HOWTO − Réseau GNU/Linux Chez Soi

Auteur : Paul Ramsey

`<pramsey@refractions.net>`

Adaptation française: Marc Tanguy

`<mtanguy@ens.uvsq.fr>`

Version 1.4 22/06/2000

Version française 1.0 18/09/2002

Historique des versions		
Version 1.0	21 Déc 1999	pr
Première version		
Version 1.1	2 Jan 2000	pr
Rajout des suggestions apportées par John Mellor à propos de bizarreries pour le réseau extérieur		
Version 1.2	22 Jan 2000	pr
Mises à jour mineures de Chris Lea à propos des cartes réseaux identiques et des informations sur la dénomination d'IP (IP aliasing).		
Version 1.3	16 Mar 2000	pr
Précisions sur la sécurité du serveur de noms et sur le support avec Caldera de la part de Nelson Gibbs		
Version 1.4	22 Jui 2000	pr
Documentation de particularités de configuration de Red Hat 6.2 Rajout d'informations sur PPPoE de Kerr First		

Résumé

Ce document décrit la mise en place d'une Red Hat comme passerelle vers Internet pour un réseau local d'entreprise ou pour chez soi. Il s'agit tout simplement de partager une connexion Internet à travers une Red Hat. Les points suivants seront couverts : masquage d'IP, DNS, DHCP, et quelques principes de base de sécurité.

Table des matières

1. Introduction

    1.1. Versions

2. Branchons tout ce qu'il faut

2.1. Avec un Concentrateur
2.2. Sans Concentrateur
2.3. Avec une seule carte réseau
3. Configuration du réseau
3.1. Configurer un pilote de réseau
3.2. Configurer le réseau interne
3.3. Configurer le réseau externe
3.4. Sécurité
4. Configurer le Masquage d'IP
5. Problèmes
5.1. ICQ ne fonctionne pas
5.2. J'ai une Caldera 2.X et pas une Red Hat 6.X
5.3. Je veux qu'une de mes machines interne soit mon serveur Web

1. Introduction

Cette page est juste un recueil de recettes de cuisine pour configurer une Red Hat en tant que passerelle pour un réseau local. Les instructions sont très simplifiées i.e. pas de discussion hasardeuse et on supposera les adresses réseaux qui devront être choisies. Les pré−requis les plus importants sont :

- vous disposez d'un accès permanent à Internet via le Câble ou l'ADSL ;
- vous avez installé avec succès une Red Hat sur au moins une de vos machines. Notez que c'est aussi valide pour les distributions dérivées de Red Hat, telle que Mandrake ;
- votre ordinateur sous GNU/Linux possède deux cartes réseaux installées et qui sont compatibles avec GNU/Linux ;
- vous avez un concentrateur Ethernet (concentrateur ou switch) si vous mettez en réseau plus d'un ordinateur ou alors un câble croisé si vous ne reliez qu'un seul ordinateur ;
- vous savez éditer des fichiers textes sur votre machine GNU/Linux ;
- vous pouvez vous connecter sous **root**. Et vous savez installer des paquetages Red Hat (RPM) à partir du cédérom de votre distribution.

Si vous ne remplissez pas l'une des conditions ci−dessus, alors ce document ne vous est probablement pas destiné.

Il n'y a rien de particulier à faire à l'installation. Choisissez simplement l'installation qui vous convient et allez−y. Ce document donne les directions pour installer de zéro tout ce dont vous aurez besoin pour votre réseau, afin d'éviter les confusions sur ce que vous avez installé ou configuré durant l'installation. Toutes les configurations seront effectuées directement sur les fichiers de configuration plutôt qu'avec les outils graphiques fournis par Red Hat. Cette solution a pour effet d'être d'une certaine façon moins facile mais certainement plus éducative et plus facilement applicable dans d'autres situations avec d'autres distributions.

1.1. Versions

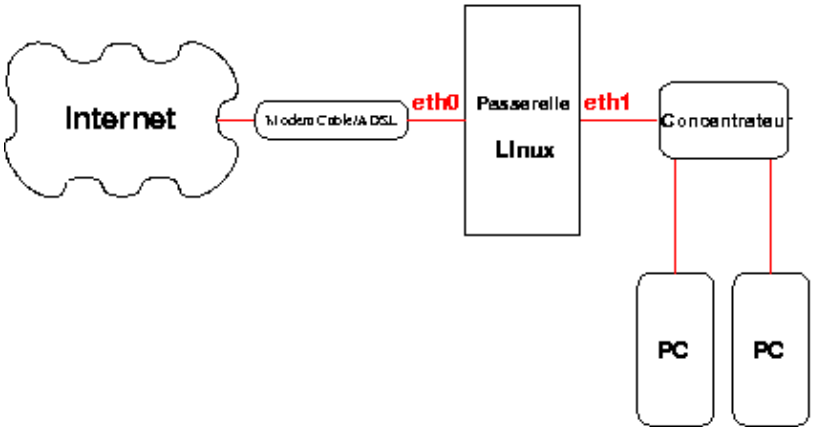
Les versions les plus à jour de ce document (en anglais) sont accessibles en suivant ce lien pour la version HTML ou celui−ci pour la version SGML

2. Branchons tout ce qu'il faut

Selon si vous utilisez un concentrateur ou pas, votre topologie de réseau différera légèrement. Je ne couvrirai que le câblage avec des prises RJ45 (celles qui ressemblent à des prises de téléphones avec 8 broches) et non le coaxial. Avec le coaxial vous pouvez relier plusieurs machines sans concentrateur, mais vous devez faire plus attention aux terminaisons etc. Évidemment si vous connaissez le réseau, ces instructions sont clairement redondantes.

