Bind

I- Introduction :

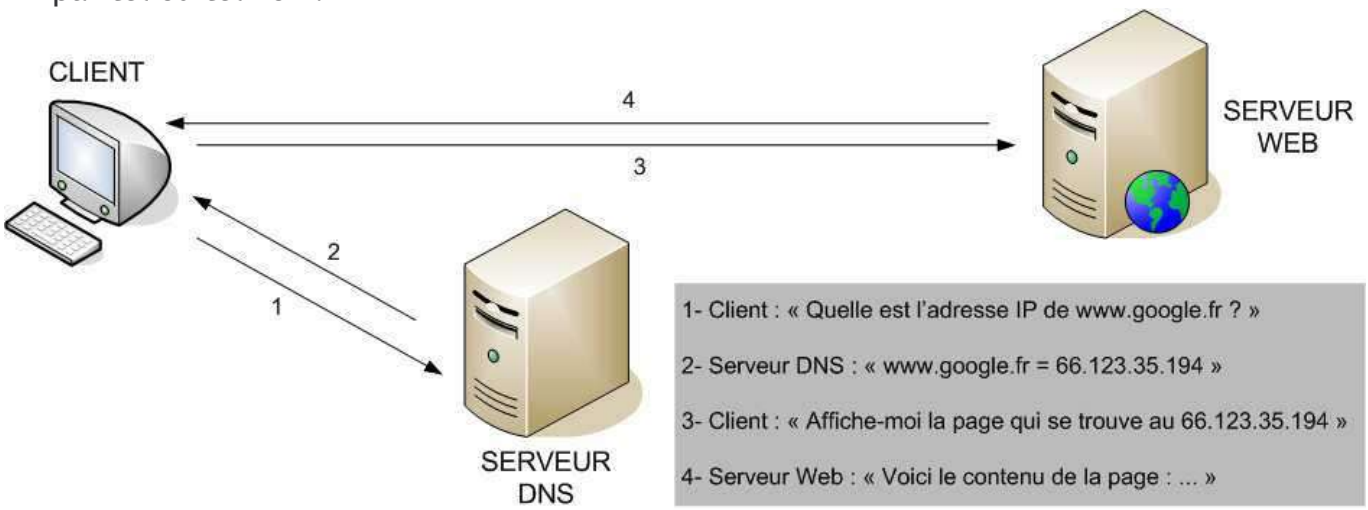
Un peu de théorie :

Le DNS est un serveur qui permet d'associer un nom de domaine à l'adresse IP d'une machine.

Les noms de machines sont composés de plusieurs parties et se lisent de droite à gauche, par exemple :

www.google.fr. ou ftp.free.fr.

- En partant de la droite, le . représente la racine.
- Le **.fr** est le domaine de premier niveau (**TLD** : Top Level Domain). Les abréviations de pays (.fr .nl .be .de ...) s'appellent des **ccTLD** (country code TLD), tandis que les autres TLD (.com .info .org .edu ...) s'appellent **gTLD** (generic TLD).
- Le nom du domaine est **.google** ou **.free** .
- Le **www** ou **ftp** est le nom de la machine qui offre le service. Ce nom dépend de l'administrateur de free ou google qui choisit dans son domaine d'appeller une machine par tel ou tel nom.



Installation :

Tout simplement les commandes habituelles :

apt-get update (mettre à jour la liste des sites sur lesquels on peut télécharger les paquets)

apt-get install bind9 (installer le paquetage et ses dépendances)

II- Configuration de bind :

Dans notre cas, nous aurons un certain nombre de fichiers à configurer. Le fichier principal pour la configuration de Bind s'appelle **named.conf** (/etc/bind/named.conf).

named.conf

Ce fichier est composé en deux parties :

- Les options principales
- Les zones de recherche directe et de recherche inversée que l'on veut déclarer

```
//////////////////////////
// OPTIONS PRINCIPALES //
//////////////////////////

options {
      directory "/etc/bind";        // Répertoire des fichiers de configuration
      version "SECRET";             // masquer la version de Bind
      forward first;                // Notre serveur répond en premier
      forwarders {
            193.252.19.3;           // DNS qui répondent si notre DNS ne
            193.252.19.4;           // connaît pas un nom (ici ceux de wanadoo)
      };
      auth-nxdomain no;
};


//////////////////////////////////////
// DECLARATION DE TOUTES LES ZONES //
//////////////////////////////////////

//////////////////////////
// Zones obligatoires //
//////////////////////////

zone "." {
      type hint;
      file "/etc/bind/db.root";
};
zone "localhost" {
      type master;
      file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
      type master;
      file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
      type master;
      file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
      type master;
      file "/etc/bind/db.255";
};
```

```
//////////////////////////////////////
// Zone de recherche directe a ajouter //
//////////////////////////////////////

zone "mynetcourse.info" {
        type master;
        file "/etc/bind/mynetcourse.info.zone";
};


////////////////////////////////
// zone de recherche inversée //
////////////////////////////////

zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/0.168.192.rev";
};
```

