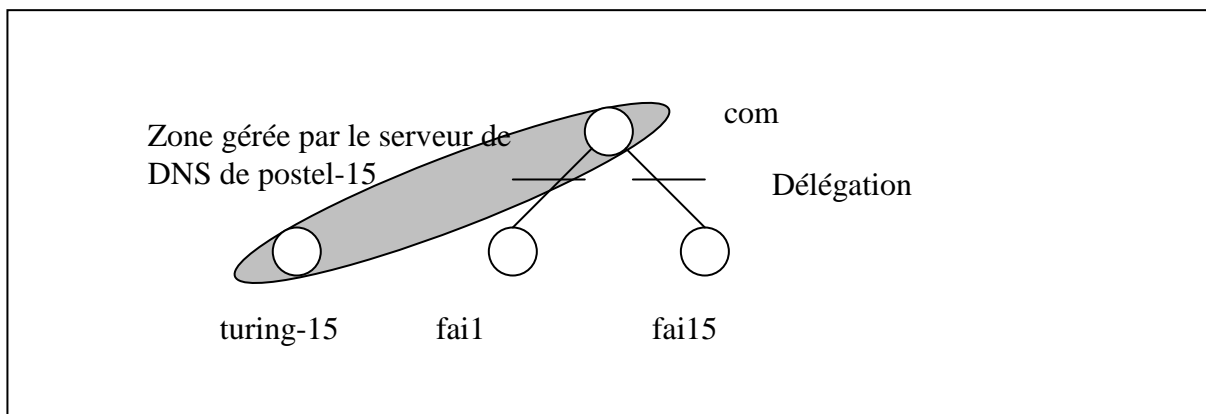


Figure 3 Délégation

Effacer les redirecteurs présents sur votre machine.

Configurer votre machine pour qu'elle utilise *postel-15* (*turing-15*) comme serveur de DNS et aller configurer *postel-15* pour une délégation vers votre serveur, c.a.d. indiquer au serveur de DNS de *postel-15* que vous êtes un serveur de nom pour votre sous-domaine. Une zone est un fichier hébergé sur un serveur et permettant une résolution de nom, un domaine est une branche de l'espace de noms. Pour différencier une zone d'un domaine demander à *postel-15* (*turing-15*) de gérer *turing-15.com* (*postel-15*).

Tester cette configuration.

### **Zone de stub (facultatif)**

En vous aidant pouvez vous définir une zone de *stub* et son utilisation.