

## Configuration réseau avec VirtualBox

8 novembre 2025

### Description

Ce tutoriel explique pas à pas comment configurer une machine Debian/Linux en tant que passerelle réseau dans VirtualBox, permettant à deux clients situés sur des réseaux différents (un en mode pont et un en réseau privé hôte) de communiquer entre eux.

---

## Table des matières

---

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Qu'est-ce qu'une passerelle réseau ?	3
1.2	Architecture du projet	3
1.3	Prérequis	3
<b>2</b>	<b>Importation des machines virtuelles</b>	<b>4</b>
2.1	Étape 1 : Ouverture de VirtualBox	4
2.2	Étape 2 : Sélection du fichier .ova	4
2.3	Étape 3 : Choix du fichier client1.ova	5
2.4	Étape 4 : Configuration du nom et des adresses MAC	6
<b>3</b>	<b>Configuration réseau des machines virtuelles</b>	<b>7</b>
3.1	Étape 5 : Accès à la configuration de la passerelle	7
3.2	Étape 6 : Activation du mode expert	7
3.3	Étape 7 : Accès aux paramètres réseau	8
3.4	Étape 8 : Configuration de l'adaptateur 1	8
3.5	Étape 9 : Configuration de l'adaptateur 2	9
3.6	Étape 10 : Configuration réseau du Client 1	10
3.7	Étape 11 : Configuration réseau du Client 2	11
<b>4</b>	<b>Configuration de la passerelle Debian</b>	<b>12</b>
4.1	Étape 12 : Démarrage de la passerelle	12
4.2	Étape 13 : Ajustement de l'affichage	13
4.3	Étape 14 : Édition du fichier interfaces	14
4.4	Étape 15 : Configuration des interfaces réseau	14
4.5	Étape 16 : Sauvegarde et redémarrage du réseau	15
4.6	Étape 17 : Vérification des adresses IP	16
4.7	Étape 18 : Activation du routage IP	16
4.8	Étape 19 : Recherche du paramètre ip_forward	17
4.9	Étape 20 : Activation du forwarding	17
4.10	Étape 21 : Désactivation du pare-feu	18
4.11	Étape 22 : Extinction de la passerelle	19
<b>5</b>	<b>Configuration du Client 1</b>	<b>20</b>
5.1	Étape 23 : Démarrage du Client 1	20
5.2	Étape 24 : Configuration en DHCP	20
5.3	Étape 25 : Redémarrage du réseau	21
5.4	Étape 26 : Vérification et ajout de route	21
<b>6</b>	<b>Configuration du Client 2</b>	<b>23</b>
6.1	Étape 27 : Démarrage du Client 2	23
6.2	Étape 28 : Édition du fichier interfaces	23
6.3	Étape 29 : Configuration IP statique	24
6.4	Étape 30 : Redémarrage du réseau	25
6.5	Étape 31 : Vérification de la configuration	25
6.6	Étape 32 : Ajout de la route vers le réseau pont	26

---

<b>7</b>	<b>Tests de connectivité</b>	<b>27</b>
7.1	Étape 33 : Redémarrage de la passerelle . . . . .	27
7.2	Étape 34 : Test depuis Client 2 vers Client 1 . . . . .	27
7.3	Étape 35 : Test depuis Client 1 vers Client 2 . . . . .	28
<b>8</b>	<b>Conclusion</b>	<b>29</b>
8.1	Récapitulatif . . . . .	29
8.2	Ce qui a été accompli . . . . .	29
8.3	Schéma récapitulatif . . . . .	29
8.4	Points clés à retenir . . . . .	29
8.5	Pour aller plus loin . . . . .	29


## 1 Introduction


### 1.1 Qu'est-ce qu'une passerelle réseau ?


Une passerelle réseau (gateway) est un équipement ou un système qui permet de faire le lien entre deux réseaux distincts. Elle route les paquets d'un réseau vers un autre, permettant ainsi aux machines de réseaux différents de communiquer entre elles.

### 1.2 Architecture du projet

Dans ce tutoriel, nous allons mettre en place trois machines virtuelles dans VirtualBox :

 **Client 1** : Machine connectée en mode *Accès par pont* (bridge), qui lui permet d'accéder au réseau local physique et d'obtenir une adresse IP via DHCP.

 **Client 2** : Machine connectée en mode *Réseau privé hôte*, isolée du réseau externe et configurée avec une IP statique.

 **Passerelle Debian** : Machine équipée de deux interfaces réseau :

- Une interface connectée au réseau pont (comme Client 1)
- Une interface connectée au réseau privé hôte (comme Client 2)

#### Information

L'objectif est de configurer la passerelle Debian pour qu'elle puisse router le trafic entre ces deux réseaux, permettant ainsi aux Client 1 et Client 2 de communiquer.

### 1.3 Prérequis

- ✓ VirtualBox installé sur votre machine hôte
- ✓ Les fichiers .ova pour les trois machines virtuelles (client1, client2, passerelle)
- ✓ Connaissances de base en ligne de commande Linux

## 2 Importation des machines virtuelles

### 2.1 Étape 1 : Ouverture de VirtualBox

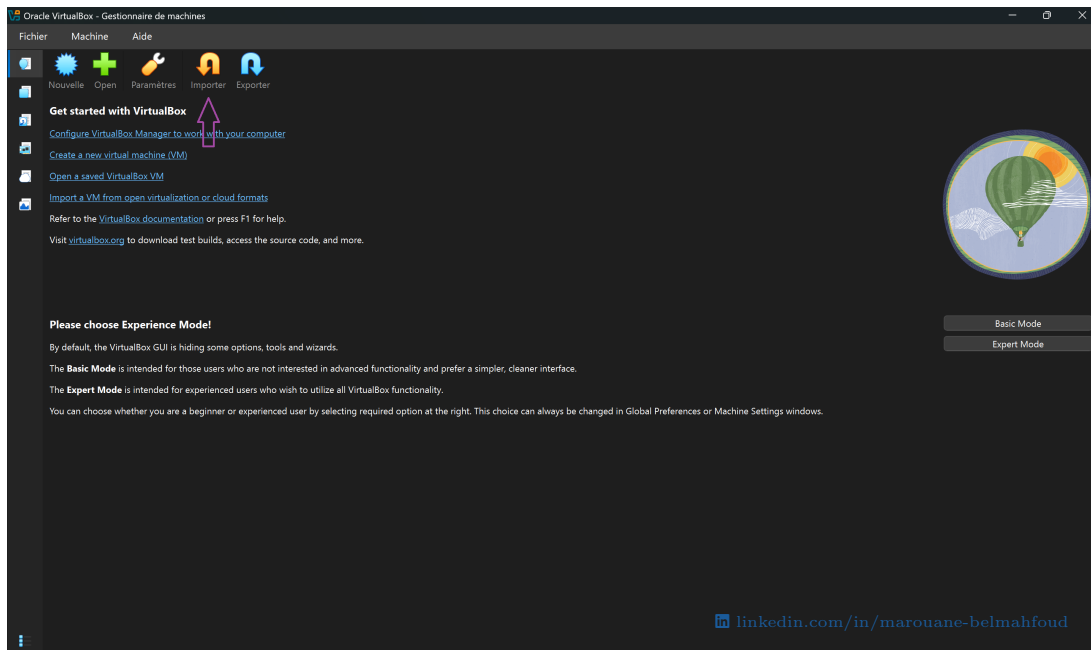


FIGURE 1 – Screen 0 – Page d'accueil de VirtualBox

Lancez VirtualBox. Vous arrivez sur la page d'accueil du logiciel. Pour importer les machines virtuelles préconfigurées, cliquez sur le bouton **Importer** dans la barre d'outils ou via le menu *Fichier* > *Importer*.

### 2.2 Étape 2 : Sélection du fichier .ova

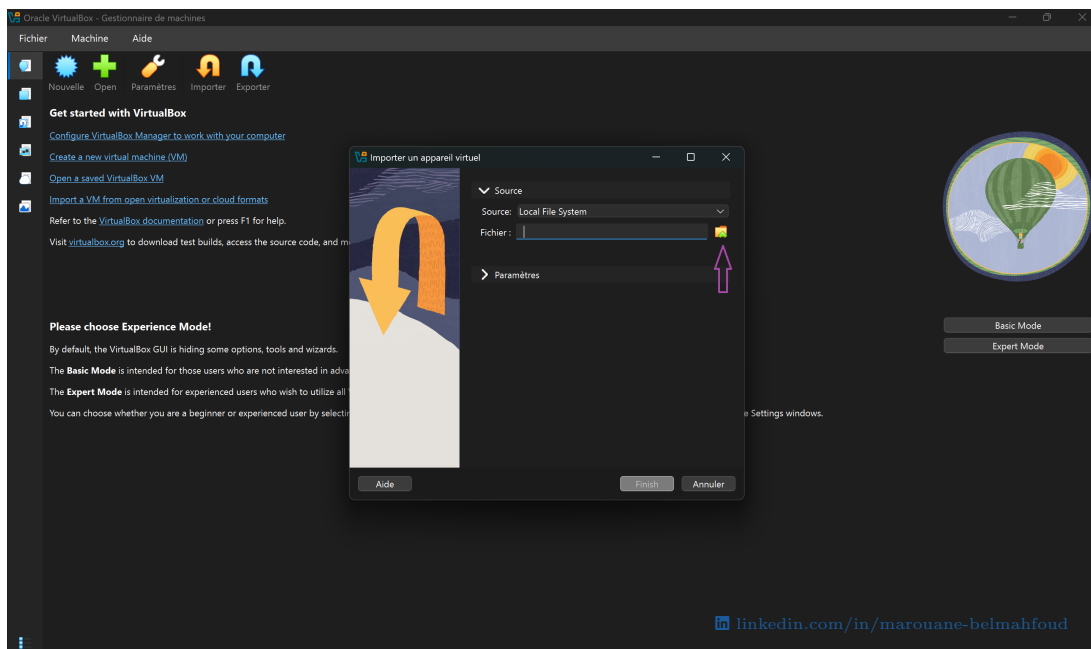


FIGURE 2 – Screen 1 – Fenêtre d'importation

Une fenêtre d'importation s'ouvre. Cliquez sur l'icône de dossier jaune à droite du champ pour parcourir vos fichiers et sélectionner le fichier .ova de la première machine virtuelle.

### 2.3 Étape 3 : Choix du fichier client1.ova

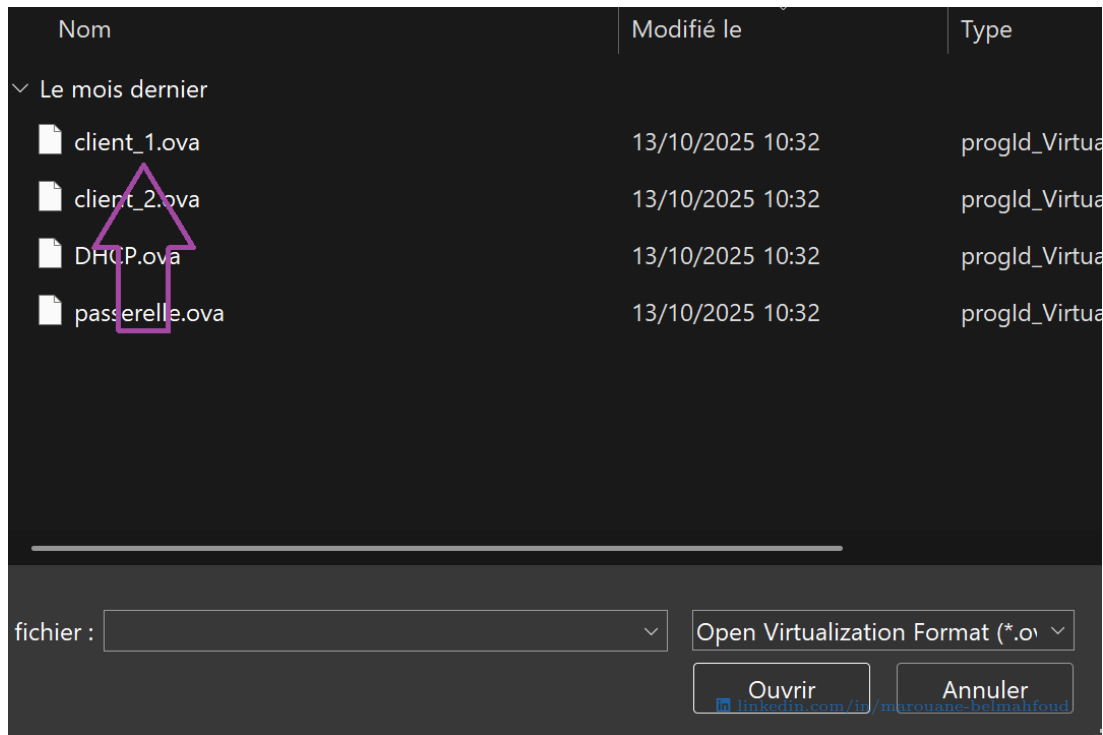


FIGURE 3 – Screen 2 – Sélection du fichier client1.ova

Dans le gestionnaire de fichiers, naviguez jusqu'au dossier contenant vos fichiers .ova et sélectionnez **client1.ova**. Cliquez sur **Ouvrir** pour continuer.

#### ⚠ Attention

Vous devrez répéter cette procédure d'importation pour les trois machines : client1, client2 et passerelle.

