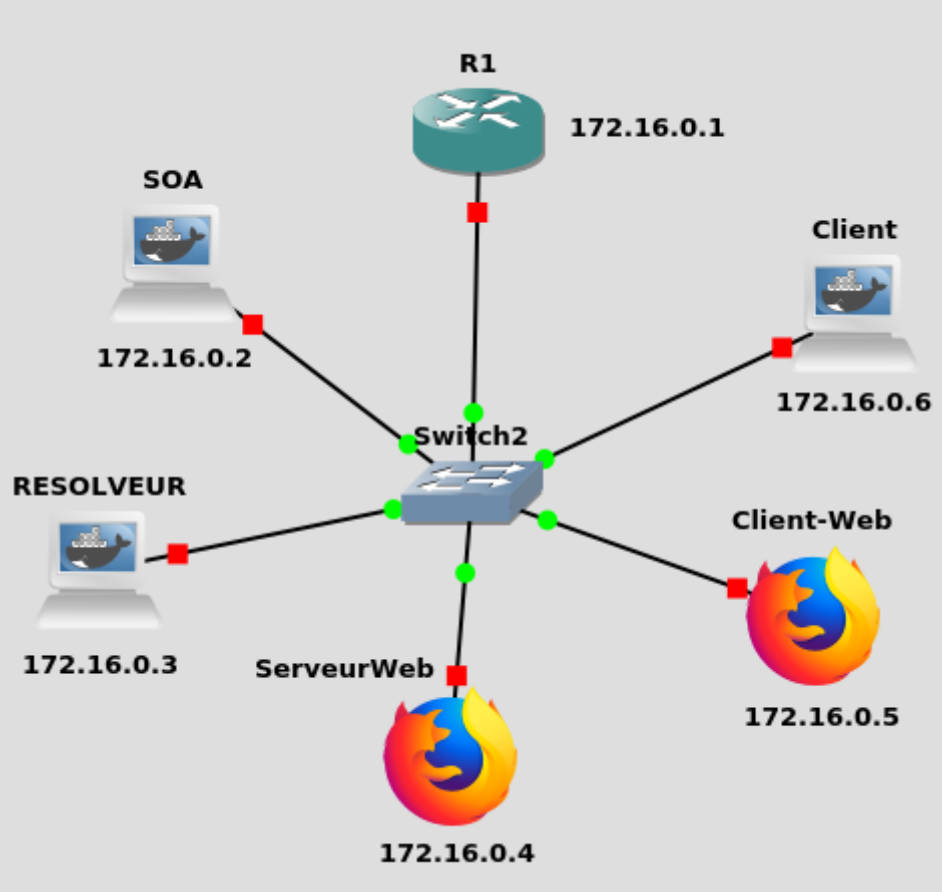
Configuration du réseau (Mission 1 - Démo) :

Groupe n°5

- **Morgan Valentin**
- **Martin Michotte**
- **Olivier Niyonkuru**

Schéma proposé :



Reseau => 172.16.0.0 (/29)

domaine => wt2-5.ephec-ti.be

1. Configuration du Résolveur

Configuration de base :

- ip => 172.16.0.3 masque => 255.255.255.248 (/29)
- gateway => 172.16.0.1
- nameserver=172.16.0.3 (lui-même)
- ⚠ **Attention ! Mettre le nameserver dans le client !**
    - `(fichier /etc/resolv.conf)`

Configuration avancée :

```
bind# cd /etc/bind
bind# cp named.conf.recursive named.conf #Copier le fichier
bind# vi named.conf                      #Modifier le fichier
```

Dans **`named.conf`**, **dans** la section **`"options"`** **modifier** les lignes suivantes :

```
allow-recursion {
        172.16.0.0/29;
};

listen-on port 53 { any; };
listen-on-v6 { none; };
```

Dans **`named.conf`**, **APRES** la section **`"options"`** **ajouter** les lignes suivantes :

```
# Notre zone
zone "wt2-5.ephec-ti.be" {
    type forward;
    forwarders {172.16.0.2;};
    forward only;
};

# Zone reverse
zone "0.16.172.in-addr.arpa" {
    type forward;
    forwarders {172.16.0.2;};
    forward only;
};
```

Puis après tous cela, on lance bind :

```
bind# named -g
```

Test du fonctionnement de notre résolveur :

Le client => dig A `www.google.com`
Le résolveur => Cherche l'adresse IP de `www.google.com` (RR de type A)

> Si le résolveur essaye de répondre (même si il n'y arrive pas) à la requête du client, celui-ci fonctionne bien.

