La Plateforme
La grande école du numérique pour tous

DHCP, DNS, FTP et SSH

Un projet de :

Jordan

Youcef

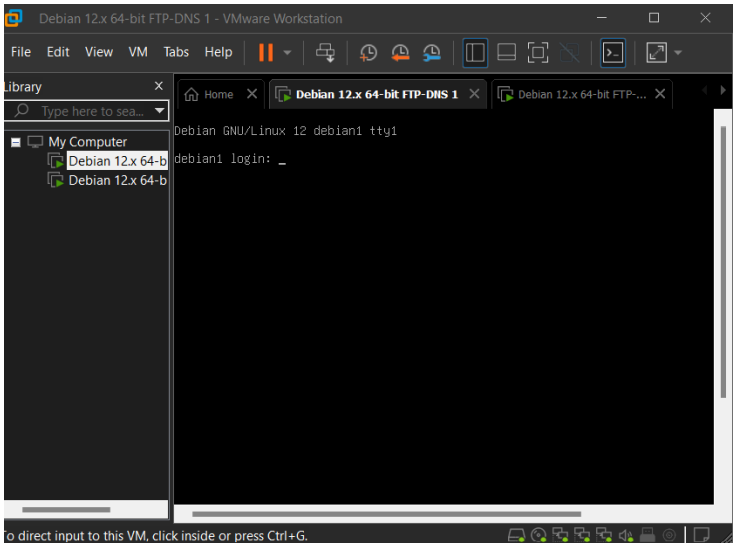
Lucas

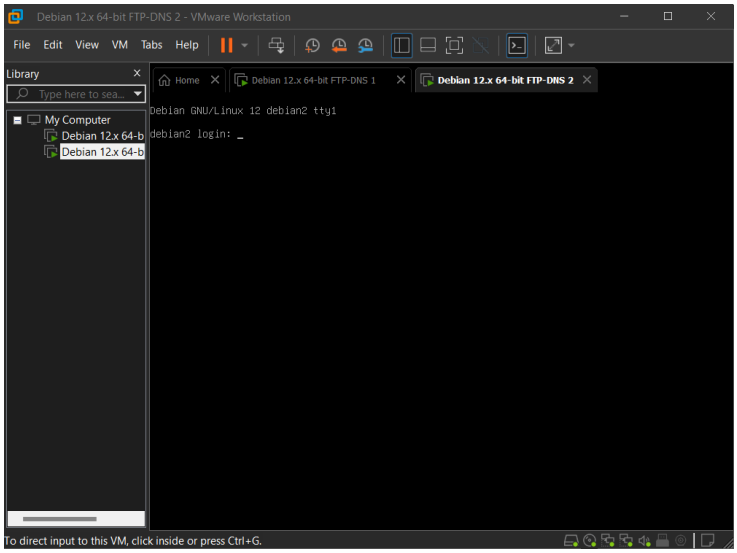
ETAPES A SUIVRE :

1. Installation de Debian sans interface graphique :

On commence par l'installation de nos deux machines virtuelles Debian sans interface graphique :

Une fois l'installation terminé on a nos deux machines qui ressemblent à ceci :





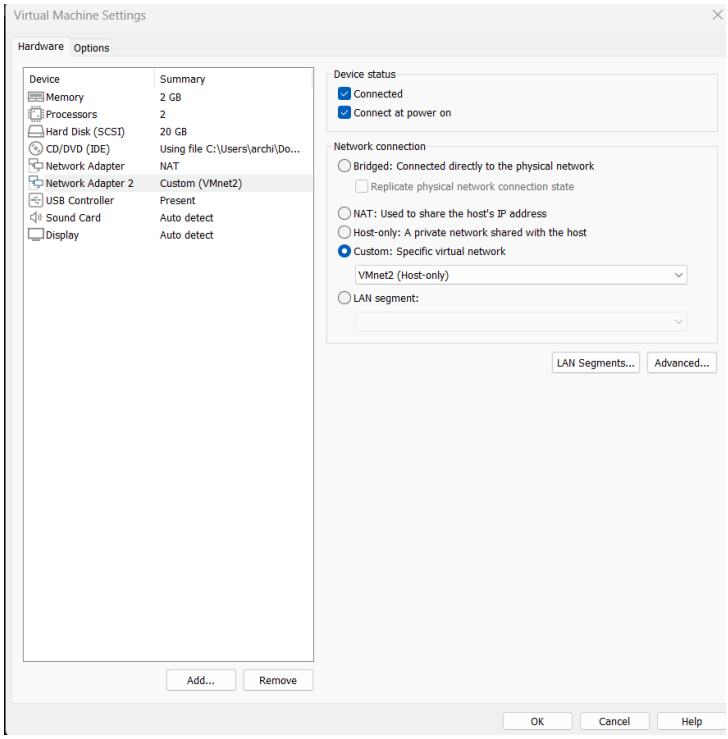
2. Mise à jour des systèmes :

Pour appliquer les mises à jour nécessaires sur les deux machines.