## 2.4 Étape 4 : Configuration du nom et des adresses MAC

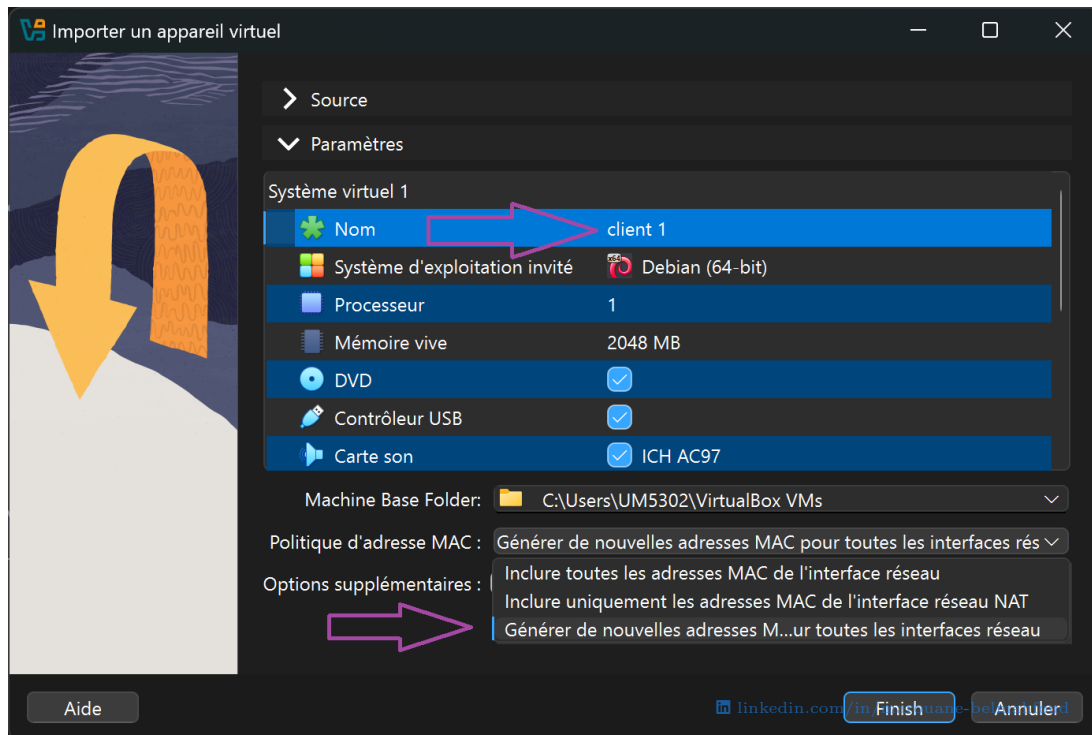


FIGURE 4 – Screen 3 – Paramètres d'importation

Avant de finaliser l'importation :

1. Dans le champ **Nom**, renommez la machine en **client1** (si ce n'est pas déjà fait).
2. Dans le menu déroulant **Politique d'adresse MAC**, sélectionnez l'option : « *Générer de nouvelles adresses MAC pour toutes les interfaces réseau* »

Cette option est importante pour éviter les conflits d'adresses MAC si plusieurs machines sont importées à partir du même fichier .ova.

Cliquez sur **Importer** pour finaliser l'importation de client1.

### ⚠ Attention

Répétez les étapes 1 à 4 pour importer client2.ova et passerelle.ova.

## 3 Configuration réseau des machines virtuelles

### 3.1 Étape 5 : Accès à la configuration de la passerelle

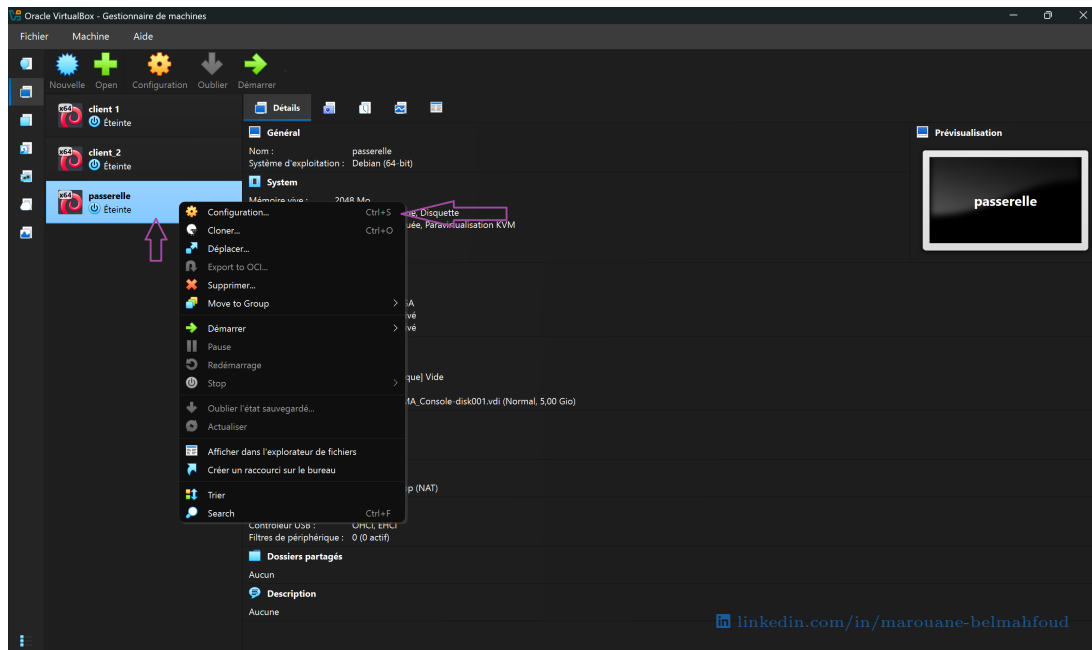


FIGURE 5 – Screen 4 – Accès aux paramètres

Une fois les trois machines importées, faites un clic droit sur la machine **passerelle** dans la liste, puis sélectionnez **Configuration**.

### 3.2 Étape 6 : Activation du mode expert

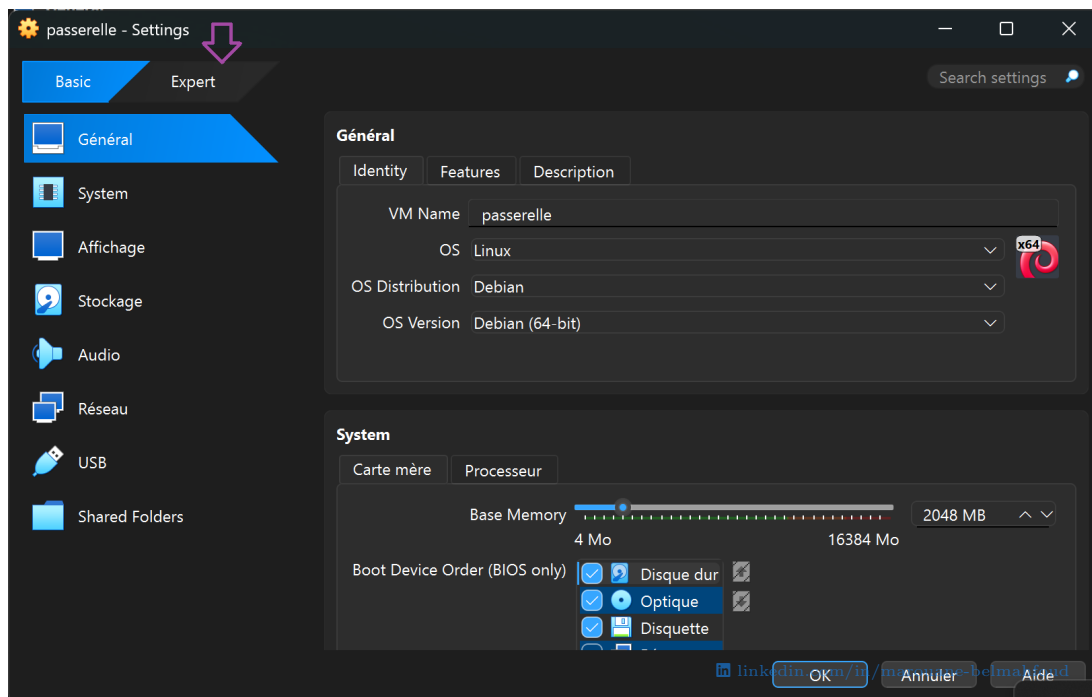


FIGURE 6 – Screen 5 – Fenêtre de configuration

Dans la fenêtre de configuration, cliquez sur le bouton **Mode Expert** en bas de la fenêtre. Ce mode permet d'accéder à tous les paramètres avancés de la machine virtuelle.

### 3.3 Étape 7 : Accès aux paramètres réseau

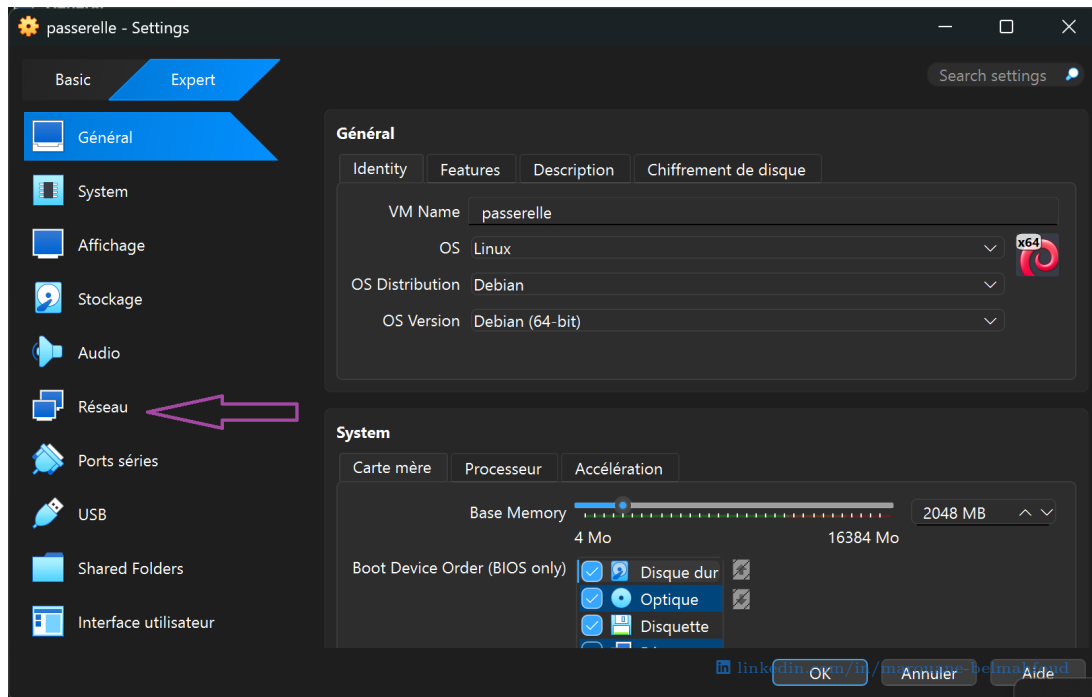


FIGURE 7 – Screen 6 – Onglet Réseau

Dans le menu latéral gauche, cliquez sur l'onglet **Réseau**. Vous allez maintenant configurer les deux adaptateurs réseau de la passerelle.

### 3.4 Étape 8 : Configuration de l'adaptateur 1

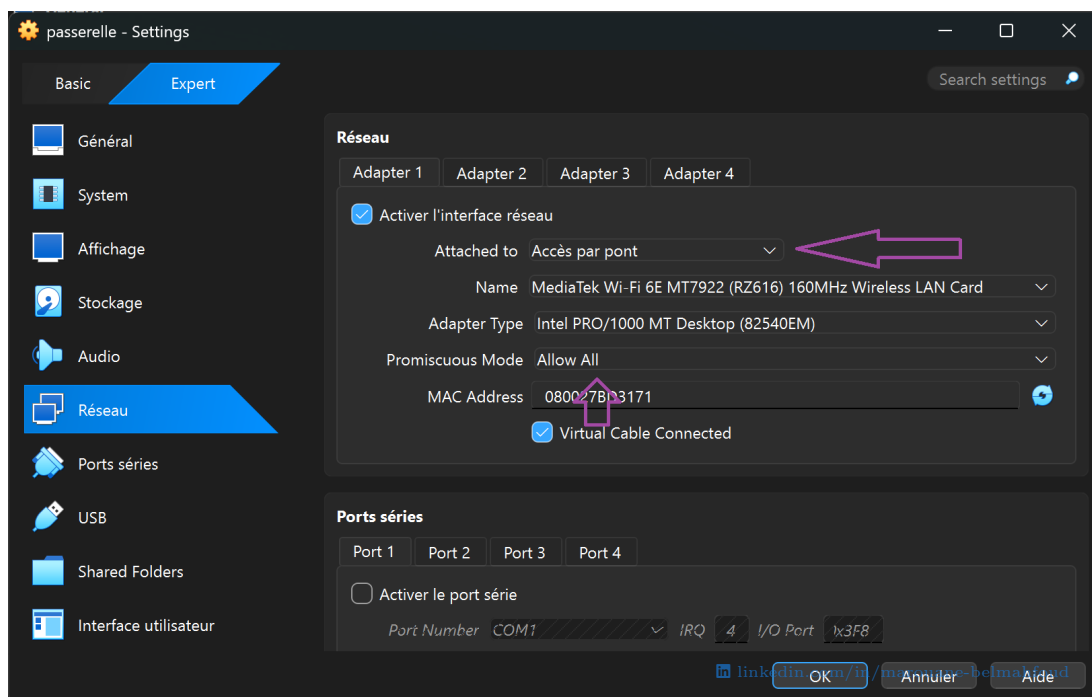


FIGURE 8 – Screen 7 – Configuration de l'adaptateur 1

Sur l'onglet **Adaptateur 1** :

1. Cochez **Activer l'interface réseau** (si ce n'est pas déjà fait)

2. Dans le menu déroulant **Attaché à**, sélectionnez **Accès par pont**
3. Dans **Mode promiscuité**, sélectionnez **Allow All**

### **i** Information

L'adaptateur 1 sera connecté au réseau physique local via le mode pont, permettant à la passerelle d'obtenir une IP sur le même réseau que votre machine hôte.

