Notice Technique : Solutions de Logiciels de Prise en Main à Distance

1. Introduction

Les logiciels de prise en main à distance permettent d'accéder et de contrôler un ordinateur distant via un réseau. Ils sont utilisés pour l'assistance technique, l'administration informatique et le télétravail. Cette notice présente plusieurs solutions disponibles ainsi qu'une recommandation finale.

2. Solutions Disponibles

2.1. TeamViewer

- **Avantages :**
  - **Interface intuitive et facile à utiliser.**
  - **Fonctionnalités avancées (transfert de fichiers, chat, gestion multi-écrans).**
  - **Sécurisé avec un chiffrement de bout en bout.**
  - **Disponible sur Windows, macOS, Linux, Android et iOS.**
- **Inconvénients :**
  - **Version gratuite limitée à un usage personnel.**
  - **Coût élevé pour les entreprises.**

2.2. AnyDesk

- **Avantages :**
  - **Léger et rapide, avec faible latence.**
  - **Sécurité renforcée avec chiffrement AES 256 bits.**
  - **Compatible avec plusieurs plateformes.**
  - **Offre une version gratuite pour un usage personnel.**
- **Inconvénients :**
  - **Moins de fonctionnalités collaboratives que TeamViewer.**
  - **Version gratuite avec limitations.**

2.3. Chrome Remote Desktop

- **Avantages :**
  - **Gratuit et intégré à Google Chrome.**
  - **Facile à installer et utiliser.**
  - **Disponible sur diverses plateformes (Windows, macOS, Linux).**
- **Inconvénients :**
  - **Fonctionnalités limitées (pas de transfert de fichiers natif, pas de chat).**
  - **Dépendance à Google Chrome.**

2.4. Microsoft Remote Desktop (RDP)

- **Avantages :**
  - **Intégré à Windows, donc pas de coût supplémentaire.**
  - **Bonne performance sur un réseau local.**
  - **Sécurité renforcée avec authentification réseau.**
- **Inconvénients :**
  - **Moins efficace sur Internet que d'autres solutions.**
  - **Nécessite une configuration avancée et un accès réseau direct.**

2.5. VNC (Virtual Network Computing)

- **Avantages :**
  - **Open source et configurable.**
  - **Fonctionne sur plusieurs systèmes d'exploitation.**
  - **Adapté aux environnements d'entreprise.**
- **Inconvénients :**
  - **Configuration technique plus complexe.**
  - **Moins performant sur des connexions lentes.**

3. Recommandation

Le choix du logiciel dépend des besoins spécifiques :

- **Pour une utilisation personnelle et gratuite : Chrome Remote Desktop ou AnyDesk.**
- **Pour une entreprise avec des besoins avancés : TeamViewer pour ses fonctionnalités complètes.**
- **Pour un usage en réseau local : Microsoft Remote Desktop.**
- **Pour une solution open source et flexible : VNC.**

Si un bon équilibre entre performances, fonctionnalités et coût est recherché, AnyDesk est un excellent compromis grâce à sa rapidité et son coût raisonnable pour les entreprises.

4. Conclusion

Chaque solution présente des avantages et des inconvénients selon l'usage prévu. Il est recommandé de tester plusieurs solutions avant de choisir celle qui correspond le mieux aux besoins spécifiques de l'entreprise ou de l'utilisateur.

Dans notre cas, nous utiliserons TeamViewer. Voici une notice d'utilisation de ce logiciel.

NOTICE D'UTILISATION DE TEAMVIEWER

1. Présentation de TeamViewer

TeamViewer est un logiciel permettant la prise en main à distance d'un ordinateur, le partage d'écran, le transfert de fichiers et la collaboration en ligne. Il est utilisé pour l'assistance technique, le travail à distance et les réunions en ligne.

