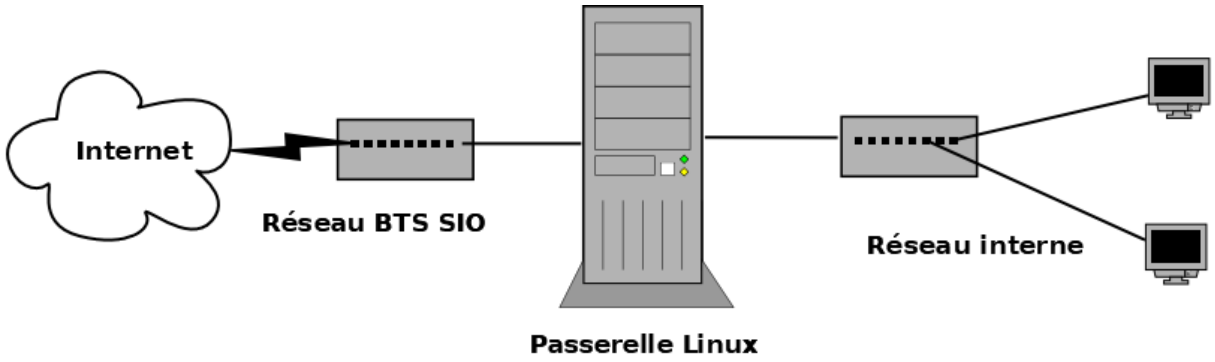
TP : Services de passerelle Linux

Objectifs :

- Comprendre la notion de passerelle ;
- Installer et configurer une passerelle sous GNU/Linux ;

Maquette à réaliser sur VirtualBox :



Pour les besoins de ce TP, vous aurez besoin :

- D'une VM Debian (passerelle) avec 2 interfaces réseau
- D'une VM Debian dans le réseau interne.

1. Rappels

a. Quel est le rôle d'une passerelle dans un réseau ?

Une passerelle c'est un routeur qui permet de relier 2 ou plusieurs réseaux.

Généralement, une passerelle permet l'accès à internet. Exemple : Box Internet

b. Combien d'interfaces possède-t-elle ? Quels sont les types d'adresses IP utilisés ?

Une passerelle possède au moins 2 interfaces réseau (une par réseau connecté).

Types d'adresses : adresse interne (côté LAN), adresse externe publique (côté Internet).

Remarque : une passerelle peut être un boitier spécialisé (routeur) ou un poste (Linux) avec plusieurs interfaces.

c. Donner des exemples de services fournis par une passerelle ?

- Le routage IP
- La translation d'adresses (NAT) et de ports (PAT)
- Pare feu : filtrage de paquets
- Service DNS, DHCP, …

2. Création et configuration de la VM (passerelle)

a. Création de la VM « passerelle »

- Cloner une nouvelle VM Debian en la nommant « Passerelle » ;
- Lire l'annexe : types de cartes réseau.
- Dans **Configuration -> Réseau**, mettez la première carte réseau en **NAT** ;
- Ajouter une 2ème interface réseau de type « **réseau interne** » ;

b. Configuration des interfaces réseau de la passerelle

- Afficher les interfaces de la VM. Quelles sont leurs noms et leurs adresses IP ?

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:70:45:d4 brd ff:ff:ff:ff:ff:ff
    inet 10.25.0.1/8 brd 10.255.255.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe70:45d4/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:de:06:7b brd ff:ff:ff:ff:ff:ff
```

Remarque : l'interface de type **NAT** est l'interface externe (relié au réseau de l'hôte physique) de votre passerelle. Cette interface est configurée automatiquement dans le réseau 10.0.0.0/8 et permet l'accès à Internet via le réseau du BTS.

Nous avons fait ce choix (type NAT) pour ne pas gaspiller des adresses IP du réseau du BTS.

- Dans quel fichier figure la configuration des cartes réseau ? Afficher son contenu :

Le fichier où figure la configuration des cartes réseau est :nano /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

auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
        address 192.168.1.254
        netmask 255.255.255.0
        dns-nameservers 8.8.8.8
                post-up iptables-restore < /etc/iptables_rules.save
```

- Configurer la 2ème carte réseau en lui attribuant la dernière adresse du réseau interne **192.168.1.0/24** (voir TP6). Ajouter la copie d'écran de la configuration :

```
auto enp0s8
iface enp0s8 inet static
        address 192.168.1.0
        netmask 255.255.255.0
        gateway 10.187.35.254
        dns-nameservers 8.8.8.8
```

3. Création et configuration de la VM cliente

a. Configuration réseau

- Créer ou utiliser une VM existante ;
- Mettre l'interface réseau en « Réseau interne » ;
- Démarrer la VM et afficher ces interfaces réseau. Quelles sont leurs noms et leurs adresses IP ?

