Un réseau c'est quoi ?

Un réseau c'est un moyen physique ***ET*** logique de relier des machines entres elles. Bien qu'il soit évident que la partie physique soit le mécanisme basique du réseau, la partie logique en est l'initiateur. Il faut "penser" son réseau avant de le construire.

Les différentes parties d'un réseau sont :

1) L'ordinateur connecté
2) Le switch auquel il est raccordé
3) Le pont qui permet à un ordinateur d'avoir 2 cartes réseaux avec la même adresse
4) Le routeur qui a 2 cartes réseaux permettant de passer d'un réseau à un autre

1) L'ordinateur connecté appelé poste

C'est un ordinateur ayant une carte réseau et relié au reste par un câble RJ45 ***droit***.

Nota Seul 2 postes relié entre eux, à l'exclusion de tout autre, utilisent un câble croisé. Plutôt que d'acheter un câble croisé il semble plus intéressant un embout de croisement. Cela rend les câbles d'usage général. Les parties de liaison poste à poste sont seules utilisatrices de cet embout.

2) Le switch

C'est un boîtier qui contient de 4 à 48 prises RJ45. Son rôle est de retransmettre tous les paquets IP qu'il reçoit.

3) Le pont (passerelle ou gateway)

C'est un ordinateur qui a 2 cartes réseau qui vont rallonger le réseau. Les réseaux RJ45 ont une longueur maximale qui dépend que la qualité des câbles. Typiquement on peut tabler sur une longueur de 70m avec un bon câble de type qualité 6. Si on a une distance plus grande on intercale un pont, ce qui permet de conserver des sections de 70m.
L'utilisation d'un pont ne se justifie que si on ne veut pas placer un switch et que l'on préfère utiliser un poste déjà présent. Celui-ci aura 2 cartes réseau en interne. De par sa fonction de pont ces cartes devront avoir la même adresse IP. (C'est le seul cas ou 2 cartes ont la même adresse)
Nota A la différence d'un switch qui est toujours allumé et donc toujours fonctionnel, un poste peut être éteint. Dans ce cas le segment qu'il gère n'est plus connecté.

4) Le routeur

C'est un poste spécialisé qui va faire passer les paquets d'une connexion de réseau à une autre connexion. Il a aussi 2 cartes réseaux. Il fait cela en gérant des classes d'adresses et des règles de transfert.
Il est à noté que le système Unix règne en maître sur les routeurs. Les tentatives de Microsoft avec Windows sont dévolu aux systèmes serveur (NT, 2000, 2003, 2008,…) et leurs possibilités sont moins développées que sous Unix.
BSD qui est un système Unix s'est fait une spécialité des réseaux et gère parfaitement le routage.

Les systèmes de connexion au net sont des routeurs.

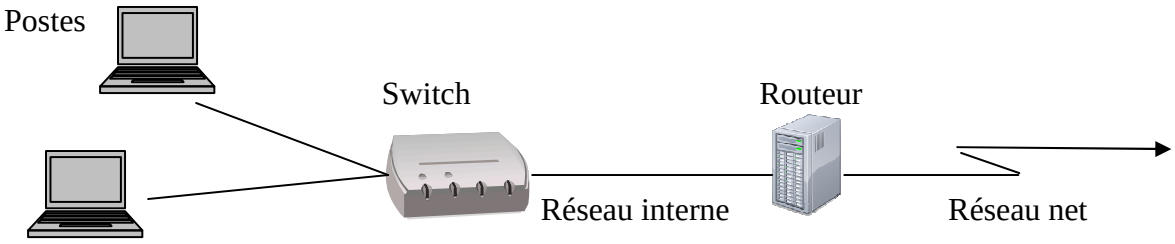
- **particuliers**

  Dans le cas de particuliers qui sont connectés au net il a presque toujours un dispositif appelé "box" qui permet de passer de leur réseau personnel au net. Cette "box" est un routeur entre le réseau RJ45 et l'ADSL. (Elle a souvent aussi un switch 4 ports)

