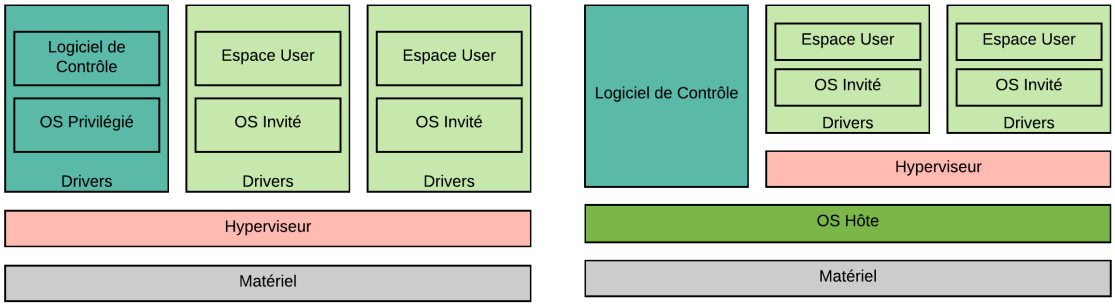
Réseaux Avancées

Introduction à la virtualisation

Hyperviseurs

Dans le cadre d'une virtualisation, on est amené à utiliser un hyperviseur. Il en existe 2 Types.



L'hyperviseur de Type 1 (gauche sur le schéma) est généralement utilisé en production.

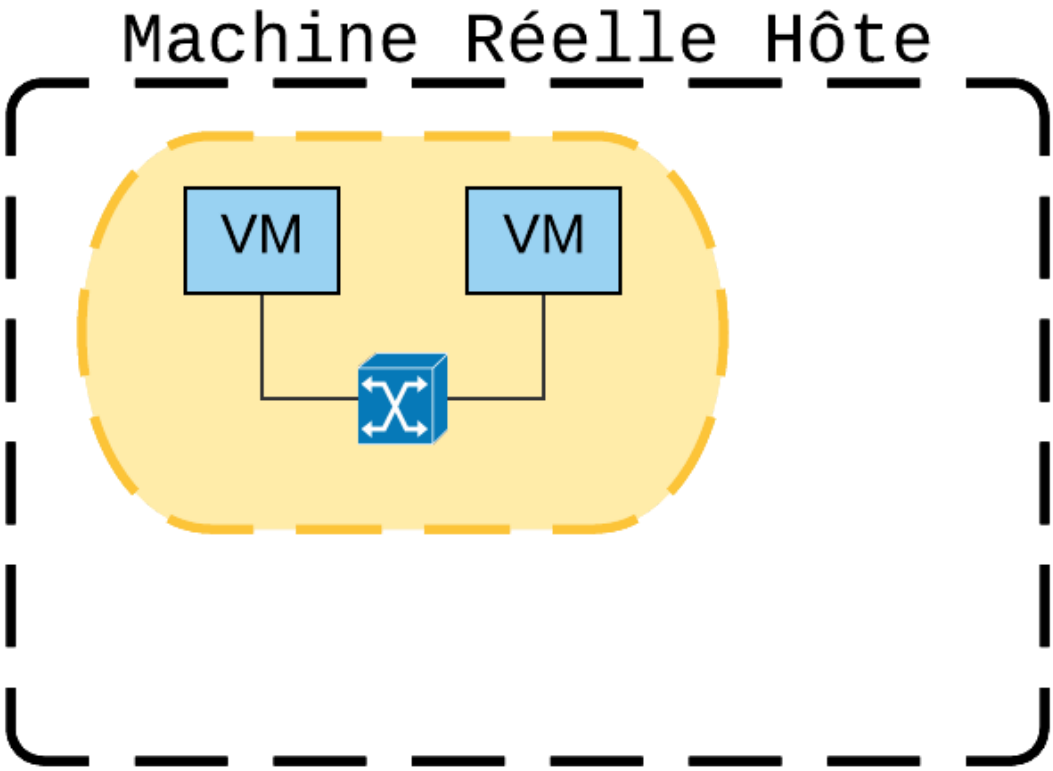
L'hyperviseur de Type 2 (Droite sur le schéma) est généralement utilisé dans le cadre de tests. Il consiste à émuler un OS dans un autre OS. (Ex : VirtualBox D'Oracle).