2. Configuration du SOA (Interne)

Configuration de base :

- ip => 172.16.0.2 masque => 255.255.255.248 (/29)
- gateway => 172.16.0.1

Configuration avancée :

```
bind# cd /etc/bind
bind# cp named.conf.authoritative named.conf #Copier le fichier
bind# vi named.conf                          #Modifier le fichier
```

Dans **named.conf**, **dans** la section **"options"** **modifier** les lignes suivantes :

```
listen-on { 172.16.0.2; };
listen-on-v6 { none; };

allow-query {
        127.0.0.1;
        172.16.0.0/29;
};

allow-recursion { none; };
recursion no;
```

Dans **named.conf**, **APRES** la section **"options"** **ajouter** les lignes suivantes :

```
# Notre zone
zone "wt2-5.ephec-ti.be" {
    type master;
    file "/etc/bind/wt2-5.ephec-ti.be"
};

# Zone reverse
zone "0.16.172.in-addr.arpa" IN {
    type master;
    file "/etc/bind/0.16.172.in-addr.arpa";
};
```

Configuration des fichiers de zone :

Toujours dans le dossier bind (/etc/bind/), ajouter/ créer 2 fichiers :

- Le fichier de **zone** => `wt2-5.ephec-ti.be`
- Le fichier de **zone reverse** => `0.16.172.in-addr.arpa`

Zone "`wt2-5.ephec-ti.be`" :

soa > wt2-5.ephec-ti.be.zone

```
$ORIGIN wt2-5.ephec-ti.be.
$TTL 604800
@       IN      SOA     ns.wt2-5.ephec-ti.be. admin.wt2-5.ephec-ti.be. (
                        1           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
; name servers => Resource records de type NS
            IN      NS      ns.wt2-5.ephec-ti.be.

; name servers => Ressource recors de type A
ns          IN      A   172.16.0.2

; services web
intranet    IN      A       172.16.0.4
b2b         IN      A       172.16.0.4
www         IN      A       172.16.0.4
mysql       IN      A       172.16.0.5
```

Zone "`0.16.172.in-addr.arpa`" :