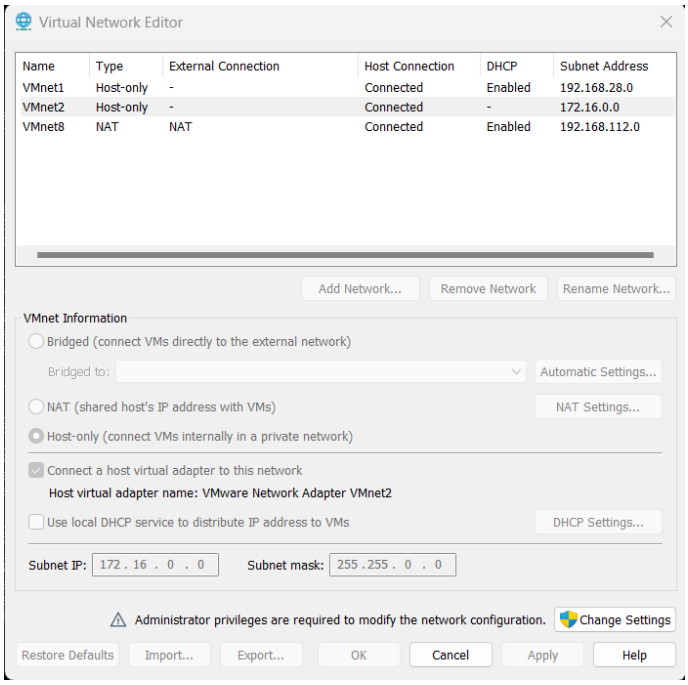
On utilise simplement les commandes **« sudo apt update »** et **« sudo apt upgrade »** . Après avoir mis à jour les paquets installés, il est recommandé de mettre à jour le système d'exploitation Debian lui-même on utilise alors la commande **« sudo apt dist-upgrade »** .

3-Configuration du Serveur DHCP :

Pour l'installation du serveur DHCP on a décidé d' ajouter une nouvelle carte réseau .



Ensuite on se rend dans **« Edit »** puis on va dans **« Virtual Network Editor »**

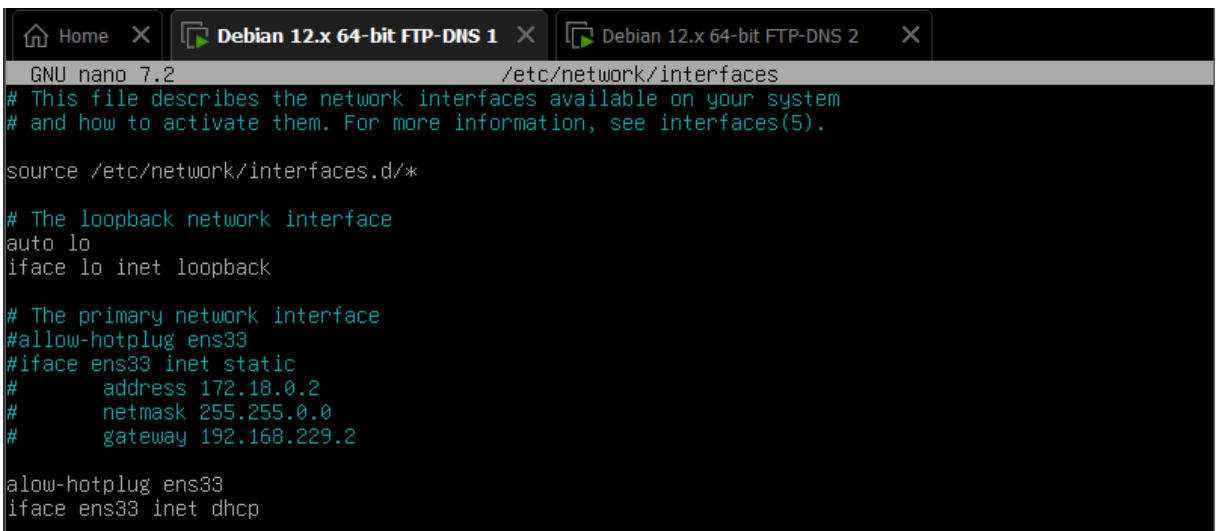


On retire le fait d'utiliser le DHCP local et on modifie le sub net IP pour le passer en classe B .

Par la suite avant toutes choses on regarde notre environnement réseau en tapant **« ip addr »** ou bien il y'a **« ip route | grep default »**

```
youcef1@debian1:~$ ip addr
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:28:de:ae brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.0.13/16 brd 172.16.255.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet 192.168.112.138/24 brd 192.168.112.255 scope global dynamic ens33
       valid_lft 1110sec preferred_lft 1110sec
    inet6 fe80::20c:29ff:fe28:deae/64 scope link
       valid_lft forever preferred_lft forever
```

-On se rend sur le fichier interfaces à l'aide de la ligne de commande suivante :



