

Passerelle LINUX

Présentation

Vous allez apprendre à configurer un serveur LINUX pour connecter un réseau privé à l'Internet par votre belle connexion Haut Débit, qu'elle soit ADSL ou Câble.

Comme l'immense majorité des connexions, câble ou ADSL utilisent maintenant PPPoE, il est vivement conseillé de lire d'abord le chapitre sur ce sujet¹.

Comme une passerelle vers l'Internet sur une connexion permanente présente quelques dangers potentiels éventuellement lourds de conséquences :

- Indiscrétions dans vos données ou destruction pure et simple de ces dernières,
- pire, emploi de votre machine comme relais pour d'autres actes de piraterie, situation qui risquerait fort de vous attirer pas mal d'ennuis,

Je vous conseille également de lire le chapitre sur la sécurité², pour avoir un premier aperçu de ce qu'il risque de vous arriver.

Pré-requis

Vous savez déjà installer LINUX et vous avez quelques notions des fichiers de configuration, des commandes en ligne, vous savez installer un "package". Il sera intéressant pour vous de savoir utiliser un éditeur de texte (Midnight Commander (mc) est d'un emploi facile et propose un outil d'édition suffisant).

Vous disposez d'une connexion Internet. Ce qui est dit ici fonctionne avec tout type de connexion, mais s'appuie sur une connexion de type PPPoE Câble ou ADSL. Alors, n'oubliez pas de lire le chapitre sur PPPoE :)

La manipulation proposée est faite sur un PENTIUM 166, mais un i486 suffirait (en faisant de préférence l'impasse sur l'interface graphique). La version utilisée dans cet exposé est la MANDRAKE 9, installée avec les options de réseaux (Si vous avez fait une installation minimale, vous serez peut-être amené à réinstaller LINUX où à recompiler le noyau avec les bonnes options...). Pour la configuration du routage, c'est IPTables qui sera utilisé.

Ce chapitre, juste destiné à montrer combien il est simple de réaliser une passerelle, est à considérer comme une introduction au chapitre suivant : "Netfilter et IPTables"³, qui vous expliquera plus en détail le fonctionnement du filtrage de paquets et les méthodes de sécurisation de votre passerelle.

1 PPPoE : <http://christian.caleca.free.fr/pppoe/>

2 Sécurité : <http://christian.caleca.free.fr/securite/>

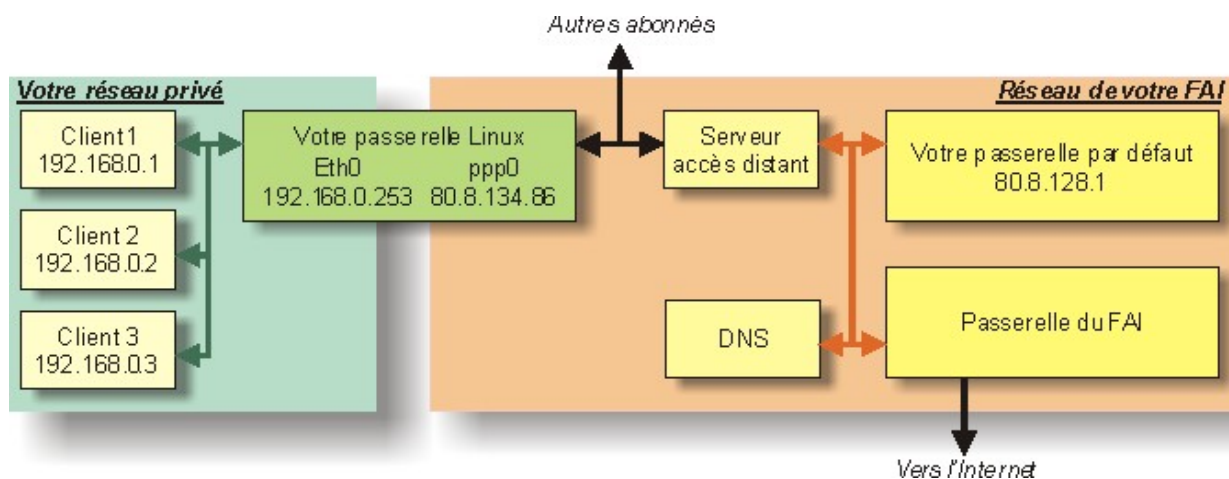
3 Netfilet et IPtables : <http://christian.caleca.free.fr/netfilter/>

Plan du chapitre

Présentation.....	1
Pré-requis.....	1
Théorie.....	3
Architecture du travail terminé.....	3
Mise en garde.....	3
Réseau privé.....	3
Attention !.....	3
Connexion au FAI.....	3
Configuration des clients.....	4
Et après ?.....	4
Une démonstration.....	4
Le masquage d'adresses.....	5
Un peu de logique.....	5
L'opération de masquage (ou camouflage).....	5
Avantages.....	5
Inconvénients.....	6
Interfaces.....	7
Pré-requis.....	7
Installation.....	7
Note de l'auteur.....	8
Configuration Ethernet.....	8
1° carte: vers le réseau local.....	8
Vérifications.....	10
Elle n'est pas activée ?.....	11
2° carte, vers le modem.....	11
Configuration de PPPoE.....	12
Vérifications.....	13
Conclusions.....	16
Résumé de la situation.....	16
Mises en garde.....	17
Passerelle simple.....	19
Netfilter et IPTables.....	19
Installation.....	19
Configuration simpliste.....	20
Vous croyez que c'est fini ?.....	20
Rendre ces choses définitives.....	20
Et la sécurité ?.....	21
Plus de confort.....	21
Le problème du DNS.....	21
La configuration IP des clients.....	21

Théorie

Architecture du travail terminé



Mise en garde

Les adresses IP définies sur le schéma sont données à titre d'exemple...

Réseau privé

Bien entendu, tout fonctionne avec TCP/IP, vous configurez donc votre réseau privé avec des adresses privées. Les réseaux 192.168.xxx.yyy sont des réseaux destinés à cet usage. Ce ne sont pas les seuls, mais comme vous avez peu de chances d'avoir plus de 254 machines sur votre réseau privé, une classe C devrait vous suffire. Vous n'avez déjà rien compris à ce que j'ai raconté ? Alors, vous devriez commencer par lire les chapitres sur les réseaux⁴, TCP/IP⁵ et le routage⁶...

Sur ce réseau privé, on trouve :

- Tous vos postes clients (ici 1, 2 et 3).
- Une interface réseau de votre passerelle LINUX.

Attention !

Dans notre exemple, l'adresse 192.168.0.0 NE DOIT PAS être utilisée par une machine, elle représente l'adresse du réseau dans son ensemble. De même, l'adresse 192.168.0.255 est réservée au "broadcast". Pour plus de détails, voire le chapitre TCP/IP sur ce site.

Connexion au FAI

La deuxième carte réseau placée dans le serveur LINUX est directement connectée au modem-câble

4 Les réseaux : <http://christian.caleca.free.fr/reseaux/>

5 TCP/IP : <http://christian.caleca.free.fr/tcpip/>

6 Le routage : <http://christian.caleca.free.fr/routage/>

ou modem ADSL. Généralement, vous n'avez droit qu'à une adresse IP "dynamique". C'est votre FAI qui vous la prête pour une durée qui, normalement, ne dépassera pas 24h. Chez Wanadoo, tout est fait pour que vous ne disposiez jamais deux fois de suite de la même adresse IP.

Théoriquement, une connexion par USB devrait aussi faire l'affaire. Elle n'est pas traitée ici, mais si vous arrivez à faire fonctionner un modem en USB sous Linux, le reste de ce chapitre est certainement exploitable, avec un minimum d'interprétation.