2.1. Avec un Concentrateur

Si vous avez un concentrateur, votre réseau local devrait ressembler à quelque chose comme ça :

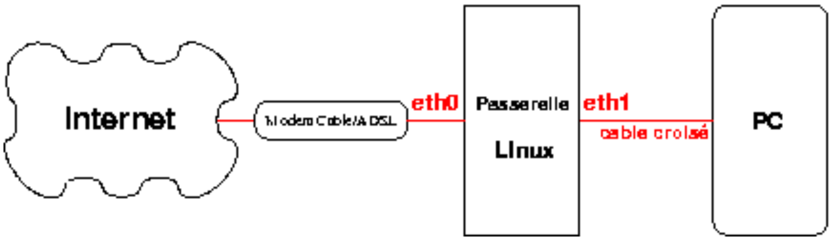


Reliez la carte eth0 sur le GNU/Linux au modem câble ou ADSL avec le câble fourni par votre fournisseur d'accès à Internet (FAI) pendant l'installation (ou un câble que vous savez fonctionner dans cette configuration. C'est important car parfois le câble doit être croisé, parfois droit.)

Reliez la carte eth1 du GNU/Linux au concentrateur avec un câble droit. De même, reliez tous les autres ordinateurs au concentrateur avec des câbles droits.

2.2. Sans Concentrateur

Si vous n'avez pas de concentrateur, vous pouvez toujours relier un seul ordinateur à votre GNU/Linux, à l'aide d'un câble croisé. Votre topologie ressemblera alors à ceci :



Reliez la carte eth0 du GNU/Linux au modem câble ou ADSL à l'aide du câble fourni par votre fournisseur d'accès. Reliez la carte eth1 du GNU/Linux à l'autre ordinateur avec un câble croisé.

2.3. Avec une seule carte réseau

Cette configuration n'est pas recommandée (dans cette configuration vos réseaux interne et externe sont sur le même lien physique, et sont donc en théorie plus vulnérable aux attaques ; en pratique, le risque est relativement faible), mais cela est *possible*.

Le noyau Linux inclue le support de la dénomination d'IP (IP aliasing), ce qui permet d'associer plusieurs adresses IP à une même carte Ethernet. Les noyaux fournis dans les distributions Red Hat et Mandrake supportent la dénomination d'IP par défaut. Pour configurer votre passerelle avec une seule carte Ethernet, dans tout ce qui suit, remplacez simplement **eth1** par **eth0:0**.

Dans ce genre de configuration à carte unique, l'utilisation d'un serveur DHCP n'est pas *recommandée.*

Branchez toutes vos machines et votre modem câble ou ADSL dans le concentrateur. Croisez les doigts, vous pouvez continuer.

3. Configuration du réseau

Bien, à partir de là, vous avez installé une passerelle sous GNU/Linux. Vous avez peut−être même configuré une de vos cartes réseaux, et mis en place la connexion vers Internet. De toutes les manières, nous allons tout reprendre depuis le départ et faire comme si rien n'était configuré.

Connectez−vous sous **root**. Toutes les instructions données dans ce document supposent que vous soyez connecté sous **root**.

Le noyau Linux se réfère à vos deux cartes Ethernet à travers eth0 et eth1, nous allons donc de même utiliser ces références. Le problème est de savoir laquelle est laquelle. Voici un moyen «simple» de savoir, garanti à 50% : poser l'ordinateur sur le bureau avec la carte mère horizontale et le panneau arrière face à vous (comme si vous alliez l'ouvrir pour travailler dessus). La carte la plus à gauche est eth0. Maintenant, notez sur un papier le fabricant et le modèle de eth0 et d'eth1.

Bien, voyons si eth0 et eth1 sont correctement et automatiquement reconnues par le noyau. Tapez **ifconfig eth0** puis **ifconfig eth1**. Dans les deux cas, si le noyau reconnaît bien vos cartes, vous devriez voir quelque chose ressemblant à ceci (en gardant bien à l'esprit que les nombres seront différents) :

```
eth0   Link encap: Ethernet   HWaddr 00:60:67:4A:02:0A
       inet adr:0.0.0.0  Bcast:0.0.0.0  Masque:255.255.255.255
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:466 errors:0 dropped:0 overruns:0 frame:0
       TX packets:448 errors:0 dropped:0 overruns:0 carrier:0
       collisions:85 lg file transmission:100
       RX bytes:800 (0.8 Kb)  TX bytes:736 (0.7 Kb)
       Interruption:10 Adresse de base:0xe400
```

Si le noyau ne reconnaît pas votre carte réseau, vous devriez alors voir quelque chose comme :

```
eth0: erreur lors de la recherche d'infos sur l'interface: Périphérique non trouvé
```

3.1. Configurer un pilote de réseau

Si les deux cartes ont été reconnues, passez directement à la prochaine section. Sinon lisez ce qui suit.

Bien, il se peut maintenant qu'une ou que vos deux cartes ne soient pas reconnues par le noyau. Ce n'est pas réellement un problème. Nous avons juste à spécifier explicitement au noyau comment trouver les cartes. Il existe beaucoup de détours et nous allons tous les couvrir. N'oubliez pas qu'en cas de grosses difficultés, vous trouverez tout dans le Ethernet HOWTO. Voici le résumé de quelques conseils :

- *vous avez une carte réseau PCI.* Vous êtes probablement en bonne position, en supposant qu'elle ne soit pas trop récente et excentrique pour qu'il existe un pilote. Vous trouverez des informations sur votre carte réseau (et d'autres) en parcourant **/proc/pci** notamment le fabricant et le modèle (n.d.t. : vous pouvez utiliser la commande suivante **lspci**) ;
- *vous avez une carte réseau ISA.* Il est possible que vous ayez à connaître l'adresse de base E/S et l'interruption (IRQ) assignés à la carte. Vous avez les manuels, n'est−ce pas ? N'est−ce pas ? Sinon, il est grand temps d'aller surfer du coté du site web du fabricant et de voir s'il a les références de votre carte. Ou si vous avez une vieille disquette de configuration DOS, démarrez sous DOS et regardez s'il existe un programme qui pourrait lire et positionner l'adresse et l'interruption ;
- *Vous avez une carte ISA Plug'n'Play.* Premièrement vous aurez à apprendre comment la configurer −− lisez le Plug'n'Play HOWTO. Heureusement, une fois que vous aurez configuré votre carte vous connaîtrez exactement son adresse de base E/S et son interruption.