---

2. Installation de TeamViewer

1. **Téléchargement**
   - **Rendez-vous sur le site officiel : https://www.teamviewer.com**
   - **Téléchargez la version adaptée à votre système d'exploitation (Windows, macOS, Linux).**
2. **Installation**
   - **Lancez le fichier d'installation.**
   - **Choisissez "Installation par défaut" et cliquez sur "Suivant".**
   - **Acceptez les conditions d'utilisation et terminez l'installation.**
3. **Pour l'installation sous debian, la manipulation est différente car nous n'avons pas d'interface graphique.**
   - **wget https://download.teamviewer.com/download/linux/teamviewer-host_amd64.deb**
   - **dpkg -i teamviewer-host_amd64.deb**
   - **apt --fix-broken install**

   Puis configurer le logiciel :

   → teamviewer setup

---

3. Connexion et Configuration

1. **Lancer TeamViewer**
   - **Ouvrez l'application après l'installation.**
   - **Une fenêtre affiche "Votre ID" et "Votre mot de passe", nécessaires pour la connexion à distance.**
2. **Créer un compte (optionnel)**
   - **Cliquez sur "S'inscrire" pour créer un compte TeamViewer.**
   - **Se connecter permet d'accéder à des fonctionnalités avancées (gestion des appareils, liste de contacts).**

---

4. Prise en main à distance

1. **Contrôler un ordinateur distant**
    - **Demandez à l'utilisateur distant de vous fournir son ID et son mot de passe TeamViewer.**
    - **Entrez l'ID dans la section "Contrôler un ordinateur à distance", puis cliquez sur "Connexion".**
    - **Saisissez le mot de passe fourni et prenez le contrôle de l'appareil.**
2. **Autoriser un accès à distance**
    - **Donnez votre ID et mot de passe à la personne qui souhaite se connecter.**
    - **Une fois la connexion établie, l'utilisateur distant pourra contrôler votre PC.**

Sous debian il suffit d'utiliser la commande pour récupérer l'ID :

→ teamviewer info

---

5. Fonctions Principales

- **Transfert de fichiers :**
    - **Dans la barre supérieure, cliquez sur "Fichier et extras" → "Ouvrir le gestionnaire de transfert de fichiers".**
    - **Sélectionnez les fichiers à envoyer ou à recevoir.**
- **Chat et communication :**
    - **Utilisez la messagerie instantanée ou l'appel audio/vidéo intégrés pendant la session.**
- **Accès non surveillé (sans intervention de l'utilisateur distant) :**
    - **Activez l'option "Accès non surveillé" dans "Options" > "Sécurité".**
    - **Configurez un mot de passe personnel pour éviter de demander un nouveau code à chaque connexion.**

---

6. Sécurité et Bonnes Pratiques

→ Ne communiquez votre ID et votre mot de passe qu'à des personnes de confiance.
→ Activez la double authentification pour une sécurité renforcée.
→ Gardez votre TeamViewer à jour pour bénéficier des dernières améliorations et corrections de sécurité.

DHCP Debian

PC-2 (client de TEST)
Adresse MAC : 08:00:27:bc:d6:46
IP 172.16.70.6

Toutes les étapes se feront en root
Lorsque je dirais de sauvegarder cela signifie de faire “ctrl+x” ensuite “o” puis entrer.
Les IP dans cette documentation sont là pour donner un exemple.

Pour configurer un serveur DHCP sous debian nous allons suivre différentes étapes:

1- Mises à jour / installation des différents logiciels pour scanner, agent relais DHCP.
2- Configuration des différents fichiers du DHCP / agent relais DHCP.
2bis- Assigner la même ip à la même machine avec l’adresse MAC
3- Commandes pour scanner le réseau.
4- Test du serveur DHCP avec une autre machine virtuelle en debian.