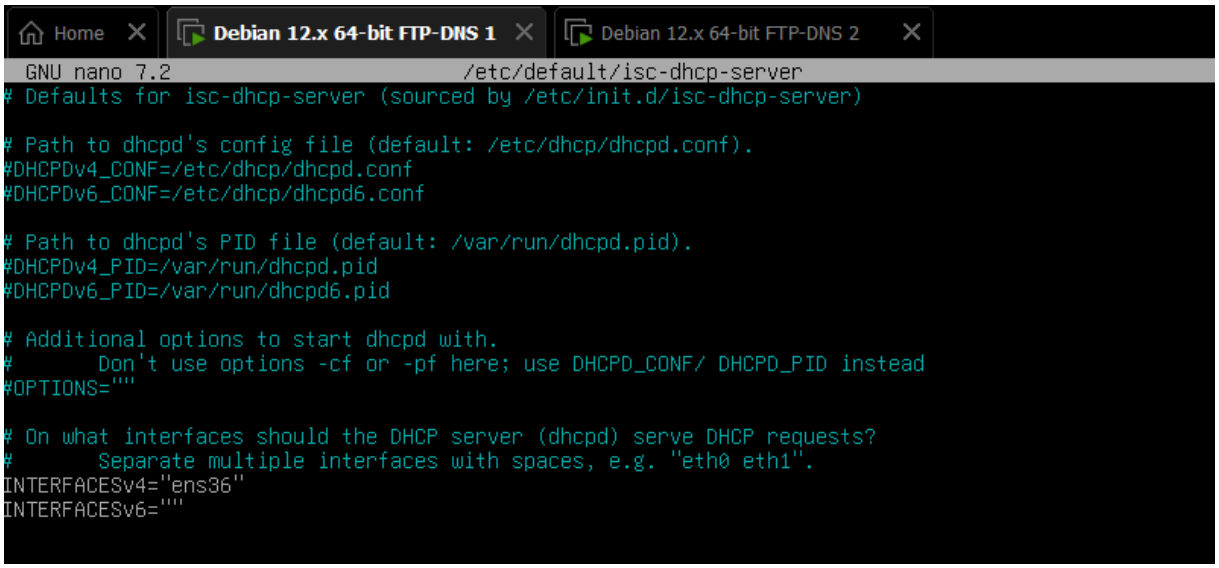
« sudo nano /etc/network/interfaces » et on y ajoute ceci :

Maintenant on passe à l'installation et la configuration du DHCP en utilisant la commande :

« sudo apt install isc-dhcp-server »

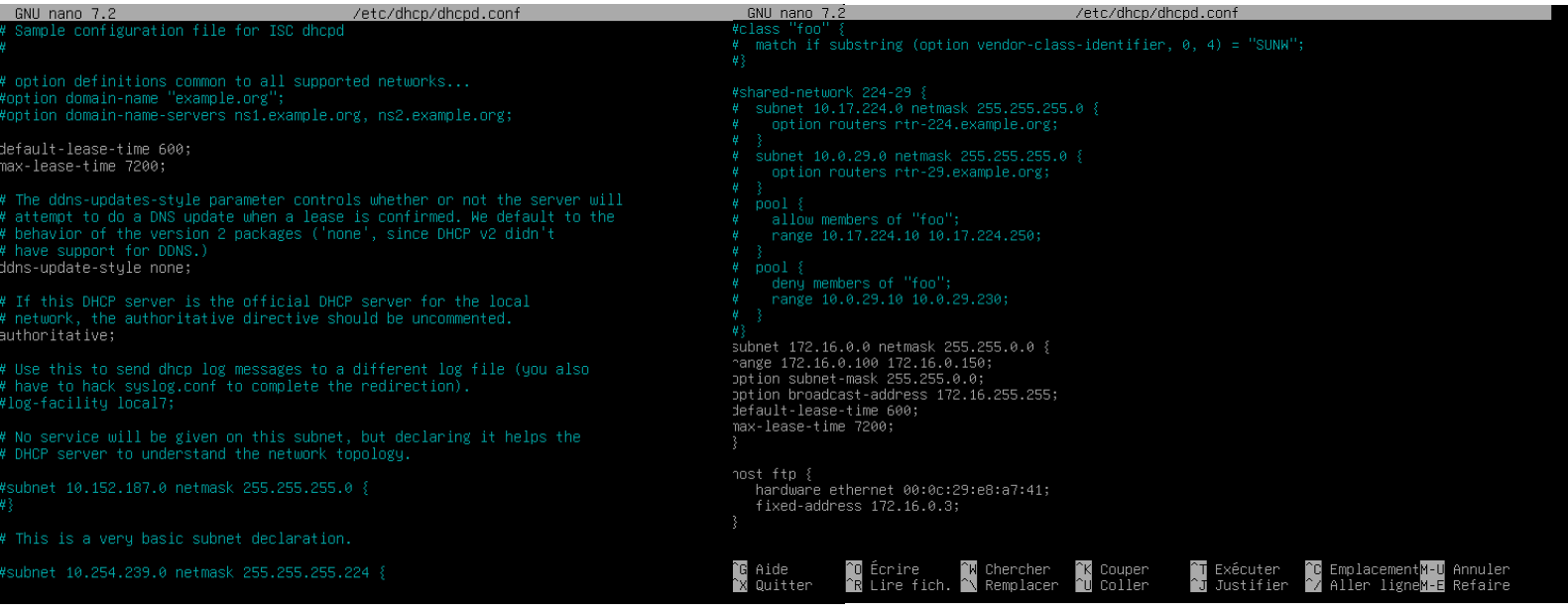
Une fois que c'est fait on se rend dans **« isc-dhcp-server »** à l'aide de la ligne de commande suivante :