Que Signifient les Différents paramètres de Configuration de Cartes Réseaux dans VirtualBox ?

	VM → Autres VM	**Hôte → VM**	**VM→ Réseau Local**	**VM→ Internet**
Réseau Interne	$\checkmark$			
Réseau Privé Hôte	$\checkmark$	$\checkmark$		
NAT	$\checkmark$		$\checkmark$	$\checkmark$
Accès par Pont (Bridge)	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$

Réseau Interne

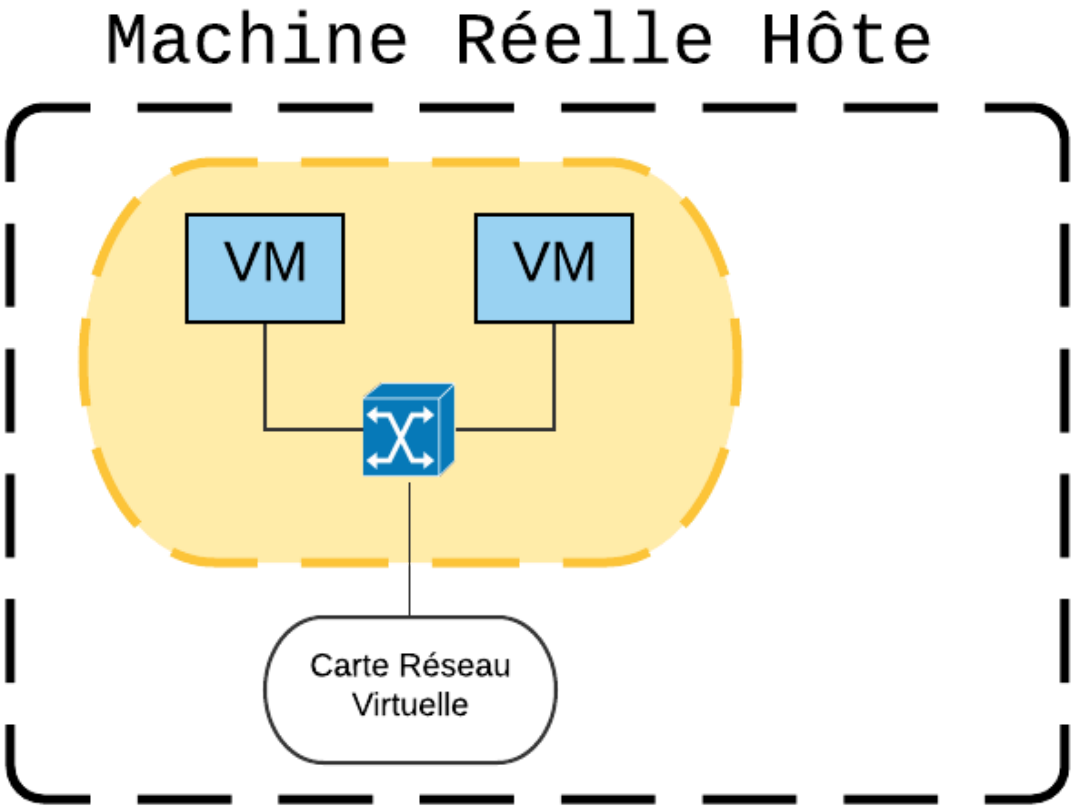
Le Réseau Interne Permets de connecter 2 Machines virtuelles entre elles par le biais d'un Switch virtuel.