Le nom de l'interface est en0ps3 et l'adresse IP est 10.0.5.1/8.

- Configurer la carte réseau en lui attribuant la 1ère adresse du réseau interne **192.168.1.0/24** (voir TP6). Ajouter la copie d'écran de la configuration :

```
# 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

auto enp0s3
iface enp0s3 inet static
        address 192.168.1.0
        netmask 255.255.255.0
        gateway 10.187.35.254
        dns-nameservers 8.8.8.8
```

b. Tests

- Tester la connectivité avec la passerelle. Noter le résultat :

```
root@Ch2Lab1:/home/centrecallbd# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.204 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.217 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.212 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=0.155 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=64 time=0.214 ms
64 bytes from 192.168.1.254: icmp_seq=6 ttl=64 time=0.200 ms
64 bytes from 192.168.1.254: icmp_seq=7 ttl=64 time=0.194 ms
64 bytes from 192.168.1.254: icmp_seq=8 ttl=64 time=0.193 ms
64 bytes from 192.168.1.254: icmp_seq=9 ttl=64 time=0.210 ms
^C
--- 192.168.1.254 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 201ms
rtt min/avg/max/mdev = 0.155/0.199/0.217/0.025 ms
```

- Tester la connectivité avec Internet (8.8.8.8 et google.com). Noter le résultat :

4. Configuration du routage sur la passerelle

Par défaut, la fonction de ***routage*** n'est pas activée sur le système Linux.

a. Activation du routage

- Editer le fichier ***/etc/sysctl.conf*** et décommenter la ligne suivant :

net.ipv4.ip_forward=1

- Pour la prise en compte de la modification, taper la commande :

sysctl -p

- Afficher la table de routage. Quel son contenu ?
- Sur la VM « client », tester la connectivité avec Internet (8.8.8.8 et google.com). Noter le résultat :

b. Configuration de la translation d'adresse (NAT) sur la passerelle

- Ajouter la règle permettant l'activation du **NAT** sur l'interface externe de votre passerelle :

iptables -t nat -A POSTROUTING -o *nomInterfaceExterne* -j MASQUERADE

- Vérifier l'ajout de la règle NAT ci-dessus et noter le résultat.

iptables -t nat -L

- Sauvegarder la règle d'iptables ci-dessus dans le fichier **/etc/iptables_rules.save** :

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

iptables-save > /etc/iptables_rules.save

- Editer le fichier ***/etc/network/interfaces*** et ajouter les informations suivantes :

```
…
iface nomInterface inet static
        address …
        netmask …
        gateway …
          post-up iptables-restore < /etc/iptables_rules.save## restauration de la règle d'Iptables pour le NAT
```

- Redémarrer le service réseau (networking) pour prendre en compte les modifications.

c. Tests

- Sur la VM « client », tester la connectivité avec Internet (8.8.8.8 et google.com). Noter le résultat :
- Sur la VM « client », afficher la table ARP et noter le résultat :

Annexes

Les types de connexions réseau sur Oracle VirtualBox

Type « NAT » :

- Les Machines Virtuelles communiquent entre elles ;
- Les Machines Virtuelles communiquent avec l'hôte et l'extérieur ;
- L'hôte et l'extérieur ne voient pas les VM.

Dans ce type, les trames allant vers l'extérieur de votre machine virtuelle auront la même adresse que votre machine hôte (peu importe l'adresse IP de votre machine virtuelle).

Particularité : Dans ce mode, la machine virtuelle ne peut être utilisée qu'en client. Elle ne peut pas recevoir de requêtes directes de l'extérieur (ex : un ping ne fonctionnera pas).

Type « Réseau Interne » :

- Les VM communiquent entre elles ;
- Les VM ne communiquent pas avec l'hôte ;
- Les VM ne communiquent pas avec l'extérieur.

Ce type permet de connecter des machines virtuelles entre-elles sur un réseau virtuel isolé.

Type : « Réseau Privé Hôte » :

- Les VM communiquent entre elles ;
- Les VM communiquent avec l'hôte ;
- Les VM ne communiquent pas avec l'extérieur.

Avec ce type de connexion réseau votre machine virtuelle ne peut communiquer qu'avec votre machine hôte.

Type « Pont » :

Les VM sont sur le même réseau que l'hôte.

Avec ce type de connexion, les trames qui sortent de votre machine virtuelle auront leurs propres (adresse MAC et adresse IP).

Iptables Linux

https://doc.ubuntu-fr.org/iptables

La translation d'adresses NAT/PAT

Consulter la page web suivante :

https://fr.wikipedia.org/wiki/Network_address_translation#:~:text=NAT%20dynamique%20PAT%20(Port%20Address,avec%20la%20NAT%20statique%20PAT.