Configuration des clients

Les clients (les postes du réseau privé) peuvent être de n'importe quelle nature, pourvu qu'ils disposent d'un OS réseau gérant le protocole TCP/IP.

Il faut donc installer TCP/IP et le configurer de la façon suivante :

- Donner une adresse IP fixe dans un réseau privé (192.168.0.x dans notre exemple).
- Indiquer comme passerelle par défaut l'adresse IP de la machine LINUX **dans le réseau privé** (Celle qui est attachée à eth0: 192.168.0.253 dans notre exemple).
- Indiquer l'adresse du DNS de votre fournisseur d'accès (vous pouvez la trouver en faisant un "nslookup" ou mieux encore, un "dig" sur la machine LINUX). Vous pourrez aussi construire votre propre DNS sur votre machine Linux, comme c'est indiqué dans le chapitre DNS⁷.

Ceci devrait suffire. Le client PPPoE que nous allons utiliser est suffisamment performant pour résoudre tout seul l'épineux problème du MTU. Voir le chapitre sur PPPoE à ce sujet.

Et après ?

Après, vous arrivez sur la passerelle de votre FAI. Elle ne fonctionne pas tout à fait comme celle que nous allons monter, mais presque ("masquerade" en moins, ici, nous avons des "vraies" adresses IP).

Nous n'allons pas ici entrer dans les détails du routage, c'est déjà fait ailleurs sur ce site, mais il faut en parler un petit peu tout de même. Lorsqu'une machine d'un réseau A (par exemple 192.168.0.0) veut communiquer avec une machine d'un réseau B (par exemple 192.168.1.0), même si ces deux machines sont physiquement connectées au même média, elles ne se verront pas. Il faut mettre en place une passerelle entre ces deux réseaux, c'est à dire une machine qui a un pied dans chaque réseau, un peu comme votre machine LINUX. En plus, il faudra expliquer à cette machine qu'elle doit établir un passage entre les deux réseaux.

Une démonstration...

Trace l'itinéraire vers wateau.auteuil.cnrs-dir.fr [193.51.136.4] avec un maximum de 30 tronçons :

Durée du ping	Nom de la machine	Adresse IP de la machine
1 <10 ms <10 ms <10 ms	LINUX	[192.168.0.253]
2 12 ms 12 ms 13 ms	ca-ol-marseille-1-1.abo.wanadoo.fr	[80.8.128.1]
3 12 ms 12 ms 35 ms	172.19.46.65	[172.19.46.65]
4 11 ms 12 ms 12 ms	GE1-1-811.ncmar301.Marseille.francetelecom.net	[193.252.227.82]

⁷ DNS : <http://christian.caleca.free.fr/dns/index.html>

C'est pas la peine d'aller plus loin :

1. Ma passerelle. Elle s'appelle poétiquement LINUX, son IP dans mon réseau : 192.168.0.253
2. La 1° passerelle du FAI, je parle pas de son nom, son IP: 80.8.128.1
3. La Passerelle de sortie du FAI: 172.19.46.65

La route complète aurait pu être tracée, nous aurions vu alors toutes les passerelles d'interconnexions de réseaux. Vous ferez la manip. vous même :

- "tracert <nom de la machine>" sous Windows (console)"
- "traceroute <nom de la machine>" sous LINUX.

Le masquage d'adresses

(encore appelé "camouflage d'adresses")

Un peu de logique

Nous devons être quelques milliers dans le monde (et peut-être plus...) à utiliser les même classes privées, elles sont faites pour ça ! Ces adresses ne transitent JAMAIS sur l'Internet. Mais alors comment faire? C'est l'objet de la fonction de masquage, appelée "MASQUERADE" chez LINUX. Génériquement, c'est du NAT (Network Address Translation), associé à du PAT (Port Address Translation). Par extension, on parle systématiquement de NAT.

L'opération de masquage (ou camouflage)

1. récupère votre socket,
2. remplace votre adresse IP par la sienne, côté extérieur,
3. remplace votre port de réponse X par un qu'il choisit lui-même (Y),
4. tient à jour une table avec votre socket et le numéro de port Y,
5. transmet la requête à votre place, avec le socket qu'il a construit,
6. récupère la réponse sur son port Y,
7. remet dans la réponse votre adresse à la place de la sienne,
8. vous transmet la réponse sur votre port X

Simple non ?

Avantages

- Votre machine est inaccessible directement depuis l'Internet puisque votre IP est inconnue, seule celle du camoufleur est visible.
- Vous n'avez besoin que d'une seule IP "officielle", celle fournie par votre FAI, pour accéder à l'Internet depuis toutes les machines de votre réseau privé.
- L'opération est complètement transparente pour le client de votre réseau privé, il suffit de

configurer correctement votre pile IP. (adresse IP interne, masque de sous réseau qui, dans notre cas serait 255.255.255.0, et adresse du DNS de votre FAI pour avoir la résolution des noms).

Inconvénients

Mais en est-ce un ? Votre machine est inaccessible directement depuis l'Internet puisque votre IP est inconnue, seule celle du camoufleur est visible. Vous ne pouvez donc pas placer un serveur derrière votre passerelle, du moins pas très simplement. Des solution existent cependant, comme nous le verrons avec Netfilter⁸.

⁸ Netfilet et IPtables : <http://christian.caleca.free.fr/netfilter/>

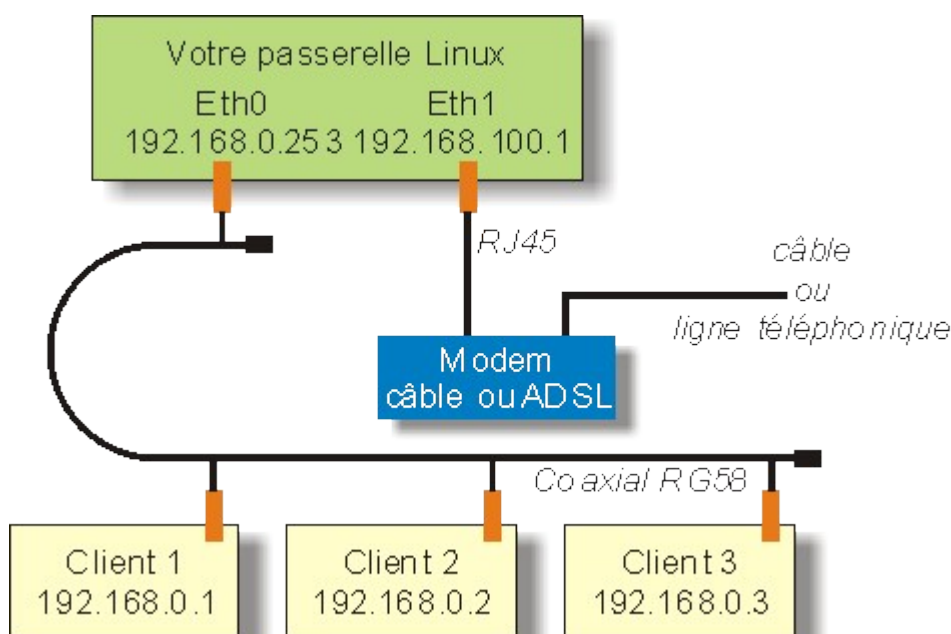
Interfaces

Pré-requis

Votre réseau privé est déjà installé, les postes disposent de leur adresse IP et ont un nom de machine. Le réseau est testé et tout fonctionne. (On supposera que les clients sont sous Windows, toutes versions confondues. Si ce n'est pas le cas, il vous faudra "traduire"). Nous supposons que le modem est utilisé avec une connexion Ethernet. C'est aussi possible d'utiliser USB, mais plus compliqué, surtout sur Linux, à cause des difficultés à trouver les drivers du modem.