Maintenant que vous connaissez le fabricant de eth0 et de eth1, vous pouvez aller sur la page de compatibilité du Ethernet HOWTO et trouver votre carte. Notez le pilote recommandé, et toute information à propos d'options spécifiques à votre carte. Notez−les quelque part !

Il est temps d'éditer le fichier de configuration ! Le fichier que vous devez éditer est le suivant `/etc/modules.conf` (n.d.t. : anciennement `/etc/conf.modules`). Ouvrez ce fichier avec l'éditeur de votre choix. Sachant qu'il y a beaucoup de possibilités et de combinaisons qui peuvent remplir ce fichier, je vais donner ma propre passerelle comme exemple. Je possède une carte PCI 10/100Mb basé sur la puce VIA Rhine, et une clone de NE2000 ISA 10Mb de base. J'utilise la carte 100Mb pour le réseau interne et la carte de 10Mb pour la connexion externe. Mon fichier `/etc/modules.conf` ressemble à cela :

```
alias parport_lowlevel parport_pc
alias eth0 ne
options ne io=0x300 irq=10
alias eth1 via-rhine
```

Mon fichier `modules.conf` se décompose de la manière suivante :

- La première ligne est ici pour configurer le port parallèle pour l'impression. Vous avez probablement une ligne similaire. Laissez−la.
- La deuxième ligne (**alias eth0 ne**) informe le noyau pour qu'il utilise le pilote NE pour le périphérique eth0.
- La troisième ligne (**options ne io=0x300 irq=10**) passe au pilote les paramètres d'adresse E/S de base et l'interruption correspondants à l'emplacement de la carte ISA. Si vous possédez une carte ISA, vous aurez très certainement à utiliser ce genre de directives. Remplacez juste les options de pilote, d'adresse et d'interruption par celles de votre carte.
- La dernière ligne (**alias eth1 via−rhine**) informe le noyau pour qu'il utilise le pilote VIA−Rhine pour eth1. Comme ma carte eth1 est une carte PCI, elle ne nécessite pas de paramètres supplémentaires (E/S, interruption) : le sous−système PCI configure le périphérique automatiquement.

Vous vérifierez bien que vous avez des entrées d'alias dans `modules.conf` pour vos deux cartes, et les lignes d'options adéquates pour toutes vos cartes ISA. Vous avez d'ailleurs peut−être déjà des lignes pour une carte Ethernet configurée lors de l'installation.

Dès que vous aurez fini de modifier votre `modules.conf`, essayez la commande **ifconfig eth0** puis **ifconfig eth1**. Vous devrez peut−être procéder par tâtonnements si vous perdez du temps avec les interruptions et les adresses E/S sans manuel du fabricant.

3.1.1. Deux cartes réseaux identiques

Voilà, vous avez voulu être malin, et vous avez acheté deux cartes réseaux identiques pour votre passerelle GNU/Linux, et maintenant vous n'arrivez pas à les faire fonctionner ensemble ? Ne vous inquiétez pas, pour les faire coexister il suffit d'employer la bonne syntaxe dans votre `modules.conf`. Pour cet exemple, les adresses E/S et les numéros d'interruptions sont fixés, et je supposerai que vous avez acheté une paire de cartes compatibles NE2000 (un choix habituel). Alors votre fichier `modules.conf` devrait ressembler à cela :

```
alias eth0 ne
alias eth1 ne
options ne io=0x330,0x360 irq=7,9
```

Les options d'adressage sont toutes données sur la même ligne, et le premier nombre pour chaque adressage est pour la carte eth0, le second nombre pour eth1.

3.2. Configurer le réseau interne

Le *réseau interne* est le réseau dans lequel toutes vos machines personnelles communiquent entre elles. Le *réseau externe* désigne le grand et effrayant Internet de l'autre côté du GNU/Linux. Généralement parlant, le réseau interne sera complètement isolé du réseau externe grâce au GNU/Linux, qui opérera alors comme pare−feu de force moyenne.

3.2.1. Le réseau

Maintenant que les pilotes fonctionnent et que vous voyez vos deux cartes eth0 et eth1 dans **ifconfig** il est temps de mettre en place le réseau interne. Je choisis arbitrairement de configurer le réseau interne sur la carte eth1 et l'externe sur eth0.

Votre réseau interne va être un réseau privé et par conséquent doit utiliser une plage d'adresse réseau spécifique pour les réseaux internes : **192.168.1.0**. Ceci est un *réseau privé de classe C*, au cas où vous voudriez impressionner vos amis (n.d.t. cela impose entre autres l'utilisation d'au maximum 254 adresses IP différentes sur le réseau interne) ;

Premièrement nous devons nous assurer que le réseau est activé. Éditez le fichier `/etc/sysconfig/network` et vérifiez que les lignes suivantes sont présentes :

```
NETWORKING=yes
FORWARD_IPV4=yes
```

La première ligne indique au système que nous voulons que les périphériques réseaux démarrent au démarrage du système. La seconde ligne demande au système d'autoriser le transfert IP. Ceci est un pré−requis pour démarrer la configuration du masquage d'IP à la section 4.

Redhat 6.2

Pour pouvoir supporter le masquage d'IP et le transfert IP, la Red Hat 6.2 requiert des modifications dans le fichier `/etc/sysctl.conf`. Vérifiez que les lignes suivantes existent et que les valeurs sont correctes :

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

Tous les paramètres concernant les interfaces réseaux sont dans les fichiers contenus dans le répertoire `/etc/sysconfig/network−scripts`. Entrez dans ce répertoire, et créez un nouveau fichier `ifcfg−eth1`. Puis rentrez ce qui suit dans le fichier `ifcfg−eth1` :

```
DEVICE=eth1
IPADDR=192.168.1.1
ONBOOT=yes
```

Ces lignes permettent aux scripts gérant le réseau de configurer eth1 au démarrage du système et de lui assigner une adresse IP particulière. Activez votre réseau avec les nouveaux paramètres avec la commande suivante : **/etc/rc.d/init.d/network restart**.