- **société**

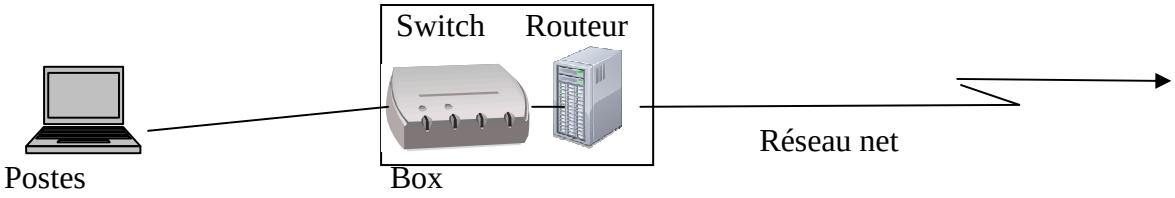
  Les sociétés ont des besoins beaucoup plus grands que les particuliers. Elles ont donc généralement des liaisons spécialisées, en général par fibre optique, qui assure des débits allant de 10M à 688M symétrique. Pour gérer ces débits et s'assurer une protection des accès et une disponibilité des connexions, elles utilisent des routeurs spécialisés type Cisco, société qui s'est spécialisée dans la fabrication de routeurs performants, ou des postes Unix frontaux.

Architecture d'un réseau



Nous allons voir l'architecture du réseau interne et le routeur. En sachant que ce schéma est une ossature de base. Les architectures réseaux des sociétés, ou quelquefois des particuliers, peuvent être bien plus compliquées.

Nota : Les box livrées par les FAI ont le routeur et le switch intégrées.



Classe d'adresses en IPV4

IPV4 a défini 3 classes, (5 en fait mais 2 sont spéciales).
Les adresses s'écrivent sur 4 nombres allant de 0 à 255 ce qui représente 1 octet, séparé par un ..

Le protocole IPV4

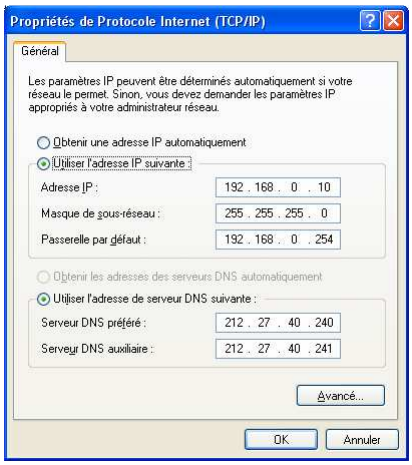
classe	début	Fin	Réservée réseau interne
A	0.0.0.0	127.127.127.127	10.0.0.0 ↔ 10.255.255.255
B	128.0.0.0	191.255.255.255	172.16.0.0 ↔172.31.0.0
C	192.0.0.0	223.255.255.255	192.168.0.0 ↔ 192.168.255.0

Adresses des postes

Windows

il faut aller dans le menu de démarrer :
Panneau de configuration → ***connexions réseau*** → click 2 fois sur ***carte(s) réseau (réseau local)*** → dans état de connexion click sur ***propriétés*** → dans propriétés descendre jusqu'à ***Protocle Internet TCT/IP*** et clicker sur ***propriétés***.

On obtient la fenêtre de paramétrage.



Si on n'est pas en DHCP, c'est-à-dire en automatique, il faut donner son adresse. Elle est dans l'espace réservé des classe A, B, ou C. Elle est probablement en classe C, donc du type 192.168.α.β. Par défaut le masque est en 255.255.255.0.

L'adresse de la passerelle est celle de votre box ou routeur vers l'extérieur. Par défaut, ou par usage, on prend l'adresse IP terminée par 254.

Les adresses de serveurs DNS sont des adresses ou on est certain d'avoir un DNS qui s'effectue correctement.

Nota : attention aux adresses DNS des FAI, elles changent assez souvent.