Installation

Il va falloir deux interfaces réseaux :



- L'une pour vous connecter à l'Internet via le modem
- L'autre pour vous connecter à votre réseau privé. (N'oublions pas que nous sommes en présence de deux réseaux distincts et que nous voulons faire une passerelle entre les deux).

Note pour les bricoleurs :

Un bricolage sordide permet de tout faire avec une seule interface, Linux permettant de faire du "multihosting", c'est à dire permettant d'attribuer deux IP différentes à la même interface. Amusant, mais pas très utile.

L'interface dédiée au modem doit impérativement être une RJ45. Nous l'installerons en dernier.

L'interface dédiée au réseau local peut être de type coaxial, c'est plus simple à câbler s'il n'y a pas trop de postes.

Attention, il y a un danger, ce type de câblage fait que s'il y a une coupure de la liaison, tout le réseau est en panne. (Pensez à terminer le câble par des bouchons 50 Ohms à chaque extrémité).

Autre problème, le RG58 ne fonctionne qu'en 10 Mb/s. Ce n'est pas gênant pour Internet, ça peut l'être pour votre réseau local.

Vous avez bien entendu la possibilité de câbler votre réseau local avec un HUB et du câble type 5 (paires torsadées sur connecteur RJ45). Ce câblage est garanti pour 100Mb/s.

Pour plus de détails sur les réseaux, voyez le chapitre qui leur est dédié⁹.

Note de l'auteur...

Je vous conseille, dans la mesure du possible, de ne pas choisir deux cartes du même type (Il en existe de type "combo" qui disposent des deux prises, BNC et RG58). Non pas que ça ne marche pas, mais vous aurez peut-être des problèmes de configuration et vous aurez sûrement des problèmes pour les identifier. Ceci dit, on peut y arriver quand même.

Pensez également que le plug and play n'est pas très copain avec LINUX. Si vous utilisez des cartes au format ISA, trouvez des cartes configurables par soft, avec la possibilité d'inhiber les fonctions plug and play. D'une manière générale, choisissez de préférence des cartes qui soient compatibles NE2000.

Avec des cartes au format PCI, vous aurez sans doute beaucoup moins de problèmes.

Configuration Ethernet

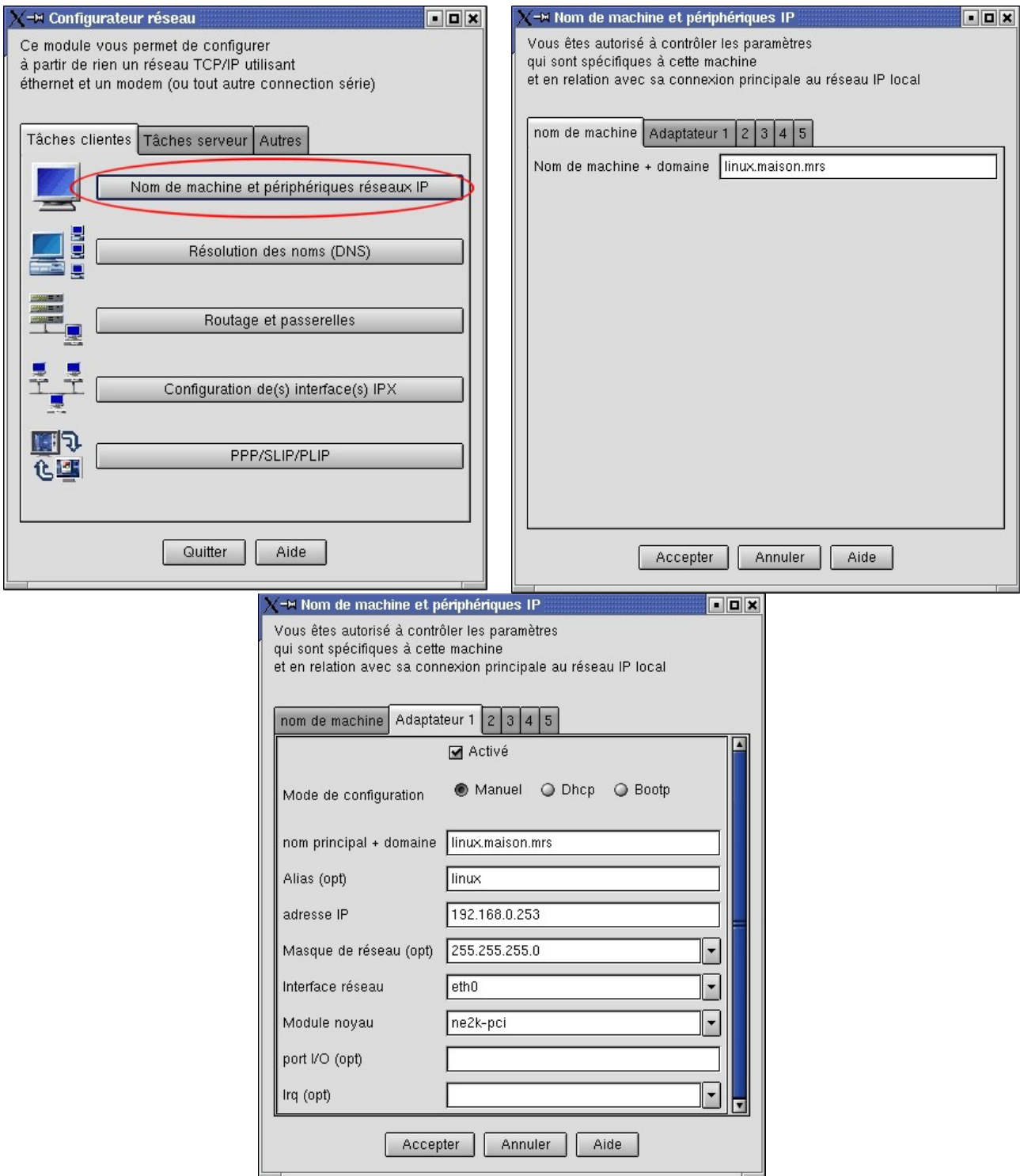
C'est là que les choses peuvent se compliquer... N'essayez pas, à moins que vous ne maîtrisiez parfaitement les fichiers de configuration de LINUX et son fonctionnement, (mais dans ce cas, vous risquez de ne rien apprendre ici), d'installer les deux cartes en même temps... Mieux vaut procéder par étapes et vérifier le bon fonctionnement de chacune d'elles avant de passer à la suivante.

1° carte: vers le réseau local

Vous devez évidemment être connecté en "root".

Je vous donne une méthode graphique avec netconf (les puristes n'aiment pas, mais c'est tellement plus facile à faire). Sous X, vous démarrez **netconf** et vous cliquez sur "Nom de la machine et périphériques réseaux IP".

⁹ Les réseaux : <http://christian.caleca.free.fr/reseaux/>



Commençons, puisqu'on y est par le nom de la machine. Ce nom ne vous sera utile que sur votre réseau local. Vous choisissez un nom original et vous le placez dans un domaine "en bois" non moins original, comme donné dans l'exemple.

