DHCP

Dynamic Host Control Protocol

Ce protocole permet aux administrateurs de réseaux TCP/IP de configurer les postes clients de façon automatique. Il a été utilisé par les fournisseurs d'accès à l'Internet par le câble, mais a été abandonné au profit d'une connexion point à point type PPP, comme pour l'ADSL.

DHCP reste cependant un protocole de configuration de clients extrêmement pratique sur un réseau local Ethernet.

Bien que dans la plupart des cas, DHCP soit un luxe sur un réseau domestique, il peut tout de même y avoir plusieurs raisons pour vous pousser à l'utiliser :

- Vous avez des portables que vous connectez sur divers réseaux, typiquement chez vous et sur votre lieu de travail (si votre administrateur vous laisse faire, c'est qu'il est bien confiant :-)),
- vous organisez chez vous des "Lan parties" avec les machines de vos collègues,
- votre réseau local contient plusieurs dizaines de machines (vous avez une famille nombreuse, peut-être),
- vous aimez bien vous compliquer la vie à bricoler avec votre Linux,
- vous aimez le luxe, tout simplement.

Avis au lecteur

La bonne compréhension de ce protocole implique un minimum de connaissances de TCP/IP. Si vous ne les avez pas, lisez d'abord le chapitre "TCP/IP"[1].

1 Chapitre TCP/IP : http://christian.caleca.free.fr/tcpip/index.html

Plan du chapitre

Protocole DHCP

Position du problème

Lorsque vous connectez une machine à un réseau Ethernet TCP/IP, cette machine, pour fonctionner correctement, doit disposer :

- D'une adresse IP unique dans votre réseau et appartenant au même réseau logique que toutes les autres machines du réseau en question,
- un masque de sous réseau, le même pour tous les hôtes du réseau,
- une adresse de DNS, pour pouvoir résoudre les noms des hôtes, surtout si votre réseau est connecté au Net,
- l'adresse de la passerelle qui vous permet justement d'accéder au Net. (Nous supposerons que votre réseau domestique n'est pas suffisamment complexe pour contenir de multiples sous-réseaux).

Si vous n'avez déjà rien compris à ce discours, alors il est nécessaire pour vous de lire d'abord les chapitres sur les réseaux[2], TCP/IP[3] et le routage[4].

Pour configurer vos hôtes locaux, vous avez deux possibilités :

- Vous passez de machine en machine, avec un petit carnet et vous configurez à chaque fois tous les paramètres de la pile IP à la main, en n'oubliant pas de tout marquer dans votre carnet. Ce n'est pas le plus compliqué, ce qui est d'avantage gênant, c'est de ne jamais oublier de noter toutes les modifications que vous pourriez être amené à faire par la suite.
- Vous installez un serveur DHCP sur votre réseau et vous dites à vos clients d'aller chercher toute leur configuration IP sur ce serveur. En gros, il remplacera votre carnet, sera naturellement à jour et vous évitera des déplacements.

Comme vous le voyez, le luxe de la seconde solution est tout de même tentant, au point que nous allons le mettre en oeuvre.

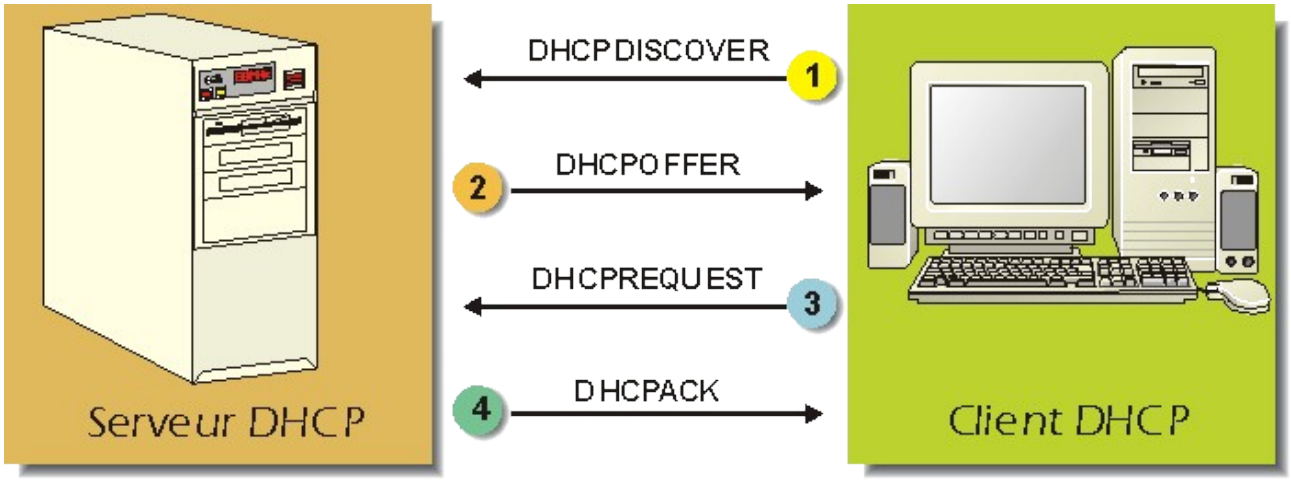
Que disent les livres ?