> Il est possible d'ajouter ou de modifier les Virtual Switch dans VirtualBox.

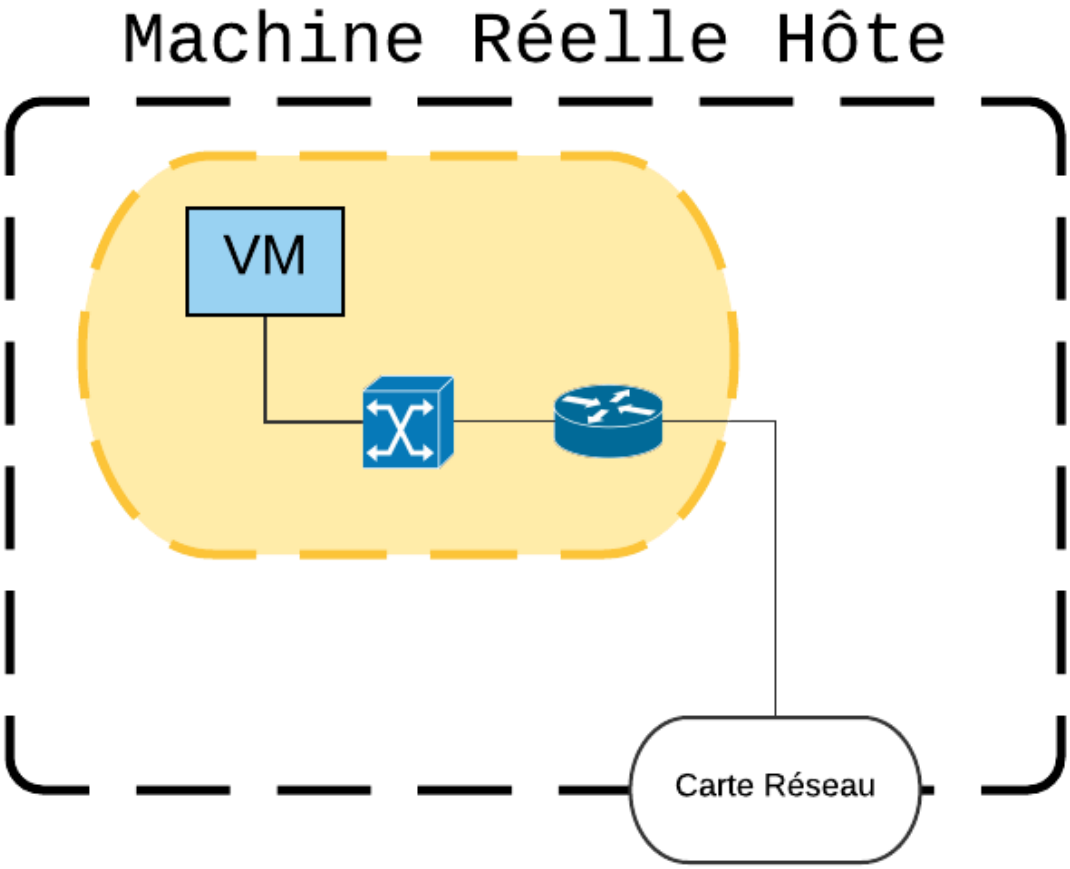
Réseau Privé Hôte

Permets de connecter des VM par le biais d'un switch virtuel et permets à l'hôte d'y accéder par le biais d'une carte réseau virtuelle.