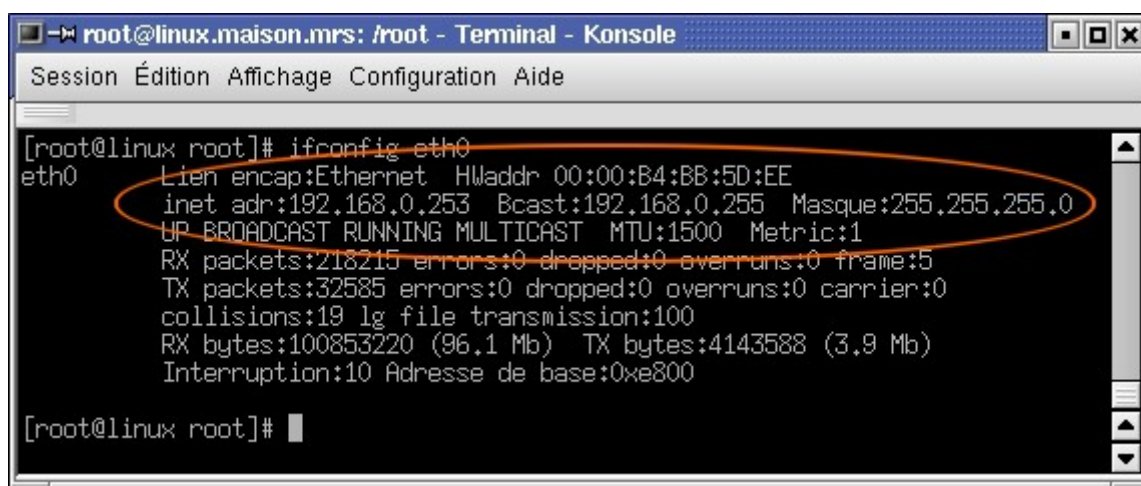
Pour l'adaptateur 1 (eth0), qui est connecté à votre réseau privé, il faut l'activer, le configurer en manuel. Choisissez une adresse IP dans votre réseau, ici 192.168.0.253, fixez le masque de sous réseau 255.255.255.0.

Dans l'exemple, il s'agit d'une carte combo PCI. Si vous avez installé Linux avec l'interface déjà en place, elle devrait avoir été détectée par l'installateur et vous devriez déjà avoir donné les renseignements nécessaires à sa configuration. Vous pouvez toujours ici ajouter une carte ou la reconfigurer.

Vous acceptez, vous quittez "netconf". Le programme vous propose d'activer les changements, faites-le. Si vous êtes curieux de nature, vous pouvez voir ce qui doit être fait. Ici, normalement, l'opération importante est le redémarrage du service "Network".

Vérifications

Vous ouvrez une console :



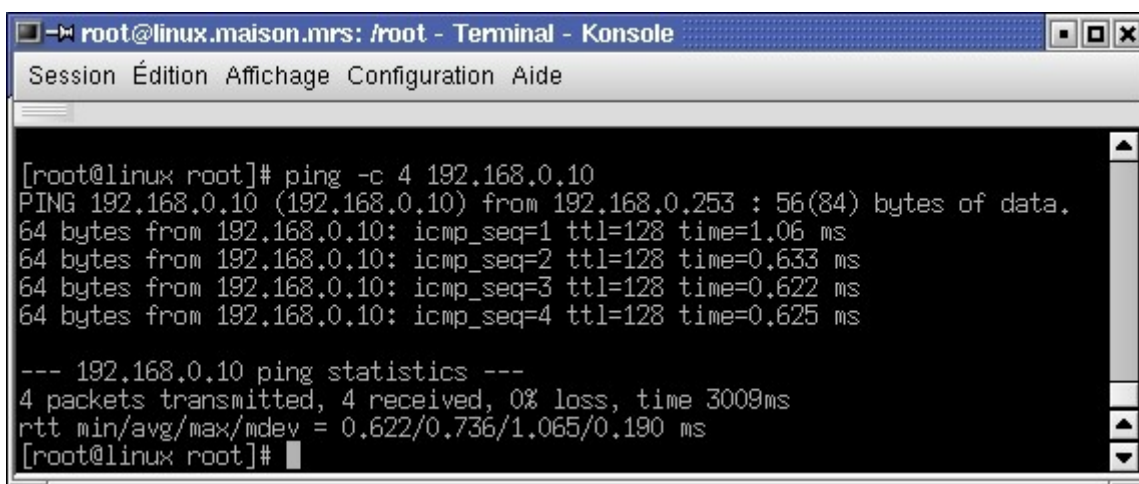
```
root@linux.maison.mrs: /root - Terminal - Konsole
Session  Édition  Affichage  Configuration  Aide

[root@linux root]# ifconfig eth0
eth0      Lien encap:Ethernet  HWaddr 00:00:B4:BB:5D:EE
          inet adr:192.168.0.253 Bcast:192.168.0.255 Masque:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:218215 errors:0 dropped:0 overruns:0 frame:5
          TX packets:32585 errors:0 dropped:0 overruns:0 carrier:0
          collisions:19 lg file transmission:100
          RX bytes:100853220 (96.1 Mb)  TX bytes:4143588 (3.9 Mb)
          Interruption:10 Adresse de base:0xe800

[root@linux root]#
```

Vous tapez "ifconfig eth0" et des choses doivent s'afficher :

- eth0: c'est la carte que vous venez d'installer. Si elle n'y est pas, c'est qu'elle n'est pas activée.
- Constatez que l'IP, le masque de sous réseau sont corrects. Vous voyez également l'adresse MAC (Ethernet HWaddr). Là, vous avez le moyen d'identifier votre carte si vous en avez plusieurs identiques. L'adresse MAC est normalement inscrite sur chaque carte, de façon lisible par l'être humain alphabétisé.



```
root@linux.maison.mrs: /root - Terminal - Konsole
Session Édition Affichage Configuration Aide

[root@linux root]# ping -c 4 192.168.0.10
PING 192.168.0.10 (192.168.0.10) from 192.168.0.253 : 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=128 time=1.06 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=128 time=0.633 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=128 time=0.622 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=128 time=0.625 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% loss, time 3009ms
rtt min/avg/max/mdev = 0.622/0.736/1.065/0.190 ms
[root@linux root]#
```

Faites maintenant un ping vers l'une quelconque de vos machines du réseau local. Ça doit passer.

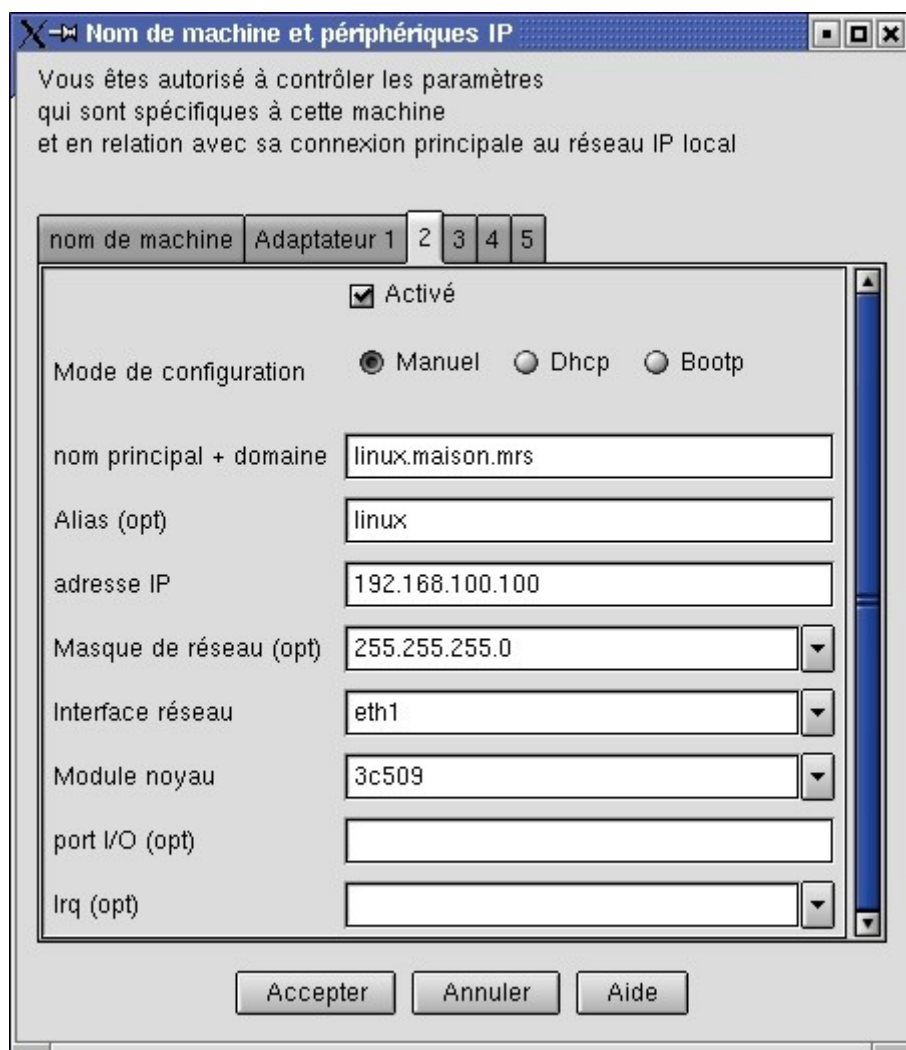
Elle n'est pas activée ?