3.2.2. Le serveur DHCP (Dynamic Host Configuration Protocol)

Un serveur DHCP (Protocole de Configuration Dynamique d'Hôte) configurera automatiquement les périphériques de votre réseau interne avec des adresses IP. Ceci est très utile pour les personnes munis d'ordinateur portable : ils n'ont qu'à brancher leurs machines et tout se configure immédiatement proprement. Si vous ne voulez pas de serveur DHCP sur votre réseau interne, passez à la section suivante.

Premièrement vous devez vous assurer que le serveur DHCP est installé. Montez votre cédérom GNU/Linux et installez le paquetage RPM `dhcp`. Ceci fait, éditez le fichier `/etc/dhcpd.conf` et mettez les lignes suivantes (et seulement celles−ci) dedans :

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.2 192.168.1.60;
  default−lease−time 86400;
  max−lease−time 86400;
  option routers 192.168.1.1;
  option ip−forwarding off;
  option broadcast−address 192.168.1.255;
  option subnet−mask 255.255.255.0;
}
```

Si vous allez configurer votre GNU/Linux en tant que cache DNS (serveur de nom de domaine), insérez alors l'option suivante :

```
option domain−name−servers 192.168.1.1;
```

Si vous savez que ni vous ni vos adresses DNS externes n'allez utiliser votre GNU/Linux comme DNS, insérez l'option suivante, où x.x.x.x et y.y.y.y représentent les adresses IP des serveurs DNS :

```
option domain−name−servers x.x.x.x, y.y.y.y;
```

Si vous voulez utiliser le partage de fichier Samba sur votre GNU/Linux pour vos ordinateurs MS−Windows, ajoutez les options suivantes pour utiliser le GNU/Linux par défaut comme serveur WINS (Windows Name Server) :

```
option netbios−name−servers 192.168.1.1;
option netbios−dd−server 192.168.1.1;
option netbios−node−type 8;
option netbios−scope "";
```

Configurer Samba et WINS est bien au−delà de la portée de ce document. Si vous avez besoin d'aide, commencez par lire le SMB HOWTO et continuez à partir de là.

Il y a encore quelques petites choses à rajouter. Éditez le fichier `/etc/rc.d/init.d/dhcpd` et cherchez la ligne suivante :

```
/sbin/route add −host 255.255.255.255 dev eth1
```

Les clients DHCP MS−Windows requièrent une adresse de diffusion particulière (Broadcast Adress) dans les réponses DHCP, et cette commande force la pile TCP/IP du GNU/Linux à la reproduire. Si vous ne trouvez pas cette ligne dans ce fichier, *ajoutez−la*. Si vous en trouvez une ressemblante, vérifiez que la carte référencée soit bien eth1.

L'étape suivante est de modifier le fichier `/etc/sysconfig/dhcpd` afin d'utiliser eth1 comme carte par défaut. Remplacez la ligne :

```
DHCPDARGS=
```

Par :

```
DHCPDARGS=eth1
```

Bien, nous sommes maintenant prêts à démarrer le DHCP. Tout d'abord démarrez le serveur DHCP avec la commande : **/etc/rc.d/init.d/dhcpd start**.

Puis dans un deuxième temps, nous devons nous assurer que le serveur DHCP démarrera au prochain réarmorçage du système. Certains paquetages RPM pour le serveur DHCP n'incluent pas les directives pour assurer le démarrage du service à chaque fois, donc nous devons le faire en invoquant la commande **chkconfig dhcpd on**.

Cette commande force la RedHat à ajouter le script de démarrage du dhcp aux différents répertoires de niveaux de démarrage dans `/etc/rc.d`. Dans les niveaux 3 et 5 (console multi−utilisateur et X multi−utilisateur) le serveur DHCP est démarré. Dans les niveaux 0, 1 et 6 (arrêt, unique utilisateur et redémarrage) le serveur DHCP est arrêté.

3.2.3. Les ordinateurs clients

Si vous avez mis en route le DHCP, configurer les ordinateurs clients est très simple : choisissez juste la configuration par DHCP. Pour les ordinateurs sous Windows, cela implique d'ouvrir le «Panneau de configuration» puis l'option «Réseaux». Trouvez le protocole TCP/IP et cliquez sur «Configurer». Cochez la case «Obtenir automatiquement une adresse IP», appliquez les changements, puis redémarrez.

Avant de redémarrer votre Windows, vous pourriez avoir besoin de taper cette commande : **tail −f /var/log/messages**. Ceci vous permettra de regarder en continue le système de log du GNU/Linux. Si tout va bien, quand vous redémarrez votre Windows, vous le verrez demander une adresse IP et le serveur DHCP lui répondre. Il suffit d'un Ctrl+C pour sortir de la commande **tail −f**.

Si vous n'avez pas mis en route le DHCP, la configuration est tout de même très simple. De même, dans la rubrique «Réseau» du «Panneau de configuration», sélectionnez le protocole TCP/IP puis cliquez sur «Paramètres». Vous pouvez alors lui spécifier une adresse IP comprise dans le réseau 192.168.1.0 sauf 192.168.1.0 (l'adresse de réseau) 192.168.1.255 (l'adresse de diffusion du réseau) ou 192.168.1.1 (l'adresse du serveur GNU/Linux). Ne donnez jamais à deux ordinateurs clients la même adresse IP. Ajoutez la passerelle à l'adresse 192.168.1.1, ce qui permettra au trafic sortant d'être routé à travers votre passerelle GNU/Linux.

Le HOWTO IP Masquerade détaille très précisément la configuration du client dans le Section Configuration.

En général, pour configurer un ordinateur client, soit par DHCP, soit par assignation d'une IP fixe dans le réseau 192.168.1.0 avec une passerelle en 192.168.1.1, positionnez l'adresse du serveur DNS à 192.168.1.1 si vous avez un serveur de cache DNS (voir ci−dessous) ou fixez les DNS aux adresses fournies par votre fournisseur d'accès à Internet.

3.2.4. Le Serveur de Noms de Domaine (DNS)

La mise en place d'un serveur de cache DNS améliorera légèrement la vitesse de navigation sur le net, car les adresses DNS les plus demandées seront mis en cache dans le réseau et n'auront pas à être récupérées à l'extérieur.

Si vous êtes intéressés par la mise en place d'un DNS complet et efficace, il y a énormément de détails complexes à apprendre. Il existe un DNS HOWTO disponible, et le livre DNS et Bind est une bonne (et très détaillée) référence papier.

Afin que vos machines clientes profitent du serveur de cache, elles doivent être configurées pour utiliser la passerelle GNU/Linux comme serveur DNS primaire. Les directives DHCP données à la section 3.2.2 sont une manière pour accomplir cela. Si vous configurez vos ordinateurs clients à la main, vous pouvez changer les configurations DNS dans les mêmes onglets de configuration que ceux utilisés pour affecter l'adresse IP de la machine.

Pour installer le serveur DNS, installez simplement le paquetage RPM **bind**. À présent, vous êtes presque prêt.

Avec cette installation, le serveur de cache fonctionnera correctement, mais si vous connaissez les adresses IP des serveurs DNS de votre fournisseur d'accès à Internet vous pouvez légèrement améliorer les performances en éditant le fichier `/etc/named.conf` et en ajoutant la ligne suivante après la ligne **directory** (où x.x.x.x et y.y.y.y désignent les serveurs DNS primaire et secondaire) :

