

|                               |                       |
|-------------------------------|-----------------------|
| BTS S.N.I.R.                  | Document ressource    |
| Lycée Jean Rostand Villepinte | Passerelle sous Linux |

# Passerelle sous Linux

L'objectif de ce document est de donner les étapes pour transformer un PC sous Linux en une passerelle (ou routeur) qui permettra de relier plusieurs réseaux. Cet ordinateur n'a pas besoin d'être très performant.

## I Étapes de la réalisation

Les différentes étapes pour transformer votre PC en passerelle sont les suivantes :

### 1. Ajout de carte(s) réseau :

Pour transformer votre PC en passerelle ou routeur, vous devez d'abord lui ajouter des cartes réseau. Votre ordinateur doit être équipé du même nombre d'interfaces réseau que de réseaux à relier. Donc en général, il faut ajouter une carte car le PC a déjà une carte réseau de base, cela permettra d'interconnecter deux réseaux.

### 2. Installation du système d'exploitation :

Il faut maintenant installer un système Linux. Nous recommandons une version Debian sans environnement graphique avec l'installation de **ssh** et les utilitaires usuels du système. ssh permettra de se connecter à distance et de reconfigurer ou de vérifier le fonctionnement de la passerelle. Après l'installation, le clavier, la souris et l'écran ne seront plus nécessaires.

Un document ressource décrit comment installer un serveur Debian.

### 3. Configuration des interfaces réseau :

Vous allez indiquer quelles sont les adresses réseau des différentes interfaces réseau (voir paragraphe III).

### 4. Application du routage :

Vous allez configurer le système pour qu'il transmette les paquets d'un réseau aux autres si nécessaires, c'est-à-dire qu'il effectue le routage entre les différents réseaux (voir paragraphe IV).

### 5. Établissement de la table de routage :

Vous allez définir l'ensemble des routes, c'est-à-dire lui signaler le chemin pour transmettre les paquets au bon système (voir paragraphe V).

### 6. Filtrage des paquets (pare-feu) :

La passerelle peut également protéger un réseau des paquets malveillants venant d'un autre réseau. Pour cela, il faut empêcher d'entrer dans le réseau ou limiter l'accès à certains serveurs uniquement. Dans ce cas, il faut mettre en place un pare-feu grâce à la commande iptables. La configuration de ces iptables est vue dans un autre document.

## II Installation d'une carte réseau

Après avoir installé la carte réseau, vous devez configurer la carte (eth1) comme indiqué dans le paragraphe suivant.

Pour obtenir la liste des interfaces réseau qui ont été détectées, on peut utiliser dans l'invite de commandes :

```
ifconfig -a
```

Vous devez trouver les deux cartes réseau ensXX et ensXX.

Si ce n'est pas le cas, normalement la nouvelle carte réseau est souvent détectée au démarrage. On peut rechercher les messages contenant « ensXX » pour avoir plus d'informations sur les cartes réseau détectées :

```
dmesg | grep ens33
```

|                               |                       |
|-------------------------------|-----------------------|
| BTS S.N.I.R.                  | Document ressource    |
| Lycée Jean Rostand Villepinte | Passerelle sous Linux |

Si la carte est détectée mais n'apparaît pas lors du ifconfig, il faudra charger le module correspondant à la carte, avec la commande :

```
modprobe <nom du module>
```

Parmi les modules courants on peut noter : ne2k-pci pour les cartes NE2000, via-rhine, rtl8139...

Les modules disponibles pour votre noyau se trouvent dans « /lib/modules/<nom du noyau>/kernel/drivers/net/ ». La commande suivante affiche les modules réseau disponibles pour le noyau en cours d'utilisation :

```
ls /lib/modules/`uname -r`/kernel/drivers/net/
```

Pour connaître le nom du module en fonction du nom commercial d'une carte, une recherche sur internet est souvent la meilleure solution.