« sudo nano /etc/default/isc-dhcp-server » et on ajoute dans l'interface v4 notre **« ens »**



Ensuite on se rend dans le fichier « dhcpd.conf » avec les commandes suivantes :

« sudo nano /etc/dhcp/dhcpd.conf »

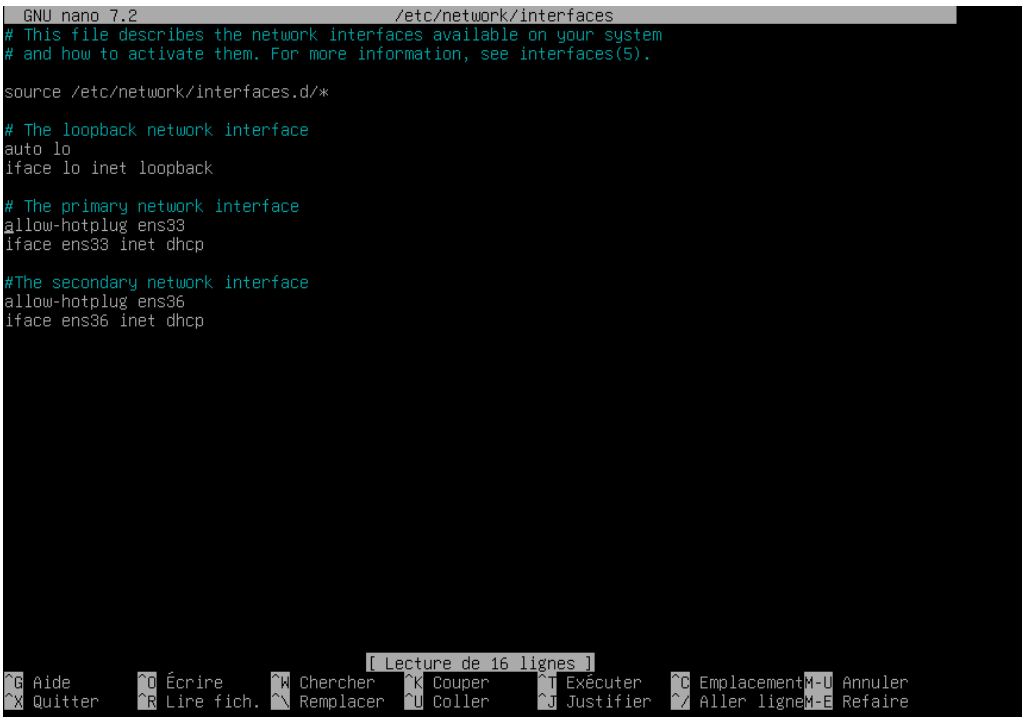


Une fois dessus on décommente « authoritative » .
Authoritative : dans le fichier de configuration dhcpd.conf indique au serveur DHCP qu'il est l'autorité pour le réseau spécifié. Cela signifie que si un client DHCP envoie une demande de configuration d'adresse IP à ce serveur, ce serveur est autorisé à répondre avec une adresse IP et d'autres informations de configuration.

Lorsque cette ligne est commentée (précédée d'un symbole dièse "#"), le serveur DHCP n'est pas considéré comme l'autorité pour le réseau. Cela signifie que s'il reçoit une demande DHCP pour un réseau spécifique pour lequel il est configuré, il transmettra cette demande à un autre serveur DHCP (s'il en existe un) qui est autorisé à répondre pour ce réseau.

Ensuite on ajoute à la fin notre subnet avec l'adresse ip qu'on a configuré juste avant ..

Juste après on retourne sur notre seconde VM et on ajoute dans le fichier **« interface »**



1. **allow-hotplug** :
    - Cette directive permet de gérer dynamiquement l'état de l'interface. Elle indique au système d'activer l'interface lorsqu'elle est branchée et de la désactiver lorsqu'elle est débranchée, sans nécessiter de redémarrage du système. Cela permet une gestion plus flexible des interfaces réseau.
2. **iface** :
    - Cette directive indique l'interface réseau à configurer, suivie du protocole à utiliser (dans ce cas, **inet** pour les réseaux IPv4).
    - La section suivante après **iface** définit la configuration réseau pour l'interface spécifiée.
3. **inet dhcp** :
    - Cette ligne indique que l'interface doit obtenir sa configuration réseau via DHCP. Cela signifie que l'interface essaiera d'obtenir une adresse IP automatiquement à partir d'un serveur DHCP sur le réseau auquel elle est connectée.