```
forwarders { x.x.x.x; y.y.y.y; };
```

Cette modification imposera à votre serveur DNS de d'abord questionner les serveurs DNS de votre FAI avant de traverser Internet à la recherche d'une adresse donnée. Les serveurs de votre FAI possèdent souvent un cache riche d'information DNS et peuvent alors fournir la réponse plus vite que votre serveur.

Le démon **named** a régulièrement des problèmes de sécurité, il est donc important d'installer la dernière version, et de modifier certains paramètres par défaut afin d'améliorer la sécurité.

1. Vérifiez votre version de **bind** afin qu'elle soit au moins égale à 8.2.2. Puis allez sur le site de mise à jour Red Hat afin de trouver la dernière version.
2. Restreignez l'accès à votre serveur de noms à votre réseau local en ajoutant la ligne **allow−query { 192.168.1/24; 127.0.0.1/32; } ;** à votre fichier `/etc/named.conf` après la ligne **forwarders**.
3. Évitez d'exécuter le serveur de noms sous **root**. Si votre serveur s'exécute sous **root**, une faille dans le serveur donnera à celui qui l'exploite les privilèges de l'administrateur. Si, par contre vous l'exécutez sous un utilisateur moins privilégié, comme l'utilisateur **nobody**, vous pouvez minimiser le risque de faille dans le serveur de nom. Pour exécuter votre serveur de nom sous **nobody**, éditez le fichier `/etc/rc.d/init.d/named` et changez la ligne **daemon named** par **daemon named −u nobody**.

   Redhat 7.x

   Dans les versions récentes de Red Hat, le démon de serveur de noms s'exécute déjà sous un utilisateur non privilégié.

Vérifiez que votre serveur DNS démarrera au démarrage de GNU/Linux à l'aide de la commande suivante : **chkconfig named on**. Une fois encore, ceci nous assure que le serveur démarrera dans les niveaux de chargements habituels (3 et 5) au démarrage de GNU/Linux.

Bien, maintenant vous pouvez démarrer votre serveur DNS : **/etc/rc.d/init.d/named start**.

3.2.5. Tester le réseau interne

Tant que nous n'aurons pas configurer le réseau externe, le service de DNS ne fonctionnera pas (car il doit pouvoir communiquer avec les autres serveurs DNS sur Internet), cependant nous pouvons tester la connectabilité interne basique avec le programme **ping**.

Sur l'un de vos ordinateurs clients, ouvrez une fenêtre de commandes MSDOS, et tapez **ping 192.168.1.1**. Ceci émettra des paquets vers votre machine GNU/Linux à des intervalles réguliers, et votre machine GNU/Linux répondra aux paquets. Si les choses se passent bien, vous devriez voir les temps de retour des paquets.

3.3. Configurer le réseau externe

Maintenant nous sommes prêts à configurer le réseau externe. Parfois cela sera difficile, cela dépend la façon dont votre FAI supporte GNU/Linux. Si vous rencontrez des difficultés, il existe un mini−HOWTO DSL qui couvre en détails les problèmes d'ADSL. Il existe aussi un mini−HOWTO Modem Câble pour l'Internet par le câble.

Le principal problème avec la plupart des connexions externes est *l'obtention d'une adresse IP*. Certains FAI distribuent des adresses IP statiques à leurs abonnés câble ou ADSL, et dans ce cas la configuration est facilitée. Cependant, la plupart des FAI ont maintenant choisi des configurations dynamiques via (vous l'avez deviné) DHCP (n.d.t. : la tendance actuelle est plutôt de se tourner vers le protocole PPPoE, aussi bien pour le câble que pour l'ADSL). Ceci signifie que votre machine GNU/Linux sera vraisemblablement *serveur* DHCP pour l'interface eth1, et *client* DHCP pour l'interface eth0.

De plus, beaucoup de FAI se sont mis à fournir leurs services à travers des protocoles non standards spécialisés ce qui oblige leurs abonnés à rester sous MS−Windows. Certains de ces cas de figures seront discutés à la fin de la section 3.3.2.

3.3.1. Avec une IP fixe

Si votre FAI vous a assigné une adresse IP statique, vous êtes en bonne voie. Premièrement, créez un fichier pour une nouvelle interface, `/etc/sysconfig/network−scripts/ifcfg−eth0` et insérez y les lignes suivantes :