Les choses se passent avec le peu de moyens dont vous disposez :

- Votre "MAC Address" que vous ne perdez jamais, puisqu'elle est écrite "en dur" dans votre interface Ethernet.
- Le "Broadcast" ou "Diffusion" qui permet d'envoyer des trames à toutes les machines du réseau physique.

Le dialogue est décrit de la manière suivante :

2 Les réseaux : http://christian.caleca.free.fr/reseaux/
3 Chapitre TCP/IP : http://christian.caleca.free.fr/tcpip/index.html
4 Le routage : http://christian.caleca.free.fr/routage/



1. Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau, du moins, en principe. Il envoie donc une trame "DHCPDISCOVER", destinée à trouver un serveur DHCP. Cette trame est un "broadcast", donc envoyé à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi sa "MAC Address".
2. Le, ou les serveurs DHCP du réseau qui vont recevoir cette trame vont se sentir concernés et répondre par un "DHCPOFFER".
   Cette trame contient une proposition de bail et la "MAC Address" du client, avec également l'adresse IP du serveur. Tous les DHCP répondent et le client normalement accepte la première réponse venue.
   Le "DHCPOFFER" sera un broadcast (Ethernet) ou non, suivant le serveur DHCP utilisé. Nous y reviendrons plus en détail sur l'exemple.
3. Le client répond alors par un DHCPREQUEST à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.
4. Le serveur DHCP Concerné répond définitivement par un DHCPACK qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

Détails sur le serveur DHCP

Un serveur DHCP dispose d'une plage d'adresses à distribuer à ses clients. Il tient à jour une base de données des adresses déjà utilisées et utilisées il y a peu (C'est ce qui explique que l'on récupère souvent la même adresse, le DHCP ayant horreur des changements ;-).

Lorsqu'il attribue une adresse, il le fait par l'intermédiaire d'un bail. Ce bail a normalement une durée limitée dans le temps. Sur un réseau d'entreprise où l'on dispose largement d'assez d'adresses pour le nombre de postes et que ces derniers sont en service toute la journée, le bail peut être d'une semaine ou plus encore. Sur le câble, le bail était seulement d'une heure.

Après expiration du bail, ou résiliation par le client, les informations concernant ce bail restent mémorisées dans la base de données du serveur pendant un certain temps. Bien que l'adresse IP soit disponible, elle ne sera pas attribuée en priorité à une autre machine. C'est ce qui explique que l'on retrouve souvent la même adresse d'une session à l'autre.

Détails sur le bail

Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration comme :

- L'adresse d'un ou de plusieurs DNS (Résolution de noms).
- L'adresse de la passerelle par défaut (pour sortir du réseau où le DHCP vous a installé).
- L'adresse du serveur DHCP (nous allons voir pourquoi).

Cette liste est loin d'être complète, il existe en effet une grande quantité d'options qui peuvent êtres transmises.

Lorsque le bail arrive à environ la moitié de son temps de vie, le client va essayer de renouveler ce bail, cette fois-ci en s'adressant directement au serveur qui le lui a attribué. Il n'y aura alors qu'un DHCPREQUEST et un DHCPACK.

Si, au bout des 7/8e de la durée de vie du bail en cours, ce dernier n'a pu être renouvelé, le client essayera d'obtenir un nouveau bail auprès d'un DHCP quelconque qui voudra bien lui répondre. Il pourra alors se faire que le client change d'adresse IP en cours de session. Normalement, cette situation ne devrait pas se produire, sauf en cas de panne du DHCP.