soa > 0.16.172.in-addr.arpa.zone

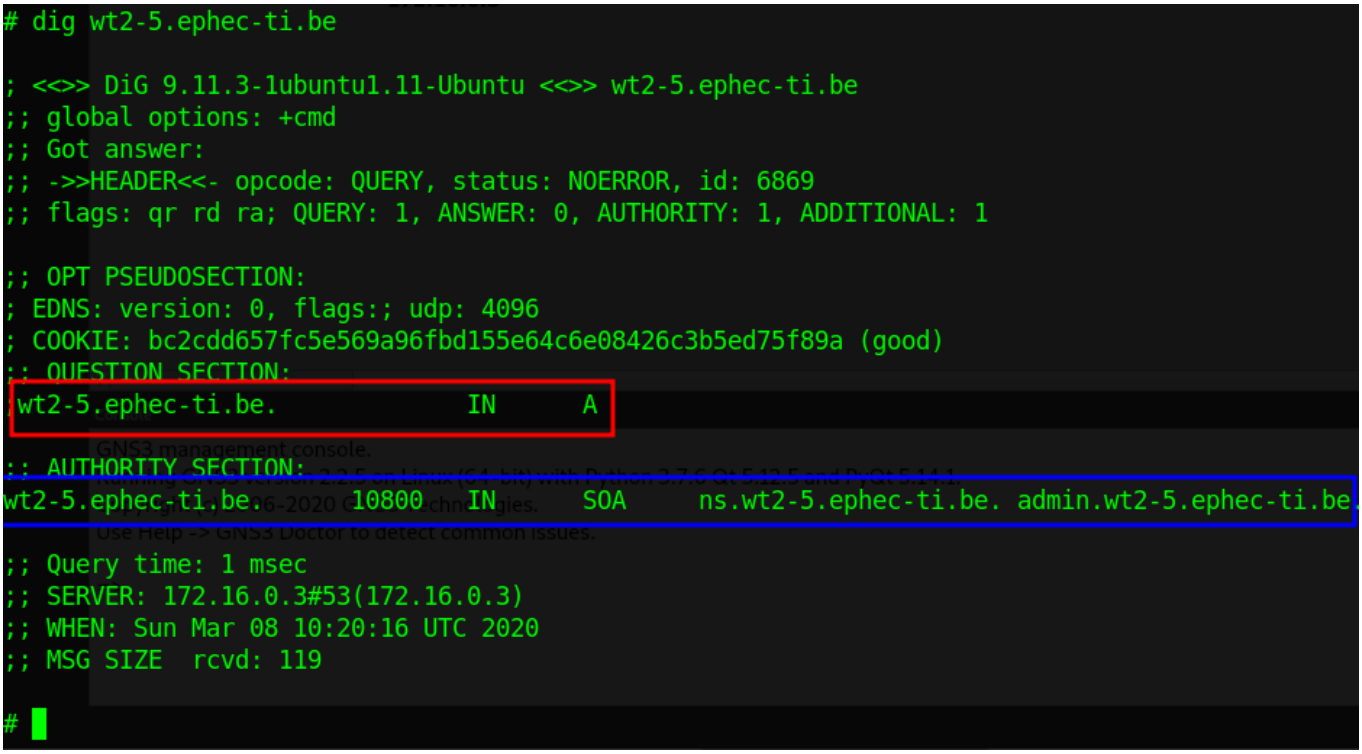
```
$ORIGIN 0.16.172.in-addr.arpa.
$TTL 604800
@       IN      SOA     ns.wt2-5.ephec-ti.be. admin.wt2-5.ephec-ti.be. (
                        1           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
; name servers => Resource records de type NS
@           IN      NS      ns.wt2-5.ephec-ti.be.

; services => Resource records de type PTR
2           IN      PTR     ns.wt2-5.ephec-ti.be.
4           IN      PTR     intranet.wt2-5.ephec-ti.be.
4           IN      PTR     www.wt2-5.ephec-ti.be.
4           IN      PTR     b2b.wt2-5.ephec-ti.be.
5           IN      PTR     mysql.wt2-5.ephec-ti.be.
```

Test du fonctionnement de notre SOA :

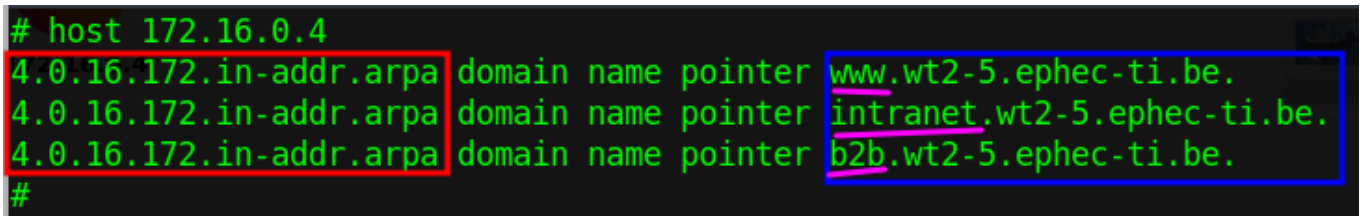
1. **Demande d'information sur le domaine**

```
Client# dig wt2-5.ephec-ti.be.
```



2. **Demande d'information sur l'ip "`172.16.0.4`" (*reverse query / iquery*)**

```
Client# host 172.16.0.4
```



3. Configuration du serveur Apache

a) On commence par créer notre site (intranet) :

```
apache# mkdir /var/www/intranet
apache# touch /var/www/intranet/index.html
apache# vi /var/www/intranet/index.html
```

b) On ajoute ensuite le code html de notre page :

```
<html>
<h1>Bienvenue dans l'intranet !</h1>
</html>
```

c) Création du fichier de config :

```
apache# cd /etc/apache2/sites-available
apache# touch intranet.conf
```

d) Configuration du fichier de config :

Dans le fichier "`intranet.conf`" (créer au point précédent), ajouter ceci :