Unix

Bien que les IHM d'Unix (Kde/Gnome/…) fournissent des programmes de configuration au même titre que Windows, la philosophie d'unix est d'avoir ses configurations décrites dans des fichiers textes. Nous allons donc voir les fichiers de configuration des connexions réseau.

Nous allons prendre comme ex. les 2 distributions les plus courantes.

Ubuntu (Debian)	**Mandriva** (Red Hat)

Nota : avant modifications des fichiers interfaces , resolv.conf , ifcfg-ethα faire un ifdown -a.
Puis une fois les modifications faites, faire un ifup -a

fichiers à modifier/configurer

Nota : vous prendrez votre éditeur de texte favori pour rentrer le texte qui est borduré.

/etc/network/interfaces	Def. des adresses IP	/etc/sysconfig/network-script/ifcfg-ethα
/etc/resolv.conf	def. des dns	/etc/resolv.conf
	def. du réseau	/etc/sysconfig/network

/etc/network/**interfaces**

```
auto lo
iface lo inet loopback

# eth0
auto eth0
iface eth0 inet static
    address   192.168.0.10
    netmask   255.255.255.0
    network   192.168.0.0
    broadcast 192.168.0.255
    gateway   192.168.0.254

# eth1
auto eth1
iface eth1 inet static
    address   171.16.5.254
    netmask   255.255.0.0
    network   171.16.0.0
```

Nota : Les # indiquent un commentaire. On a supposé qu'il y a 2 cartes réseau dans l'ordinateur.

./etc/sysconfig/network-script/**ifcfg-ethα**

```
DEVICE=ethα
ONBOOT=yes
BOOTPROTO=static
BROADCAST=192.168.0.255
IPADDR=192.168.0.10
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
GATEWAY=192.168.0.254
```

Nota : Bien mettre après *DEVICE*= eth**0** ou eth**1** suivant le nom que l'on a donné à la connexion

/etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=home
FORWARD_IPV4=true
GATEWAY=192.168.0.254
GATEWAYDEV=eth1
```

Nota : Il est évident que GATEWAYDEV réfère la carte réseau qui est connectée à la passerelle.

/etc/**resolv.conf**