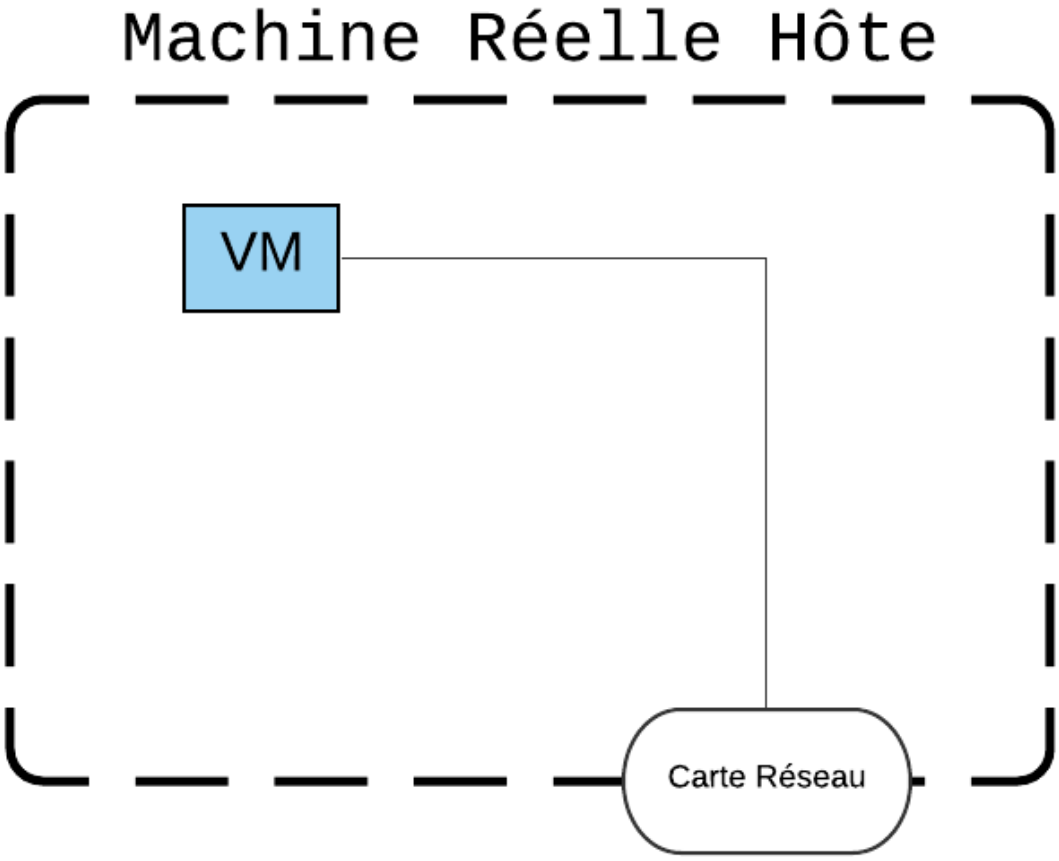
NAT

Le Nat ou Network Access Translation est la manière la plus sécurisée autoriser l'accès au réseau local à une VM. Le routeur évite par exemple les pollutions DHCP issues de la configuration des VM. Elle est aussi utile quand le réseau extérieur est considéré comme hostile et permets d'éviter que d'autres terminaux n'accèdent à votre VM sans y avoir explicitement autorisé l'accès dans le routeur. Ce dernier agit ici comme un pare-feu et protège votre VM.



Connexion par Pont (Bridge)

Ce mode de connexion donne à une VM accès une carte réseau comme si celle-ci lui était directement attachée.



Mode Promiscuité

Dans le cadre d'un échange d'informations sur le biais d'un réseau local, les paquets réseaux possèdent l'adresse de leur destinataire. En règle générale, si un paquet n'est pas dédié à l'adresse MAC de la carte réseau, celle-ci va '*dropper*' le paquet et ne pas y prêter attention.

Si, dans le cadre d'une résolution de problèmes sur le réseau interne ou dans le cadre d'un sniffing [1], on souhaite intercepter des paquets qui ne nous sont pas dédiés. Il est possible de forcer la carte réseau à ne pas '*dropper*' le paquet. Pour ce faire, on utilise un mode sur la carte réseau appelé **Mode Promiscuité**.