1- Installation des différents logiciels

En commençant par arp scan qui permet de récupérer les adresses MAC des machines du réseau.
apt install arp scan

Pour ce qui est des Vlans, il faut installer l’extension.
apt install vlan

et les activer avec
modprobe 8021q

Pour l’agent relais DHCP
Commençons par l’installer.
apt install isc-dhcp-relay

2- Configuration des différents fichiers du DHCP

Pour ce qui est des fichiers du DHCP avec les vlans, nous devons dans un premier temps ajouter les interfaces vlans.
nano /etc/network/interfaces

et obtenir un fichier similaire à celui là avec nos vlans.

```
# The primary network interface
allow-hotplug enp0s3
#iface enp0s3 inet manual
#iface enp0s3 inet dhcp
iface enp0s3 inet static
        address 172.16.2.1
        netmask 255.255.255.128



# Vlan 60 - Wifi_Public
auto enp0s3.60
iface enp0s3.60 inet static
        address 172.16.20.1
        netmask 255.255.255.128
        vlan-raw-device enp0s3

# Vlan 70 - Filaire_Public
auto enp0s3.70
iface enp0s3.70 inet static
        address 172.16.21.1
        netmask 255.255.255.128
        vlan-raw-device enp0s3
```

Puis il faut redémarrer le fichier de configurations pour prendre en compte les modifications.
systemctl restart networking

puis modifier le fichier de configuration du DHCP
nano /etc/dhcp/dhcpd.conf

```
subnet 172.16.2.0 netmask 255.255.255.128 {
  range 172.16.2.2 172.16.2.126;
  option routers 172.16.2.1;
}

# Vlan 60 - Wifi_Public
subnet 172.16.20.0 netmask 255.255.255.128 {
        range 172.16.20.2 172.16.20.126;
        option routers 172.16.20.1;
}

# Vlan 70 - Filaire_Public
subnet 172.16.21.0 netmask 255.255.255.128 {
        range 172.16.21.2 172.16.21.126;
        option routers 172.16.21.1;
}
```

ne pas oublier de les ajouter dans isc.
nano /etc/default/isc-dhcp-server

avec cette ligne là qui correspond au différents vlans.

```
INTERFACESv4="enp0s3 enp0s3.60 enp0s3.70 enp0s3.80 enp0s3.90 enp0s3.100 enp0s3.110 enp0s3.120"
```

Voici les différentes commandes à mettre dans un switch cisco.

```
interface Vlan10
 ip helper-address 192.168.10.1

interface Vlan20
 ip helper-address 192.168.20.1
```

Puis redémarrer le service DHCP.

```
systemctl restart isc-dhcp-server
```

Pour l'agent relais DHCP,
nous devons ouvrir le fichier

```
nano /etc/default/isc-dhcp-relay
```

Puis configurer les lignes INTERFACES et SERVERS comme la capture d'écran en dessous.

```
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

#
# This is a POSIX shell fragment
#

# What servers should the DHCP relay forward requests to?
SERVERS="172.16.2.1"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES="enp0s3.60 enp0s3.70 enp0s3.80 enp0s3.90 enp0s3.100 enp0s3.110 enp0s3.120 "

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

Nous avons donc dans SERVERS l'IP de notre serveur DHCP. et dans INTERFACES les différentes interfaces virtuelles en fonction des vlans que nous avons configurés.

Puis il ne reste plus que faire :

```
systemctl restart isc-dhcp-relay
```

2bis- Configuration supplémentaire pour le serveur DHCP fasse en sorte qu'il assigne toujours la même configuration IP à un poste donné

Éditer la configuration du serveur DHCP

Éditer la configuration du serveur DHCP qui se trouve généralement à :

```
nano /etc/dhcp/dhcpd.conf
```

Ajouter une section comme celle-ci pour réserver une IP spécifique à l'adresse MAC du poste :

```
host PC-2 {
        hardware ethernet 08:00:27:bc:d6:46;          # Adresse MAC de la machine
        fixed-address 172.16.2.6;       # IP à assigner
}
```

Redémarrer le serveur DHCP

Après avoir sauvegardé les modifications, redémarre le service DHCP :

```
systemctl restart isc-dhcp-server
```

3- Commandes pour scanner le réseau

Nous avons vu précédemment comment installer arp nous allons maintenant voir comment l'utiliser.

Tout d'abord la commande pour scanner le réseau afin d'obtenir les adresses MAC des machines du réseau est :