```
nameserver 212.27.40.240
nameserver 212.27.40.241
```

Nota : l'ex. donné est un des DNS de Free.
Si c'est celui de Google que l'on veut, on met 8.8.8.8
Pour une société c'est le DNS du routeur de celle-ci.

Commandes diverses

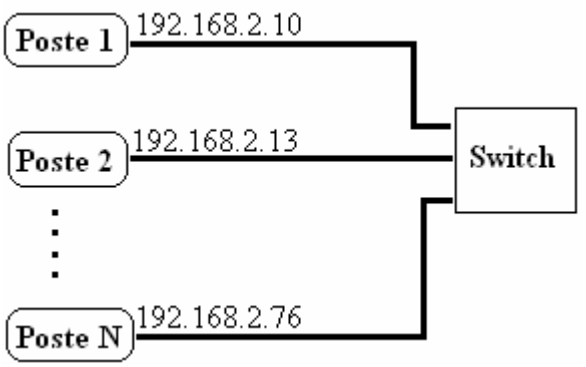
/etc/init.d/networking restart : redémarre tout
ifdown ethα : arrêt 1 interface réseau
ifdown -a : arrêt de toutes les interfaces
ifup ethα : redémarrer 1 interface réseau
ifup -a : arrêt de toutes les interfaces

On a vu comment configurer les adresses IP des postes.
Maintenant comment relier ces postes entre eux pour faire un réseau.

Actuellement les postes sont reliés à un **switch**.
Le switch est un appareil qui peut relier de 4 à 48 postes entre eux par des prises RJ45. Les swith à 4 ou 8 RJ45 sont un petit boîtier en plastique avec une alimentation par transfo séparée. Ceux à 12, 24 ou 48 prises sont généralement placé dans des rack 19" avec une alimentation 220v intégrée.
Le rôle du switch est de transmettre le paquet IP en amplifiant le signal.

Les postes se relient au switch par des **câbles RJ45 droits**.
Les câbles sont classés par catégorie :
Cat. 3 = câbles très quelconques, mais pas cher
Cat. 4 = câbles correctes
Cat. 6 = Câbles supérieur, plus coûteux.
Souvent la Cat. 6 blinde le signal ce qui lui confère une plus grande immunité aux parasites, cela apporte une plus grande sécurité du réseau.

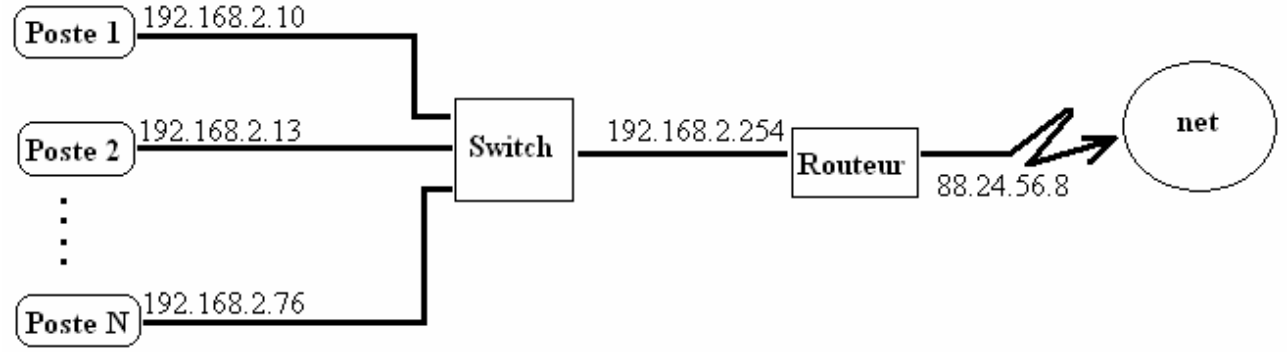
Notre réseau interne est donc ainsi fait:



Nous avons pris dans l'ex. les adresses 192.168.2.α comme adresses de réseau réservé.

Chaque poste doit avoir une adresse IP **unique** sur le réseau.

Si on continu notre architecture pour insérer un routeur sur l'extérieur on obtient :

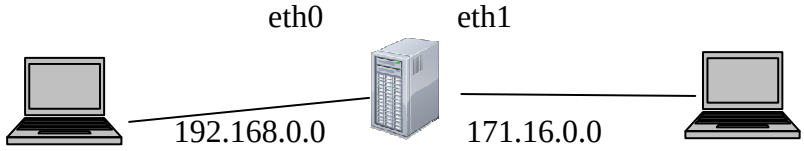


On observe que le routeur (notre box ou un routeur de société) a 2 adresses IP : Une du coté net, c'est celle qui permet de se connecter aux FAI. Et l'autre du coté réseau interne avec des adresses réservées.
Pour les particuliers, dans de nombreux cas, le routeur et le switch sont intégrés ensembles dans le même appareil. Ils forment la Box.

Donc dans la plupart des cas on aura cette configuration de réseau qui est absolument classique tant chez les particuliers que dans les petites et moyennes entreprises.

Il faut donc faire un vrai routeur. On peut le faire très difficilement avec Windows serveur car il impose d'avoir un des coté du routeur avec l'adresse 192.168.0.1 ce qui complique les déploiements.
On va donc le faire tout naturellement avec un Unix.
Dans ce routeur il y a **2 cartes réseau**. Il faut donc configurer les adresses IP comme il faut, avec 2 classes d'adresses différentes.

