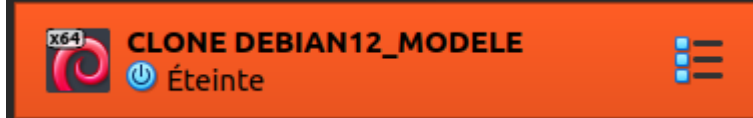


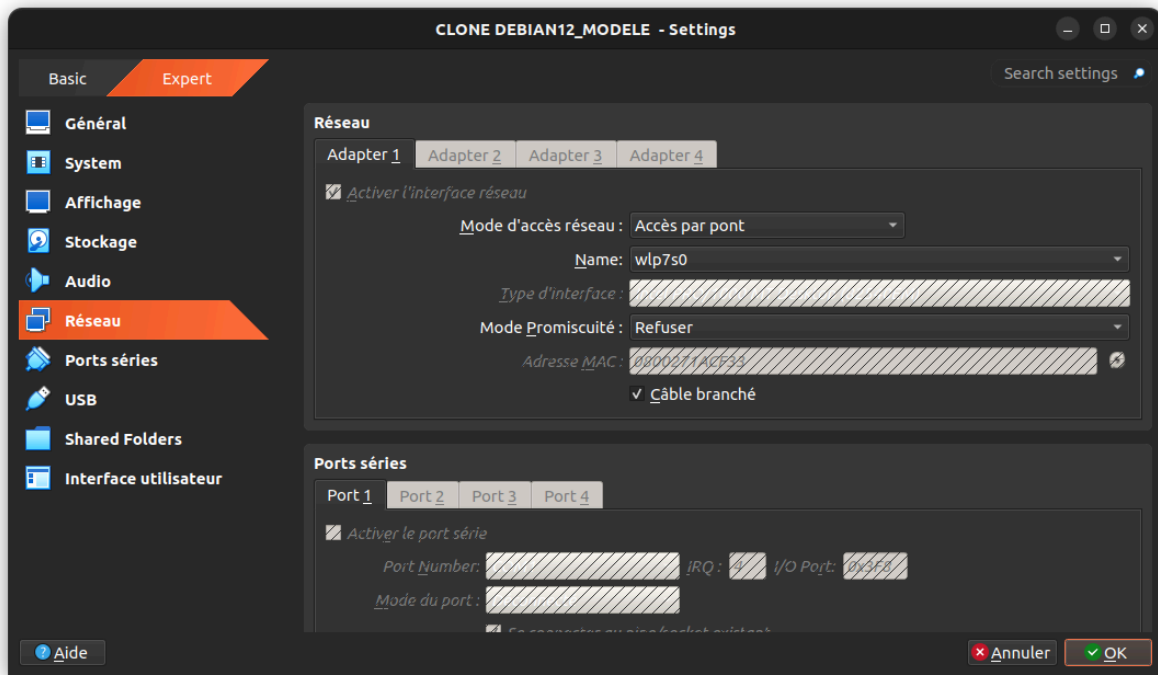
Labo DNS

1°) Installation de bind9

Je commence déjà par choisir une machine debian sans interface graphique afin de commencer la mise en place de mon DNS. Dans mon cas j'ai choisis de prendre la DEBIAN 12



Avant de commencer l'installation de bind 9, on vérifie les paramètres réseaux, la machine doit être bridgé et être en DHCP:



Ici on voit bien que la machine est en accès par pont, qu'elle est en DHCP, on va maintenant procéder au mise à jour et à l'installation de bind 9.

```
root@debian12:~# apt install bind9_
```

```
root@debian12:~# apt install bind9
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
bind9 est déjà la version la plus récente (1:9.18.41-1~deb12u1).
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-6.1.0-18-amd64
Veuillez utiliser « apt autoremove » pour le supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 80 non mis à jour.
```

Cela confirme que Bind9 est installé.

on vas maintenant vérifiez que bind9 est à l'écoute avec la commande “ps -ef | grep named” :

```
root@debian12:~# ps -ef | grep named
bind      1234      1  0 18:30 ?        00:00:00 /usr/sbin/named -f -u bind
root      1252      637  0 18:32 tty1    00:00:00 grep named
```

On voit bien ici que bind9 est à l'écoute.

Quel est l'utilisateur/groupe propriétaire du processus lancé ?