```
ip neigh show
```

4- Test du serveur DHCP avec une autre machine virtuelle en debian.

Pour tester notre serveur DHCP,

→ Pour cela il faut la machine debian configurer avec le serveur DHCP ainsi qu'une machine avec un Windows 10 qui servira de client.

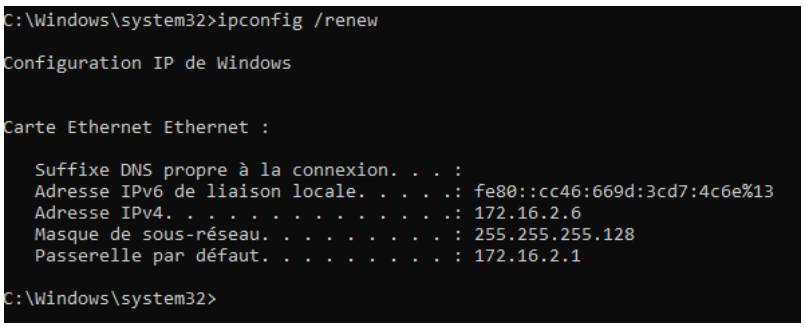
→ Dans la configuration des 2 machines virtualbox :

- Aller dans l'onglet réseau.
- Puis sélectionner le mode d'accès réseau : Réseau interne.
- Name : intnet.

Une fois celà effectué, il faut se rendre sur la machine virtuelle qui sert de client.
Ouvrir un CMD en tant qu'administrateur.
Il ne reste plus que faire la commande suivante :

```
ipconfig /renew
```

nous pouvons nous apercevoir que si les configurations précédentes ont bien été effectué la machine recevra l'ip que nous lui avons attribué et elle sera toujours la même.



Toutes les étapes se feront en root
Lorsque je dirais de sauvegarder cela signifie de faire “ctrl+x” ensuite “o” puis entrer.
Les IP dans cette documentation sont là pour donner un exemple.

Pour configurer un serveur DHCP sous debian nous allons suivre différentes étapes:

1- Mises à jour / installation du DHCP.
2- Configuration des différents fichiers du DHCP.
3- Test du serveur DHCP avec une autre machine virtuelle en debian.
4- Changer le nom de l’hôte sous debian.
5- Installation et configuration de TFTP.
6- Test de TFTP avec une autre machine virtuelle en debian

1- Mises à jour / installation du DHCP

apt update Mise à jour du debian.

apt install isc-dhcp-server Permet d’installer les fichiers de configuration du server DHCP

2- Configuration des différents fichiers du DHCP

ip a Pour récupérer l’interface juste après le “2:” normalement il s’agit de enp0s3

nano /etc/default/isc-dhcp-server Pour accéder au fichier texte du dhcp server et le modifier

→ Les lignes à modifier sont : DHCPv4_CONF à dé-commenter et spécifier l'interface dans INTERFACESv4.Puis sauvegarder.

