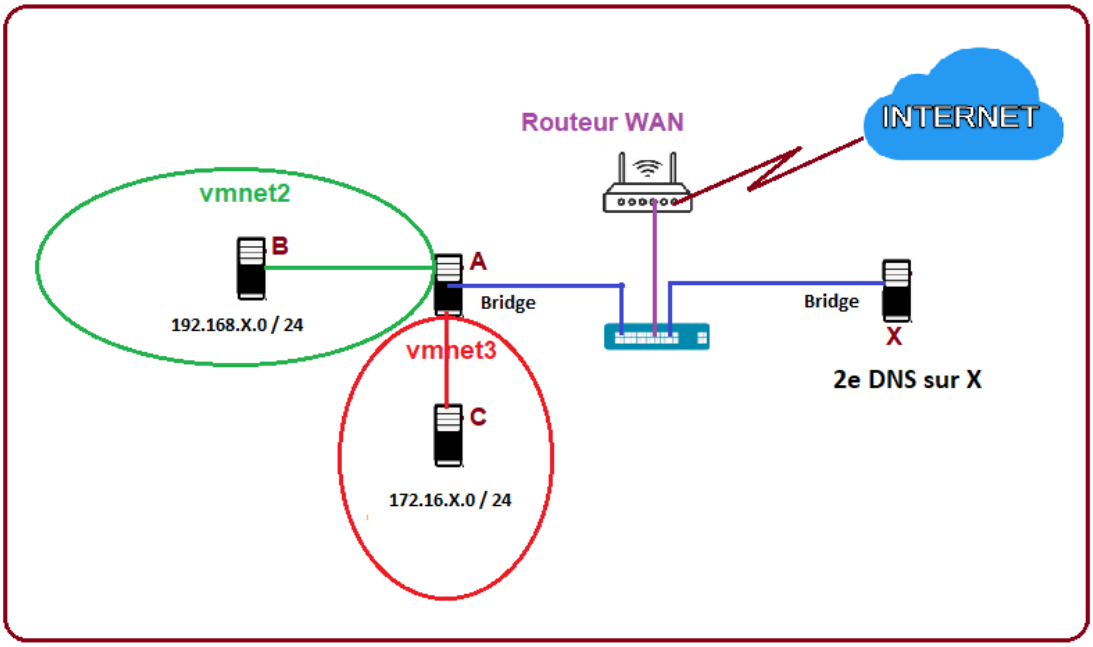

# Lab
# Serveur DNS (Bind)
# DNS secondaire (esclave)
# et DNS transmetteur (forwarder)


*M. Setra*

# 1. Configuration d'un serveur DNS secondaire (serveur DNS esclave)




**Configurez le DNS secondaire sur la machine Linux B (sur vmnet2)**
**Entre les DNS A et B**

---

**Configuration dans le fichier /etc/named.conf**

Supposons que vous avez un DNS primaire (sur machine A) dont la zone est : **teccart.tld** et que son adresse IP est 192.168.1.1

Sur la machine C (sur vmnet3), vous allez configurer un DNS secondaire (esclave) rattaché au DNS primaire sur A.
Il faut ajouter la section suivante dans le fichier /etc/named.conf : qui configure le DNS sur C comme serveur DNS secondaire (esclave)

```
zone "teccart.tld."  IN {
      type slave;
      file "slaves/teccart.tld.db";
      masters { 172.16.100.1; };
};
```

L'adresse 192.168.1.1 étant l'adresse IP du DNS master (machine A).

Il suffit de redémarrer le service DNS sur le secondaire (C), et vérifier que le transfert de zone s'est effectué :

- Avec **wireshark** sur la machine A ou C, vous pouvez vérifier le transfert de zone qui se fait entre les deux DNS.

- Ou dans le fichier journal /var/log/messages : `tail -20 /var/log/messages`

- aussi vérifier le dossier **/var/named/slaves**).

1. Après avoir démarré le service DNS secondaire sur C faire les vérifications suivantes:
    a. Fichier journal
    b. Résolution de nom de domaine (teccart.tld.) sur le DNS C secondaire.
    c. Fichier de zone transféré sur le dossier : **/var/named/slaves/** du DNS secondaire.

a. Fichier journal: **`tail /var/log/messages`**

Vous remarquerez des informations concernant le transfert de zone. En cas de problème, vous allez trouver des messages d'erreurs qui vont aider à identifier le problème.

b. Faire un test de résolution de nom de la zone **teccart.tld** avec la commande **dig** sur C :

```
dig  www.teccart.tld
```

c. Vérifiez dans le dossier: **/var/named/slaves** le fichier de zone **teccart.tld.db**.

---

## 2. Limiter le transfert de zone vers certains DNS (avec adresses IP)

La configuration précédente permet le transfert de zone vers n'importe quel DNS. Il n'y aucune restriction sur les DNS secondaires. L'administrateur doit limiter le transfert de zone uniquement vers certains DNS secondaire.

Ceci peut être réalisé sur le DNS primaire avec la configuration suivante :

Sur la machine A (DNS primaire), Il faut ajouter dans la section de déclaration de la zone l'option : allow-transfer :

```
zone "teccart.tld."  IN {
      type master;
      file "teccart.tld.db";
      allow-transfer { 172.16.100.2; };
};
```

Avec l'adresse IP 172.16.100.2 étant l'adresse du DNS secondaire (Machine C).

# Serveur DNS (Bind) transmetteur : transmission de requêtes vers d'autres DNS

**Pour l'exercice qui suit, nous allons créer une autre zone DNS (suffice de domaine), chaque élève va utiliser comme suffixe : son nom de famille ou prénom, par exemple moi je vais utiliser : setra.tld comme suffixe. Il faut créer cette 2e zone sur le DNS A par exemple ou sur C. Si vous voulez ajouter une autre machine D sur vmnet3 pour cet exercice.**

## 1. Transmission spécifique à une zone (forward spécifique) (entre deux DNS : A et X)

a. Configurer sur X (C ou D), un DNS primaire (maitre) avec comme suffixe votre nom ou votre prénom.
Ajouter des enregistrements dans le fichier de zone. Faire les tests.

b. Par exemple, j'utilise le suffixe **setra.tld** pour le DNS sur la machine X :
- Nom de son suffixe de domaine : setra.tld
- L'adresse IP du DNS de X : par exemple **IP(X)**

Dans /etc/named.conf du DNS de A:
- Ajoutez la section suivante pour configurer le forward spécifique

```
zone "setra.tld." IN {
        type forward;
        forwarders { IP(X); }
};
```

- Redémarrez le DNS A : **systemctl restart named**
- Démarrez wireshark
- Faire une résolution d'un enregistrement de la zone setra.tld : www.setra.tld
- Vérifiez le résultat et consulter la capture avec wireshark

---

## 2. Transmission globale vers le DNS du collège ou autre DNS (8.8.8.8 ou 1.1.1.1) (forward global)

Configuration dans le fichier : /etc/named.conf dans le section options en haut du fichier :

```
forward only;
forwarders { 8.8.8.8; 1.1.1.1; };
```

- Redémarrez le DNS : **systemctl restart named**
- Démarrez wireshark
- Faire une résolution d'un enregistrement : www.google.ca
- Vérifiez les échanges entre les deux DNS avec wireshark.

**Question : Est-possible que le DNS C ou D transfert leurs requêtes vers le DNS A pour résoudre les noms de domaine Internet ?**