C'est pas encore grave. tapez la commande: `ifup eth0` (ce qui veut dire: "active l'interface eth0"). Si tout se passe bien, vous devez récupérer la main au bout d'un temps normalement court.

Refaites alors `ifconfig`. Si `eth0` n'apparaît toujours pas, c'est que votre carte est mal configurée. Vérifiez le module noyau, l'IRQ, les E/S (en notation hexa à la mode C: `0x310` par exemple) si c'est une carte ISA autre que de marque 3Com. En effet, le driver 3Com est capable de trouver tout seul ces informations, même sur une carte qui n'est pas "plug & play".

2° carte, vers le modem

Bien que ce ne soit pas absolument nécessaire, nous allons tout de même configurer complètement cette interface. En effet, la plupart des modems, câble comme ADSL, proposent un mini serveur HTTP qui permet au minimum de connaître avec plus ou moins de détails l'état du modem. L'exemple donné ici est fait avec un modem câble Thomson TCM290, utilisé par Câble Wanadoo.



L'interface utilisée ici est une antique 3Com 509b sur bus ISA. Vous la configurez de la même manière que la précédente, mais en choisissant des valeurs adaptées à votre modem.

- Le TCM290 dispose par défaut de l'IP 192.168.100.1, nous choisissons par exemple, les valeurs données dans l'illustration.
- Le modem ADSL Alcatel Speed Touch Home, quant à lui, propose par défaut l'adresse 10.0.0.138. Dans ce cas, il faudrait par exemple choisir une IP=10.0.0.1 et un masque 255.0.0.0

Acceptez cette configuration. Vous pouvez ensuite faire les mêmes vérifications que pour eth0, en faisant cette fois-ci un ping sur votre modem.

A ce stade, vous avez vos deux adaptateurs réseau qui sont opérationnels. Si ça suffit du côté du réseau privé, il va encore falloir faire un effort du côté du Net. En effet, il reste à configurer PPPoE.

Configuration de PPPoE

Pour la suite, la lecture préalable du chapitre dédié à PPPoE¹⁰ est fortement recommandée, mais depuis le temps que je le dis, vous l'avez certainement fait. Toujours pas ? Nous nous contenterons alors de "recettes de cuisine", mais tout de même, allez le lire, ce chapitre...

Assurez-vous d'abord que les paquetages RPM **ppp** et **rp-pppoe** sont installés, **ppp** est nécessaire à PPPoE. Pour installer et configurer convenablement votre connexion PPPoE, vous aurez à renseigner les fichiers `/etc/ppp/pppoe.conf` et `/etc/ppp/chap-secrets`.

NDRL : Sous Debian, PPPoE est fournis par le paquet du même nom, soit, `pppoe`. Celui-ci peut-être

¹⁰ PPPoE : <http://christian.caleca.free.fr/pppoe/>

aisément configuré avec l'utilisation du paquet `pppoe-conf`.

Rp-pppoe peut fonctionner de deux manières :

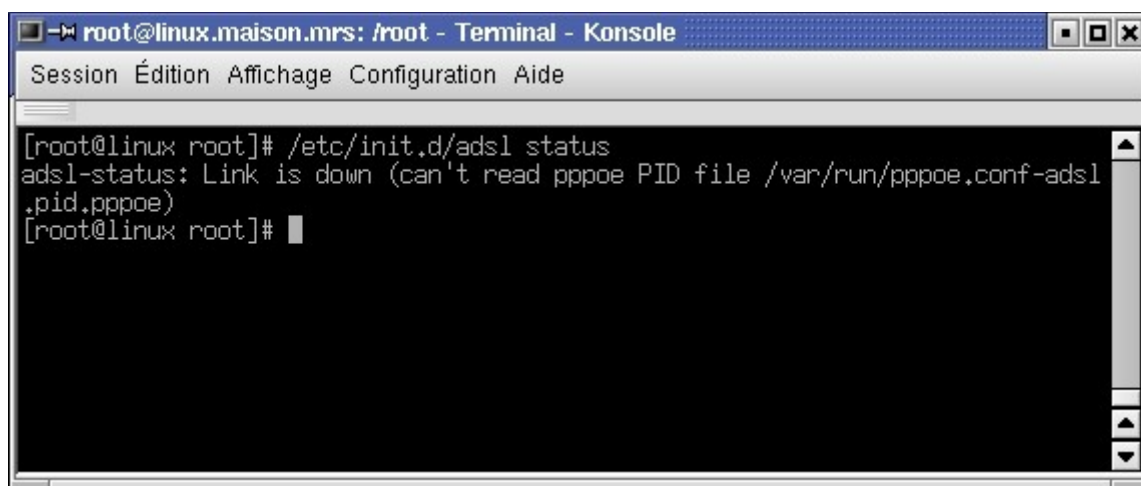
- A la mode d'une connexion RTC, avec une interface graphique pour établir et fermer la connexion,
- A la mode "connexion permanente"; qui est vivement conseillée ici. Dans ce cas, pas d'interface graphique, mais un démon à charger au démarrage.

Pour plus de détails, consultez la page `rp-pppoe`¹¹ dans le chapitre `pppoe` de ce site. Si ce n'est toujours pas fait, contentez-vous d'utiliser le script de configuration fourni avec `rp-pppoe`. Dans la distribution Mandrake 9, c'est `/usr/sbin/pppoe-setup`. Répondez aux questions posées et le script mettra à jour les fichiers de configuration.

Le paquetage **rp-pppoe** a été conçu initialement pour ADSL. Ça ne l'empêche absolument pas de fonctionner aussi avec le câble. Ne vous étonnez pas si toutes les commandes contiennent "ADSL".

Vérifications

Nous allons ici détailler une procédure de vérification de l'établissement d'une connexion PPPoE. Peut-être n'en aurez-vous pas besoin, mais ça peut toujours servir...