Dans les manuels, il est recommandé de ne pas créer de baux inutilement courts, ceci entraînant une augmentation significative du broadcast sur le réseau. Le compromis est à trouver entre la durée moyenne de connexion des utilisateurs, la réserve d'adresses IP du serveur, le nombre d'abonnés...

En règle générale, un FAI dispose toujours de moins d'adresses que d'abonnés, parce que tous les abonnés ne se connectent pas en même temps. Une mauvaise analyse des statistiques peut alors entraîner de graves problèmes (que nous avons connus sur le câble) aux heures de pointe.

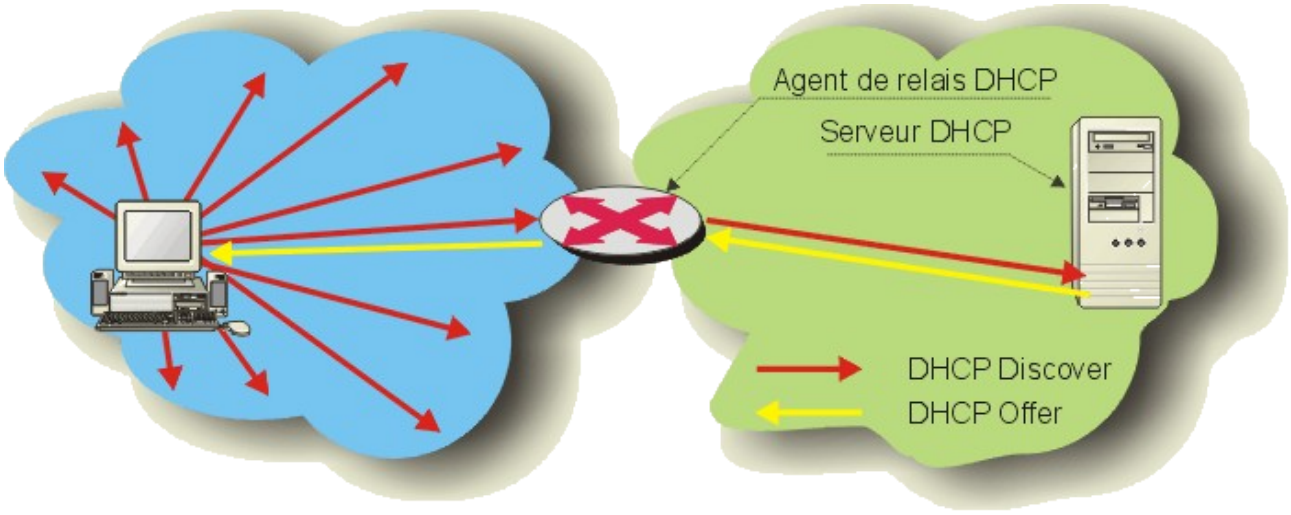
Question subsidiaire

Il doit donc y avoir nécessairement un serveur DHCP par réseau et il doit disposer d'une adresse IP dans la même classe que celle qui constitue sa plage d'adresses?

Non, pas nécessairement. Votre réseau physique peut être formé de plusieurs sous réseaux logiques, avec des routeurs entre chaque sous réseau et le tout peut fonctionner avec un seul serveur DHCP...

Mais alors, comment la négociation peut-elle se faire, puisque, normalement, un "broadcast" n'est pas retransmis par les routeurs ?

Les requêtes DHCP doivent pouvoir atteindre le serveur qui est situé sur un autre réseau logique, elles doivent donc passer les routeurs, ce qui n'est théoriquement pas possible. Il est alors nécessaire d'installer sur un ou plusieurs routeurs un agent de relais qui va intercepter les requêtes en broadcast et les transmettre à un serveur DHCP connu de cet agent.



C'est l'agent de relais situé sur la passerelle qui va faire l'intermédiaire et le client réussira tout de même à obtenir un bail, donné par un DHCP situé sur un autre réseau et transmis par l'agent de relais.