## 3.5 Étape 9 : Configuration de l'adaptateur 2

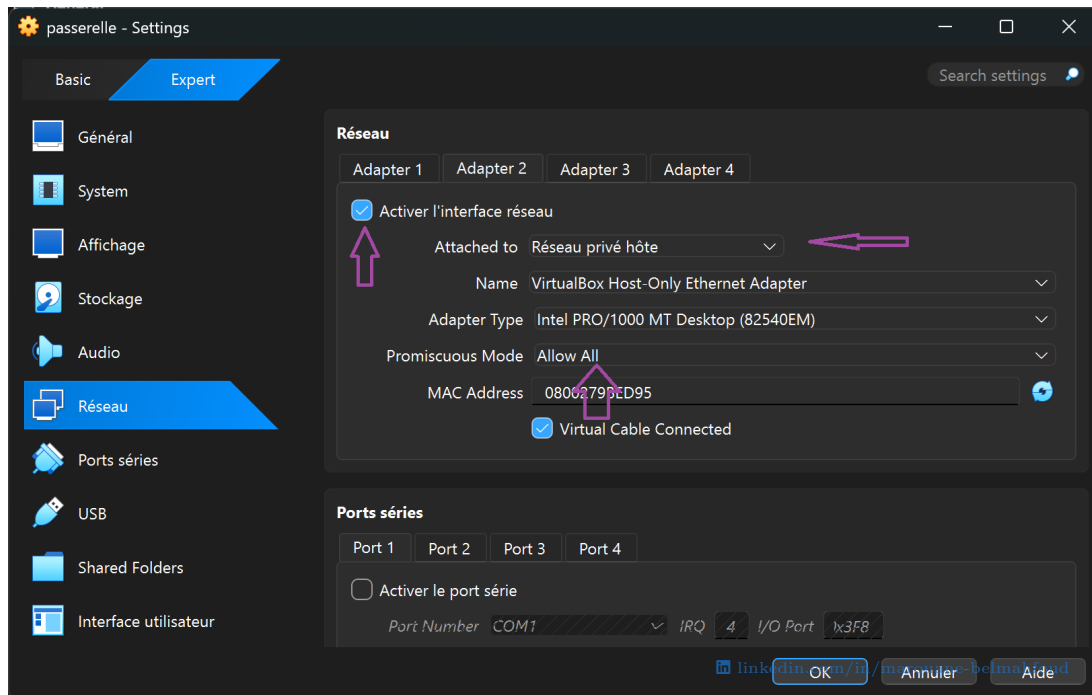


FIGURE 9 – Screen 8 – Configuration de l'adaptateur 2

Passez à l'onglet **Adaptateur 2** :

1. Cochez **Activer l'interface réseau**
2. Dans **Attaché à**, sélectionnez **Réseau privé hôte**
3. Dans **Mode promiscuité**, sélectionnez **Allow All**

### **i** Information

L'adaptateur 2 sera connecté au réseau privé hôte, créant un réseau isolé entre la passerelle et le client2.

### **A** Attention

La passerelle doit avoir deux adaptateurs réseau pour faire le lien entre les deux réseaux.

### 3.6 Étape 10 : Configuration réseau du Client 1

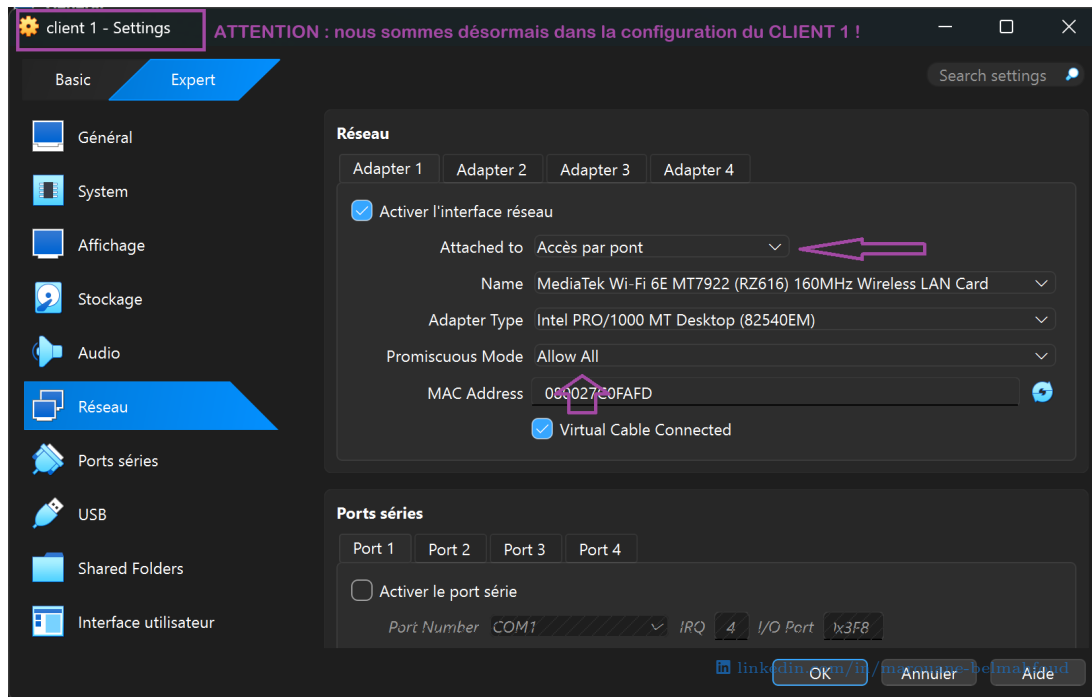


FIGURE 10 – Screen 9 – Configuration réseau de Client 1

Faites un clic droit sur **client1** ; **Configuration** ; **Réseau** :

1. Sur l'adaptateur 1, sélectionnez **Accès par pont**
2. Mode promiscuité : **Allow All**
3. Ne touchez pas à l'adaptateur 2 (il doit rester désactivé)

#### **i** Information

Client 1 sera sur le même réseau que l'adaptateur 1 de la passerelle (réseau pont).

### 3.7 Étape 11 : Configuration réseau du Client 2

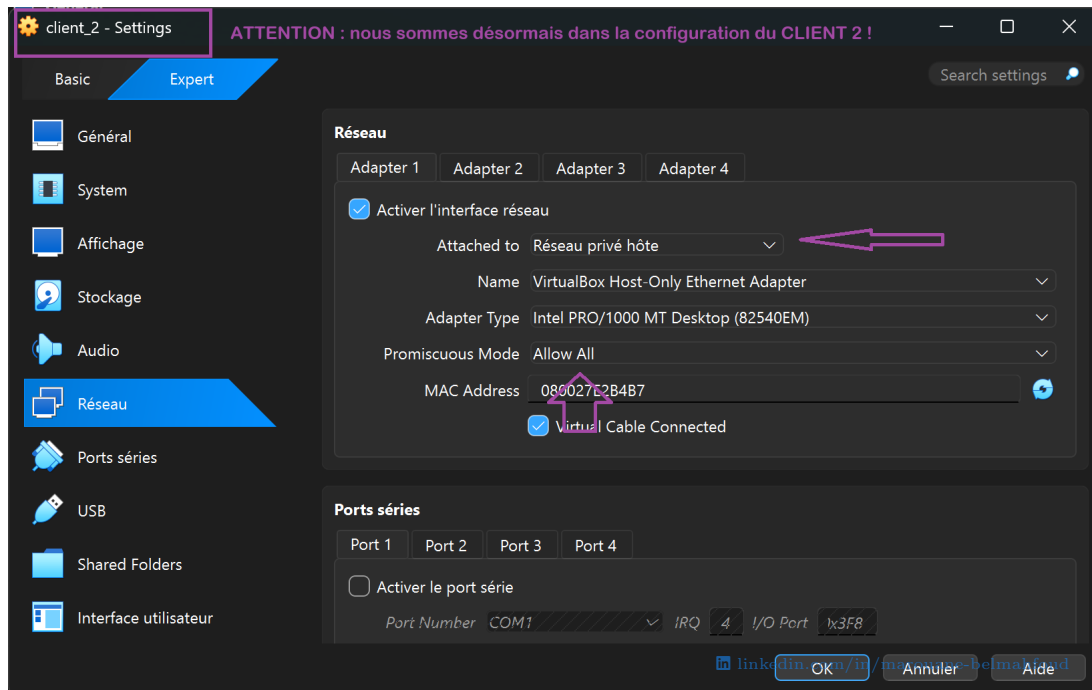


FIGURE 11 – Screen 10 – Configuration réseau de Client 2

Faites un clic droit sur **client2** ↵ **Configuration** ↵ **Réseau** :

1. Sur l'adaptateur 1, sélectionnez **Réseau privé hôte**
2. Mode promiscuité : **Allow All**

#### **i** Information

Client 2 sera sur le même réseau que l'adaptateur 2 de la passerelle (réseau privé).

Cliquez sur **OK** pour valider toutes les configurations.

## 4 Configuration de la passerelle Debian

### 4.1 Étape 12 : Démarrage de la passerelle

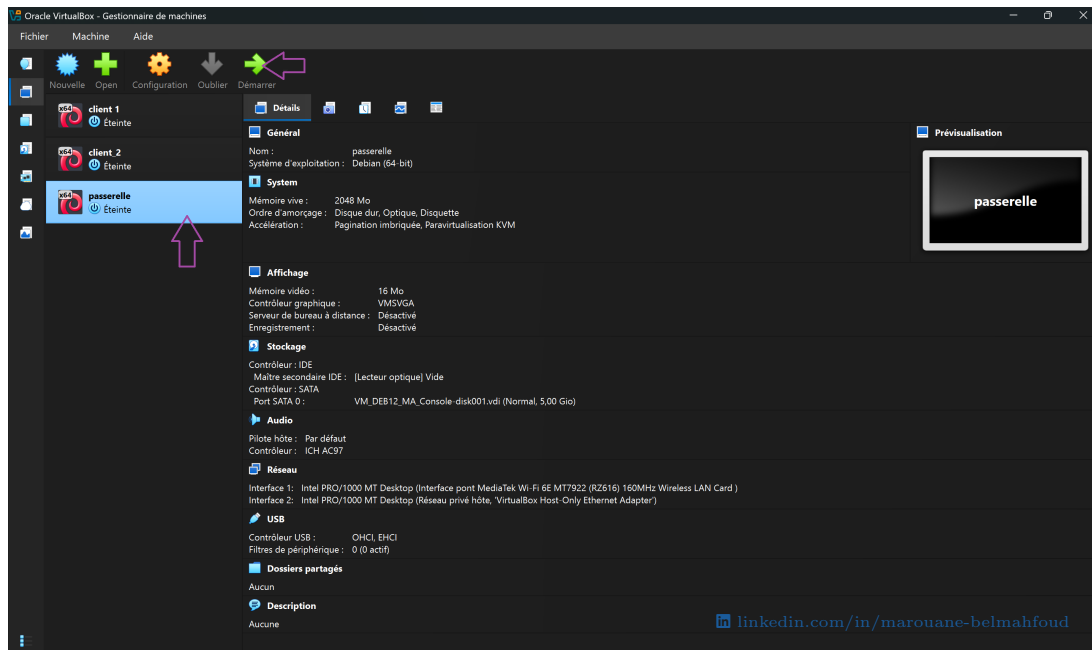


FIGURE 12 – Screen 11 – Démarrage de la VM

Sélectionnez la machine **Passerelle** dans la liste, puis cliquez sur le bouton **Démarrer** (flèche verte) dans la barre d'outils.