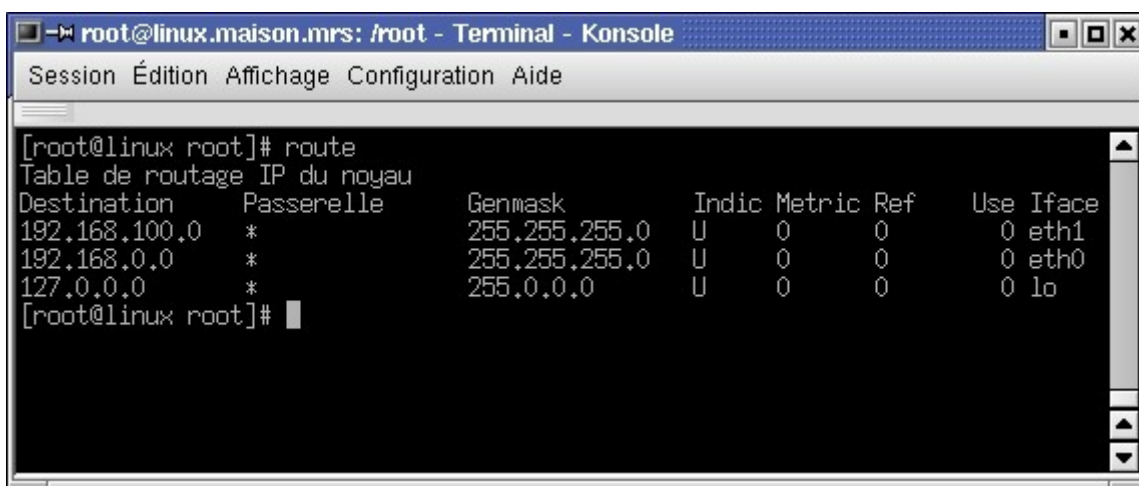
Nous supposons que vous avez fait tout ce qu'il faut pour configurer correctement PPPoE, mais que le démon n'est pas encore chargé. Vérifiez ça en faisant :

```
/etc/init.d/adsl status
```

Vous devez obtenir ce qui est inscrit dans l'illustration. Éventuellement, faites un :

```
/etc/init.d/adsl stop
```

¹¹ `rp-pppoe` : http://christian.caleca.free.fr/pppoe/rp-pppoe_&_linux.htm

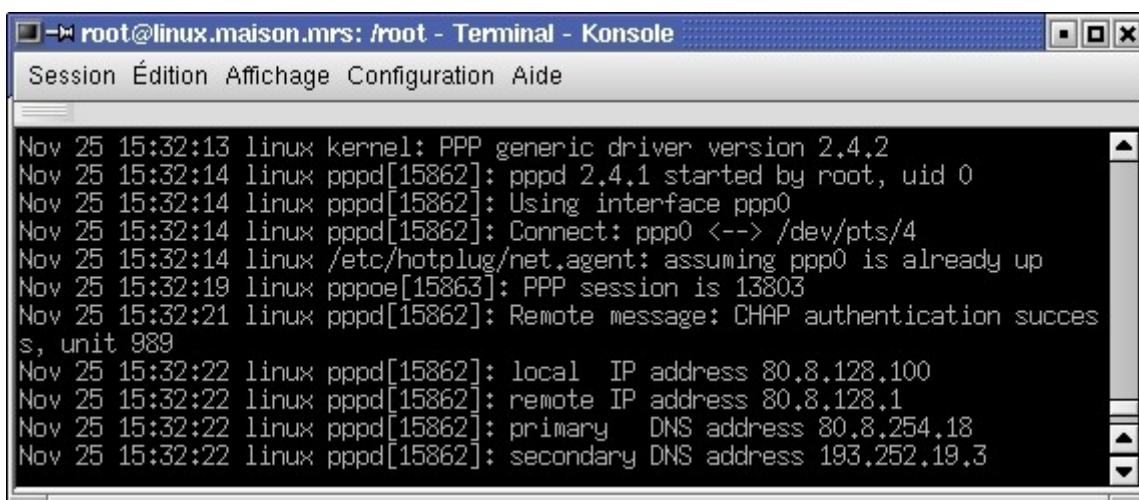


```
[root@linux root]# route
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
192.168.100.0    *                255.255.255.0   U        0      0        0 eth1
192.168.0.0      *                255.255.255.0   U        0      0        0 eth0
127.0.0.0        *                255.0.0.0       U        0      0        0 lo
[root@linux root]#
```

Vérifiez ensuite votre table des routes. Elle doit être comme celle-ci. La commande est tout simplement :

```
route
```

Notez qu'aucune route par défaut n'est définie.



```
Nov 25 15:32:13 linux kernel: PPP generic driver version 2.4.2
Nov 25 15:32:14 linux pppd[15862]: pppd 2.4.1 started by root, uid 0
Nov 25 15:32:14 linux pppd[15862]: Using interface ppp0
Nov 25 15:32:14 linux pppd[15862]: Connect: ppp0 <--> /dev/pts/4
Nov 25 15:32:14 linux /etc/hotplug/net.agent: assuming ppp0 is already up
Nov 25 15:32:19 linux pppoe[15863]: PPP session is 13803
Nov 25 15:32:21 linux pppd[15862]: Remote message: CHAP authentication success, unit 989
Nov 25 15:32:22 linux pppd[15862]: local IP address 80.8.128.100
Nov 25 15:32:22 linux pppd[15862]: remote IP address 80.8.128.1
Nov 25 15:32:22 linux pppd[15862]: primary DNS address 80.8.254.18
Nov 25 15:32:22 linux pppd[15862]: secondary DNS address 193.252.19.3
```

Ouvrez, maintenant une nouvelle console, dans laquelle vous allez lire les journaux. Tapez dans cette console :

```
tail -f /var/log/messages
```

Et retournez dans la première console pour démarrer PPPoE :

```
/etc/init.d/adsl start.
```

Vous devez observer quelque chose d'analogue à l'illustration. Notez que vous avez obtenu :

- Une IP (dans l'exemple 80.8.128.100),
- une passerelle par défaut (80.8.128.1)
- deux adresses de DNS.

```

root@linux.maison.mrs: /root - Terminal - Konsole
Session Édition Affichage Configuration Aide

[root@linux root]# ifconfig ppp0
ppp0      Lien encap:Protocole Point-à-Point
          inet adr:80.8.128.100 P-t-P:80.8.128.1  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:3
          RX bytes:1796 (1.7 Kb)  TX bytes:1491 (1.4 Kb)

[root@linux root]#

```

Vous devez maintenant disposer d'une nouvelle interface nommée ppp0. Vous pouvez le vérifier en faisant :

```

ifconfig ppp0

root@linux.maison.mrs: /root - Terminal - Konsole
Session Édition Affichage Configuration Aide

[root@linux root]# route -n
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
80.8.128.1       0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.100.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.0.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0          80.8.128.1     0.0.0.0         UG    0      0        0 ppp0

[root@linux root]#

```

Vérifiez vos routes, une route par défaut doit apparaître, pointant sur la passerelle du FAI à travers ppp0 (la dernière ligne). Un

```
route -n
```

sera peut-être plus lisible.

ppp sait mettre en place une route par défaut, à la condition qu'il n'y en ait pas déjà une lors de son démarrage. Faites éventuellement attention à ce détail.

```

root@linux.maison.mrs: /root - Terminal - Konsole
Session Édition Affichage Configuration Aide

;; Query time: 83 msec
;; SERVER: 80.8.254.18#53(80.8.254.18)
;; WHEN: Mon Nov 25 15:40:49 2002
;; MSG SIZE rcvd: 436

[root@linux root]#

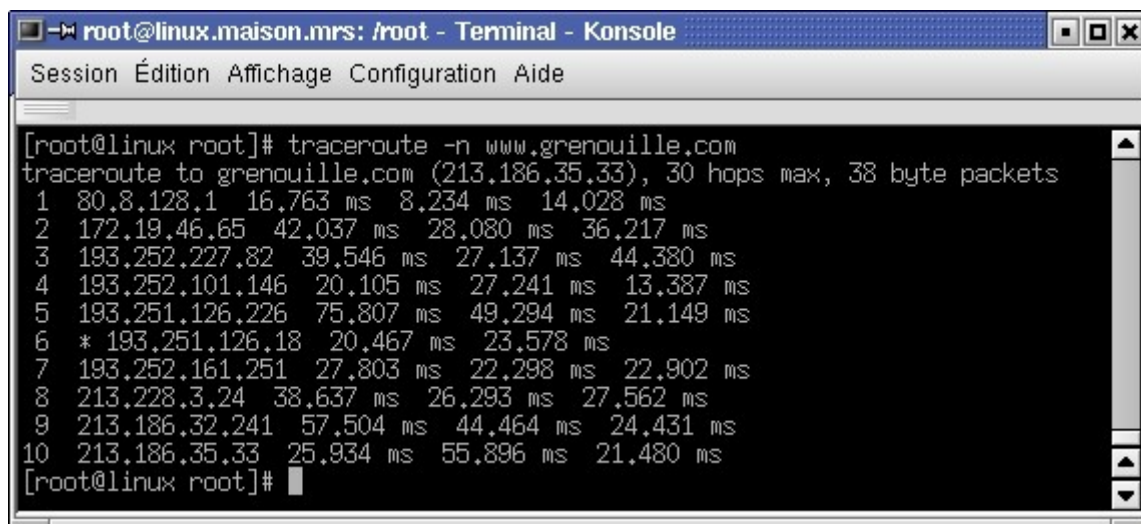
```