Le processus *named* a été lancé par l'utilisateur bind, appartenant également au groupe bind.

```
root@debian12:~# ps -ef | grep named
bind      1234      1  0 18:30 ?        00:00:00 /usr/sbin/named -f -u bind
root      1252      637  0 18:32 tty1    00:00:00 grep named
```

2°) Exploitation d'un serveur cache

Étape 1 : Adressage IP

```
root@debian12:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1a:cf:33 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.183/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 42714sec preferred_lft 42714sec
    inet6 fe80::a00:27ff:fe1a:cf33/64 scope link
        valid_lft forever preferred_lft forever
```

La machine est bien configuré en DHCP elle obtient une adresse par ce serveur. Or étant donné que je ne suis pas au lycée je n'obtiens pas une ip en “172.17.123|124.X”

Étape 2 : Résolveur

On va maintenant configurer le résolveur de façon à indiquer que notre machine fait office de serveur DNS.

Pour cela on se rend dans le fichier **/etc/resolv.conf** puis on rajoute la ligne suivante :

```
nameserver 127.0.0.1
```

```
GNU nano 7.2 /etc/resolv.conf
#nameserver 192.168.1.254
nameserver 127.0.0.1

Lecture de 2 lignes
Aide Écrire Chercher Couper Exécuter Emplacement M-U Annuler M-A Marquer M-] -> Crochet M-O Précédent
Quitter Line fich. Remplacer Coler Justifier Aller ligne M-E Refaire M-B Copier M-] -> Retrouver M-K Suivant
```

J'ai configuré le fichier *resolv.conf* afin que la machine utilise son propre service DNS, via l'adresse 127.0.0.1.

```
root@debian12:~# nslookup www.cisco.com
Server:      192.168.1.254
Address:     192.168.1.254#53

Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = www.cisco.com.akadns.net.
www.cisco.com.edgekey.net canonical name = www.cisco.com.edgekey.net.
www.cisco.com.edgekey.net canonical name = www.cisco.com.edgekey.net.
www.cisco.com.edgekey.net.globalredir.akadns.net canonical name = www.cisco.com.edgekey.net.globalredir.akadns.net.
Name:      e2867.dsca.akamaiedge.net
Address:   29.46.188.98
Name:      e2867.dsca.akamaiedge.net
Address:   2a02:26f0:2b00:9a31:b93
Name:      e2867.dsca.akamaiedge.net
Address:   2a02:26f0:2b00:98c:b93

root@debian12:~# nslookup localhost
Server:      192.168.1.254
Address:     192.168.1.254#53

** server can't find localhost: NXDOMAIN

root@debian12:~# nslookup 127.0.0.1
** server can't find 1.0.0.127.in-addr.arpa: NXDOMAIN
```

Quel est le rôle de la commande nslookup ? Expliquez les informations qui s'affichent après saisie des commandes et ce que signifie non_authoritative answer

La commande *nslookup* permet d'interroger un serveur DNS pour obtenir la résolution d'un nom ou d'une adresse IP. L'information affichée indique le serveur DNS utilisé et la réponse fournie. La mention *non-authoritative answer* signifie que la réponse provient du cache d'un DNS intermédiaire et non du serveur faisant autorité pour la zone.



STOP 1 : Appelez moi pour que je puisse vérifier cette partie du travail.

3°) Configuration d'un serveur DNS pour le domaine GSB

Étape 1 : Adressage IP et nom de la machine

Votre serveur DNS doit avoir l'adresse IP suivante : 172.16.50.11/24, passerelle = 172.16.50.254, carte en réseau interne nommé subnet_dns. Dans le fichier /etc/resolv.conf, il doit toujours y avoir nameserver 127.0.0.1.

Je commence tout d'abord par changer par changer les configuration réseaux de la carte et je passe de DHCP à STATC en même temps je déclare la nouvelle adresse ip et passerelle conformément au recommandation :

```
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

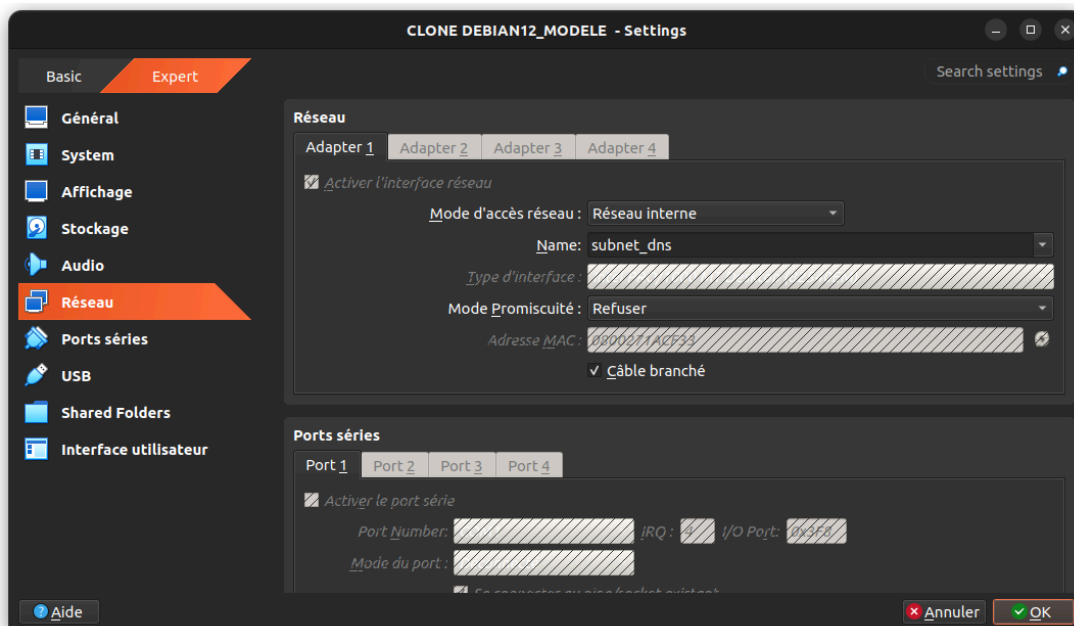
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 172.16.50.11/24
gateway 172.16.50.254
```