Paramètres Réseaux d'un Hôte

- **Adresse IP statique**: Une adresse logique IP (V4) qui est fixe. Peut être fournie par un FAI éventuellement. Répartie sur 4 octets
- **Masque de sous réseau**: Masque binaire pour une adresse IP permettant de séparer la partie réseau de la partie hôte
- **Adresse IP dynamique**: Adresse IP reçue dynamiquement via un serveur extérieur et renouvelée à intervalles réguliers (ex: chaque fois que l'ordinateur est redémarré).
- **Adresses IP supplémentaires**: Adresse IP qu'une interface utilise en plus de celle de base
- **Serveur DNS**: Adresse IP Serveur qui permet de faire le lien entre adresse IP et FQDN, nom de domaines via le protocole DNS
- **Host Name**: Nom d'hôte Local d'une machine et/ou nom d’hôte DNS
- **Passerelle par défaut**: Passerelle / routeur vers laquelle seront dirigés les paquets dont le chemin vers la destination est inconnu. L'équivalent d'un panneau "toute directions"

- **Passerelles supplémentaires**: Passerelles correspondant au chemin vers des réseaux connus.
- **Firewall**: Dispositif qui autorise/interdit le trafic réseau sur base de certains critères
- **Carte réseau** :
  - **Mac Adresse**: Adresse matérielle d'une interface Ethernet. Sur 48bits. La première partie correspond au constructeur. Se note en hexadécimal
  - **Duplex** :
    - **Half** : donnée circulent sur une paire de fils en UP/DOWN -> 100Mb total
    - **Full** : une paire de fils pour les données en UP, une autre pour en DOWN -> 100Mb / direction
  - **Débit** : Nombre maximal de bits/secondes qui peuvent circuler par une interface

Configuration des paramètres réseaux sous interface graphique

> fonctionnement d'un masque réseau : Une adresse ip représente aussi bien le périphérique que le réseau dans lequel il se situe, on peut différencier les deux en regardant le masque sous-réseau
>
> un masque de sous réseau : 255.255.255.0 possède plus de sous-réseaux possibles et moins d'hotes que 255.255.0.0
>
> si on prends un exemple : 192.168.1.34 avec le masque 255.255.255.0 nous dit que 192.168.1.0 désigne le sous-réseau. 192.168.1.255 désigne l'adresse de broadcast pour cela. et 34 est l'adresse de ce pc sur ce sous-réseau.

IP Statique / DHCP

Windows

Panneau de Configuration > Réseau et Internet > Centre Réseau et Partage > Connexions : Ethernet / wifi > Propriétés > gestion de Réseau > protocole Internet Version4 (TCP/IPV4)

Linux

Une adresse ipv4 est codée sur 32 bits, et une ipv6 sur 128 bits.

> On effectue ces configurations en tant que Root
>
> ```
> 1 su -root
> ```

> on peut aussi modifier le clavier via la commande : $ setxkbmap be

Vérifier la configuration d'un réseau

```
1 ip addr show
```

```
1 ip -6 addr show
```