## 4.2 Étape 13 : Ajustement de l'affichage

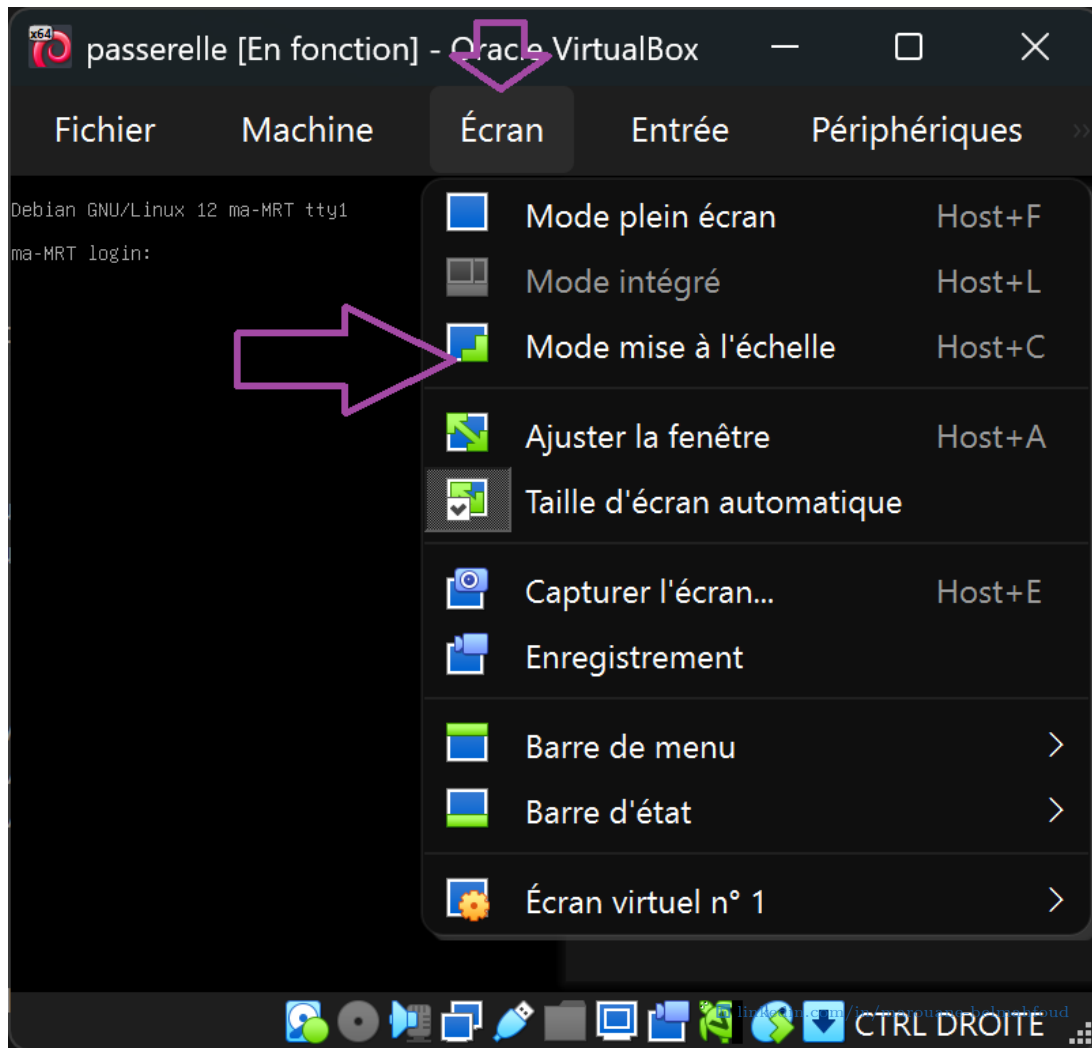


FIGURE 13 – Screen 12 – Mode mise à l'échelle

Une fois la machine démarrée, allez dans le menu **Affichage**  $\downarrow$  **Mode mise à l'échelle** pour agrandir la fenêtre et faciliter la lecture.

### 4.3 Étape 14 : Édition du fichier interfaces

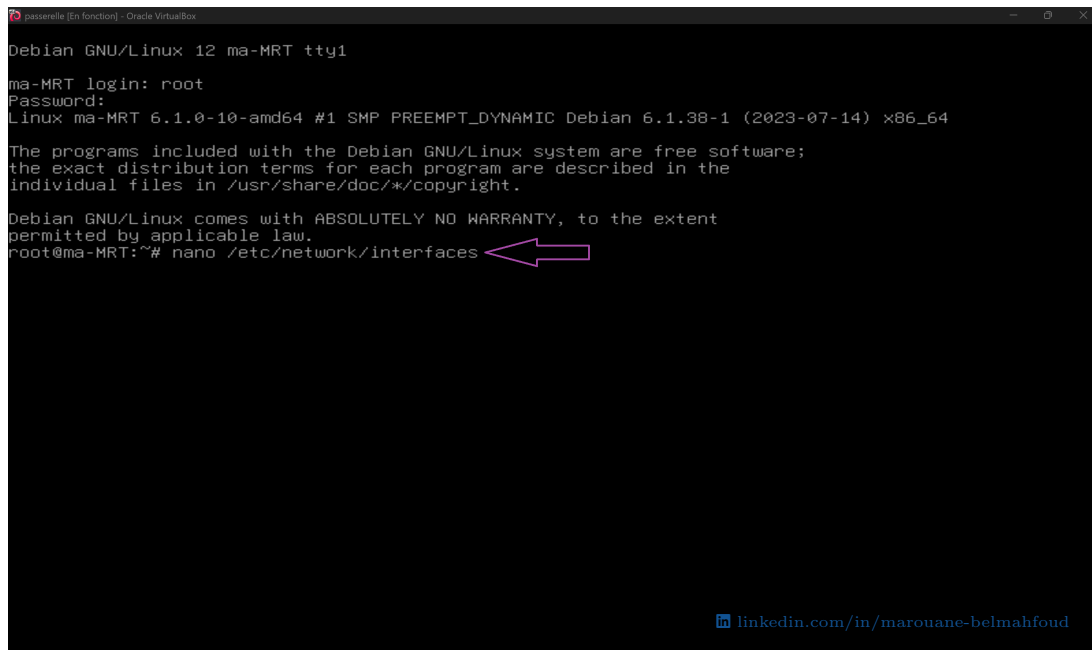


FIGURE 14 – Screen 13 – Commande nano

Connectez-vous à la machine (identifiant et mot de passe fournis avec la VM), puis ouvrez le fichier de configuration réseau :

```
sudo nano /etc/network/interfaces
```

### 4.4 Étape 15 : Configuration des interfaces réseau

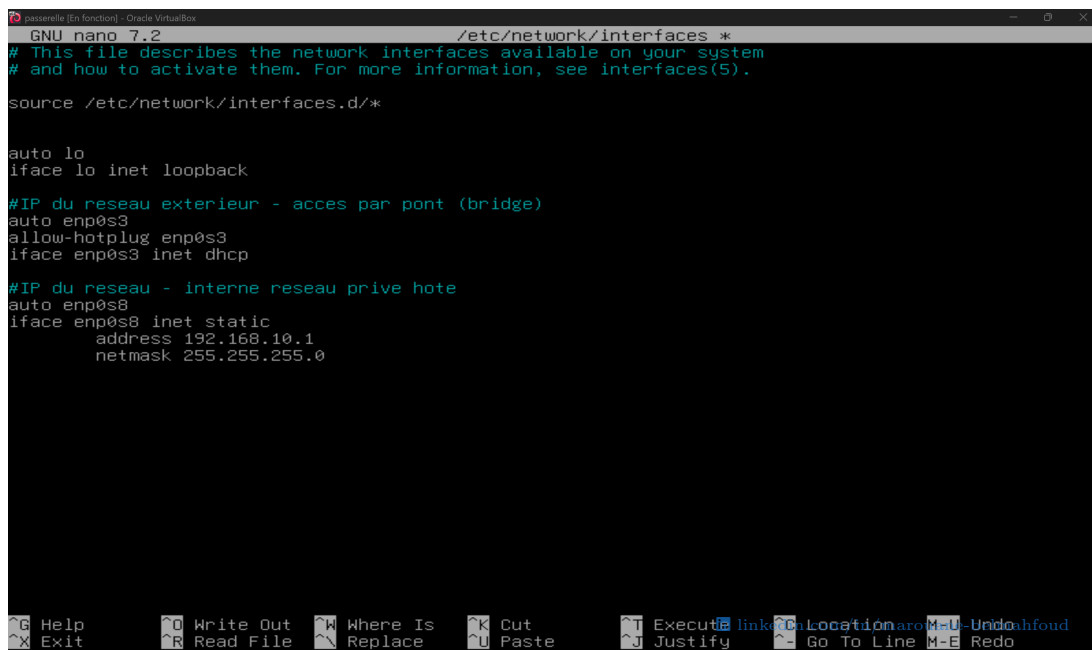


FIGURE 15 – Screen 14 – Contenu du fichier interfaces

Dans le fichier ouvert, configurez les deux interfaces réseau :  
**Interface enp0s3 (réseau pont) :**

```
auto enp0s3
iface enp0s3 inet dhcp
```

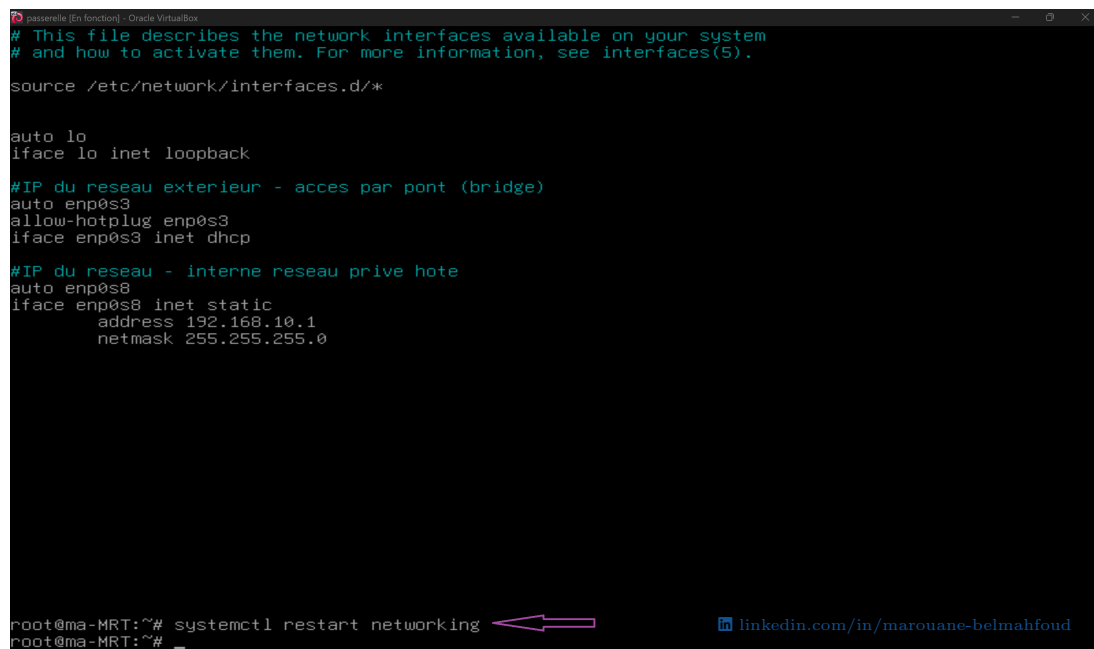
Interface **enp0s8** (réseau privé hôte) :

```
auto enp0s8
iface enp0s8 inet static
address 192.168.10.1
netmask 255.255.255.0
```

### **i** Information

**enp0s3** obtient automatiquement une IP via DHCP sur le réseau pont  
**enp0s8** a une IP fixe (192.168.10.1) sur le réseau privé

## 4.5 Étape 16 : Sauvegarde et redémarrage du réseau



```
passerelle [En fonction] - Oracle VirtualBox
# 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/*

auto lo
iface lo inet loopback

#IP du reseau exterieur - acces par pont (bridge)
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet dhcp

#IP du reseau - interne reseau prive hote
auto enp0s8
iface enp0s8 inet static
    address 192.168.10.1
    netmask 255.255.255.0

root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# _
```

FIGURE 16 – Screen 15 – Sauvegarde et redémarrage

Sauvegardez le fichier avec **Ctrl+O**, puis quittez avec **Ctrl+X**.  
Redémarrez le service réseau pour appliquer les changements :

```
sudo systemctl restart networking
```

## 4.6 Étape 17 : Vérification des adresses IP

```

root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# 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:bd:31:71 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.66/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86378sec preferred_lft 86378sec
    inet6 2001:861:62:dcc0:a00:27ff:febd:3171/64 scope global dynamic mngtmpaddr
        valid_lft 86373sec preferred_lft 14373sec
    inet6 fe80::a00:27ff:febd:3171/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9b:ed:95 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe9b:ed95/64 scope link
        valid_lft forever preferred_lft forever
root@ma-MRT:~#

```

FIGURE 17 – Screen 16 – Commande ip a

Vérifiez que les interfaces ont bien reçu leurs adresses IP :

```
ip a
```

Vous devez voir :

- ✔ **enp0s3** : adresse IP obtenue via DHCP (ex : 192.168.1.66)
- ✔ **enp0s8** : adresse IP statique 192.168.10.1