```
  GNU nano 5.4                          /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
#INTERFACESv6=""
```

nano /etc/network/interfaces Pour configurer le réseau du serveur.

→ il faudra commenter la ligne iface enp0s3 inet dhcp
puis ajouter en dessous:

iface enp0s3 inet static
address 172.16.2.1
netmask 255.255.255.128

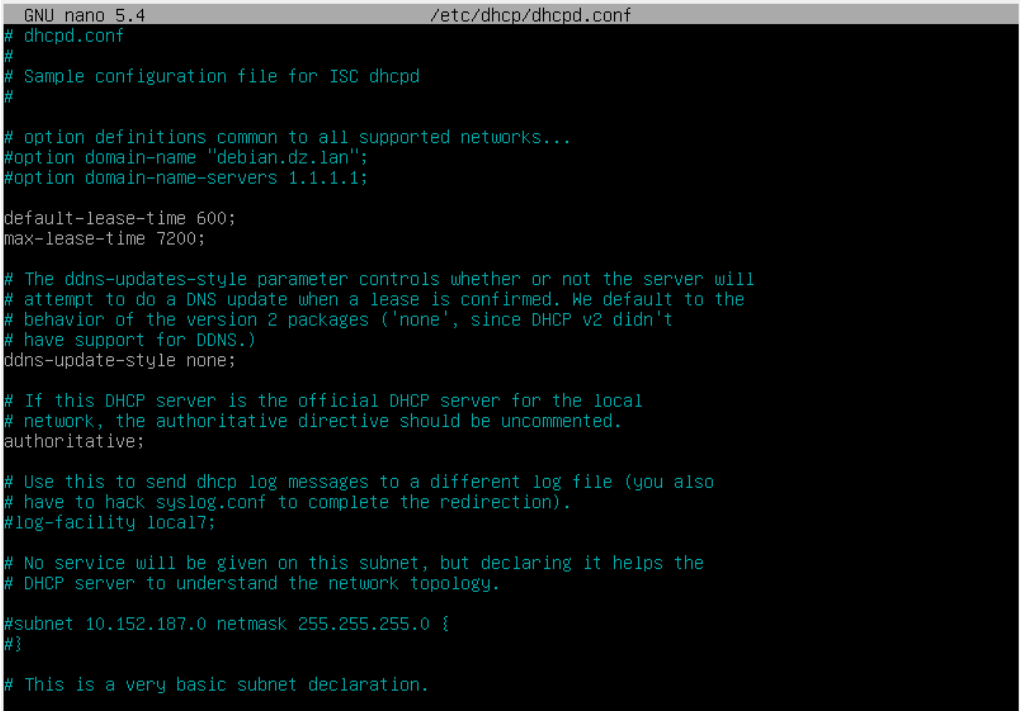
```
  GNU nano 5.4                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

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 dhcp
iface enp0s3 inet static
        address 172.16.2.1
        netmask 255.255.255.128
```

Puis enregistrer

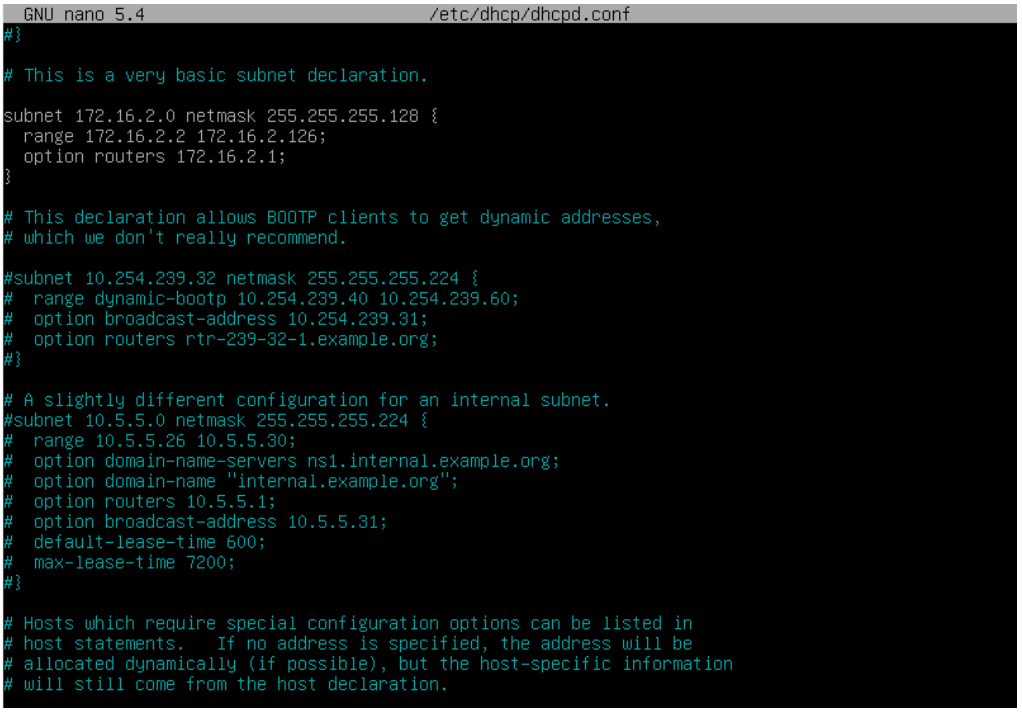
Le reste de la configuration se passera dans un seul est même fichier qui est :

nano /etc/dhcp/dhcpd.conf

→ il suffit de compléter, dé-commenter ou commenter certaines lignes de façon à obtenir un fichier de configuration similaire à la capture d'écran.