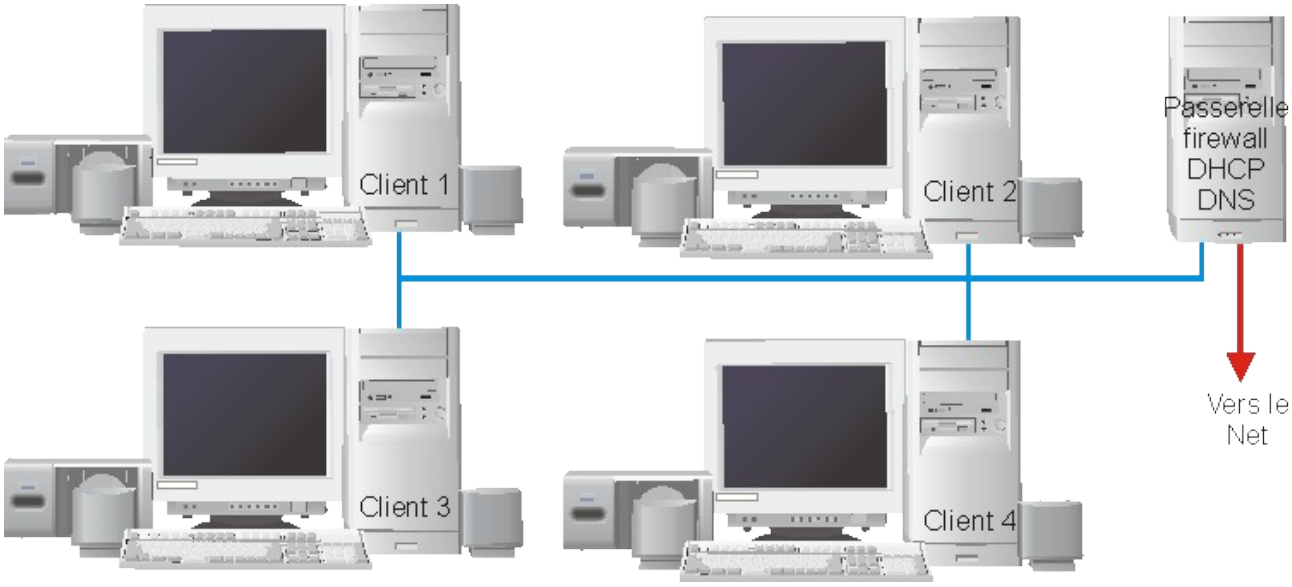
Nous ne pousserons pas le luxe jusque là, mais la solution existe. Le serveur DHCP sera même capable d'envoyer des paramètres différents, suivant le sous réseau du client...

Serveur DHCP

Topologie du réseau

Nous allons prendre une configuration simple, avec une machine Linux qui va cumuler plusieurs fonctions :

- Passerelle entre le réseau local et l'Internet,
- firewall,
- serveur DHCP,
- serveur DNS. (Pourquoi pas, puisqu'on est dans le luxe...).



- Les clients peuvent être de tout type : Windows, Mac OS, Linux...
- dans l'exemple, la passerelle est construite avec Linux Mandrake 9.

Nous allons donc installer sur la passerelle un serveur DHCP. Le DNS est tout à fait optionnel, mais ce serait bien qu'il y soit, il peut même y être déjà, ça n'est absolument pas gênant. S'il n'y est pas encore, vous pourrez le rajouter par la suite.

Les fonctions de passerelle et de firewall ne sont pas non plus fondamentales, nous pourrions nous contenter d'un serveur Linux, non connecté au Net (mais qui peut le plus peut le moins).

Nous pourrions même ajouter un autre serveur au réseau local, chargé du DNS et du DHCP et ne laisser à la passerelle que les fonctions de routage et de firewall.

Installation du serveur DHCP

Sur Mandrake, ça se fait très simplement en installant les paquetages dhcp-common et dhcp-server. Dans la version 9 de Mandrake, vous disposez de la version 3.0 du serveur. Il y a un seul fichier de configuration : /etc/dhcpd.conf, que vous pourrez configurer avec un éditeur de texte, où à travers

l'interface Webmin. Ce que nous aurons à faire est suffisamment simple pour pouvoir le faire à la main.

Configuration du serveur

Le principe

Comme nous l'avons vu plus haut, un serveur DHCP, en plus de fournir la configuration IP "de base" (Adresse et masque), peut aussi transmettre un nombre plus ou moins grand de paramètres supplémentaires. Nous aurons donc au moins deux choses à configurer :

- La réserve d'adresses dont le serveur pourra disposer pour les attribuer aux clients,
- les paramètres optionnels à leur communiquer dans la foulée, comme l'adresse d'un DNS et de la passerelle par défaut. Dans le cas d'un réseau domestique; ce sera suffisant, mais il y a beaucoup d'autres options, plus ou moins spécifiques aux divers systèmes d'exploitation.