## 4.7 Étape 18 : Activation du routage IP

```

root@ma-MRT:~# nano /etc/sysctl.conf

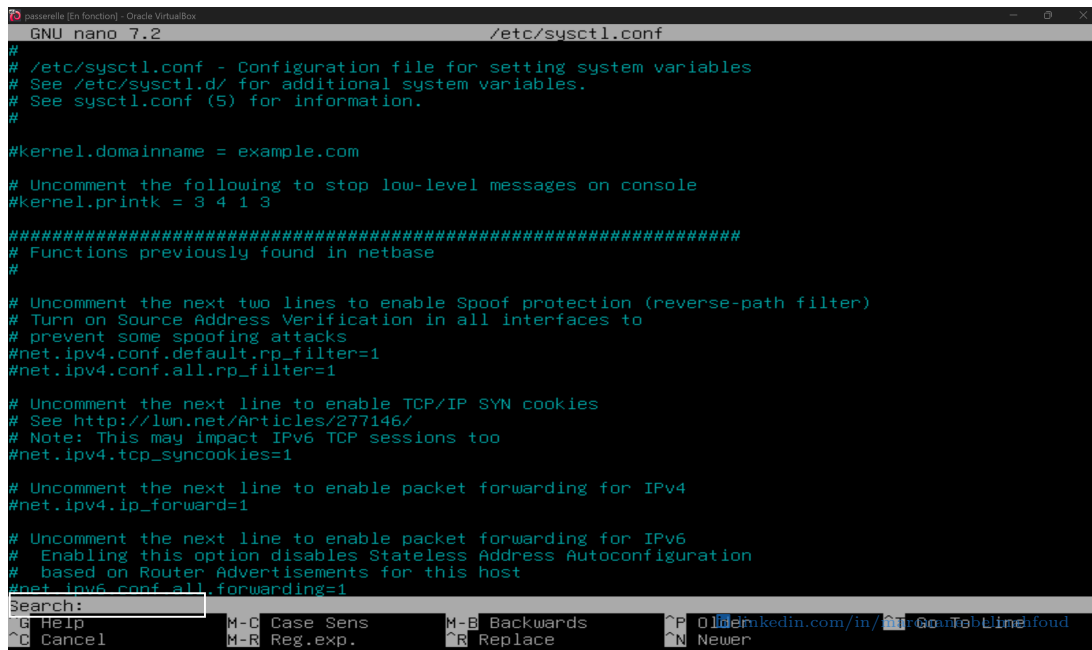
```

FIGURE 18 – Screen 19 – Édition de sysctl.conf

Pour que la passerelle puisse router les paquets entre les deux réseaux, il faut activer le forwarding IP. Ouvrez le fichier de configuration système :

```
sudo nano /etc/sysctl.conf
```

## 4.8 Étape 19 : Recherche du paramètre ip\_forward



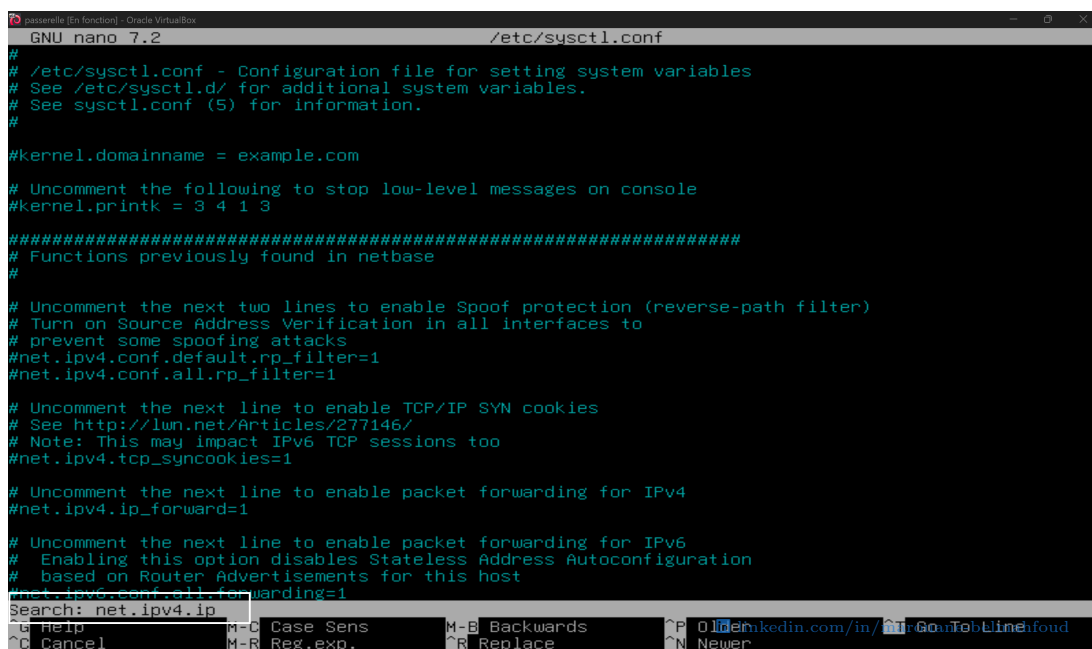
```
GNU nano 7.2 /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
search:
^G Help      M-C Case Sens  M-B Backwards  ^P linkedin.com/in/marouane-belmahfoud
^C Cancel    M-R Reg.exp.     ^R Replace      ^N Newer
```

FIGURE 19 – Screen 20 – Ligne net.ipv4.ip\_forward

Dans le fichier, recherchez la ligne suivante (utilisez Ctrl+W pour chercher) :

```
#net.ipv4.ip_forward=1
```

## 4.9 Étape 20 : Activation du forwarding



```
GNU nano 7.2 /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
search: net.ipv4.ip
^G Help      M-C Case Sens  M-B Backwards  ^P linkedin.com/in/marouane-belmahfoud
^C Cancel    M-R Reg.exp.     ^R Replace      ^N Newer
```

FIGURE 20 – Screen 21 – Décommenter la ligne

Décommentez cette ligne en retirant le symbole # au début :

```
net.ipv4.ip_forward=1
```

Sauvegardez avec `Ctrl+O` et quittez avec `Ctrl+X`.

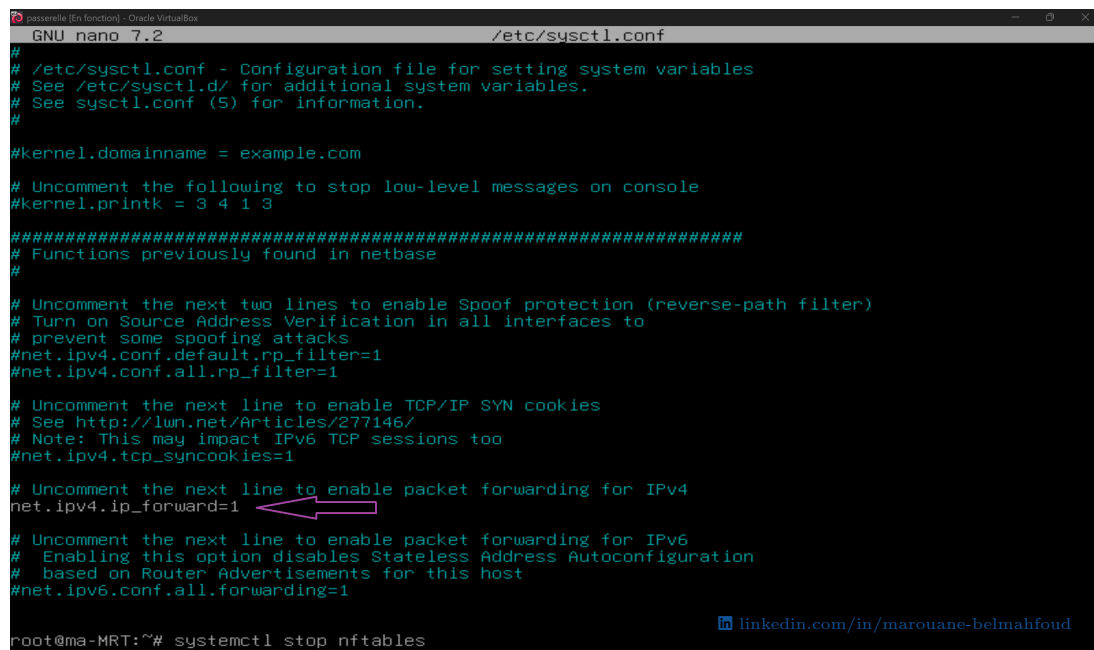
### ⚠ Attention

Cette étape est cruciale. Sans l'activation du forwarding IP, la passerelle ne pourra pas transférer les paquets entre les deux réseaux.

Appliquez immédiatement la modification :

```
sudo sysctl -p
```

## 4.10 Étape 21 : Désactivation du pare-feu



```
GNU nano 7.2 /etc/sysctl.conf
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf(5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
#####
root@ma-MRT:~# systemctl stop nftables
```

FIGURE 21 – Screen 22 – Arrêt de nftables

Pour faciliter les tests, désactivez temporairement le pare-feu :

```
sudo systemctl stop nftables
```

### ⚠ Attention

Dans un environnement de production, vous devriez configurer iptables ou nftables pour sécuriser votre passerelle

## 4.11 Étape 22 : Extinction de la passerelle

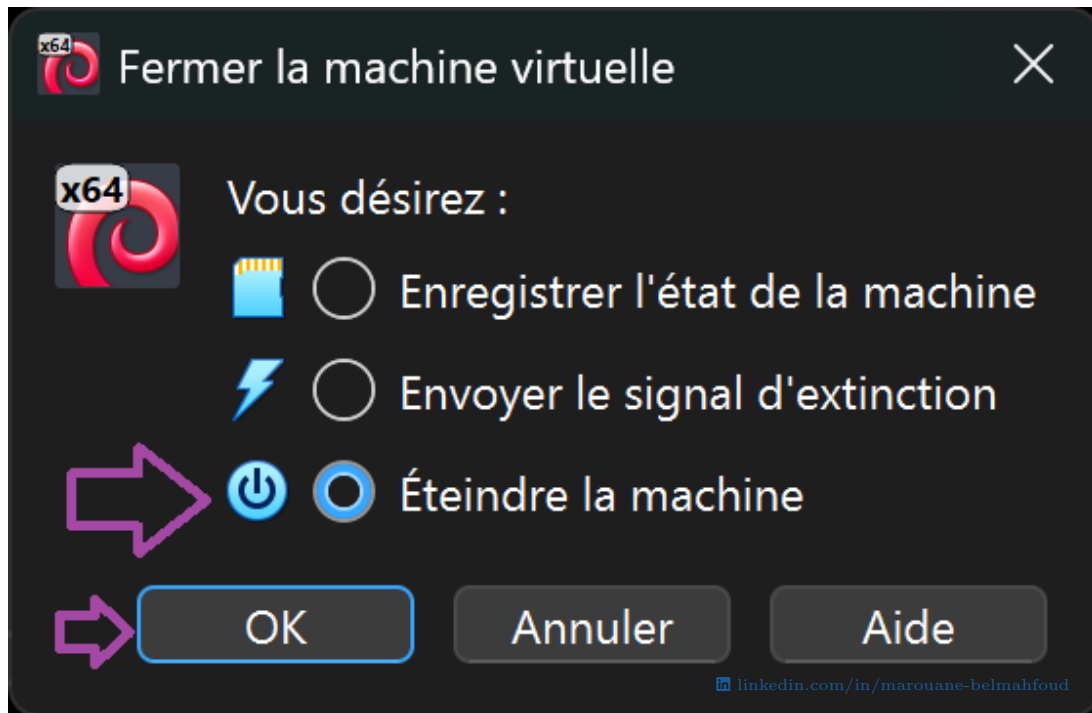


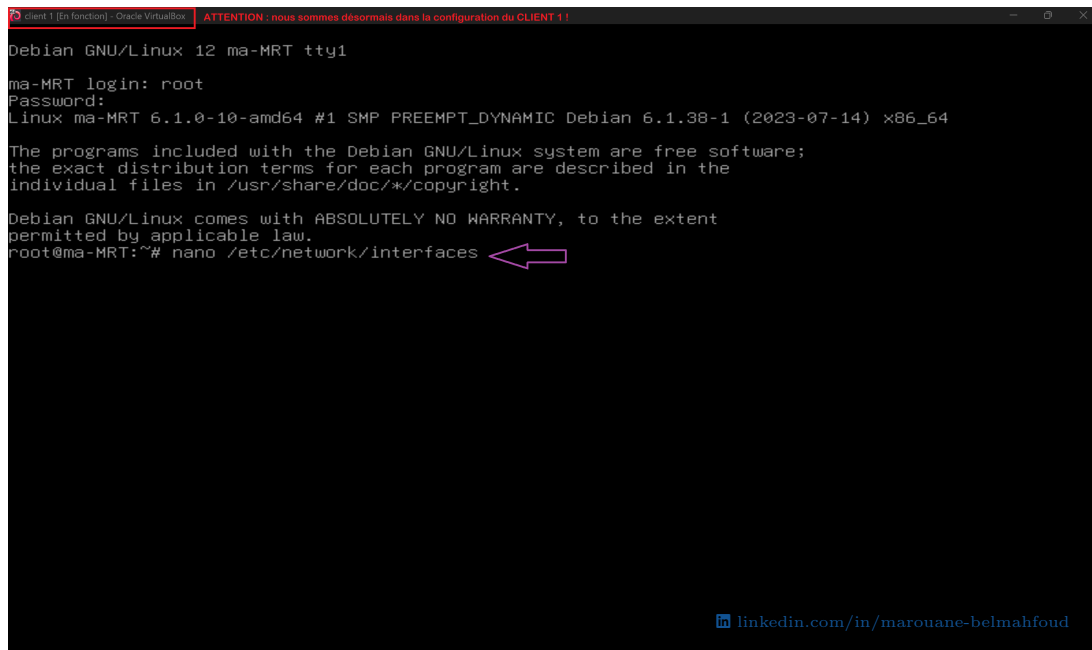
FIGURE 22 – Screen 23 – Extinction de la VM