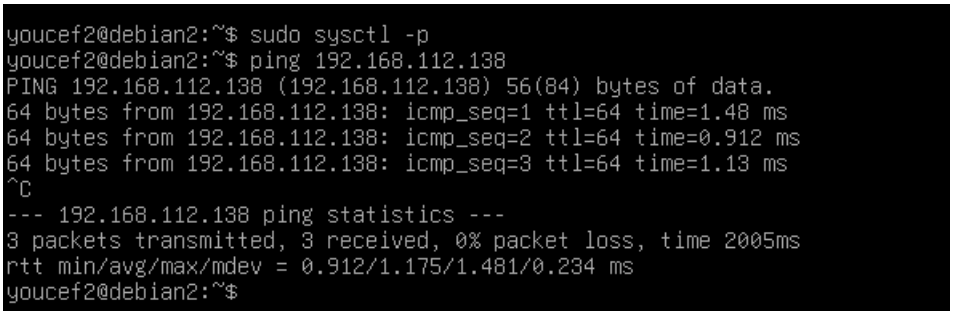
Pour s'assurer que notre DHCP fonctionne on utilise la commande **« sudo systemctl status isc-dhcp-server »**

Entre chaque manipulation il faut s'assurer de restart le dhcp et le network à l'aide des commandes suivantes :

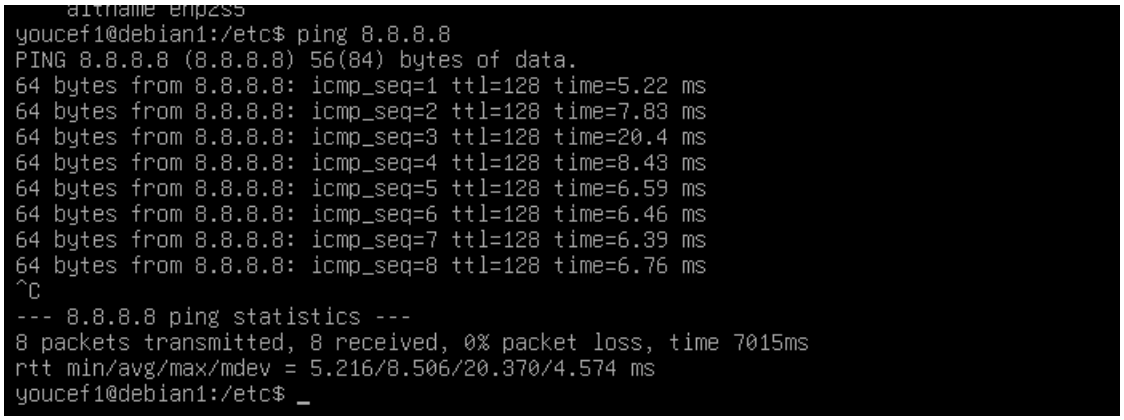
« sudo systemctl restart isc-dhcp-server »

« sudo systemctl restart networking »

Pour s'assurer que les deux VM puissent communiquer entres elles , il suffisait d'effectuer un ping :



On effectue un ping 8.8.8.8 pour vérifier la connectivité réseau d'une machine à Internet.



Avant de passer à l'installation de FTP , même si c'est sur l'autre machine virtuelle on procède par effectuer un snapshot, ce qui nous permet de sauvegarder notre travail opérationnel et fonctionnel et d'y pouvoir y revenir si besoin .

4. Installation du Serveur FTP :

On commence par installer ftp avec la commande :

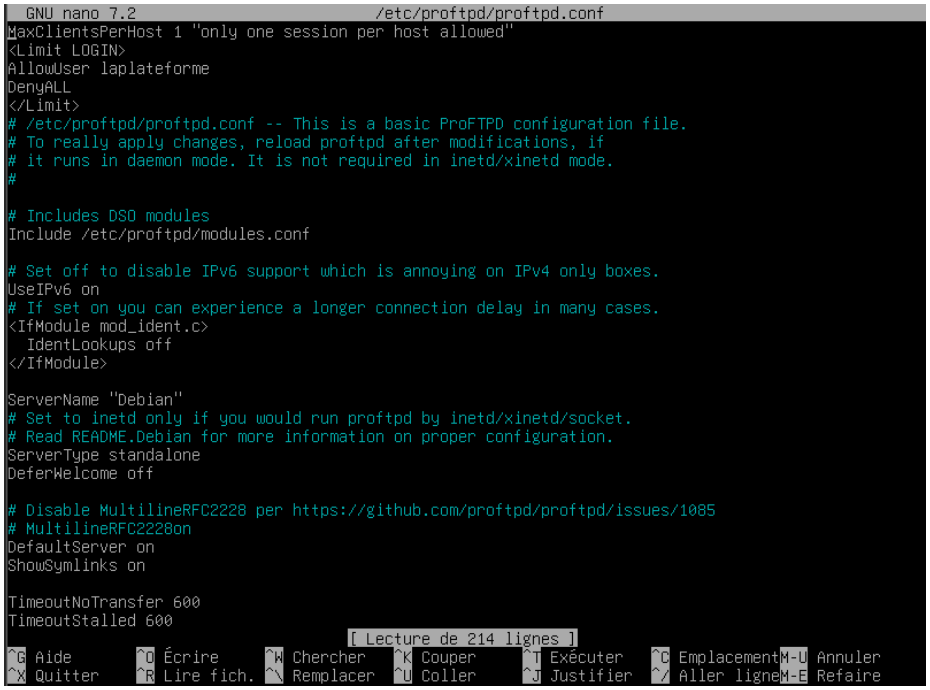
« sudo apt install proftpd »