Prenons la classe d'adresse interne en **171.16.0**.α et la classe d'adresse entre le routeur et celui qui va sur le net en **192.168.0**.α. On pouvait tout aussi bien prendre 192.168.**5**.α. à la place de 171.16.0.α.



On suppose que le routeur s'insère dans un réseau déjà existant et a en

- ETH0
  - une adresse 192.168.0.***x*** qui lui est fourni par un DHCP.
  - Il a comme passerelle par défaut 192.168.0.254 (celle de la box ou du routeur sur le net)
  - DNS 212.27.40.240, 212.27.40.241 (C'est le DNS de Free).
- ETH1
  - une adresse 171.16.0.254.
  - DNS 212.27.40.240, 212.27.40.241 (C'est le DNS de Free).
  - Il peut ou non être serveur DHCP (voir configuration DHCP p.9)

Il faut indiquer au routeur qu'il doit passer tous les paquets de 192.168.0.- en 171.16.0.- et réciproquement. On voit apparaître une notion de réseau et de n° de poste.

Sous Unix la notion de routage est implémentée nativement. Il faut juste la configurer. *(Tout se fait bien sur en ligne de commande*.)

Indiquer que l'on accepte le forward de ipv4[1]

echo 1 > /proc/sys/net/ipv4/ip_forward

Maintenant il ne reste plus qu'à travailler sur les iptables qui sont les règles du ***firewall*** d'Unix.

1) Configurer iptables pour accepter le forward

iptables -A FORWARD -j ACCEPT

2) Configurer iptables pour un masquerade de 171.16.0.0

*iptables -t nat -A POSTROUTING -o **eth0** -s **171.16.0.0/24** -j MASQUERADE* [2]

Nota : Les postes clients devront avoir leurs adresses sur le réseau 171.16.0.x avec un gateway sur l'adresse du serveur (par ex. 171.16.0.254). Ils auront toujours leurs DNS.

Les iptables

C'est la partie la plus complexe de la gestion d'un routeur sous Unix.
Par ***défaut*** le firewall ***n'accepte rien***. Il faut lui donner les règles explicitement.

Voir les liens suivants :
http://www.netfilter.org/
http://www.misfu.com/Telechargement/iptables.pdf
http://jeanyves.bossard.free.fr/docs/securite/iptables.pdf
http://irp.nain-t.net/doku.php/130netfilter:010_architecture

Les règles sont stockées dans un fichier texte que le processus *init* de Unix vient lire et exécuter. On trouve donc des fichiers qui ont des règles dans ce style. On trouvera ci-dessous des exemples
http://www.nbs-system.com/dossiers/howto-iptables.html

On le voit l'administration Unix passe par une compréhension et des modifications de ce type de fichier.

---

[1] On l'a "vue" dans le fichier *network* de la Mandriva avec la ligne *FORWARD_IPV4=true*.

[2] -o eth0 c'est la carte vers le réseau 192.168.0.0 . –s c'est la carte eth1 vers le réseau 171.16.0.0. Si les adresses ne sont pas les mêmes, il faut adapter les paramètres de la ligne d'iptables.