Éteignez proprement la machine passerelle :

- Cliquez sur le bouton de fermeture de la fenêtre
- Sélectionnez **Éteindre la machine**
- Cliquez sur **OK**

## 5 Configuration du Client 1

### 5.1 Étape 23 : Démarrage du Client 1



```
client1 [En fonction] - Oracle VirtualBox ATTENTION : nous sommes désormais dans la configuration du CLIENT 1
Debian GNU/Linux 12 ma-MRT tty1
ma-MRT login: root
Password:
Linux ma-MRT 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

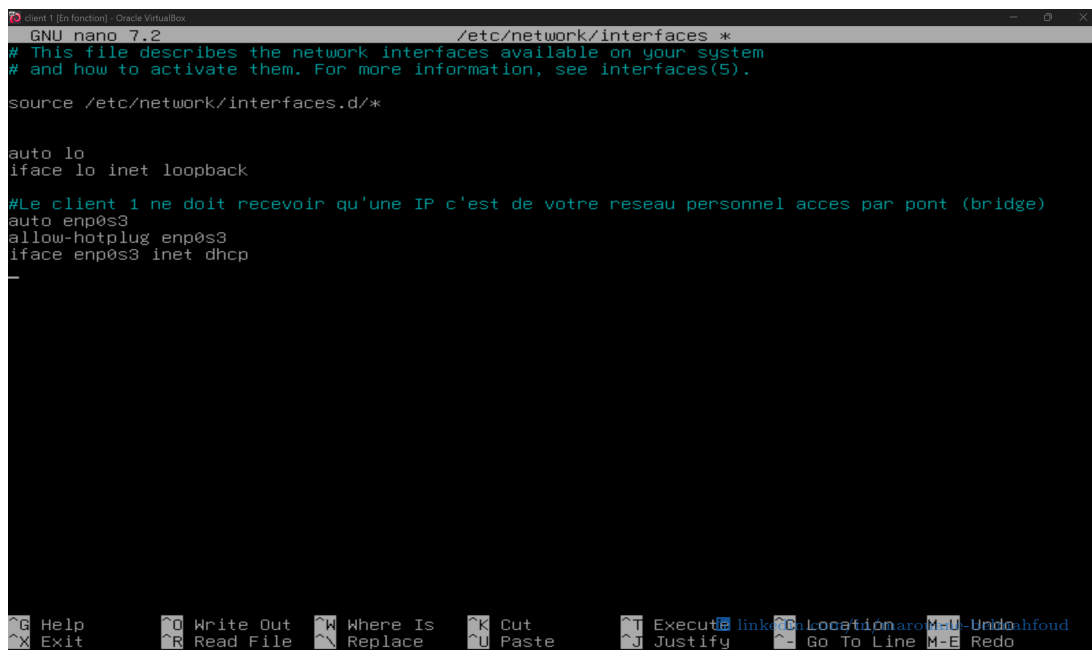
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ma-MRT:~# nano /etc/network/interfaces
```

FIGURE 23 – Screen 24 – Lancement de client1

Sélectionnez la machine **client1** et cliquez sur **Démarrer**.  
Connectez-vous, puis ouvrez le fichier de configuration réseau :

```
sudo nano /etc/network/interfaces
```

### 5.2 Étape 24 : Configuration en DHCP



```
GNU nano 7.2 /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/*

auto lo
iface lo inet loopback

#Le client 1 ne doit recevoir qu'une IP c'est de votre reseau personnel acces par pont (bridge)
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet dhcp
```

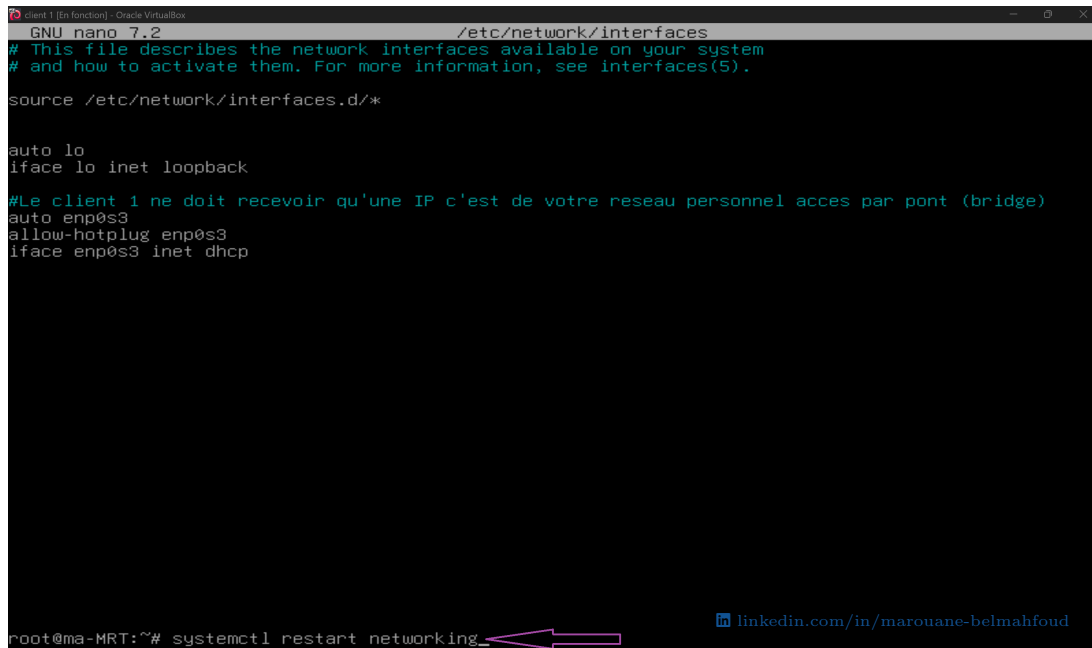
FIGURE 24 – Screen 25 – Configuration DHCP

Configurez l'interface réseau pour obtenir une IP automatiquement :

```
auto enp0s3
iface enp0s3 inet dhcp
```

Sauvegardez et quittez.

### 5.3 Étape 25 : Redémarrage du réseau



```
client 1 [En fonction] - Oracle VirtualBox
GNU nano 7.2 /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/*

auto lo
iface lo inet loopback

#Le client 1 ne doit recevoir qu'une IP c'est de votre reseau personnel acces par pont (bridge)
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet dhcp

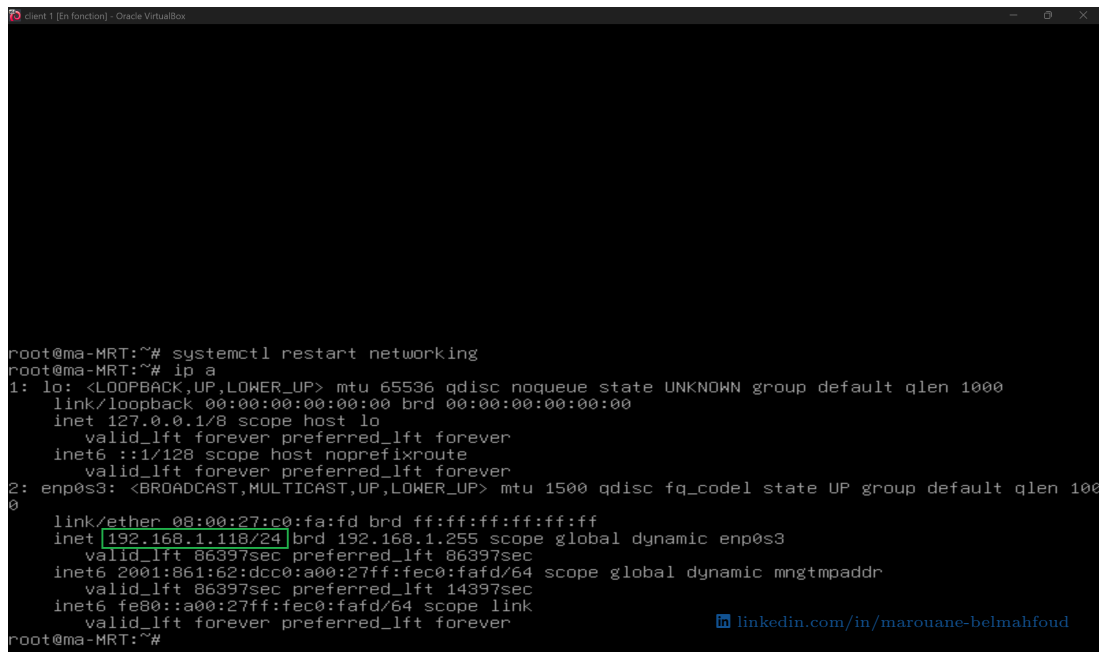
root@ma-MRT:~# systemctl restart networking_
```

FIGURE 25 – Screen 26 – Redémarrage réseau

Redémarrez le service réseau :

```
sudo systemctl restart networking
```

## 5.4 Étape 26 : Vérification et ajout de route



```
root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# 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:c0:fa:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.118/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86397sec preferred_lft 86397sec
    inet6 2001:861:62:dcc0:a00:27ff:fec0:fafd/64 scope global dynamic mngtmpaddr
        valid_lft 86397sec preferred_lft 14397sec
    inet6 fe80::a00:27ff:fec0:fafd/64 scope link
        valid_lft forever preferred_lft forever
root@ma-MRT:~#
```

FIGURE 26 – Screen 27 – Ajout de route statique

Vérifiez que l'adresse IP a été attribuée :

```
ip a
```

Vous devriez voir une adresse IP du type 192.168.1.118 (selon votre réseau).  
Ajoutez maintenant une route pour joindre le réseau privé via la passerelle :

```
sudo ip route add 192.168.10.0/24 via 192.168.1.66
```

### **i** Information

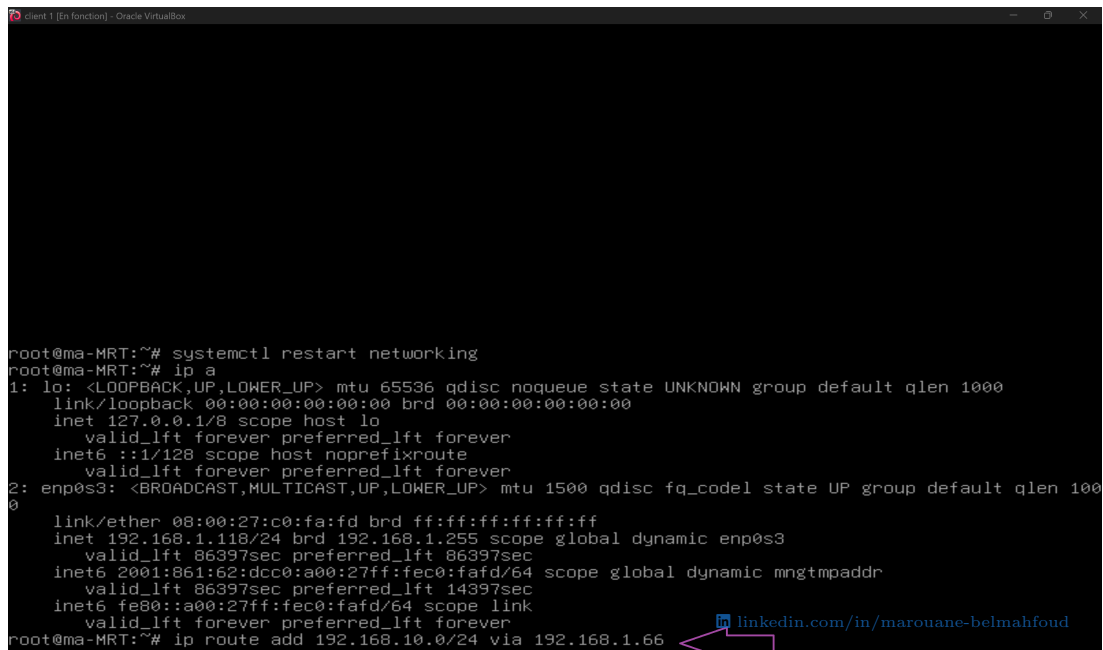
Cette commande indique au client1 que pour atteindre le réseau 192.168.10.0/24 (réseau privé où se trouve client2), il doit passer par l'adresse 192.168.1.66 (adresse de la passerelle sur le réseau pont).

### **!** Attention

Remplacez 192.168.1.66 par l'adresse IP réelle de votre passerelle sur le réseau pont (visible avec `ip a` sur la passerelle, interface `enp0s3`).