```
DEVICE=eth0
IPADDR=x.x.x.x
NETMASK=y.y.y.y
ONBOOT=yes
```

Remplacez juste les x.x.x.x et y.y.y.y par les valeurs données par votre FAI. Puis éditez le fichier `/etc/resolv.conf` et entrez les informations suivantes :

```
search domaine_du_FAI
nameserver n.n.n.n
nameserver m.m.m.m
```

Le *domaine_du_FAI* devrait vous être fourni par votre FAI. De même, entrez les adresses des serveurs DNS primaire et secondaire aux lignes n.n.n.n et m.m.m.m. Si vous avez mis en place votre machine GNU/Linux en tant que serveur DNS, vous pouvez ajouter une ligne avant les autres entrées **nameserver 127.0.0.1**. Ceci forcera votre serveur GNU/Linux à utiliser en priorité le serveur de cache DNS avant de demander l'information aux serveurs DNS extérieurs.

3.3.2. Avec un DHCP

Si votre FAI utilise une configuration basée sur un DHCP, vous devez alors créer un fichier de configuration pour une nouvelle interface `/etc/sysconfig/network−scripts/ifcfg−eth0` avec les lignes suivantes :

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Maintenant vérifiez que le démon client **dhcpcd** est installé sur votre système. Prenez votre cédérom d'installation de GNU/Linux et installez le paquetage RPM **dhcpcd**.

C'est le moment de tester notre nouvelle configuration réseau. Utilisez juste la commande **/etc/rc.d/init.d/network restart**. Maintenant testez votre connexion vers le réseau externe avec le programme **ping**. Pingez un ordinateur sur Internet, comme par exemple **www.yahoo.com** et observez le retour.

3.3.3. Bizarreries et Anomalies

Votre situation peut différer d'une des situations simplistes décrites ci−dessus. Voici quelques courtes remarques sur les diverses difficultés et des liens vers des ressources de référence auxquelles les adresser. Merci à John Mellor pour avoir fourni les liens et l'impulsion nécessaire à l'ajout de cette section.

3.3.3.1. PPP Over Ethernet (PPPoE)

Plusieurs FAI ADSL (France Télécom, par exemple) obligent leurs abonnés à se connecter au service via le protocole "Point à Point à travers Ethernet" (PPPoE). À cette fin, ils fournissent un programme client MS−Windows : ce qui n'est pas très utile pour les utilisateurs GNU/Linux. Heureusement, PPPoE est un protocole simple et qui a fait l'objet de développements sous GNU/Linux.

- Le Client PPPoE de Roaring Penguin est très fortement recommandé par Kerr First ;
- PPPoE sous GNU/Linux avec France Télécom ;
- PPPoE sous GNU/Linux avec Sympatico (Informations Générales).

3.3.3.2. Trucs idiots à propos du DHCP

Un des tours favoris auxquels les FAI jouent est de restreindre votre service à un nom de machine unique, ou même à une unique carte d'interface réseau. Ceci en général afin de vous empêcher de brancher de multiples ordinateurs sur le port Internet d'un concentrateur (bien sûr, avec GNU/Linux et le masquage d'IP vous obtiendrez le même effet avec une sécurité accrue et sans que votre FAI puisse le deviner!).

Si votre FAI vous a donné un nom de machine et insiste pour que vous configuriez votre Windows avec ce nom afin d'utiliser leur service, alors vous devez vous assurer que votre machine GNU/Linux renvoie ce nom de machine quand il requiert une adresse au serveur DHCP.

Le client DHCP de Red Hat est lancé quand vous positionnez la variable BOOTPROTO à dhcp dans le fichier de configuration d'interface, mais il est lancé sans référence à un nom de machine particulier. Pour le lancer avec un nom de machine donné, sous Red Hat 6.x ou 7.x, éditez le fichier `/etc/sysconfig/network`, en changeant la ligne :

HOSTNAME=

Par ceci :

HOSTNAME=votre_nom_de_machine_assignée_par_votre_FAI

Cette opération peut ne pas fonctionner sur certaines dérivées de Red Hat. Si tel est le cas, ouvrez le script `/sbin/ifup` pour voir si l'appel à dhcpcd et pump inclue le paramètre −h $HOSTNAME. S'il ne l'inclue pas, ajoutez−le, de façon à ce que l'appel ressemble à **/sbin/dhcpcd −i $DEVICE −h $HOSTNAME** et **/sbin/pump −i $DEVICE −h $HOSTNAME**.

3.3.4. Vue d'ensemble des entrées réseaux

Maintenant vous pouvez admirer le travail. Tapez **ifconfig** pour voir tous les périphériques réseaux configurés. Sur ma machine passerelle, cela ressemble à ceci :

```
eth0  Lien encap:Ethernet  HWaddr 00:60:67:4A:02:0A
      inet adr:24.65.182.43  Bcast:24.65.182.255  Masque:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:2054256 errors:0 dropped:0 overruns:1 frame:0
      TX packets:1316599 errors:0 dropped:0 overruns:0 carrier:0
      collisions:89 lg file transmission:100
      RX bytes:1478576846 (1410.0 Mb)  TX bytes:203407515 (193.9 Mb)
      Interruption:10 Adresse de base:0xe400
eth1  Lien encap:Ethernet  HWaddr 00:80:C8:D3:30:2C
      inet adr:192.168.1.1  Bcast:192.168.1.255  Masque:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:81652 errors:0 dropped:0 overruns:0 frame:0
      TX packets:116131 errors:0 dropped:0 overruns:0 carrier:0
      collisions:37938 lg file transmission:100
      RX bytes:26228293 (25.0 Mb)  TX bytes:109197036 (104.1 Mb)
      Interruption:5 Adresse de base:0xe800
lo    Lien encap:Boucle locale
      inet adr:127.0.0.1  Masque:255.0.0.0
      UP LOOPBACK RUNNING  MTU:3924  Metric:1
      RX packets:359890 errors:0 dropped:0 overruns:0 frame:0
      TX packets:359890 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 lg file transmission:0
      RX bytes:145538898 (138.7 Mb)  TX bytes:145538898 (138.7 Mb)
```

Notez que l'interface eth0 a une adresse IP fantaisiste, alors que l'adresse d'eth1 est une adresse de réseau privé interne.

Vous pouvez regarder les routes de réseaux en tapant la commande **route**. Sur ma passerelle, cela ressemble à ceci :