Nous avons vu qu'un seul serveur DHCP pouvait être utilisé pour plusieurs réseaux logiques interconnectés, pourvu que les interconnexions disposent d'un agent de relais DHCP. Dans un tel cas, le serveur DHCP devra disposer d'au moins une étendue d'adresses IP par réseau logique dont il aura la charge.

En ce qui concerne les options, nous disposons d'une architecture hiérarchique :

- Nous pouvons définir des options globales, qui seront les mêmes pour tous les clients du DHCP, tous sous réseaux confondus,
- nous pouvons définir également des options propres à chaque sous réseau, celles-ci écrasant les options globales, en cas de conflit.
- Si l'on veut aller encore plus loin, sachez que DHCPd peut créer des groupes distincts de machines dans un même sous réseau et même gérer des clients de façon individuelle.

Une configuration basique

Ce que nous voulons faire

- Nous avons un seul réseau, avec des IP choisies dans la classe C privée 192.168.0.0, donc avec un masque 255.255.255.0.
- Nous avons donc une passerelle par défaut unique pour tous nos hôtes du réseau, dans l'exemple, ce sera 192.168.0.253.
- Nous disposons enfin d'un DNS, également unique pour tous les hôtes du réseau, il est sur la même machine, à savoir 192.168.0.253. Le "domaine" que nous avons construit sur notre réseau local s'appelle maison.mrs. Il n'a aucune réalité sur le Net, mais ça n'a pas d'importance, puisque c'est un domaine qui ne doit pas être visible depuis le Net.
- Sur la totalité de la classe C disponible, nous allons réserver les adresses comprises entre 192.168.0.1 et 192.168.0.9 pour les clients du réseau. Cette plage constituera la réserve d'adresses que le DHCP pourra fournir aux clients.
  Bien entendu, nous aurions pu en mettre plus, mais il faut toujours se garder quelques

adresses sous le coude, pour les machines configurées manuellement, comme les serveurs que l'on place sur le réseau.

- Un dernier point important, c'est la durée de vie du bail que le DHCP va attribuer aux clients. L'un des avantages de DHCP, c'est de pouvoir attribuer une configuration IP qui ne sera valide que dans un laps de temps donné, à charge pour le client de demander le renouvellement de ce bail avant chaque expiration. Ce temps de vie pourra aller de quelques minutes à l'infini, suivant les besoins. Sur un réseau qui évolue peu, le bail peut être sans problèmes de quelques jours, à quelques semaines, voire plusieurs mois. Sur un réseau où les hôtes vont et viennent, il sera plus sage de ne laisser vivre les configurations que quelques heures. Bien entendu, plus le bail est court, plus le trafic généré par DHCP devient important et plus la charge du serveur augmente. Ceci dit, ce n'est pas un argument très significatif sur un réseau ne dépassant pas une dizaine de clients.
  Dans l'exemple, nous utiliserons une heure (3600 secondes).

Note importante

Le daemon DHCPd écoute par défaut sur toutes les interfaces réseau actives sur le serveur. Ce n'est pas forcément souhaitable, c'est même assez souvent ennuyeux.

Fort heureusement, ce comportement par défaut peut être modifié, mais pas dans le fichier de configuration. Il faut utiliser un paramètre dans la ligne de commande qui va démarrer DHCPd.

Dans le cas de Mandrake, il faut éditer le script /etc/rc.d/init.d/dhcpd. Il est bien documenté et vous trouverez aisément la variable INTERFACES qu'il faut initialiser avec le nom de la ou des interfaces qui doivent êtres écoutées. Dans notre exemple, nous aurons :

```
INTERFACES="eth0"
```

Ce que nous écrivons dans dhcpd.conf

```
# Les trois lignes qui suivent doivent être présentes
# même si pour le moment, elles ne nous servent pas.
# Elles concernent la mise à jour dynamique du DNS
# que nous verrons plus tard


ddns-domainname "maison.mrs";
ddns-update-style none;
ddns-updates off;

# tous les clients sont acceptés, même si l'on ne connaît pas
# leur adresse MAC.
allow unknown-clients;

# Durée de vie du bail
max-lease-time 3600;
default-lease-time 3600;

# Les options que l'on va refiler aux clients
option domain-name-servers 192.168.0.253;
option domain-name "maison.mrs";
option routers 192.168.0.253;

# La définition du seul "sous-réseau" dont nous disposons
# Avec la plage d'IP à distribuer.
subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.1 192.168.0.9;
}
```

Cette configuration simplissime va suffire à nos besoins, du moins dans un premier temps.