Le réseau

Dans notre ex. de réseau précédent on a vu qu'il y avait 2 parties dans une adresse IP :

- la partie *réseau*
- la partie *n° de poste*

La partie n° poste est la caractéristique des postes à devoir avoir tous un n° différents les uns des autres.
La partie réseau c'est ce qui détermine l'adresse d'un réseau. C'est en IPV4 le masque de sous réseau qui le détermine.
Supposons que l'on ait une adresse 192.168.40.27 si on lui donne un masque 255.255.255.0 pour avoir le réseau on fait une opération ***et*** entre l'adresse IP et le masque.
Dans l'opération et : 1 et 1 donne 1, x et 0 donne 0
255 c'est 1 partout dans l'octet. Donc

192.168.40.27
& 255.255.255.0
192.168.40.-

Il ne reste que 192.168.40, le réseau a donc l'adresse 192.168.40 et le poste a comme n° 27
Autre ex.
J'ai une classe d'adresse en 172.18.50.71 et mon masque est 255.255.0.0

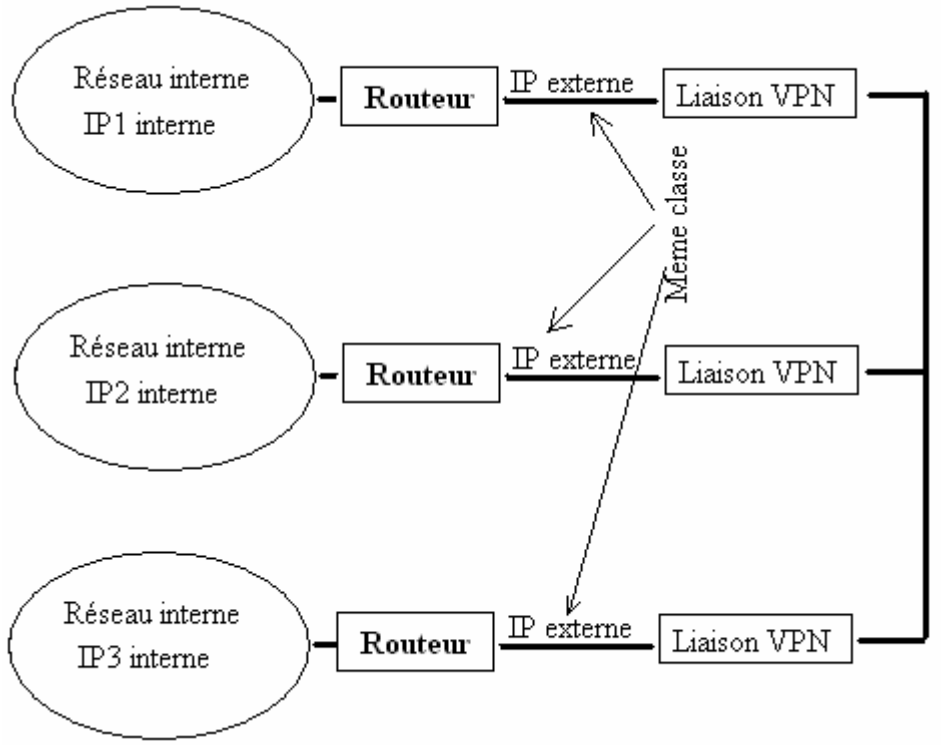
172.18.50.71
& 255.255.0.0
172.18.-.-

Donc le poste a comme réseau 172.18 et comme n° 50.71

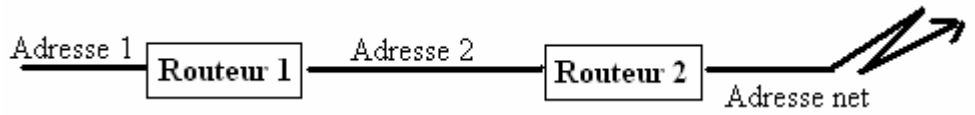
On peut alors différencier sur un même réseau des sous réseaux avec le masque.

Supposons que l'on ait un réseau 192.168.10.- et que notre masque ne soit plus 255.255.255.0 mais 255.255.255.128. On a créer 2 sous réseaux celui dont les postes ont un n° > à 128 et ceux dont le n° est < à 128. Ainsi sous une même classe d'adresse on a 2 sous réseaux. Cela peut permettre de segmenter 2 services dans une entreprise avec une même classe d'adresse. Segmenter veut dire que les postes d'un segment ne voient pas les postes de l'autre segment.

Dans certaines entreprises le réseau est plus compliqué. Il existe des segmentation du réseau du à des besoins spécifiques. Ex. le centre de recherche est dans une ville, le centre administratif dans une autre et les usines de production dans d'autres. On a alors un morcellement géographique du réseau.



On voit que 2 routeurs sont reliés par une même classe d'adresse. On a donc, en simplifiant le schéma et en considérant que la société a un accès au net:



L'adresse 1 est l'adresse du réseau interne de la société. L'adresse 2 est l'adresse des routeurs en VPN, celle qui relie tous les routeurs entre eux.

Les ponts

Le pont n'a qu'une utilité limitée. Il permet de relier 2 segments d'un même réseau. En fait il fait office d'amplificateur de signal.
Si on a un ordinateur bien placé géographiquement et que l'on ne veut pas faire la dépense d'un switch mais que l'on a 2 cartes réseau dans l'ordinateur, alors il peut être utile de faire un pont.