III - Fichiers de zone :

Recherche directe : /etc/bind/mynetcourse.info.zone

Ce fichier contient les noms des machines dans le domaine, mappées avec leur @ IP

```
; en-tête du fichier
$TTL 86400
@       IN      SOA     srv.mynetcourse.info. admin.mail.mynetcourse.info. (
        20051103;
        28800;
        14400;
        3600000;
        86400 );

;     déclarations d'un serveur de nom (NS) et d'un serveur de mail (MX)
      IN    NS          srv.mynetcourse.info.
      IN    MX    10    mail.mynetcourse.info.

; exemples d'enregistrements de type A

poste1      IN    A     192.168.0.101
poste2      IN    A     192.168.0.102
poste3      IN    A     192.168.0.103
poste4      IN    A     192.168.0.104
poste5      IN    A     192.168.0.105
srv         IN    A     192.168.0.253
mail        IN    A     192.168.0.254

; exemples d'enregistrements d'alias (CNAME)

www     IN      CNAME   srv         // www est un alias de srv.mynetcourse.info
pop     IN      CNAME   mail
imap    IN      CNAME   mail
smtp    IN      CNAME   mail
```

Recherche inversée : /etc/bind/0.168.192.rev

Ce fichier contient les @ IP du réseau mappées avec leur noms dans le domaine

```
; en-tête
$TTL 86400
@       IN      SOA     srv.mynetcourse.info. admin.mail.mynetcourse.info. (
        20051103;
        28800;
        14400;
        3600000;
        86400 );

;     déclaration du serveur DNS
      NS    srv.mynetcourse.info.

; déclaration d'enregistrements de type PTR
1     PTR   poste1.mynetcourse.info.      // l'@ 192.168.0.1 s'appelle poste1
2     PTR   poste2.mynetcourse.info.      // l'@ 192.168.0.2 s'appelle poste2
3     PTR   poste3.mynetcourse.info.      // l'@ 192.168.0.3 s'appelle poste3
4     PTR   poste4.mynetcourse.info.      // l'@ 192.168.0.4 s'appelle poste4
5     PTR   poste5.mynetcourse.info.      // l'@ 192.168.0.5 s'appelle poste5
```

Explications :

En-tête :

$TTL 3D	Durée de vie de la zone exprimée en secondes par défaut.
@ IN SOA	désigne l'enregistrement de "début d'autorité" (Start Of Authority)
	il est suivi du serveur DNS primaire et de l'adresse du responsable
(xxxxxxxx;	N° de version. Par habitude : AAAAMMJJ (ex : 20051103)
xxxxxxxx;	Refresh : Temps d'attente pour le rafraîchissement du DNS secondaire.
xxxxxxxx;	Retry : Temps d'attente du serveur secondaire pour refaire une requête.
xxxxxxxx;	Expire : Temps pendant lequel le DNS secondaire doit garder les zones.
xxxxxxxx;)	TTL (Time To Live) : temps de vie par défaut de tous les enregistrements.

Enregistrements :

1 Hôte	2 classe	3 type	(4 priorité)	5 valeur
poste23	IN	A		192.168.0.23
www	IN	CNAME		srv3.greta.fr.

1 Soit une machine (nom) soit toutes les machines de la zone (@)

2 IN

3 voir chapitre suivant

4 La priorité la plus basse l'emporte sur une requête de même type (exemple MX)

5 Donnée à enregistrer

Types d'enregistrements possibles :

A :
Hôte local. Utilisé pour lier un nom de domaine DNS avec une adresse IP.

PTR :
Pointeur (PTR). Utilisé pour lier une adresse IP avec un nom de domaine.

NS :
Serveur de nom. Utilisé pour lier un nom de domaine DNS avec le nom d'un ordinateur qui fait serveur DNS.

CNAME :
Nom canonique. Utilisé pour lier un nom de domaine DNS canonique avec un autre nom principal ou canonique.