Maintenant on créer notre user et on lui définit un mot de passe à l'aide de la commande :

« sudo add user laplateforme »

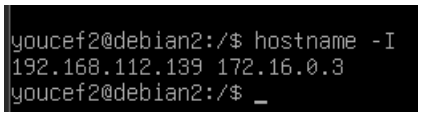
Une fois que l'user créer et l'installation terminé on se rend sur le dossier **« proftpd»** avec la commande suivante :

« sudo nano /etc/proftpd/proftpd.conf »

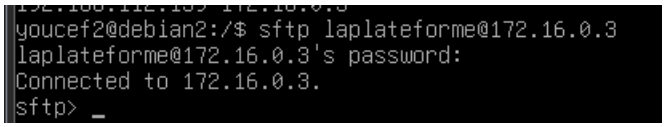


Une fois dedans on y ajoute le nombre de Client que l'on souhaite et on autorise user »laplateforme » de s'y connecter .

Avant de pouvoir se connecter on récupère notre IP avec la commande : « **hostname -I »**

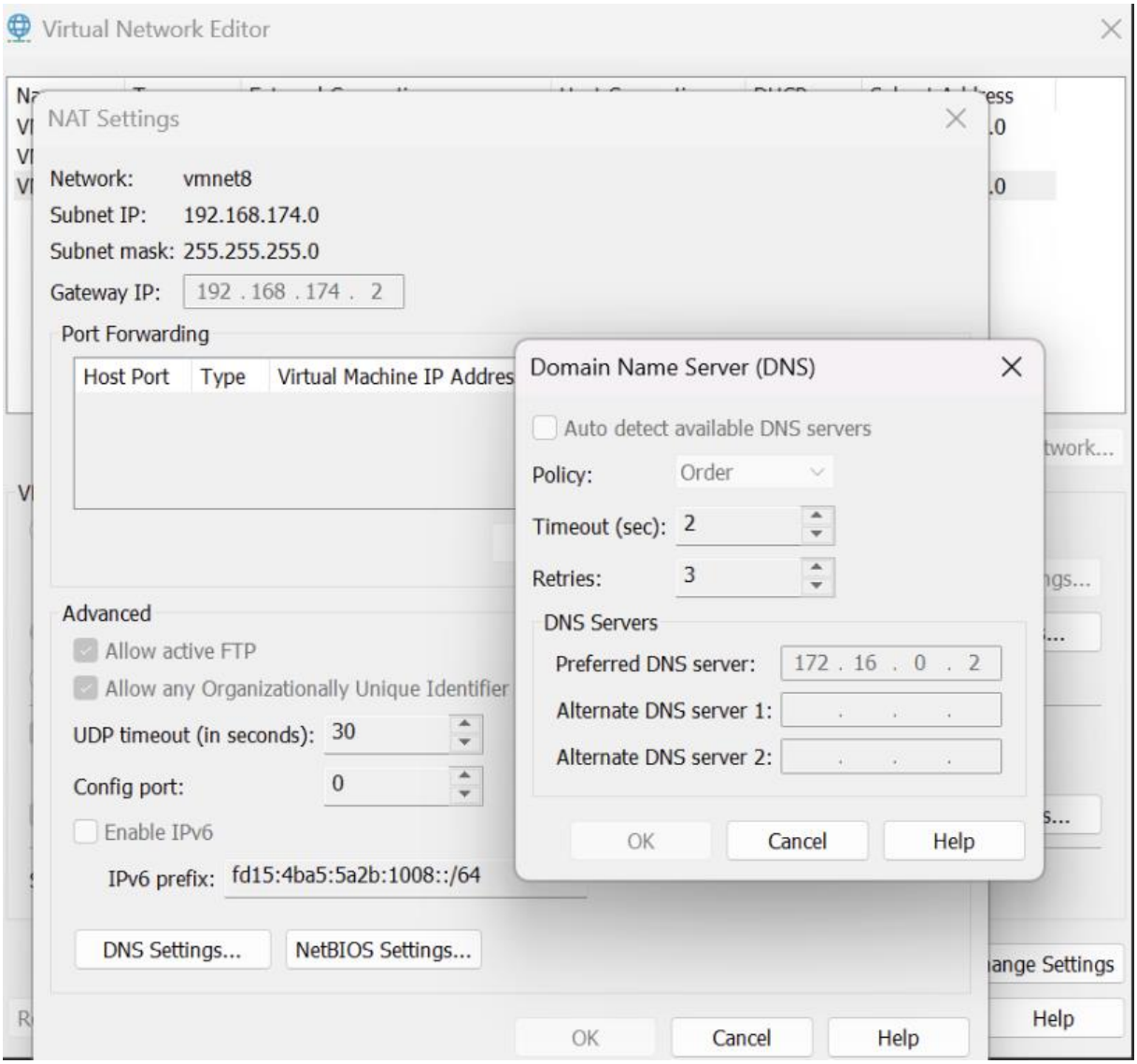


Pour se connecter il suffit de taper : **« sftp laplateforme « notre ip » »** et d'entrer le mot de passe .