Sous Windows il suffit de sélectionner les 2 interfaces réseau et de cliquer sur pont.
Alors les 2 cartes réseau ont la même adresse IP et le même masque.

Actuellement les administrateurs réseau préfèrent utiliser un switch plutôt qu'un pont. Dans le cas du pont construit avec un poste, le segment est perdu si on éteint le poste. Avec un switch qui est toujours allumé cet inconvénient n'existe pas.

Par contre sur des architectures utilisant d'autre technologie que le câble RJ45, le pont peut avoir sont utilité. Ex. avoir un pont entre un réseau RJ45 et WiFi, ou CPL.

Les commandes usuelles réseau

On voit ici les commandes utiles pour configurer un réseau et vérifier ce que l'on fait.
On a vu comment déterminer l'adresse d'un poste.
Un fois ce poste insérer dans un réseau il faut savoir s'il peut dialoguer avec les autres postes.

1) Vérifier la configuration du poste

Windows	Unix	
ipconfig	***Ifconfig -a***	Permet d'afficher la configuration des cartes réseaux d'un poste

2) Vérifier qu'un poste peut être contacté

ping <adresse du poste à contacter>

Attention : les firewall limitent les ping. Pour faire des tests lors de l'installation d'un réseau il peut être utile de supprimer le firewall. Puis une fois tout testé et prêt à fonctionner normalement, remettre en service le firewall.

3) Donner la route parcourue par les paquets

Windows	Unix	
route	***route -n***	Permet d'afficher la route

4) Donner l'adresse MAC d'une carte

Windows	Unix	
arp	***arp -a***	Permet d'afficher la route

5) Tracer le chemin d'un poste à un autre

Traceroute <adr. IP>

6) *Sniffer un réseau* (copie de : http://fr.wikipedia.org/wiki/Comparaison_de_packet_sniffers)

	Créateur	Coût	Licence
Kismet	Mike Kershaw (dragorn)	Gratuit	GPL
snoop	Sun Microsystems	Gratuit	CDDL
tcpdump	The Tcpdump team	Gratuit	BSD
Wireshark	The Wireshark team	Gratuit	GPL

Systèmes d'exploitation supportés

Client	Windows	Mac OS X	Linux	BSD	Solaris
Kismet	✓ Oui	✓ Oui	✓ Oui	✓ Oui	
snoop					✓ Oui
tcpdump	✓ Oui	✓ Oui	✓ Oui	✓ Oui	✓ Oui
Wireshark	✓ Oui	✓ Oui	✓ Oui	✓ Oui	✓ Oui

Le DHCP

On a derrière le routeur un nombre important de machines, on veut donc un service DHCP.

- On désire configurer la liaison ethα comme étant en dhcp.

	Mandriva /etc/network/**interfaces**	**Ubuntu** /etc/network/**interfaces**
Ancien	DEVICE=ethα ONBOOT=yes BOOTPROTO=static	# eth0 auto eth0 iface eth0 inet static
Nouveau	DEVICE=ethα ONBOOT=yes BOOTPROTO=dhcp	# eth0 auto eth0 iface eth0 inet dhcp

- Il faudra configurer le service dhcp.

	Mandriva	Ubuntu
Pour cela il faut aller dans le fichier :	/etc/dhcpd.conf	/etc/dhcp3/dhcp.conf

