

## Serveurs de noms

Prénom :

Nom :

Groupe :

## 1 Gestion du réseau virtuel

Le réseau virtuel utilisé lors de ce TP a été réalisé avec **NEmu** (Network Emulator), un émulateur de réseaux virtuels distribués et dynamiques utilisant QEMU (logiciel d'émulation de machines). NEmu a été conçu par des membres du LaBRI, pour plus d'informations consulter le site <http://nemu.valab.net>.

### 1.1 Création des machines, lancement de NEmu

Après s'être positionné dans votre sous-répertoire `~/VMs/VNET`, exécutez le script `./vnet dns`. Le script lance le logiciel "NEmu" qui va simuler le réseau décrit dans le fichier `dns.py`.

Deux commandes de NEmu vous seront utiles : `quit()` et `save()`.

A chaque machine virtuelle est associée une fenêtre graphique où tourne un terminal. Pour travailler dans une machine virtuelle, il faut positionner la souris dans la fenêtre associée à la machine, puis clic sur le bouton droit de la souris.

La souris peut être "bloquée" (par un clic sur le bouton gauche de la souris) dans une fenêtre associée à une machine virtuelle, pour "débloquer" la souris, il faut taper "Ctrl Alt" dans la fenêtre incriminée.

### 1.2 Information sur les machines

Les commandes Linux nécessaire au TP sont réalisables uniquement par l'administrateur des machines (login : root, passwd : plop).

Les machines virtuelles utilisent la distribution Linux, **Debian**.

L'éditeur de texte `jed` est préinstallé.

La commande `startx` permet de remplacer le terminal textuel par un environnement graphique basique). Un clic sur un bouton de la souris permet d'accéder au menu :

1. `exit` pour quitter l'environnement graphique,
2. `application -> reseau -> surveillance -> Wireshark` pour lancer Wireshark, renifleur et analyseur de trames réseau.

### 1.3 Arrêt d'une machine virtuelle

Dans le terminal associé à la machine, exécutez la commande `halt` avant de détruire la fenêtre associée à la machine (c'est à dire de cliquer sur l'icône de destruction de la fenêtre).

### 1.4 Sauvegarde des machines et restauration des machines

**Sauvegarde des machines :** après l'arrêt propre de toutes les machines, exécutez la commande `save()` de NEmu. Le fichier `~/dns.tgz` contiendra la sauvegarde des machines virtuelles. Pour finir, quittez NEmu en tapant la commande `quit()` de NEmu.

**Restauration des machines :** après s'être positionné dans votre sous-répertoire `~/VMs/VNET`, exécutez le script `./restore ~/dns.tgz`, avant de créer le réseau via le script `./vnet dns`.

## 2 Objectif du TP : DNS

Vous utiliserez un réseau de trois machines virtuelles Unix (distribution Debian). L'une des machines (`serveur1`) jouera le rôle de serveur primaire pour la zone `localdomain`, une autre machine (`serveur2`) sera un serveur secondaire de cette zone, et la troisième machine (`client`) sera un simple client DNS.

Dans un second temps, vous configurerez `serveur2` comme serveur primaire pour la sous-zone `appareils.localdomain`.

## 3 Configuration réseau

Vous donnerez une adresse IP prédéfinie (voir le tableau ci-contre) aux interfaces `eth0` des 3 machines.

Il faut ajouter au fichier `/etc/network/interfaces` la configuration de l'interface pour configurer une interface réseau de manière pérenne.

Dans l'exemple présenté, la configuration pérenne correspond à la commande `ifconfig 10.1.5.125 netmask 255.255.255.0 broadcast 10.1.5.255`.

```
auto eth0
iface eth0 inet static
    address 10.1.5.125
    netmask 255.255.255.0
```

machine	adresse IP
client	10.1.5.100
serveur1	10.1.5.1
serveur2	10.1.5.2

**Important :** Conservez la déclaration de l'interface `lo` qui est indispensable. Elle porte l'adresse de *loopback* `127.0.0.1` qui sert à la communication entre programmes.

La commande `ifup eth0` démarre l'interface réseau `eth0` (`ifdown eth0` pour arrêter l'interface `eth0`).

Ecrivez le nom de la machine (par exemple `client`) dans le fichier `/etc/hostname`. Le nom sera pris en compte au prochain démarrage.

Associez le nom de la machine à l'adresse `127.0.0.1` dans `/etc/hosts` (sans enlever la ligne `localhost`).

### 3.1 Vérification

- Rebootez les 3 machines proprement (commande `reboot`).
- Vérifiez que les interfaces réseau sont bien actives via la commande : `ifconfig` et qu'elles communiquent bien entre elles, avec la commande : `ping adresse-ip -c1`.