## 6 Configuration du Client 2

### 6.1 Étape 27 : Démarrage du Client 2

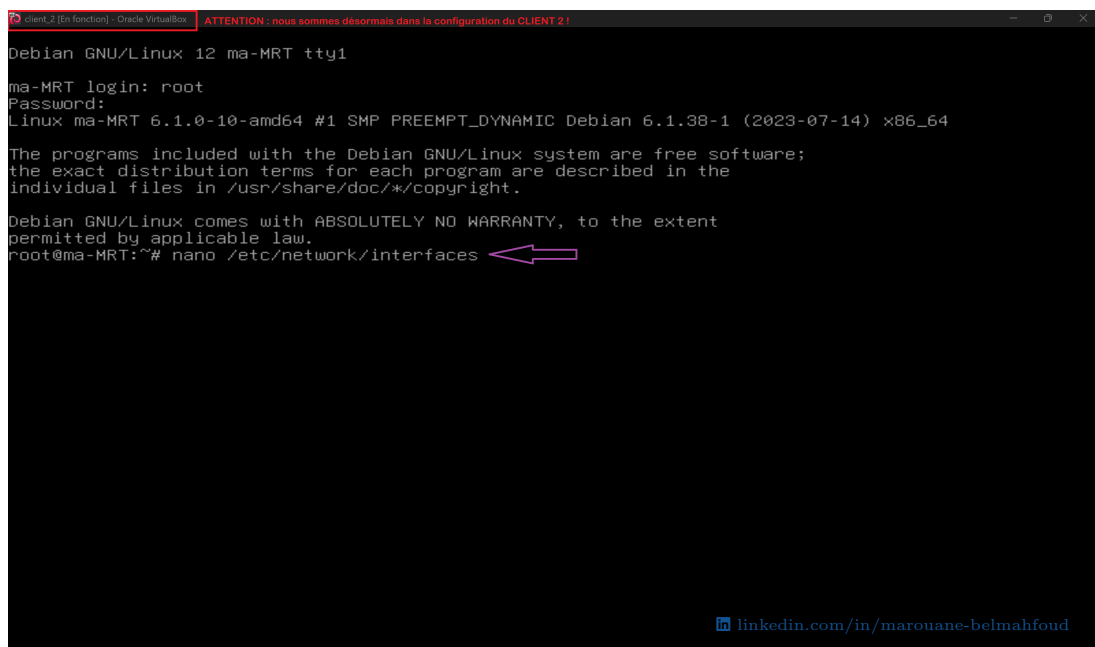


```
client 1 [En fonction] - Oracle VirtualBox
root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        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:c0:fa:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.118/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86397sec preferred_lft 86397sec
    inet6 2001:861:62:dcc0:a00:27ff:fec0:fafd/64 scope global dynamic mngtmpaddr
        valid_lft 86397sec preferred_lft 14397sec
    inet6 fe80::a00:27ff:fec0:fafd/64 scope link
        valid_lft forever preferred_lft forever
root@ma-MRT:~# ip route add 192.168.10.0/24 via 192.168.1.66
```

FIGURE 27 – Screen 28 – Lancement de client2

Démarrez la machine **client2** et connectez-vous.

### 6.2 Étape 28 : Édition du fichier interfaces



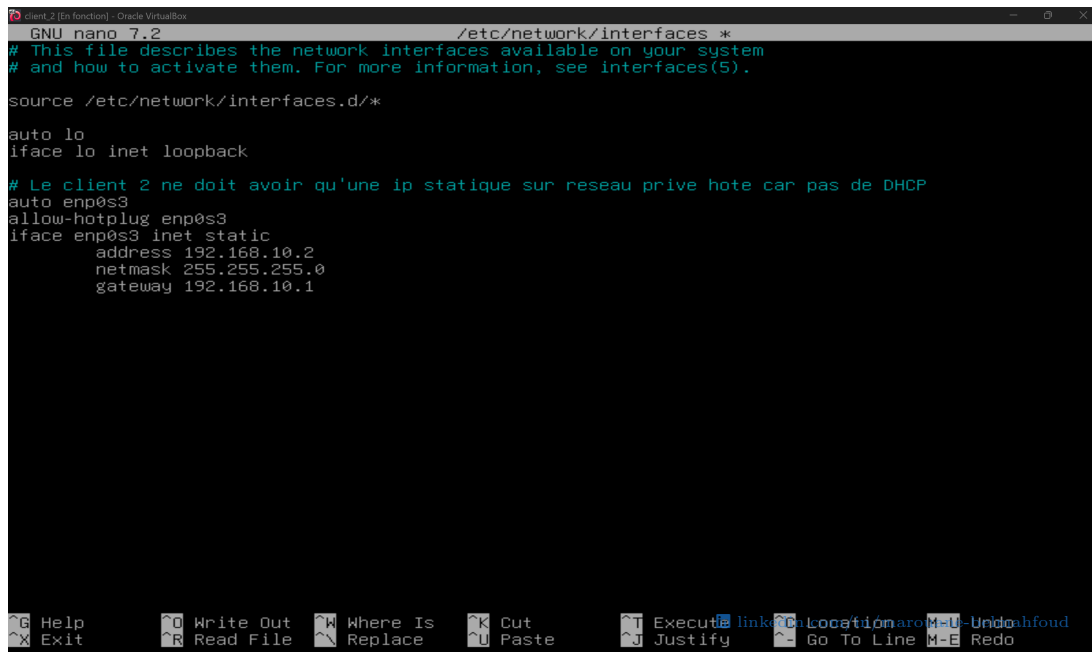
```
client 2 [En fonction] - Oracle VirtualBox ATTENTION : nous sommes désormais dans la configuration du CLIENT 2 !
Debian GNU/Linux 12 ma-MRT tty1
ma-MRT login: root
Password:
Linux ma-MRT 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ma-MRT:~# nano /etc/network/interfaces
```

FIGURE 28 – Screen 29 – Ouverture du fichier

Ouvrez le fichier de configuration réseau :

```
sudo nano /etc/network/interfaces
```

### 6.3 Étape 29 : Configuration IP statique



```
GNU nano 7.2 /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/*

auto lo
iface lo inet loopback

# Le client 2 ne doit avoir qu'une ip statique sur reseau prive hote car pas de DHCP
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.10.2
    netmask 255.255.255.0
    gateway 192.168.10.1
```

FIGURE 29 – Screen 30 – IP statique pour client2

Configurez l'interface avec une adresse IP statique sur le réseau privé :

```
auto enp0s3
iface enp0s3 inet static
address 192.168.10.2
netmask 255.255.255.0
gateway 192.168.10.1
```

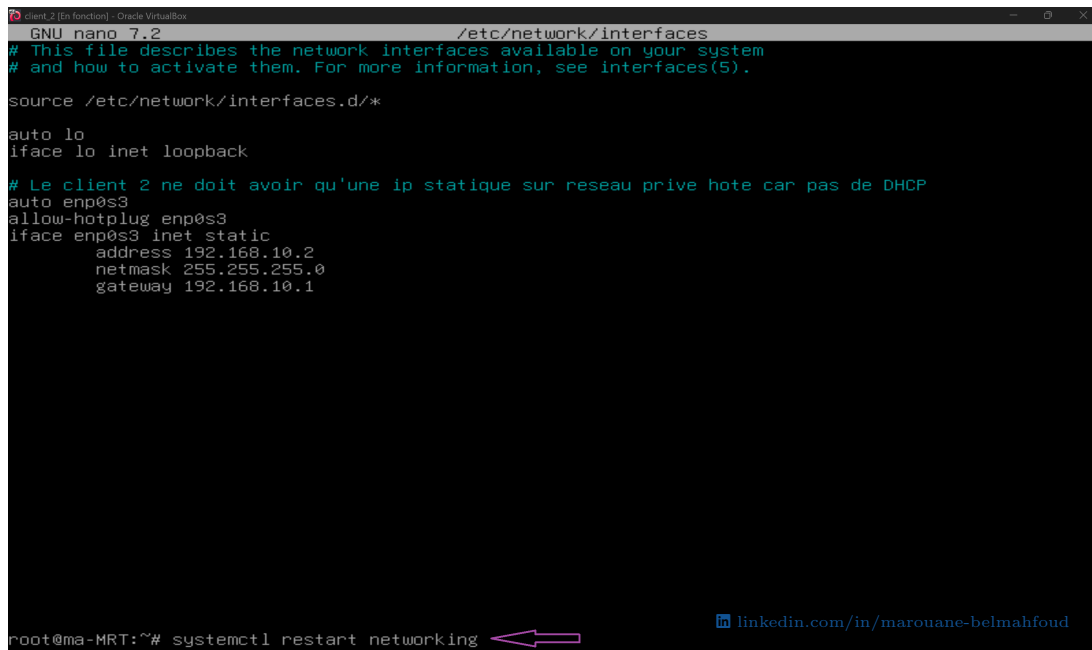
#### **i** Information

**address** : IP du client2 (192.168.10.2)

**gateway** : IP de la passerelle sur le réseau privé (192.168.10.1)

Sauvegardez et quittez.

## 6.4 Étape 30 : Redémarrage du réseau



```
GNU nano 7.2 /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/*

auto lo
iface lo inet loopback

# Le client 2 ne doit avoir qu'une ip statique sur reseau prive hote car pas de DHCP
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.10.2
    netmask 255.255.255.0
    gateway 192.168.10.1

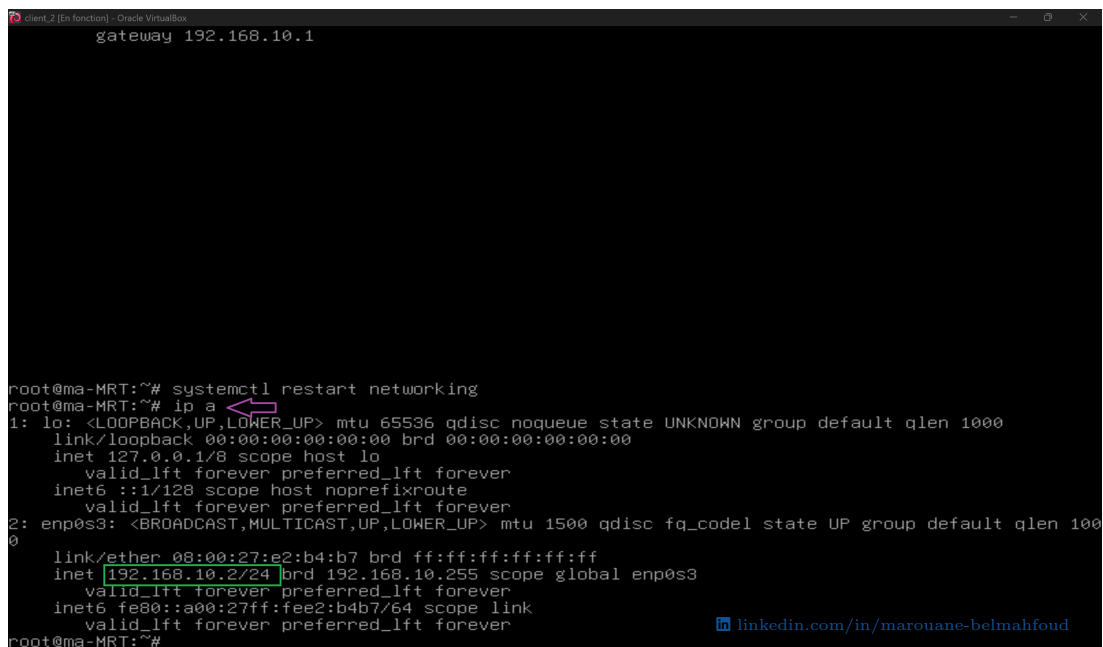
root@ma-MRT:~# systemctl restart networking
```

FIGURE 30 – Screen 31 – Redémarrage du service réseau

Redémarrez le service réseau :

```
sudo systemctl restart networking
```

## 6.5 Étape 31 : Vérification de la configuration



```
gateway 192.168.10.1

root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# 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:e2:b4:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/24 brd 192.168.10.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee2:b4b7/64 scope link
        valid_lft forever preferred_lft forever

root@ma-MRT:~#
```

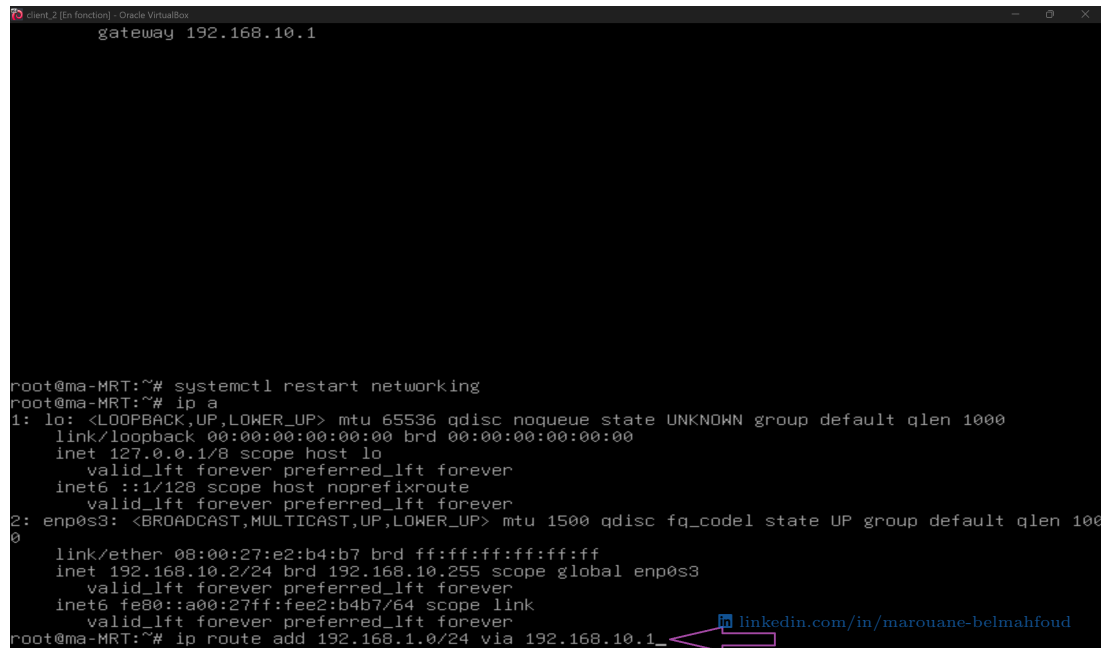
FIGURE 31 – Screen 32 – Vérification avec ip a

Vérifiez que l'adresse IP statique a bien été appliquée :

```
ip a
```

L'interface enp0s3 doit afficher l'adresse 192.168.10.2.