Afficher niveau 2 (Mac) :

```
ip link show
ip link show NOM_PERIPHERIQUE
```

vérifier routes

```
ip route show
```

Afficher le fichier DNS

```
cat /etc/resolv.conf
```

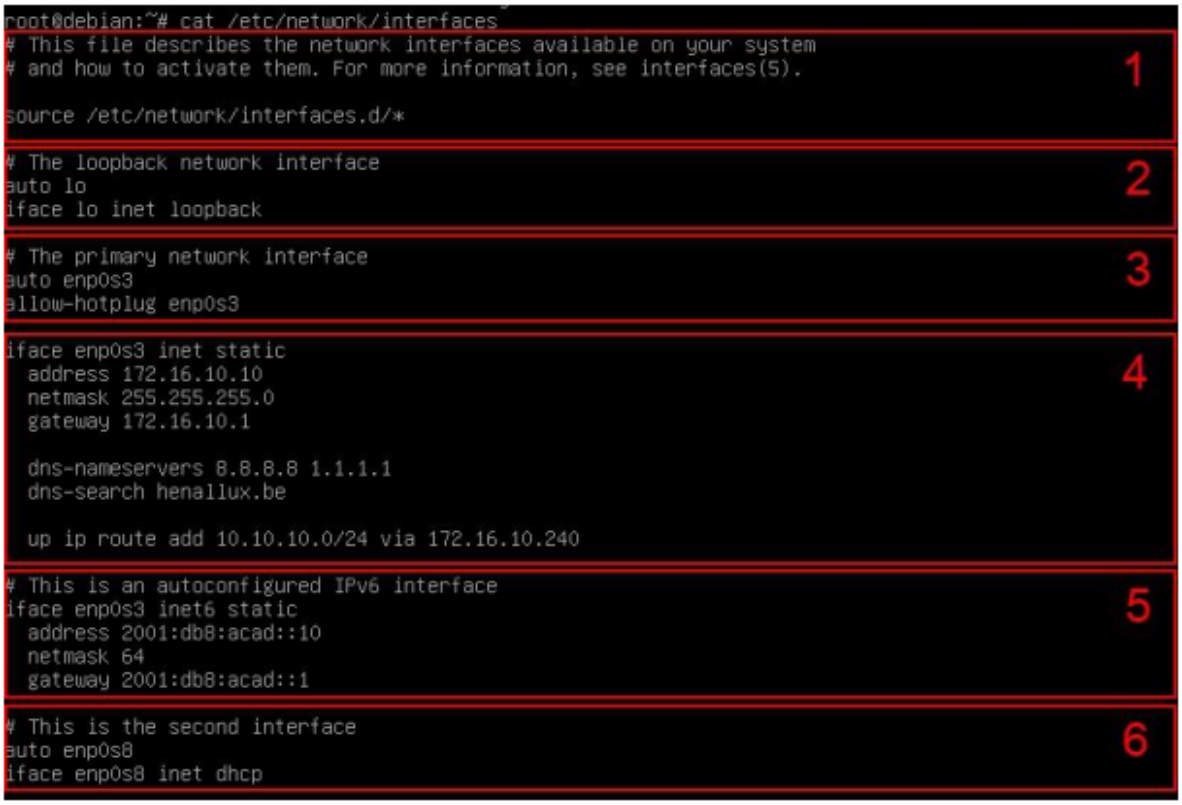
> un fichier de configuration veut généralement dire que les configurations effectuées seront persistantes (sauvegardées même si la machine reboot)

```
cp fichier_a_copier destination
```

nano : editeur

cat : affiche le contenu d'un fichier

/etc/network/interface :: fichier qui contient les configurations du network



1. C'est l'entête du fichier. IL ne faut pas le modifier. Les lignes commençant par le # sont des commentaires et ne seront pas utilisées. Néanmoins, évitez de les modifier.
2. C'est la définition de l'interface loopback. Laissez-le également tel qu'il est. Il ne faut surtout pas le retirer.
3. Cette section active l'interface enp0s3 au boot du serveur. Elle permet également éventuellement de détecter une interface connectée « à chaud »

4. Ici nous configurons le protocole IPv4 sur notre interface enp0s3. Inet sousentend IPv4, en opposition avec inet6, pour l'IPv6. Les paramètres vus ici sont les principaux, mais il en existe d'autres, comme par exemple :
    - hwaddress ether 00:01:04:1b:2C:1F qui va forcer le remplacement de la Mac Address de votre carte réseau.
    - La configuration d'une 2° adresse sur une interface. Cela se configure comme une nouvelle interface de type enp0s3:0, enp0s3:1, ... Il s'agira d'une nouvelle interface, donc il faudra utiliser auto afin qu'elle soit configurée au boot. Elle réagira à ifquery de la même façon que l'interface sur laquelle on place cet alias. :
5. Nous configurons ici un 2° protocole sur cette interface, à savoir l'IPv6
6. Nous configurons une 2° interface en DHCP IPv4.