Vous pouvez de même retrouver à tout moment le DNS principal fourni par votre FAI, avec la commande :

```
dig
```

Seules les dernières lignes sont intéressantes ici.

Vous pouvez maintenant renseigner tous vos postes du réseau local, en ce qui concerne le DNS.



```
root@linux.maison.mrs: /root - Terminal - Konsole
Session Édition Affichage Configuration Aide

[root@linux root]# traceroute -n www.grenouille.com
traceroute to grenouille.com (213.186.35.33), 30 hops max, 38 byte packets
 1 80.8.128.1 16.763 ms 8.234 ms 14.028 ms
 2 172.19.46.65 42.037 ms 28.080 ms 36.217 ms
 3 193.252.227.82 39.546 ms 27.137 ms 44.380 ms
 4 193.252.101.146 20.105 ms 27.241 ms 13.387 ms
 5 193.251.126.226 75.807 ms 49.294 ms 21.149 ms
 6 * 193.251.126.18 20.467 ms 23.578 ms
 7 193.252.161.251 27.803 ms 22.298 ms 22.902 ms
 8 213.228.3.24 38.637 ms 26.293 ms 27.562 ms
 9 213.186.32.241 57.504 ms 44.464 ms 24.431 ms
10 213.186.35.33 25.934 ms 55.896 ms 21.480 ms
[root@linux root]#
```

Voilà. PPPoE est en place et vous avez un accès au Net. Vous pouvez vous en assurer en faisant par exemple, un traceroute vers www.grenouille.com¹² :

```
traceroute -n www.grenouille.com
```

Pour la suite, vous exploiterez le script `/etc/init.d/adsl` avec SystemV pour lancer automatiquement votre session PPPoE au démarrage. Mandrake propose plusieurs solutions graphiques pour maintenir les niveaux de démarrage, utilisez la solution que vous préférez.

Conclusions

Résumé de la situation

Vous disposez maintenant d'une machine qui possède deux connexions réseaux :

- L'une : eth0 sur votre réseau privé, protocole TCP/IP, la pile est configurée manuellement, en fonction de vos paramètres de réseau,
- L'autre peut paraître un peu plus complexe et nous sommes allés tellement vite qu'il faudrait maintenant faire le point.
 - Eth1 est, comme son nom l'indique, une interface Ethernet. Elle ne sert à rien d'autre d'important qu'à supporter la connexion **PPP over Ethernet** vers votre fournisseur d'accès. En aucun cas, la configuration IP de cette interface n'est utilisée pour accéder à l'Internet.
Je sais que ce n'est pas facile à comprendre, mais lorsque vous aurez tout compris de

¹² <http://www.grenouille.com/>

ce qui est dit sur ce site, vous n'aurez plus de difficultés.

PPPoE, c'est, répétons-le du **Point to Point Protocol over Ethernet**, la couche IP que l'on peut ajouter par dessus ne sert à rien pour PPPoE. Elle ne sert ici qu'à une chose : permettre d'accéder au serveur HTTP situé dans le modem. Si vous n'avez rien à faire de cette fonctionnalité, vous pouvez vous contenter de définir votre carte Ethernet, sans lui attribuer d'IP ni de masque de sous réseau et en décochant la case "Activé", ça n'empêchera absolument pas PPPoE de fonctionner par dessus.

- ppp0, en revanche, est un lien ppp monté par rp-pppoe lorsque la session est ouverte. Ce lien dispose d'une adresse IP dynamique, fournie par votre FAI, selon un principe proche de DHCP, mais ce n'est pas DHCP, c'est un serveur d'accès distant. Tout ça est expliqué en détail dans le chapitre sur PPPoE¹³ (peut-être l'avez-vous déjà lu ?). Ce lien ppp0, qui n'existe que lorsqu'une session PPPoE a été ouverte avec succès, présente donc :
 - Une adresse IP dynamique (renouvelable à chaque session PPPoE, session qui ne peut dépasser 24h),
 - un masque de sous-réseau,
 - une adresse de passerelle par défaut pour les connexions hors du réseau de votre FAI,
 - deux adresses de DNS pour la résolution des noms.

Mises en garde

A ce stade, même si votre machine LINUX est connectée aux deux réseaux, elle ne fonctionnera pas encore en tant que passerelle pour votre réseau privé. Il faut encore:

- Mettre en oeuvre le système de "masquerading" sur la machine LINUX,
- vous assurer que tous vos postes du réseau privé sont correctement configurés :
 - Une IP dans la même classe (192.168.0.0 dans notre exemple), mais toutes différentes,
 - un masque de sous réseau convenable, 255.255.255.0 dans l'exemple,
 - la passerelle par défaut pointant sur votre machine Linux (192.168.0.253 dans l'exemple),
 - au moins un DNS, le premier des deux que votre FAI vous propose (voir plus haut). Attention, le FAI peut être amené à changer de DNS. Votre machine Linux en sera automatiquement informée, mais pas les clients de votre réseau. Si vous en restez là, il sera de votre responsabilité de vérifier périodiquement que le DNS n'a pas changé. D'ailleurs, vous vous apercevrez vite que quelque chose ne va plus...

Tout ce que vous pouvez faire pour l'instant, c'est:

- Vous connecter à l'Internet depuis votre machine LINUX
- Envoyer des pings depuis votre machine LINUX vers :
 - Votre réseau privé (avec les adresses IP, nous n'avons pas mis en place de résolutions de noms pour le réseau privé),
 - l'Internet. Ici, le DNS du FAI saura, en principe, résoudre les noms.

13 PPPoE : <http://christian.caleca.free.fr/pppoe/>

Ne vous attendez pas à "voir" la machine LINUX dans votre voisinage réseau Windows! LINUX n'utilise pas NetBIOS. Si vous voulez le faire, il vous faudra installer SAMBA sur LINUX, qui crée une couche de dialogue avec NetBIOS, mais ceci est une autre histoire... Si vous voulez le faire et ne savez pas comment, consultez au moins le SMB HOWTO¹⁴, mais ne faites pas tout en même temps :)

14 SMB : <http://www.freenix.org/unix/linux/HOWTO/SMB-HOWTO.html>

Passerelle simple

Comme je suis prof depuis assez longtemps pour avoir compris qu'il n'y a rien de plus frustrant que de se taper des heures de théorie avant de pouvoir passer, enfin, à la pratique, nous allons d'abord réaliser vite fait une passerelle opérationnelle. Sommaire, rudimentaire, mais opérationnelle.

Après, nous verrons plus en détail comment tout ceci fonctionne.