## 6.6 Étape 32 : Ajout de la route vers le réseau pont



```
client_2 [En fonction] - Oracle VM VirtualBox
gateway 192.168.10.1

root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW state UNKNOW 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:e2:b4:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/24 brd 192.168.10.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee2:b4b7/64 scope link
        valid_lft forever preferred_lft forever
root@ma-MRT:~# ip route add 192.168.1.0/24 via 192.168.10.1
```

FIGURE 32 – Screen 33 – Route vers le réseau pont

Ajoutez une route pour joindre le réseau pont (où se trouve client1) via la passerelle :

```
sudo ip route add 192.168.1.0/24 via 192.168.10.1
```

### **i** Information

Cette commande indique au client2 que pour atteindre le réseau 192.168.1.0/24 (réseau pont où se trouve client1), il doit passer par 192.168.10.1 (la passerelle).

### **!** Attention

Adaptez le réseau 192.168.1.0/24 selon votre réseau local réel. Utilisez la commande `ip route` sur client1 pour connaître votre réseau.

## 7 Tests de connectivité

### 7.1 Étape 33 : Redémarrage de la passerelle

Avant de tester, redémarrez la machine **Passerelle** pour vous assurer que tous les paramètres sont actifs.

### 7.2 Étape 34 : Test depuis Client 2 vers Client 1

```

root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# 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:e2:b4:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/24 brd 192.168.10.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee2:b4b7/64 scope link
        valid_lft forever preferred_lft forever
root@ma-MRT:~# ip route add 192.168.1.0/24 via 192.168.10.1
root@ma-MRT:~# show ip route
-bash: show: command not found
root@ma-MRT:~# ping 192.168.1.118
PING 192.168.1.118 (192.168.1.118) 56(84) bytes of data:
64 bytes from 192.168.1.118: icmp_seq=1 ttl=63 time=2.64 ms
64 bytes from 192.168.1.118: icmp_seq=2 ttl=63 time=1.90 ms
64 bytes from 192.168.1.118: icmp_seq=3 ttl=63 time=1.83 ms
64 bytes from 192.168.1.118: icmp_seq=4 ttl=63 time=1.73 ms
64 bytes from 192.168.1.118: icmp_seq=5 ttl=63 time=2.40 ms
64 bytes from 192.168.1.118: icmp_seq=6 ttl=63 time=2.00 ms
64 bytes from 192.168.1.118: icmp_seq=7 ttl=63 time=1.79 ms
64 bytes from 192.168.1.118: icmp_seq=8 ttl=63 time=3.16 ms
64 bytes from 192.168.1.118: icmp_seq=9 ttl=63 time=1.89 ms
^C
--- 192.168.1.118 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8018ms
rtt min/avg/max/mdev = 1.732/2.149/3.158/0.457 ms
root@ma-MRT:~#

```

FIGURE 33 – Screen 34 – Ping de client2 vers client1

Depuis le **client2**, testez la connectivité vers le client1 :

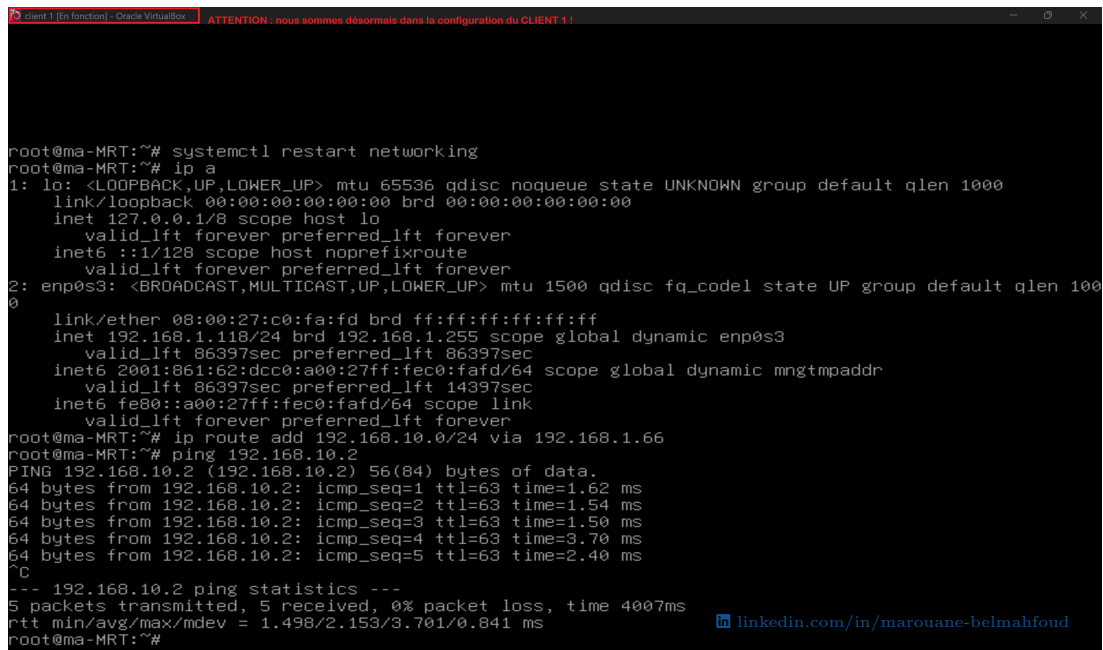
```
ping 192.168.1.118
```

**Résultat attendu :** Les paquets doivent passer et vous devez recevoir des réponses. Cela prouve que :

- ✔ Le client2 peut joindre la passerelle
- ✔ La passerelle route correctement vers le réseau pont
- ✔ Le client1 reçoit les paquets et répond

Utilisez **Ctrl+C** pour arrêter le ping.

### 7.3 Étape 35 : Test depuis Client 1 vers Client 2



```

client 1 [En fonction] - Oracle VirtualBox
ATTENTION : nous sommes désormais dans la configuration du CLIENT 1 !

root@ma-MRT:~# systemctl restart networking
root@ma-MRT:~# 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:c0:fa:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.118/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 86397sec preferred_lft 86397sec
    inet6 2001:861:62:dcc0:a00:27ff:fec0:fafd/64 scope global dynamic mngtmpaddr
        valid_lft 86397sec preferred_lft 14397sec
    inet6 fe80::a00:27ff:fec0:fafd/64 scope link
        valid_lft forever preferred_lft forever
root@ma-MRT:~# ip route add 192.168.10.0/24 via 192.168.1.66
root@ma-MRT:~# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data:
64 bytes from 192.168.10.2: icmp_seq=1 ttl=63 time=1.62 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=63 time=1.54 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=63 time=1.50 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=63 time=3.70 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=63 time=2.40 ms
^C
--- 192.168.10.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.498/2.153/3.701/0.841 ms
root@ma-MRT:~#

```

FIGURE 34 – Screen 35 – Ping de client1 vers client2

Depuis le **client1**, testez la connectivité inverse vers le client2 :

```
ping 192.168.10.2
```

**Résultat attendu :** Les paquets passent également dans ce sens. La communication bidirectionnelle est établie !

#### ✓ Succès

Si les deux pings fonctionnent, félicitations ! Votre passerelle Debian est opérationnelle et permet aux deux clients de communiquer malgré leurs réseaux différents.

---

## 8 Conclusion

---

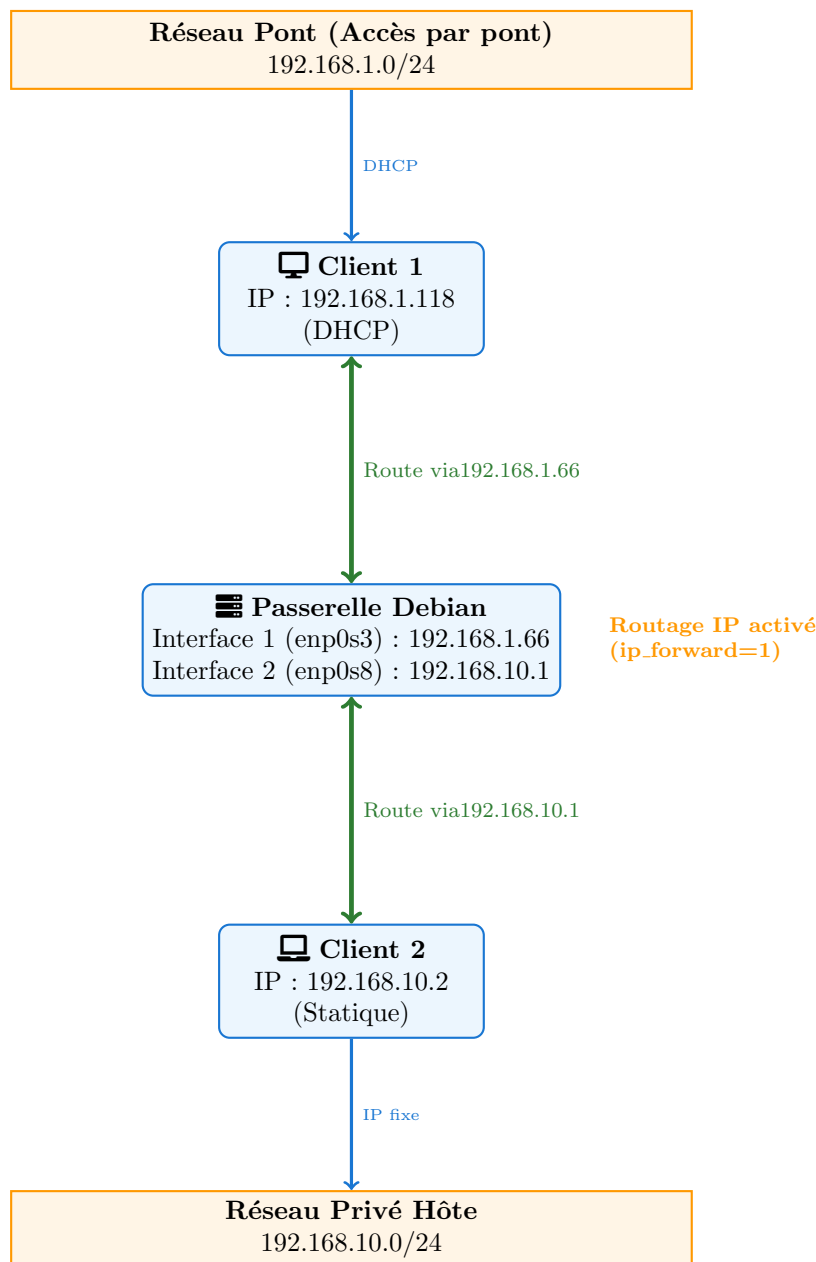
### 8.1 Récapitulatif

Vous avez réussi à mettre en place une passerelle Debian/Linux fonctionnelle dans VirtualBox. Cette configuration permet à deux machines situées sur des réseaux différents de communiquer entre elles.

### 8.2 Ce qui a été accompli

1. **Importation et configuration** de trois machines virtuelles avec des paramètres réseau adaptés
2. **Configuration de la passerelle** avec :
  - Deux interfaces réseau (pont et réseau privé)
  - Adresses IP correctement assignées
  - Routage IP activé (`ip_forward`)
  - Pare-feu désactivé (pour les tests)
3. **Configuration des clients** avec :
  - Client1 en DHCP sur le réseau pont
  - Client2 en IP statique sur le réseau privé
  - Routes statiques vers la passerelle
4. **Vérification** de la connectivité bidirectionnelle

### 8.3 Schéma récapitulatif



### 8.4 Points clés à retenir

- 🔑 Le **routage IP** doit être activé sur la passerelle (`net.ipv4.ip_forward=1`)
- 🔑 Les **routes statiques** doivent être configurées sur chaque client pour indiquer que le trafic vers l'autre réseau passe par la passerelle
- 🔑 Le **mode promiscuité** (Allow All) est nécessaire pour que VirtualBox autorise le routage de paquets entre les interfaces
- 🔑 Les **adresses MAC** doivent être uniques pour chaque machine (d'où la génération lors de l'importation)

### 8.5 Pour aller plus loin

- ➔ **Persistance des routes** : Les routes ajoutées avec `ip route add` sont temporaires. Pour les rendre permanentes, ajoutez-les dans le fichier `/etc/network/interfaces` avec la directive `up`

```
ip route add...
```

- **Pare-feu** : En production, configurez iptables ou nftables pour sécuriser votre passerelle
- **NAT** : Si vous souhaitez que le client2 accède à Internet via la passerelle, vous devrez configurer une règle de NAT (masquerading)
- **DNS** : Configurez un serveur DNS pour permettre la résolution de noms

✓ Tutoriel terminé avec succès