## 4 Résolution locale par `/etc/hosts`

Les applications qui tournent sur les machines ont souvent besoin de *résoudre des noms*, c'est-à-dire déterminer le numéro IP qui correspond à une adresse comme `www.iut.u-bordeaux1.fr`. Elles appellent pour cela le *resolver* qui fait partie de la bibliothèque C.

1. Ce module obtient ses informations de plusieurs sources (fichiers locaux, appel à des serveurs, base de données etc.), selon le paramétrage indiqué dans `/etc/nsswitch.conf` à la ligne "de clef `hosts`".
2. Le fichier local qui concerne la résolution est `/etc/hosts`. Modifiez celui de `client` pour qu'il "connaisse" `serveur1`. Testez votre modification avec la commande : `ping serveur1 -c1`. Espionnez avec "Wireshark" sur `serveur1` les trames arrivant ou partant. Listez les paquets IP envoyés et reçus dans le tableau suivant

adresse IP émetteur	adresse IP destinataire	protocole sur IP	port émetteur	port destinataire

Une requête DNS est-elle envoyée ?

3. Quel est le résultat de la commande `ping serveur2 -c1` ? Expliquez.

## 5 Configuration de serveur1 en serveur DNS

1. Sur `serveur1`, lancez le serveur DNS via la commande : `/etc/init.d/bind9 start`.

Pour tous serveurs DNS, il faut vérifier que le fichier `/etc/bind/named.conf.options` contienne l'option "allow-query { any; }". Le fichier doit contenir :

```
options {
    #des commentaires
    auth-nxdomain no; # conform to RFC1035
    allow-query { any; };
};
```

### 5.1 Configuration d'un client DNS

Le fichier `/etc/resolv.conf` sert à configurer un client DNS. Les deux entrées les plus classiques sont :

- `domain` : le nom du domaine local.
- `nameserver` : l'adresse IP du serveur de noms à interroger. Il peut y avoir plusieurs serveurs (au plus 3). Les serveurs sont sollicités dans l'ordre.

1. Constatez d'abord que la commande : "`nslookup localhost.`" échoue, sur `client`.
2. Dans le fichier `/etc/resolv.conf` du `client`, ajoutez la ligne suivante : `nameserver 10.1.5.1`. A quoi sert cette ligne ?

3. Réessayez la commande : `nslookup localhost..`
4. Observez (via `Wireshark` sur `serveur1` ) les trames qui circulent lors d'une interrogation par le client (`nslookup localhost.`).

Listez les paquets IP envoyés et reçus dans le tableau suivant

adresse IP émetteur	adresse IP destinataire	protocole sur IP	port émetteur	port destinataire

Pourquoi le le protocole transport utilisé est UDP ?

5. Arrêtez le serveur de noms (commande `/etc/init.d/bind9 stop`).

Observez (via **Wireshark** sur `serveur1`) les trames qui circulent lors d'une interrogation par le client (`nslookup localhost.`). Listez les paquets IP envoyés et reçus dans le tableau suivant.

Expliquez ce qui se passe.

adresse IP émetteur	adresse IP destinataire	protocole sur IP	port émetteur	port destinataire

6. Il faut configurer `serveur1` en tant que client DNS. Vérifiez et modifiez si nécessaire le fichier `/etc/resolv.conf` de `serveur1`. il doit contenir uniquement la ligne suivante : `nameserver localhost.` A quoi sert cette ligne ?

## 5.2 Configuration du serveur : déclaration d'une zone

Sur `serveur1`, on va maintenant ajouter une zone “`localdomain`” décrite dans le fichier `db.localdomain`.

À chaque modification dans `db.localdomain`, (1) incrémentez le numéro de série, (2) relancez le serveur DNS et (3) vérifiez que le serveur a été correctement relancé en regardant le “journal” (la fin du fichier `/var/log/syslog`) via la commande : `tail /var/log/syslog`.

1. Copiez le fichier `/etc/bind/db.empty` dans `/etc/bind/db.localdomain`
2. Modifiez le fichier `db.localdomain` comme suit pour déclarer `dns1` comme serveur de nom primaire (`dns1.localdomain.`) avec l'adresse email de l'administrateur :  
`root@dns1.localdomain.`  

```
@      IN      SOA      dns1.localdomain.  root.dns1.localdomain. (
                                ...
                                ...)
```
3. Ajoutez les déclarations de `dns1` (10.1.5.1) `dns2` (10.1.5.2) et `poste` (10.1.5.100).
4. Déclarez `dns1` comme serveur de noms de la zone.
5. Inspirez-vous de la déclaration de “`localhost`” dans `/etc/bind/named.default-zones.conf` pour déclarer “`localdomain`” dans le fichier `/etc/bind/named.conf`.
6. Donnez les lignes ajoutées à `/etc/bind/named.conf`.