Netfilter et IPTables

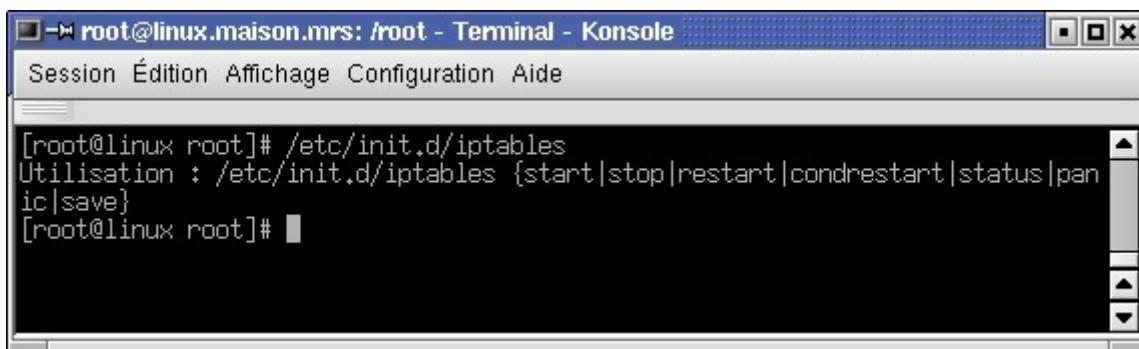
Installation

Netfilter, c'est le système de gestion des paquets. C'est lui qui va permettre de réaliser le routage dans de bonnes conditions. La distribution Mandrake 9 l'intègre sous forme de modules. A priori, vous n'aurez pas de difficultés, la configuration par défaut intègre tout ce qu'il faut.

IPTables, c'est en quelque sorte l'interface qui permet de configurer Netfilter. Là, il vous faudra vérifier que le paquetage iptables est bien installé. Il existe également un paquetage nommé ipchains, pour assurer la compatibilité avec l'ancien système en usage sur les noyaux Linux 2.2.x.

Attention, ces deux paquetages sont incompatibles. N'utilisez pas IPChains, utilisez IPTables, c'est beaucoup mieux.

Le paquetage iptables inclut un script SystemV qui permet de faire beaucoup de choses intéressantes.



```
root@linux.maison.mrs: /root - Terminal - Konsole
Session Édition Affichage Configuration Aide

[root@linux root]# /etc/init.d/iptables
Utilisation : /etc/init.d/iptables {start|stop|restart|condrestart|status|panic|save}
[root@linux root]#
```

Notez que IPTables n'est pas un démon. Ce script n'a pour but que de configurer de diverses manières les règles de filtrage de paquets.. Ainsi :

- Stop
Permet de vider toutes les règles, avec des valeurs "ACCEPT" par défaut. Il n'y aura plus de passerelle NAT, plus de filtrage de paquets. Tout peut entrer et sortir librement de la machine.
- Panic
Permet la même chose, mais avec des valeurs "DROP" par défaut. Plus rien ne passera nulle part. A réserver en cas d'alerte rouge.
- Save
Permettra de sauvegarder un jeu de règles, de manière à pouvoir les recharger avec la

commande Start

- Start ou Restart
Permettent de charger un jeu de règles préalablement enregistrées avec la commande save.

Configuration simpliste

Dans la suite, ne confondez pas le script `/etc/init.d/iptables` avec `/sbin/iptables`, qui est un exécutable.

<u>Incantation magique</u>	<u>Signification</u>
<code>/etc/init.d/iptables stop</code>	<i>Toutes les règles sont nettoyées.</i>
<code>iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE</code>	<i>On applique le "masquering" sur tout ce qui doit sortir par ppp0</i>
<code>echo 1 > /proc/sys/net/ipv4/ip_forward</code>	<i>On déverrouille le "forwarding"</i>

Et voilà. La passerelle fonctionne. Assurez-vous d'abord que votre connexion PPPoE est bien active, par exemple en faisant un

```
ifconfig ppp0
```

qui doit vous indiquer que cette interface est bien montée. Si ce n'est pas le cas, commencez par arriver à obtenir ce lien.

Essayez maintenant, depuis un poste quelconque de votre réseau local, de faire un ping sur www.oleane.fr :

```

C:\ Invite de commandes

G:\>ping www.oleane.fr

Envoi d'une requête 'ping' sur www.oleane.fr [213.56.30.252] avec 32 octets de données :

Délai d'attente de la demande dépassé.
Réponse de 213.56.30.252 : octets=32 temps=80 ms TTL=245
Réponse de 213.56.30.252 : octets=32 temps=90 ms TTL=245
Réponse de 213.56.30.252 : octets=32 temps=20 ms TTL=245

Statistiques Ping pour 213.56.30.252:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),
    Durée approximative des boucles en millisecondes :
        minimum = 20ms, maximum = 90ms, moyenne = 47ms

G:\>_

```

Vous croyez que c'est fini ?

Rendre ces choses définitives

Les règles iptables sont volatiles. Si vous rebootez votre machine, il faudra les réécrire. Pour éviter ce désagrément, une fois vos règles établies, faites :

```
/etc/init.d/iptables save
```

Ça vous permettra de les sauvegarder et de pouvoir les recharger au prochain reboot par :

```
/etc/init.d/iptables start
```

Commande qui peut être lancée automatiquement au démarrage, comme tous les scripts qui se trouvent dans ce répertoire.

Le déverrouillage du "forwarding" est également volatile par défaut. Pour remédier à ce problème, éditez le fichier `/etc/sysconfig/network`. Dedans, il y a une ligne `FORWARD_IPV4="no"`. Mettez "yes" à la place de "no". Au prochain redémarrage de votre machine, le routage sera activé par défaut.

Et la sécurité ?

Votre passerelle fonctionne, certes, mais c'est un vaste trou béant au sens de la sécurité. Pour faire quelque chose de propre, il vous faudra lire le chapitre sur la sécurité¹⁵ et aussi celui sur Netfilter¹⁶, pour comprendre mieux ce qu'il y a à faire.

Dans l'état actuel des choses, vous être fortement exposé à toutes sortes d'ennuis...

Plus de confort

Le problème du DNS

Sur vos postes du réseau privé, vous devez indiquer "en dur" l'adresse IP des DNS de votre FAI. Ce n'est pas pratique, parce qu'ils peuvent changer sans vous le dire. Il vaut mieux installer sur votre passerelle un service DNS qui pourra soit résoudre les noms directement par lui même, soit servir de proxy DNS, c'est à dire retransmettre au DNS de votre FAI les requêtes de résolution que vous lui adresserez.

Dans ce cas, vous indiquerez sur vos clients l'adresse de votre passerelle pour le DNS et c'est elle qui se chargera de vous communiquer les résolutions.

A vous de voir ce qui vous convient le mieux. Normalement, un proxy DNS est suffisant. Vous pouvez faire ça assez simplement avec BIND. Lisez le chapitre consacré au DNS¹⁷ pour en savoir plus.

La configuration IP des clients

Configurer ses clients du réseau privé à la main, c'est bien, mais c'est vite fastidieux si vous en avez beaucoup. Il existe une possibilité de faire ça automatiquement au démarrage de vos machines en utilisant les services de DHCP. Vous pouvez aussi installer un serveur DHCP sur votre passerelle. C'est vraiment du luxe pour un petit réseau domestique, mais comme ce luxe ne vous coûtera rien de plus que de lire le chapitre sur DHCP¹⁸...

Mais, avant tout, pensez d'abord à la sécurité et passez à Netfilter au plus vite ;-)

15 Sécurité : <http://christian.caleca.free.fr/securite/>

16 Netfilet et IPtables : <http://christian.caleca.free.fr/netfilter/>

17 DNS : <http://christian.caleca.free.fr/dns/>

18 DHCP : <http://christian.caleca.free.fr/dhcp/>