### III Configuration des interfaces réseau

Le fichier à modifier pour configurer les interfaces réseau est « /etc/network/interfaces ». Il est possible de l'éditer via la commande :

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

#### III.1 Fichier de configuration « /etc/network/interfaces »

Une passerelle possédant au moins deux interfaces réseau, le fichier interfaces contiendra la configuration du rebouclage logiciel lo, et des interfaces ensXX et ensXX. Les adresses seront statiques et non en DHCP.

Pour plus de détails, se référer à la documentation « Configuration interfaces réseau ».

**Exemple de fichier « /etc/network/interfaces » :**

```
# Configuration du rebouclage logiciel (localhost)
auto lo
iface lo inet loopback
# Configuration de la première carte réseau
auto ens33
allow-hotplug eth0
iface ens33 inet static
    address 192.168.0.25
    netmask 255.255.255.0
# Configuration pour l'accès à l'extérieur des réseaux connectés à la passerelle
gateway 192.168.0.254
dns-nameservers 192.168.0.254
dns-domain example.com
# Configuration de la seconde carte réseau
auto ens37
allow-hotplug ens37
iface ens37 inet static
    address 192.168.10.254
    netmask 255.255.255.0
```

Pour que ce fichier fonctionne, il faut obligatoirement que le paquet "resolvconf" soit installé.

|                               |                       |
|-------------------------------|-----------------------|
| BTS S.N.I.R.                  | Document ressource    |
| Lycée Jean Rostand Villepinte | Passerelle sous Linux |

## III.2 Test de la configuration

Vous devez tester les deux interfaces en exécutant la commande ping et en donnant une adresse dans chacun des réseaux et vérifier qu'il n'y a aucun message d'erreur.

**Exemple :**

```
ping 192.168.0.1
ping 192.168.10.1
```

## IV Activation du routage

Pour qu'un ordinateur sous linux puisse router des paquets d'une interface à une autre (l'autoriser à agir comme un routeur), il faut obligatoirement activer le routage. Ceci est réalisé par la commande suivante :

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

Cette simple commande va indiquer à l'ordinateur qu'il doit faire passer les paquets d'une interface à l'autre en fonction de l'adresse du réseau de destination (donc se comporter comme un routeur classique).

**Une fois lancée, cette commande n'est active que jusqu'au redémarrage de l'ordinateur. Pour la rendre permanente, il faut modifier le fichier /etc/sysctl.conf (fichier qui est exécuté au lancement de l'ordinateur). En décommentant la ligne suivante.**

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Maintenant il faut tester le routage en allant sur une des machines en exécutant d'un des ordinateurs d'un des réseaux vers un des ordinateurs de l'autre réseau.

**Attention :** il faut que les deux ordinateurs aient pour adresse de passerelle l'adresse de l'interface de votre passerelle.

**Exemple :** à partir du poste 192.168.10.1

```
ping 192.168.0.1
```

L'adresse de la passerelle du poste 192.168.10.1 doit être 192.168.10.254 et l'adresse de la passerelle du poste 192.168.0.1 doit être 192.168.0.25.

## V Établissement de la table de routage

L'étape suivante est la définition des règles de routage. Ces règles précisent pour toutes les adresses d'un réseau, le moyen de l'atteindre, c'est-à-dire les routes. L'ensemble de ces règles constitue ce qu'on appelle la table de routage.

### V.1 Description du routage

Les routes peuvent être obtenues grâce à la commande route :

```
root@debian1:~# route
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref    Use Iface
default          192.168.0.254   0.0.0.0          UG    0      0      0 ens33
192.168.0.0      0.0.0.0         255.255.255.0    U     0      0      0 ens33
```

Les colonnes indiquent chacune une information sur la route paramétrée :

- x La destination (Réseau) : adresse IP qui indique quels sont les paquets de données qui vont suivre cette route selon leur destination.
- x La passerelle (Gateway) : adresse IP qui indique par où les paquets vont passer pour arriver à destination. Ils seront envoyés à cette adresse.