7. Relancez le serveur de noms (commande `/etc/init.d/bind9 restart`). Etudiez le “journal des commandes système” (la fin du fichier `/var/log/syslog`) via la commande : `tail /var/log/syslog` pour vérifier que le serveur DNS a démarré correctement. Vérifiez que les noms définis (`dns1.localdomain`, `poste.localdomain`, etc.) sont bien résolus via la commande `nslookup nom-machine`.
8. Définissez un synonyme “`www.localdomain.`” pour “`dns1.localdomain.`”.

## 5.3 Configuration du serveur : résolution inverse

1. Mettez en place la résolution inverse du sous-réseau 10.1.5.0/24 (le nom de la zone est `5.1.10.in-addr.arpa`, les données seront stockées dans `/etc/bind/db.localdomain-rev`).
2. Testez via la commande `nslookup -type=ptr 10.1.5.1`.

3. Donnez le contenu de `/etc/bind/db.localdomain-rev`.

4. Donnez les lignes ajoutées à `/etc/bind/named.conf`.

## 6 Configurer serveur2 en serveur secondaire

La machine `serveur2` (alias `dns2.localdomain`) va jouer le rôle de serveur secondaire pour la zone `localdomain` et la zone inverse `5.1.10.in-addr.arpa`

1. Vérifiez que `bind9` est installé sur `serveur2`
2. Sur le serveur primaire, déclarez le serveur `dns2.localdomain` dans la liste des serveurs susceptibles de renseigner sur `localdomain` (ajoutez la ligne `@ IN NS dns2` dans `db.localdomain`).

3. Sur le serveur secondaire, déclarez les zones dont il est esclave, en précisant l'emplacement du fichier de stockage. Format de la déclarations dans `named.conf` (à suivre à l'espace près) :

```
zone "le-nom-de-la-zone" {
    type slave;
    file "le-fichier-de-stockage";
    masters { ip-serveur-maitre ; };
};
```

Le fichier de stockage est créé et modifié par l'utilisateur `bind` du groupe `bind` qui n'a pas le droit d'écriture sur `/etc/bind`. Donc, le fichier de stockage doit être dans le répertoire `/var/run/named`.

4. Relancez les deux serveurs.
5. Vérifiez que la machine `client` peut consulter les deux serveurs via la commande suivante : `nslookup requête [adresse-IP-serveur-DNS]` (par exemple, `nslookup www.localdomain. 10.1.5.2`).
6. Configurez-la machine `client` pour qu'il utilise les deux serveurs de nom.
7. Sur `serveur1` arrêtez le service DNS (`/etc/init.d/bind9 stop`) vérifiez que la machine `client` peut encore résoudre les adresses. Notez le délai.
8. Donnez les lignes ajoutées à `/etc/bind/named.conf` de `serveur2`

## 7 Délégation d'un sous-domaine

1. Sur le serveur primaire de la zone `localdomain`, pour déclarer le sous-domaine `appareils.localdomain` dont le serveur primaire est `dns2`, vous ajoutez dans `db.localdomain`, la ligne suivant : `appareils IN NS dns2`
2. Définissez cette zone sur `serveur2`, avec quelques entrées (télé, magnétoscope, console de jeux...). il faut modifier le fichier `named.conf` et construire le fichier `db.appareils.localdomain`.
3. Testez votre configuration sur `client`, à l'aide des commandes `nslookup` telles que `nslookup console.appareils.localdomain. 10.1.5.1`
4. Et pour finir, configurer `serveur1` pour qu'il soit le serveur secondaire de la zone `appareils.localdomain`.



5. Ecrivez les lignes ajoutées au fichier `/etc/bind/named.conf` de `serveur1`.

6. Ecrivez les lignes ajoutées au fichier `/etc/bind/named.conf` de `serveur2`.

7. Donnez le contenu de `/etc/resolv.conf` sur `client`.

8. Donnez le contenu de `/etc/bind/db.appareils.localdomain` sur `serveur2`.

## 8 Sur Internet

Utilisez la commande `nslookup`, pour faire les recherches suivantes sur votre poste de travail (qui est relié au réseau Internet). Aidez vous des manuels. **Indice** : Il faut utiliser l'option `-type` de la commande `nslookup`.

1. Trouvez l'adresse IP de `dagobah`. Donnez la commande tapée.
  
2. Trouvez l'adresse IP de `dagobah`. . Donnez la commande tapée.
  
3. Recherchez, **plusieurs fois après un délai de plusieurs minutes**, l'adresse IP du serveur "`www.lemonde.fr`". Donnez la commande tapée. Qu'observez vous ? Expliquez.
  
4. Quelle est l'adresse IP du serveur de nom de `iut.u-bordeaux1.fr` ? Donnez la commande tapée.
  
5. Quels sont ses serveurs de mails de `iut.u-bordeaux1.fr` ? Donnez la commande tapée.

### Bilan

1. Combien d'adresses IP peuvent être associées à un nom ?
2. Combien de noms peuvent être associées à une adresse IP ?