5. Installation du Serveur DNS :

Sur notre seconde carte réseau , on commence par désactiver la détection automatique des serveurs DNS disponible et on lui définit le serveur DNS préférer en lui donnant l'adresse IP de notre première machine.



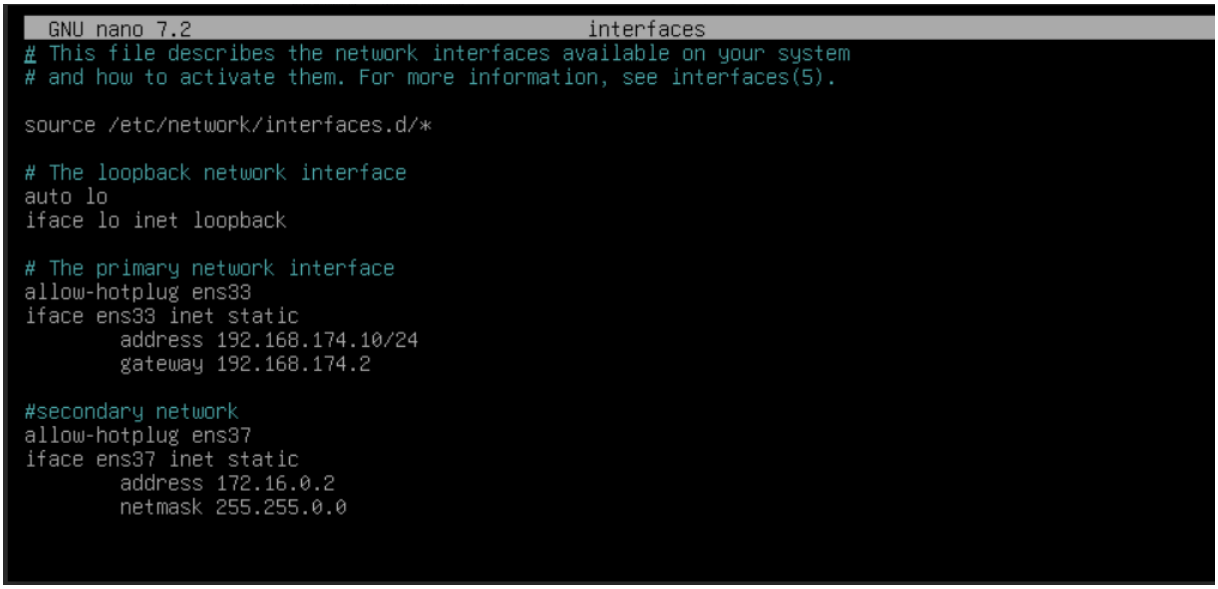
« On précise que notre première carte réseau nous sert d'accès à Internet »

Installation du serveur **BIND** sur la première machine :

« sudo apt install bind9 »

Une fois l'installation terminée, on se rend sur le fichier interfaces :

« sudo nano /etc/network/interface »



Nous avons décidé de modifier la configuration pour que l'interface réseau soit configurés avec une adresses IP statiques . Cette étape est essentielle pour notre serveur DNS car il a besoin d'une interface réseau avec une adresse IP statique pour être toujours accessible.

Configuration DNS :

On se rend dans le fichier **« named.conf.options »**

allow-query { any; }; : Cette ligne spécifie que le serveur BIND acceptera les requêtes de résolution DNS de n'importe quelle adresse IP. C'est un paramètre de contrôle d'accès qui détermine qui peut faire des requêtes à votre serveur DNS.

Forwaders : utilisé pour définir les serveurs DNS auxquels BIND doit transmettre les requêtes qu'il ne peut pas résoudre avec les données dont il dispose localement. Ici, 8.8.8.8 est l'adresse du serveur DNS de Google, ce qui signifie que toutes les requêtes que le serveur DNS ne peut pas résoudre seront envoyées à ce serveur pour résolution.

```
root@debian1:/# cat /etc/bind/named.conf.options

options {
        directory "/var/cache/bind";
        allow-query { any; };



        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
                8.8.8.8;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;
        auth-nxdomain no;
        listen-on-v6 { any; };
};
```

Ensuite on se rend sur le **« named.conf.local »**

zone "ftp.com" IN {: indique le chemin vers le fichier sur le serveur DNS qui gère les enregistrements pour le domaine ftp.com.Cette déclaration commence la configuration de la zone pour le domaine ftp.com. IN représente l'Internet class et est souvent utilisé dans les configurations de zone DNS.

type master;: Cela indique que le serveur BIND agit en tant que serveur maître pour la zone ftp.com. Cela signifie qu'il détient le fichier de zone autoritaire, qui contient les enregistrements DNS réels.

file "/etc/bind/db.ftp.com";: Ceci spécifie le chemin vers le fichier de données de la zone pour le domaine ftp.com. Ce fichier doit contenir tous les enregistrements DNS pour le domaine,

Ensemble, cette configuration informe le serveur DNS que pour toute requête liée à ftp.com, il doit consulter le fichier spécifié (/etc/bind/db.ftp.com) pour déterminer comment répondre à la requête

```
root@debian1:/# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "ftp.com" IN {
        type master;
        file "/etc/bind/db.ftp.com";
};

//zone "16.172.in-addr.arpa" {
//      type master;
//      file "etc/bind/db.172";
//};
root@debian1:/# cat /etc/bind/named.conf.local
```