Pour configurer une interface IPV4, on peut :

- DHCP : rien d'autres à config
- Statique : il faut alors obligatoirement définir une adresse ip et un masque réseau. (+gateway), (+un ou plusieurs serveurs DNS), un ou plusieurs search Domain.

Firewall

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

Windows

Dans le menu Démarrer (Windows + R) : **firewall.cpl**

Dans Windows il et possible de classer de privé ou publique les réseaux et ainsi d'y appliquer des règles de firewall différent pour protéger son ordinateur

Linux

afficher l'adresse ip

```
ip addr
```

tester la connectivité

```
ping IP_ADDRESS
```

Comment appliquer une configuration sur un serveur linux ?

- Reboot le serveur

- redémarrer le service réseau

```
systemctl restart networking
```

- redémarrer l'interface configurer
  - $ ifdown NOM_INTERFACE --> déconfigure l'interface
  - $ ifup NOM_INTERFACE -- > configure l'interface
  - $ ipquerry NOM_INTERFACE --> renvoie la liste des config

Hostname d'un serveur :

- hostnamectl
  - configure à chaud et d'une manière persistante
  - stocké dans le fichier /etc/hostname

  --> il faut se déconecter et se reconnecter pour voir les changements
- changer l'hostname
  - $ hostnamectl set-hostname MyDebian10
- afficher le status de l'host name
  - $ hostnamectl status
- hostname
  - affiche l'hostname
  - peut aussi le changer mais pas de manière persistante

Retirer la configuration d'une interface

$ ip addr flush dev NOM_INTERFACE

> idem mais pour ipv6 : $ ip -6 addr flush dev NOM_INTERFACE

ajouter/supprimer un alias

$ ip [-6] addr [add / suppr] 192.168.0.10/24 dev NOM_INTERFACE

> le -6 est à mettre si on veut configurer cette interface en IPV6

> pour supprimer un alias, il faut mettre suppr et non add

Configurer une interface en DHCP

> Attention à ne pas oublier d'effacer la configuration statique de l'interface avant
>
> > $ ip addr flush dev NOM_INTERFACE

$ dhclient -v NOM_INTERFACE

--> démarre le processus client DHCP

On peut le tuer avec $ pkill dhclient

mais attention, sa configuration ne sera pas retirée

Edition DNS

> a eviter

on peut le faire en modifiant le fichier : /etc/resolv.conf

La suppression du default gateway et sa reconfiguration

$ ip route del defaut

$ ip route add defaut via 172.16.10.1

> idem avec un -6 pour une ipv6

creation et suppression des routes statiques

$ ip route add 192.168.1.0/24 via 172.16.10.40

$ ip route add 192.168.1.0/24 via 172.16.10.40 dev NOM_INTERFACE

$ ip route del 192.168.1.0/24

> idem avec -6 pour ipv6

mettre une interface up et down

$ ip link set NOM_INTERFACE down

$ ip link set NOM_INTERFACE up

changer la mac adresse d'une interface

$ ip link set dev NOM_INTERFACE address MAC:ADRESS:XXX:XXXX

Configuration des services de base dans un réseau IP

> pour windows server cfr notes 4A du cours

Configuration d'un DHCP / DNS

DHCP

DHCP signifie dynamic host Configuration Protocol et il permets d'assigner automatiquement des adresses ip aux machines sur le réseau. Il délivre pour celà un bail

Un bail DHCP contient :

- la durée du bail
- l'adresse ip attribuée à la machine
- les paramètres réseaux du default Gateway / serveur DNS

On configure donc dans un serveur dns une plage d'adresse qui seront attribuées aux machines

DNS

DNS signifie Domain Name System

un Dns est utilisé pour lier les noms aux ip (www.google.com à 2a00:1450:400e:806::2004)

il fonctionne en cascade, si le premier dns ne connait pas l'information, il va remonter et demander celle-çi à un autre dns (son supérieur hiérarchique si on veut).