MX :
Serveur de messagerie (MX). Utilisé pour lier un nom de domaine DNS avec le nom d'un ordinateur qui échange ou transmet du courrier.

IV- Test de votre serveur DNS :

Vérification de la configuration :

On peut utiliser les commandes suivantes pour vérifier d'une part la config et d'autre part les zones de recherches directes et inversées :

named-checkconf /etc/bind/named.conf

named-checkzone mynetcourse.info /etc/bind/mynetcourse.info.zone

named-checkzone mynetcourse.info /etc/bind/0.168.192.rev

Tant que vous n'avez pas OK comme réponse après ces commandes, vous devez corriger les erreurs qui se trouvent dans vos fichiers de configuration ou de zones.

Le fichier /etc/resolv.conf :

Vous devez changer le contenu du fichier /etc/resolv.conf en lui indiquant le domaine auquel vous appartenez et l'adresse IP du serveur DNS à tester (127.0.0.1 pour tester votre machine).

```
search          mynetcourse.info
nameserver      127.0.0.1
```

La commande host :

Cette commande permet de tester le serveur DNS. Pour voir les détails de la commande **host**, voyez la page de manuel (**man host**).

Test de la recherche directe :

host poste4 ... devrait vous donner 192.168.0.104

Test de la recherche inversée :

host 192.168.0.103 ... devrait vous donner poste3.mynetcourse.info

Test des noms canoniques (CNAME) :

host pop ... devrait vous donner 192.168.0.254

Test des forwarders (DNS publics qui prennent le relai) :

host www.google.fr ... devrait vous donner une adresse IP publique

La commande nslookup :

La commande nslookup permet aussi de tester le DNS. Tapez nslookup :

>help	si vous ne savez pas l'utiliser.
>set type=NS	pour pouvoir lister les entrées de type NS (sinon remplacez par autre chose, ANY pour tous)
>mynetcourse.info	pour tester sur le domaine mynetcourse.info

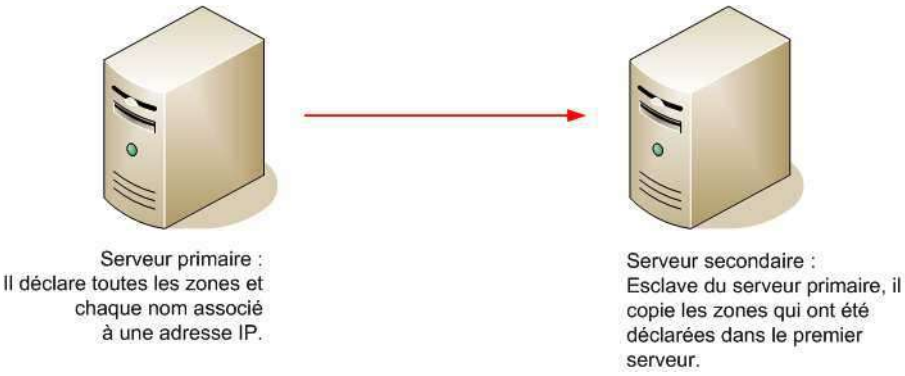
voir **man nslookup** pour plus de détails.

V- DNS Secondaire, réplication de zones :

Le principe :

Le DNS secondaire sert à répondre aux requêtes à la place du DNS primaire pour ne pas surcharger le premier ou pour le remplacer temporairement s'il tombe en panne.

La configuration est la même sauf que les zones ne sont pas créés mais copiées.



En pratique avec Bind :

Dans named.conf, au lieu de déclarer les zones comme en haut de la page 3, on déclare une zone esclave de la façon suivante :

```
zone  "mynetcourse.info" {
      type slave;
      file "/etc/bind/mynetcourse.info.zone.slave";
      masters {
            192.168.0.90;
      }
}

zone  "0.168.192.in-addr.arpa" {
      type slave;
      file "/etc/bind/0.168.192.rev.slave";
      masters {
            192.168.0.90;
      }
}
```

Dans cet exemple, Bind va recopier les fichiers de zone du serveur DNS qui se trouve à l'adresse 192.168.0.90

VI- Sur Internet ...

Sites avec plus ou moins d'infos sur l'installation et la configuration du DNS :

http://www.linux-kheops.com/doc/cours/jgourdin/outils-tcp-ip/Linux-dns.html

http://www.egs-howto.com/fr/systemes/linux_dns.php

http://lea-linux.org/reseau/dns1.html