Le fichier de zone pour ftp.com définit les paramètres essentiels et les serveurs responsables du domaine. L'enregistrement SOA inclut des informations de contact et des numéros de série pour

suivre les mises à jour. Les intervalles de rafraîchissement et d'expiration dictent quand les serveurs secondaires vérifient et considèrent les données comme obsolètes. Les enregistrements NS et A lient les noms de sous-domaines à des adresses IP spécifiques, dirigeant le trafic vers l'hôte désigné pour le service FTP.

```
root@debian1:/# cat /etc/bind/db.ftp.com
;
; BIND data file for ftp.com
;
$TTL    604800
@       IN      SOA     ftp.com  admin.ftp.com (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns
ns      IN      A       172.16.0.2
dns     IN      A       172.16.0.3
root@debian1:/#
```

6. Test de Connexion au Serveur SFTP :

```
jordan@debian2:/etc/proftpd$ sftp laplateforme@172.16.0.3
The authenticity of host '172.16.0.3 (172.16.0.3)' can't be established.
ED25519 key fingerprint is SHA256:jZxkIV0qAgdAZ4QJNQURbNOf4TeKnyVo0ZYLFDDe5f8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.16.0.3' (ED25519) to the list of known hosts.
laplateforme@172.16.0.3's password:
Connected to 172.16.0.3.
sftp>
```

7. Paramètres de Sécurité Additionnels :

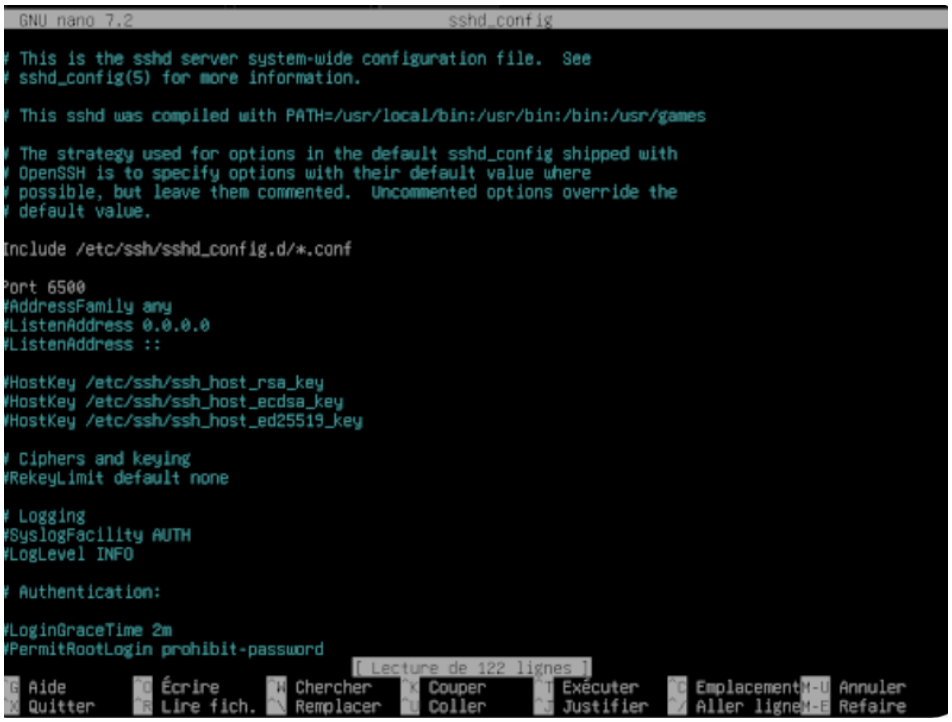
Afin de renforcer la sécurité du serveur SFTP :

Nous avons limité l'accès seulement à l'utilisateur « laplateforme »

```
  GNU nano 7.2                                          proftpd.conf
MaxClientsPerHost 1 "only one session per host allowed"
<Limit LOGIN>
AllowUser laplateforme
DenyALL
```

« sudo nano /etc/ssh/sshd_config » et on enlève le #port 22, on décommente et on écrit Port 6500

Cela nous permet de sécuriser notre connexion, le port 22 étant le port par défaut et pouvant être utilisé comme porte d'entrée par des individus mal intentionnés.



Ensuite nous utilisons la commande **« sudo lsof -i :6500 »** pour être sûr que le port écouté est bien le 6500

```
jordan@debian:/etc/ssh$ sudo lsof -i :6500
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd    1129 root    3u  IPv4  25873      0t0  TCP *:6500 (LISTEN)
sshd    1129 root    4u  IPv6  25884      0t0  TCP *:6500 (LISTEN)
```

Nous utilisons maintenant la première machine et nous nous connectons de manière sécurisée à l'adresse dns.ftp.com sur le port 6500.

```
jordan@debian:~$ sftp -oPort=6500 laplateforme@dns.ftp.com
laplateforme@dns.ftp.com's password:
Connected to dns.ftp.com.
sftp> _
```