```
  Table de routage IP du noyau
  Destination     Passerelle   Genmask         Indic Metric Ref Use Iface
  255.255.255.255 *            255.255.255.255 UH    0      0     0 eth1
  192.168.1.0     *            255.255.255.0   U     0      0     0 eth1
  24.65.182.0     *            255.255.255.0   U     0      0     0 eth0
  127.0.0.0       *            255.0.0.0       U     0      0     0 lo
  default         24.65.182.1  0.0.0.0         UG    0      0     0 eth0
```

Ici nous pouvons voir que le réseau externe est configuré, que le réseau interne aussi, ainsi que la boucle locale, l'adresse spéciale de diffusion 255.255.255.255 est configurée, et la route par défaut pointe vers la passerelle du FAI. Parfait !

À ce point vous avez l'extérieur, et l'intérieur. Il ne reste qu'à ouvrir les portes entre les deux. Avant toute chose, nous devons nous assurer qu'aucun monstre ne puisse rentrer de l'extérieur.

3.4. Sécurité

Un des inconvénients d'avoir une connexion permanente vers Internet via l'ADSL ou le câble est que votre ordinateur est exposé aux menaces de trous de sécurité potentiels 24 heures sur 24, 7 jours sur 7. Utiliser

GNU/Linux comme passerelle réduit les risques, car il cache les autres ordinateurs : ainsi en ce qui concerne le reste d'Internet, seul votre machine GNU/Linux est disponible pour des connexions. Ceci signifie que votre réseau interne est au mieux aussi sécurisé que votre machine GNU/Linux, c'est pourquoi je vais vous donner quelques astuces basiques pour améliorer cette sécurité.

Premièrement, il est nécessaire de bloquer les personnes malintentionnées. Pour cela, éditez le fichier `/etc/hosts.deny` et vérifiez qu'il ressemble exactement à cela :

```
#
# hosts.deny  This file describes the names of the hosts which are
#             *not* allowed to use the local INET services, as decided
#             by the '/usr/sbin/tcpd' server.
#
#            The portmap line is redundant, but it is left to remind you that
#        the new secure portmap uses hosts.deny and hosts.allow. In particular
#             you should know that NFS uses portmap!
ALL: ALL
```

Ceci demande au "TCP wrappers" −− qui contrôle 95% des connexions entrantes −− de refuser toutes les connexions de tous les hôtes. C'est plutôt une bonne règle ! Malheureusement, elle vous empêchera aussi de vous connecter à votre GNU/Linux à partir de votre réseau interne, ce qui est gênant, donc nous allons rajouter une exception. Éditez le fichier `/etc/hosts.allow` et vérifiez qu'il ressemble exactement à cela :

```
#
# hosts.allow  This file describes the names of the hosts which are
#              allowed to use the local INET services, as decided
#              by the '/usr/sbin/tcpd' server.
#
ALL: 127.0.0.1
ALL: 192.168.1.
```

Ceci indique au "TCP wrappers" qu'il doit autoriser les connexions à tous les services à partir de la machine locale (127.0.0.1) et à partir du réseau interne (192.168.1.).

Bien, vous avez maintenant bloqués les méchants à l'extérieur, avec un bon cadenas. Si vous voulez utiliser des systèmes de blocage et d'alarmes, vous allez devoir être beaucoup plus sophistiqués. Le Security HOWTO est une bonne lecture pour commencer si vous voulez en apprendre plus pour sécuriser votre machine GNU/Linux.

4. Configurer le Masquage d'IP

Ça y est ! Les préliminaires sont terminés, c'est ici que la magie commence. Le masquage d'IP est un des services vraiment magique que GNU/Linux propose. Il existe des produits commerciaux pour MS−Windows qui font la même chose, mais ils sont loin d'approcher la même efficacité : un vieux 386 peut joyeusement fournir des services de masquage d'IP à un bureau entier de taille moyenne, alors qu'il ne pourrait même pas lancer MS−Windows 95", sans parler du support ajouté du masquage d'IP." (Il est aujourd'hui possible d'utiliser le "partage de connexion" de MS−Windows pour faire du masquage d'IP mais il toujours impossible de faire tourner MS−Windows 2000 sur un 386.)

GNU/Linux a des capacités de pare−feu extrêmement variées, et nous allons les utiliser dans leur manière la plus simple et la plus rudimentaire. Si vous voulez apprendre comment maîtriser les pare−feux, vous devriez lire à la fois le HOWTO du pare−feu et des serveurs mandataires pour une compréhension de la théorie et le HOWTO IPCHAINS pour les instructions à propos de l'outil de pare−feux **ipchains** fourni avec le noyau Linux 2.2.X (et par extension avec la Red Hat 6.X). (n.d.t. : un nouvel outil **iptables** est fourni avec le noyau Linux 2.4.x, sa documentation peut être trouvé ici) Il y a aussi un très bon HOWTO IP Masquerade disponible qui donne beaucoup de détails pour ajuster le masquage d'IP.

n.d.t. : Attention à votre version de noyau/distribution

Afin d'utiliser au mieux les ressources disponibles, une lecture attentive du HOWTO IP Masquerade est nécessaire. En effet, les différentes versions de noyaux Linux impliquent l'utilisation d'outils adaptés. De plus en plus de distributions récentes fournissent des outils graphiques de configuration pour le pare−feu.

Configurer un simple masquage d'IP est très très facile une fois que les réseaux interne et externe sont opérationnels. Éditez le fichier `/etc/rc.d/rc.local` et ajoutez les lignes suivantes à la fin :