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName intranet.wt2-5.ephec-ti.be
    DocumentRoot /var/www/intranet/

    <Directory />
        Options FollowSymLinks
        AllowOverride all
    </Directory>

    <Directory /var/www/intranet/>
        Options FollowSymLinks MultiViews
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

e) Activer notre configuration :

```
apache# cd /etc/apache2/sites-available
apache# a2ensite intranet.conf
apache# service apache2 reload
```

Test du fonctionnement de notre serveur apache :

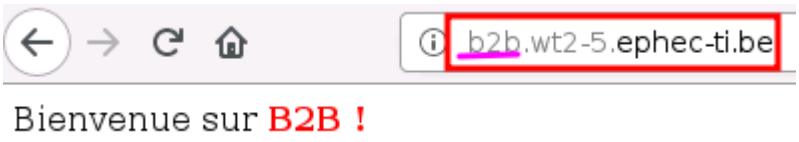
Bienvenue sur l'intranet !

----------PHP----------

Version courante de PHP : 7.3.14-1~deb10u1

----------PHP----------

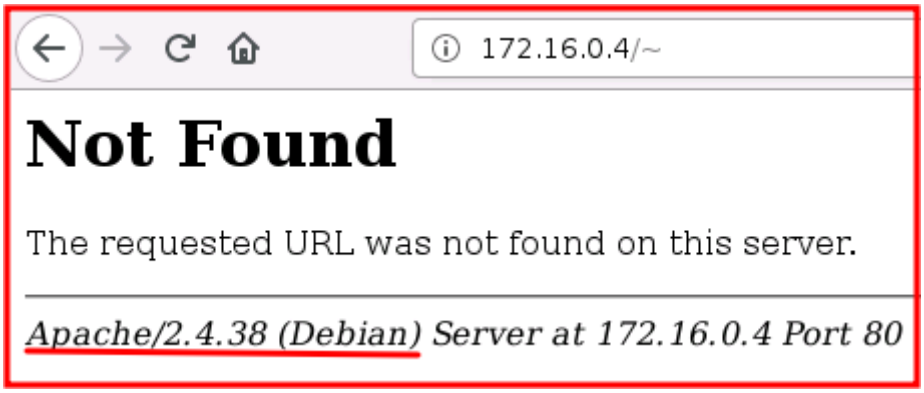
On fait la même chose pour les 2 autres sites (b2b et www), ce qui donne après test ceci :



Securité :

Lorsque l'on "tombe" sur une page qui n'existe pas, on a un message d'erreur avec des informations sur notre version d'apache, notre système d'exploitation, et d'autres encore...
En connaissant notre verson d'apache et notre OS, un hacker peut facilement trouver un "exploit" pour "attacker" notre serveur.\

Screenshot de la situation :



Solution ?

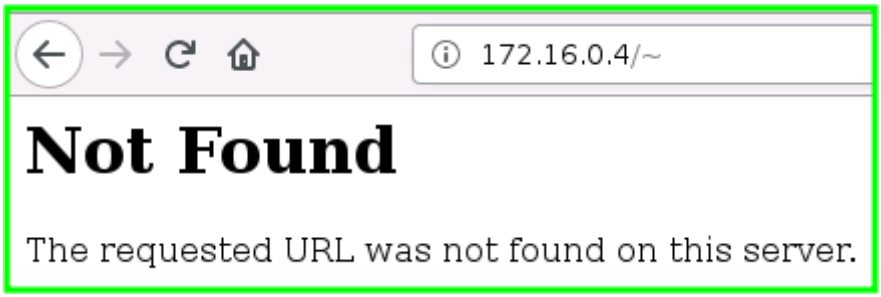
Modifier le fichier "`apache2.conf`" (/etc/apache2/apache2.conf) et ajouter ces lignes-ci (tout en bas du fichier) :

```
# Security
ServerSignature Off
ServerTokens Prod
```

On doit ensuite redémarer apache :

```
apache# service apache2 restart
```

Voilà le problème régler !



BONUS :

Si une machine tente de contacter notre serveur web sur son ip, il va refuser (erreur 403) afin de laisser uniquement les "bons" nom de domaine / les noms de domaines authorisé.