Après avoir pensé à redémarrer la carte réseaux on affiche les interface réseaux à l'aide de la commande "IP A"

```
root@debian12:~# ifdown enp0s3
ifdown: interface enp0s3 not configured
root@debian12:~# ifup enp0s3
root@debian12:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1a:cf:33 brd ff:ff:ff:ff:ff:ff
    inet 172.16.50.11/24 brd 172.16.50.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe1a:cf33/64 scope link
        valid_lft forever preferred_lft forever
```

On met maintenant la machine en réseau interne nommer "subnet_dns" :



On modifie alors `etc/hosts` pour qu'il contienne les lignes suivantes

```
root@debian12:~# cat /etc/hosts
127.0.0.1    localhost.localdomain localhost
172.16.50.11 master.gsb.com master
```

On modifie le fichier `hostname` afin qu'il contienne cela :

```
root@debian12:~# cat /etc/hostname
master.gsb.com
```

Le rôle des fichiers `/etc/hosts` et `/etc/hostname`:

Le fichier `/etc/hosts` me permet de définir localement la correspondance entre une IP et un nom de machine, comme 172.16.50.11 pour master.gsb.com.

Le fichier `/etc/hostname` sert à indiquer le nom d'hôte de ma machine ; conformément aux recommandations j'y ai mis `master.gsb.com`.

Étape 2 : Configuration de la zone de recherche directe gsb.com

Je commence par copier le fichier à l'aide de la commande suivante :

```
root@master:~# cp /etc/bind/db.local db.gsb.com
```

Une fois le fichier copié je le modifie afin de renseigner le nom de domaine ainsi que les adresses IP correspondantes à votre contexte :

```
;  
; BIND data file for local loopback interface  
;  
$TTL      604800  
@         IN      SOA    localhost. root.localhost. (  
                2      ; Serial  
                604800 ; Refresh  
                86400  ; Retry  
                2419200 ; Expire  
                604800 ) ; Negative Cache TTL  
;  
@         IN      NS     master.gsb.com.  
@         IN      A      slave.gsb.com.  
  
master   IN      A      172.16.50.11  
dhcp     IN      A      172.16.50.10  
relais   IN      A      10.20.30.10  
slave    IN      A      172.16.50.13
```

Dans le fichier "`named.conf.local`", je déclare la zone directe "gsb.com" :

```
root@master:~# cat /etc/bind/named.conf.local
zone "gsb.com" {
    type master;
    file "/etc/bind/db.gsb.com";
};
```

puis je redémarre le service :

```
root@master:~# service bind9 restart
```

je teste avec la commande nslookup : **nslookup master, nslookup dhcp et nslookup master.gsb.com**

```
root@master:/etc/bind# nslookup master
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   master.gsb.com
Address: 172.16.50.11

root@master:/etc/bind# nslookup dhcp
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   dhcp.gsb.com
Address: 172.16.50.10

root@master:/etc/bind# nslookup master.gsb.com
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:   master.gsb.com
Address: 172.16.50.11
```

On peut voir que ça passe par notre serveur dns qui est l'adresse IP de notre machine qui est la **172.16.50.11**.

Quel est le rôle de la directive search dans /etc/resolv.conf ? Que se passe t-il si on l'enlève et qu'on teste la commande nslookup master et la commande nslookup master.gsb.com ?

La directive search gsb.com permet d'ajouter automatiquement le domaine gsb.com lorsque je fais une requête DNS avec un nom court. Ainsi, taper nslookup master revient à interroger master.gsb.com.

Si on l'enlève, la commande nslookup master ne fonctionne plus alors que nslookup master.gsb.com continue de répondre correctement.

cherchez sur internet le rôles des enregistrements suivants : SOA, NS, A, CNAME.