```
ddns-update-style interim;          # Required for dhcp
ignore client-updates;
subnet 192.168.1.0[3] netmask 255.255.255.0 {
   range 192.168.1.128 192.168.1.254;          # le range des adresses
   option subnet-mask          255.255.255.0    # le masque
   option broadcast-address    192.168.1.255;   # broadcast par default
   option routers              192.168.1.254;   # le gateway
   option domain-name          "your-domain.org";
   option domain-name-servers  40.175.42.254, 40.175.42.253; # DNS par défaut
   option netbios-name-servers 192.168.1.100;   # WINS server pour Windows
# DHCP requests are not forwarded. Applies when there is more
# than one ethernet device and forwarding is configured.
#  option ipforwarding off;
   default-lease-time 21600;  # temps en s où le client garde son adr.
   max-lease-time 43200;      # temps max en s où le client garde son adr.
   option time-offset -18000; # Eastern Standard Time
#  option ntp-servers 192.168.1.1;  # Default NTP server
#  option netbios-name-servers     192.168.1.1;
# Don't change this unless you understand Netbios very well
# --- Selects point-to-point node (default is hybrid).
#  option netbios-node-type 2;
# We want the nameserver "ns2" to appear at a fixed address.
# Name server with this specified MAC address will recieve this IP.
    host ns2 {
        next-server ns2.your-domain.com;
        hardware ethernet 00:02:c3:d0:e5:83;
        fixed-address 40.175.42.254;
     }
# Laser printer obtains IP address via DHCP. This assures that the
# printer with this MAC address will get this IP address every time.
   host laser-printer-lex1 {
        hardware ethernet 08:00:2b:4c:a3:82;
        fixed-address 192.168.1.120;
   }
}
```

- Démarrer le dhcp

Mandriva	Ubuntu
*/etc/rc.d/init.d/***dhcpd start**	*service* **dhcpd start**

[3] Les adresses en gras sont évidement à adapter en fonction des besoins

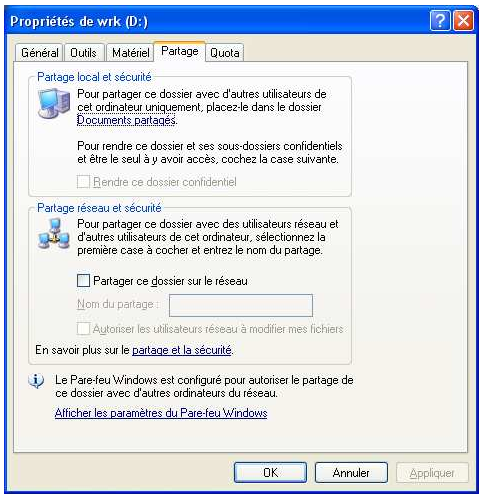
Liaison entre postes

Les liaisons possibles sont :

1) Entre poste Windows
2) Entre postes Unix
3) Entre poste Mac
4) Entre poste Unix et Windows et Mac

De Windows à Windows

Pour pouvoir communiquer entre postes Windows il faut partager les répertoires (disques) que l'on veut accéder.



Une fois ce partage effectué on peut, au moyen du réseau, se connecter à l'ordinateur distant et parcourir le(s) répertoire(s) partagé(s).

Nota : Il ne faut pas oublier qu'il y a des sécurités et qu'il faut se connecter, éventuellement, sur un compte utilisateur avec un mot de passe.

D'Unix à Unix

Il y a Plusieurs moyens d'échanger des fichiers sous Unix.

1) NFS

Il permet de "monter" les arborescentes distantes afin d'avoir un système de fichiers unifié.

2) FTP

Echanger des répertoires/fichiers.

3) SSHFS

On peut se connecter sur son poste à distance et travailler en mode sécurisé.

De Mac à Mac

L'ancienne génération de Mac avait un protocole d'échange réseau AppleTalk peu performant.
La version OS X étant basée sur un système Unix, il accepte tous les protocoles d'Unix à Unix

D'Unix à Windows

SAMBA

Sur un poste Unix, cela simule le protocole Windows, (ou ancien Mac) et permet de partager des répertoires, des imprimantes, etc.