LE FTP et le TFTP

Le ftp et le tftp sont deux protocoles de partage de fichiers sur un réseau.

FTP

FTP veut dire **File Transfert Protocol**.

Le ftp se base sur l'architecture **client/serveur** et opère sur le **port 21**. La connexion est effectuée **en clair** et offre la possibilité accueillir des utilisateurs anonymes. La connexion est TCP et nécésite une connexion TCP.

Il est possible de sécuriser la connexion via un certificat ssl/tls (ftps). Ou encore d'utiliser le SFTP (port 22) qui est le transfert de fichier sécurisé lié au ssh (port 22).

TFTP

TFTP signifie **Trivial File Transfert Protocol**. Il s'agit d'un autre protocole de transfert de fichier. Plus simple, il est utilisé quand l'authentification et la visibilité des directory n'est pas nécessaire. fonctionne en **udp** et s'utilise sur le **port 69**. L'utilisation que l'udp a pour conséquence de laisser l'utilisateur gérer lui même la perte de paquets.

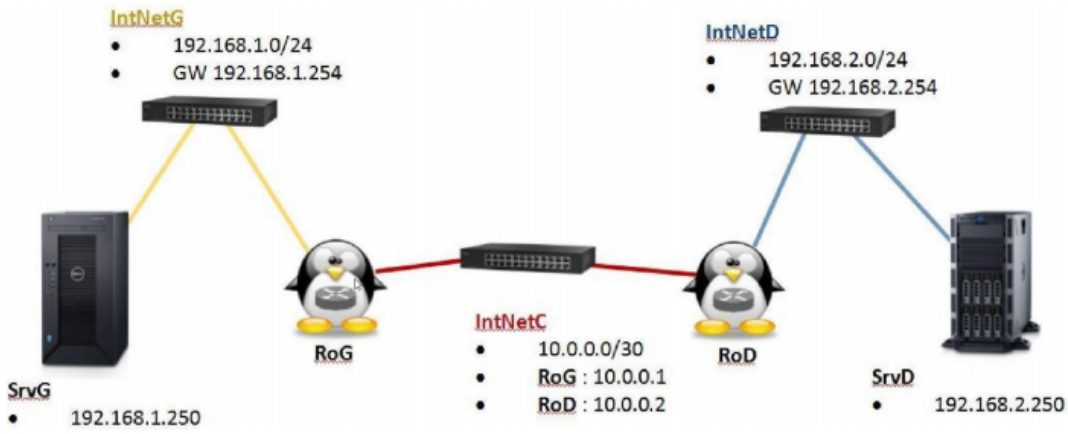
Il était à l'origine utilisé pour charger des fichiers de démarrage de Workstation sans disque dur

Comment configurer FTP sur Windows serveur ?

CFR Partie 5 du cours

Routage inter-réseaux

Dans les exemples suivants, on utilise un system linux pour simuler un routeur.



???? 6.1

nano /etc/network/interfaces

auto enp0s3 iface enp0s3 inet static

address

192.168.1.250 netmask

255.255.255.0 gateway

192.168.1.254

redirection de paquets ip dans linux

temporaire

sysctl -w net.ipv4.ip_forward=1

permantente

Editer le fichier /etc/sysctl.conf et y ajouter (ou décommenter) la ligne :

```
$ net.ipv4.ip_forward=1 o
```

Redémarrer le service :

```
$ sysctl -p /etc/sysctl.conf
```

La commande traceroute permets de voir le chemin emprunté par le trafic

passer le par défaut

Vous avez configuré votre routage en utilisant des routes par défaut. Supprimer maintenant les routes par défaut et configurez votre routage en utilisant des routes statiques.

---

1. Méthode de piratage ↩