<u>Enregistrement :</u>	<u>signification</u>
<u>SOA</u>	Définit le serveur maître de la zone, les paramètres de mise à jour (serial, refresh, retry, expire) et l'administrateur responsable.
<u>NS</u>	Indique quels serveurs DNS sont autoritaires pour le domaine et doivent être consultés pour la zone.
<u>A</u>	Associe un nom de domaine à une adresse IPv4, permettant la résolution nom → IP.
<u>CNAME</u>	Crée un alias : un nom de domaine pointe vers un autre nom de domaine au lieu d'une adresse IP.

Pour effectuer cela je dois ajouter la ligne suivante au fichier :

```
intranet IN CNAME master.gsb.com.
```

Ce qui nous donneras cela, je n'oublie pas d'incrémenter le numéro de série afin que les modifications soient présent en compte et je redémarre le service :

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA     master.gsb.com. root.gsb.com. (
                        3          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS      master.gsb.com.

master   IN      A        172.16.50.11
dhcp     IN      A        172.16.50.10
relais   IN      A        10.20.30.10
slave    IN      A        172.16.50.13
intranet IN      CNAME    master.gsb.com.
```

```
root@master:/etc/bind# systemctl restart bind9
```

Je teste maintenant avec le “nslookup intranet.gsb.com”

```

root@master:/etc/bind# nslookup intranet.gsb.com
Server:         127.0.0.1
Address:        127.0.0.1#53

intranet.gsb.com    canonical name = master.gsb.com.
Name:   master.gsb.com
Address: 172.16.50.11

```



STOP 2 : Appelez moi pour que je puisse vérifier cette partie du travail.

Étape 3 : Configuration des résolutions inverses

On va maintenant procéder à la création de zone inverses du nom vers l'ip :

- une pour le sous réseau 10.20.30.0/24,
- l'autre pour le sous réseau 172.16.50.0/24.

Pour cela je dois créer un fichier de zone inverse, je copie le fichier nommer “db.127”, et je le modifie pour qu’il ressemble à cela :

```

root@master:/etc/bind# cp db.127 db.172.16.50
GNU nano 7.2 db.172.16.50
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      master.gsb.com. root.gsb.com. (
; Serial
                1          ; Refresh
                604800     ; Retry
                86400      ; Expire
                2419200    ; Negative Cache TTL
                604800 )
;
@         IN      NS       master.
@         IN      NS       slave.
11        IN      PTR      master.gsb.com.
10        IN      PTR      dhcp.gsb.com.
13        IN      PTR      slave.gsb.com.

```

Puis je déclare la zone inverse dans le fichier “named.conf.local”

```

GNU nano 7.2 named.conf.local
zone "gsb.com" {
    type master;
    file "/etc/bind/db.gsb.com";
};
zone "50.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.16.50";
};

```

je redémarre le service dns et test avec la commande “nslookup 172.16.50.11” :

```
root@master:/etc/bind# systemctl restart bind9
root@master:/etc/bind# nslookup 172.16.50.11
11.50.16.172.in-addr.arpa      name = master.gsb.com.
```

Expliquez le rôle de l'enregistrement PTR ?

Un enregistrement **PTR** sert à réaliser une *résolution inverse*, c'est-à-dire retrouver le **nom de domaine associé à une adresse IP**.

Recommencez l'étape 3 en créant une nouvelle zone de recherche inversée pour le sous réseau 10.20.30.0/24.

Je commence tout d'abord par copier un fichier de configuration déjà existant pour gagner du temps je copie le fichier que je viens de créer à savoir le **db.172.16.50** :

```
root@master:/etc/bind# cp db.172.16.50 db.10.20.30
```

Je le modifie afin de suivre les recommandations données :

```
GNU nano 7.2 db.10.20.30
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      master.gsb.com. root.gsb.com. (
; Serial
; Refresh
; Retry
; Expire
; Negative Cache TTL
)
;
@         IN      NS       master.
@         IN      NS       slave.
1         IN      PTR      relais.gsb.com.
```

Encore une fois je n'oublie pas d'incrémenter le numéro de série afin que les modifications soient prises en compte. De plus je n'oublie pas de déclarer la zone inverse dans le fichier de zone **"named.conf.local"** :

```
GNU nano 7.2 named.conf.local
zone "gsb.com" {
    type master;
    file "/etc/bind/db.gsb.com";
};
zone "50.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.16.50";
};
zone "30.20.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10.20.30";
};
```

Une fois tout cela effectué je relance le service et je teste avec la commande **"nslookup 10.20.30.1."**

```
root@master:/etc/bind# systemctl restart bind9
root@master:/etc/bind# nslookup 10.20.30.1
1.30.20.10.in-addr.arpa name = relais.gsb.com.
```