```
  GNU nano 5.4                              /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
#option domain-name "debian.dz.lan";
#option domain-name-servers 1.1.1.1;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.
```



```
  GNU nano 5.4                              /etc/dhcp/dhcpd.conf
#}

# This is a very basic subnet declaration.

subnet 172.16.2.0 netmask 255.255.255.128 {
  range 172.16.2.2 172.16.2.126;
  option routers 172.16.2.1;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
#  option domain-name "internal.example.org";
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.
```

Puis enregistrer

il ne reste plus qu'à rallumer le DHCP :
systemctl restart isc-dhcp-server

3- Test du serveur DHCP avec une autre machine virtuelle en debian.

→ Pour cela il faut la machine debian configurer avec le serveur DHCP ainsi qu'une machine avec un debian qui servira de client.

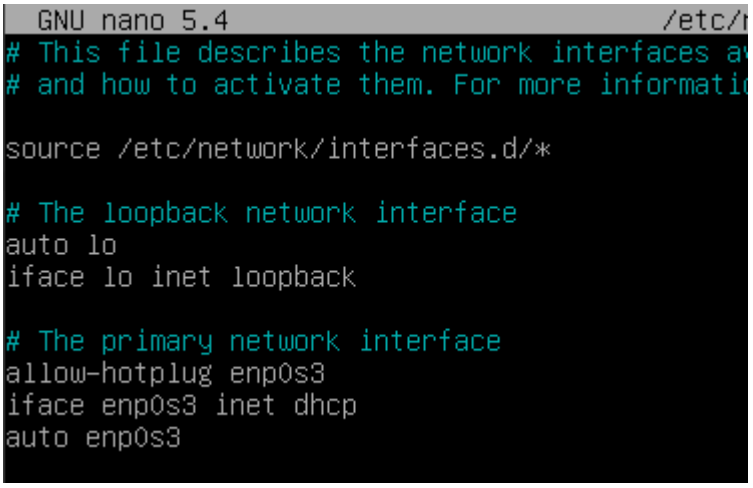
→ Dans la configuration des 2 machines virtualbox :

- Aller dans l'onglet réseau.
- Puis sélectionner le mode d'accès réseau : Réseau interne.
- Name : intnet.

Une fois celà effectué, il faut se rendre sur la machine virtuelle qui sert de client.

nano /etc/network/interfaces Permet d'ouvrir le fichier qui contient l'interface de réseau de la machine.

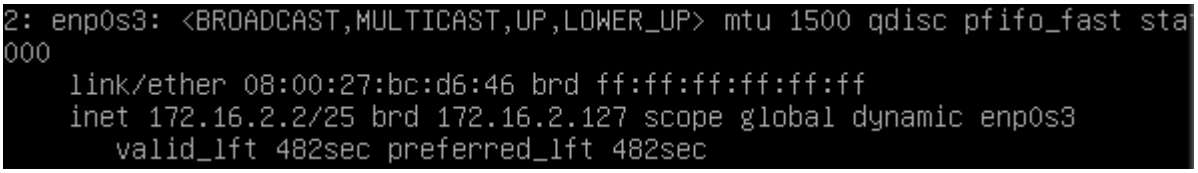
→ ajouter les lignes manquantes pour que le fichier ressemble à celui là:



Puis enregistrer

systemctl restart networking

ip a Vérifier que l'ip obtenu sur la machine client correspond à la plage donner au serveur DHCP



4- Changer le nom de l'hôte sous debian.

Pour changer le nom de l'hôte, il suffit d'effectuer la commande suivante :

→ hostnamectl set-hostname "new_hostname"

Exemple : hostnamectl set-hostname "LOLEsport"