```
# 1) Remettre les règles des tables à zéro
/sbin/ipchains −F input
/sbin/ipchains −F forward
/sbin/ipchains −F output
# 2) Configurer les temporisations du MASQ et autoriser les paquets entrants
#    pour la du DHCP.
/sbin/ipchains −M −S 7200 10 60
/sbin/ipchains −A input −j ACCEPT −i eth0 −s 0/0 68 −d 0/0 67 −p udp
# 3) Refuser tous les paquets transférés à part ceux provenant du réseau local.
#    Camoufler ces derniers.
/sbin/ipchains −P forward DENY
/sbin/ipchains −A forward −s 192.168.1.0/24 −j MASQ
# 4) Charger les modules pour des services spécifiques.
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
```

Les deux dernières lignes insèrent des modules noyaux qui autorisent le FTP et le RealAudio pour les ordinateurs dans le réseau interne. Il existe d'autres modules pour des services spéciaux que vous pouvez ajouter ensuite si vous en avez besoin :

- CUSeeMe (**/sbin/modprobe ip_masq_cuseeme**)
- Internet Relay Chat (**/sbin/modprobe ip_masq_irc**)
- Quake (**/sbin/modprobe ip_masq_quake**)
- VDOLive (**/sbin/modprobe ip_masq_vdolive**)

Maintenant vous êtes prêts à essayer le masquage d'IP ! Lancez le script `rc.local` avec la commande **/etc/rc.d/rc.local** et ça devrait aller. Asseyez−vous devant un autre ordinateur et essayez le surfer sur la toile. Avec un peu de chance, tout devrait aller comme sur des roulettes.

5. Problèmes

Il y a beaucoup de choses qui peuvent mal se passer en utilisant un document comme celui−ci, car il existe plein de cas spéciaux. La majorité des problèmes viennent de la configuration des périphériques réseaux interne et externe. J'essaierai de répondre à ceux qui rencontrent des problèmes, en essayant de voir ce qui ne va pas et en ajoutant des liens ici pour que les personnes avec des problèmes liés à des cas spéciaux puissent trouver de l'aide. Vous pouvez me joindre sans problème à l'adresse suivante pramsey@refractions.net.

5.1. ICQ ne fonctionne pas

Reportez vous tout simplement au HOWTO IP Masquerade.

5.2. J'ai une Caldera 2.X et pas une Red Hat 6.X

Bien, tout d'abord félicitations pour aller à contre−courant ! Deuxièmement, Nelson Gibbs (ngibbs@pacbell.net) a envoyé de bonnes nouvelles, car la plupart de ces instructions fonctionneront pour vous. Il y a des changements importants à noter cependant :

1. Une spécification de passerelle **GATEWAY=xxx.xxx.xxx.xxx** dans `/etc/sysconfig/network-scripts/ifcfg-eth0` et `eth1` pour les interfaces (l'interface locale utilise l'adresse IP distante et l'interface distante utilise l'adresse IP de la passerelle du FAI) ;
2. Vérifiez que le script `/etc/sysconfig/daemons/dhcpd` positionne la variable **ROUTE_DEVICE** à eth1 et *non* eth0 ;
3. Le fichier `/etc/dhcpd.conf` requiert un paramètre de sous−réseau pour chaque interface (Je ne suis pas trop sûr du pourquoi et du comment lorsque j ai fait mon deuxième test : subnet 213.102.154.201 netmask 255.255.255.255 { } sans aucune autre option le dhcp écoutait et envoyait aussi bien sur eth0 que eth1). Le serveur DHCP renvoie des erreurs si un seul des 2 sous−réseaux est listé ;
4. n'ajoutez *pas* de route vers **255.255.255.255**, le script `/etc/rc.d/init.d/dhcpd` fourni par Caldera fixe déjà le problème. *Changez* chaque référence de eth0 à eth1 dans ce script.

5.3. Je veux qu'une de mes machines interne soit mon serveur Web

C'est du gâteau ! En revanche, *vous aurez besoin d'une adresse IP statique* pour que la liste de recommandations suivantes fonctionne. Si vous avez une adresse IP dynamique, vous devrez rajouter des scripts pour vous assurer que l'adresse IP soit mise à jour dans les commandes de transfert de port quand l'adresse change.

Gardez à l'esprit que transférer un port externe vers une machine interne rend votre machine interne 'moins' interne qu'avant, heureusement ceci peut être fait de manière totalement transparente et sans réelle dégradation de performance. Un des effets de bord de l'implémentation du masquage d'IP dans le noyau Linux est la possibilité de faire des choses plutôt géniales avec les paquets quand il passe à travers la couche réseau, et l'utilitaire **ipmasqadm** est construit de manière à en tirer avantage.

Pour certaines raisons **ipmasqadm** n'est pas fourni avec toutes les dérivées de Red Hat ou de Mandrake, donc vous aurez probablement à le télécharger sur le site du mainteneur −− il existe aussi un paquetage RPM de disponible ainsi que le code source.

Une fois que vous avez le paquetage Red Hat, installez−le, et ajoutez les lignes suivantes à votre fichier `/etc/rc.d/rc.local` :

```
/usr/sbin/ipmasqadm portfw −f
/usr/sbin/ipmasqadm portfw −a −P tcp −L x.x.x.x 80 −R 192.168.1.x 80
```

La première commande efface les règles de transfert de port, la seconde ajoute un transfert du port 80 externe vers le port 80 du machine en interne. Notez que l'adresse IP statique tient dans l'espace d'adresse x.x.x.x et l'adresse IP interne dans l'espace 192.168.1.x.

À partir de là, les requêtes externes vers le port 80 seront envoyées de manière transparente au port 80 de la machine interne. Notez que vous ne pourrez tester à l'aide de telnet ou en vous connectant au port 80 de la passerelle d'une machine interne : le transfert de port honore seulement les requêtes en provenance de l'interface *externe*.