|                               |                       |
|-------------------------------|-----------------------|
| BTS S.N.I.R.                  | Document ressource    |
| Lycée Jean Rostand Villepinte | Passerelle sous Linux |

- x Le masque de sous-réseau (Genmask) : suite de 4 octets (comme une adresse IP) qui permet d'indiquer quelle est la taille de chaque partie de l'adresse IP (partie réseau et partie hôte).
- x Les indicateurs : état de la route (ici U signifie que la route est active (Up) et G que la route est une passerelle (Gateway).
- x Les sauts (Metric) : nombre qui indique combien d'intermédiaires il reste avant d'arriver à la destination. Cette information n'est plus utilisée (sauf par des programmes comme routed (RIP)).
- x Les références (Ref) : nombre qui indique le nombre de références associées à cette route. Cette information n'est pas utilisée.
- x L'utilisation (Use) : compteur d'utilisation de la route.
- x L'interface réseau (Iface) : nom de l'interface réseau qui sera utilisée pour cette route.

Cette table indique que le réseau 192.168.0.0/24 est connecté directement sur l'interface eth0 et que le chemin par défaut si aucune route n'est précisée dans la table est 192.168.0.254 (passerelle par défaut).

Il n'est normalement pas nécessaire d'ajouter les règles de routage pour les réseaux auxquels la machine est connectée. En effet, la configuration d'une carte réseau à l'aide de la commande **ifconfig** ajoute automatiquement à la table de routage une règle pour envoyer les paquets à destination de ce réseau par l'interface réseau qui y est connectée.

## V.2 Modification du routage

La commande **route** devient réellement nécessaire lorsqu'il faut définir les passerelles à utiliser pour l'envoi des paquets destinés à une machine à laquelle la machine locale ne peut accéder directement.

La syntaxe utilisée est donc la suivante :

```
route add -net adresse netmask masque gw passerelle interface
```

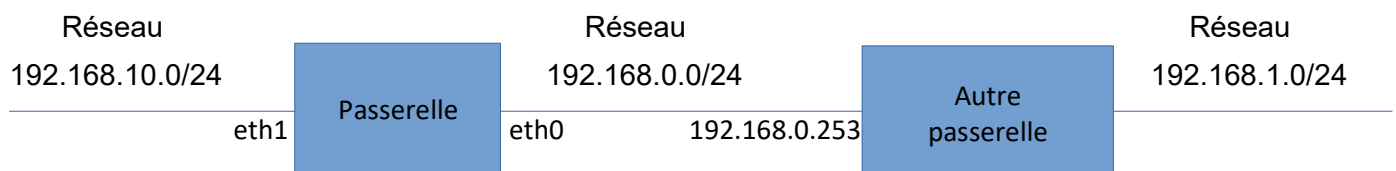
**passerelle** est l'adresse IP de la passerelle à utiliser pour router les paquets qui vérifient les critères de cette règle. Les autres paramètres sont les mêmes que pour les règles de routage classique.

**adresse** est l'adresse IP de la destination, que celle-ci soit un réseau ou une machine

**masque** est le masque de sous-réseau **masque**.

**interface** est l'interface réseau vers laquelle doivent être envoyés les paquets qui vérifient les critères de sélection de cette règle.

Par exemple, supposons qu'une machine soit connectée à un réseau d'adresse 192.168.0.0, et que sur ce réseau se trouve une passerelle d'adresse 192.168.0.253 permettant d'atteindre un autre réseau, dont l'adresse est 192.168.1.0/24.



La passerelle aura typiquement la règle de routage suivante :

```
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.253 eth0
```

La règle permet d'envoyer à la passerelle 192.168.0.253 tous les paquets à destination du réseau 192.168.1.0.

**Attention :** Pour que les routes que vous avez ajoutées, soient prises en compte lors du prochain démarrage, il faut que vous copiez ces commandes dans le fichier « **/etc/rc.local** » avant la commande exit.

Le test du routage est d'exécuter un ping vers n'importe quel ordinateur :

```
ping www.google.fr
```