Dans ce fichier, il y a des directives, qui sont obligatoires :

- les directives ddns-xxx serviront plus tard, ce sera la cerise sur le gâteau, pour ceux qui utilisent BIND 9 (le serveur DNS). Elles doivent cependant figurer dans la configuration pour que le démon dhcpd puisse démarrer,
- allow unknown-clients
  C'est en principe la configuration par défaut, mais autant le spécifier. Ça veut dire que le DHCP acceptera tous les clients qui feront une requête DHCP. Dans le cas contraire, le serveur ne répondrait qu'aux machines dont il connaît l'adresse MAC.
- Il existe une subtile différence entre les directives max-lease-time et default-lease-time, la page "man dhcpd.conf" vous indiquera quelle est cette différence. Contentons nous pour l'instant d'assigner la même valeur aux deux, ici 3600 secondes.

Et des options qui seront dans la pratique, des paramètres de configuration optionnels. Ici :

- domain-name-servers
  qui attribuera aux hôtes une adresse de DNS. Dans l'exemple, notre DNS à nous. Si nous n'en avons pas, il faudra ici mettre l'IP du DNS de notre fournisseur d'accès. Eventuellement, nous pouvons spécifier plusieurs DNS.
- domain-name
  est vraiment optionnel, ça permettra aux clients de savoir dans quel domaine ils sont enregistrés.
- routers
  c'est la passerelle par défaut. Il pourrait y avoir plusieurs routeurs, mais tous les systèmes ne savent pas gérer de façon efficace une information contenant plusieurs passerelles.

Toutes les options qui figurent avant le paragraphe "subnet 192.168.0.0 netmask 255.255.255.0" sont des options globales, il n'y a ici aucune option d'étendue (de sous-réseau) de définie.

Cette configuration doit nous permettre de fonctionner dans notre contexte. Il nous suffit de lancer ou de relancer le serveur :

```
/etc/init.d/dhcpd restart
```

Et ça devrait fonctionner.

Les clients DHCP

Configuration des clients

Vous devez aller dans la configuration TCP/IP, enlever tout ce qu'il y a concernant l'IP, le masque de sous réseau, DNS, passerelle et juste dire que vous voulez une configuration dynamique (DHCP). Relancez vos services réseaux, la méthode la plus simple et la plus bestiale étant le "reboot", et voilà. Une fois le système remonté, vous devez avoir hérité d'une configuration automatique.

Tout pour contrôler, réparer etc.

Dans cette partie nous verrons, suivant le système employé,

- Windows 95/98
- Windows NT4/2000
- Linux (Mandrake 9)

quels sont les outils pour contrôler l'état du client DHCP.

Je demande aux utilisateurs de Be/OS, de MAC/OS et de tous ceux que j'oublie, de bien vouloir m'excuser de ne pas leur apporter mon soutien. J'ai déjà dans mon petit bureau (4 M^2) trois PC dont un sur lequel sont installés trois systèmes, je n'ai plus de place...

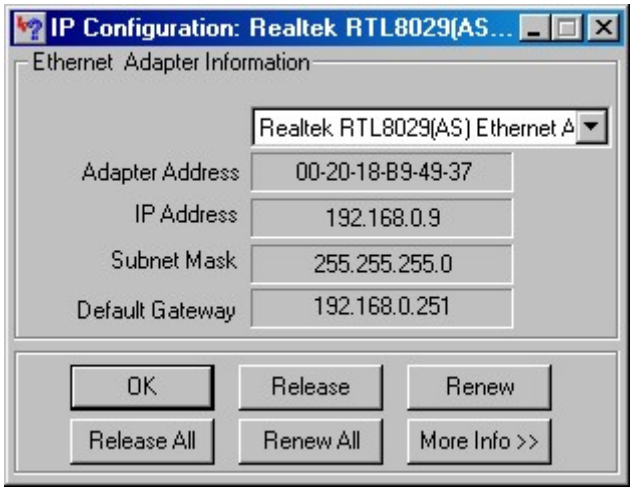
Windows 95/98

Configuration

Par le panneau de configuration, icône "réseau", cliquez sur "TCP/IP -> <votre carte réseau>. L'adresse IP doit être configurée dynamiquement, c'est d'ailleurs le choix par défaut à l'installation.

Vérification

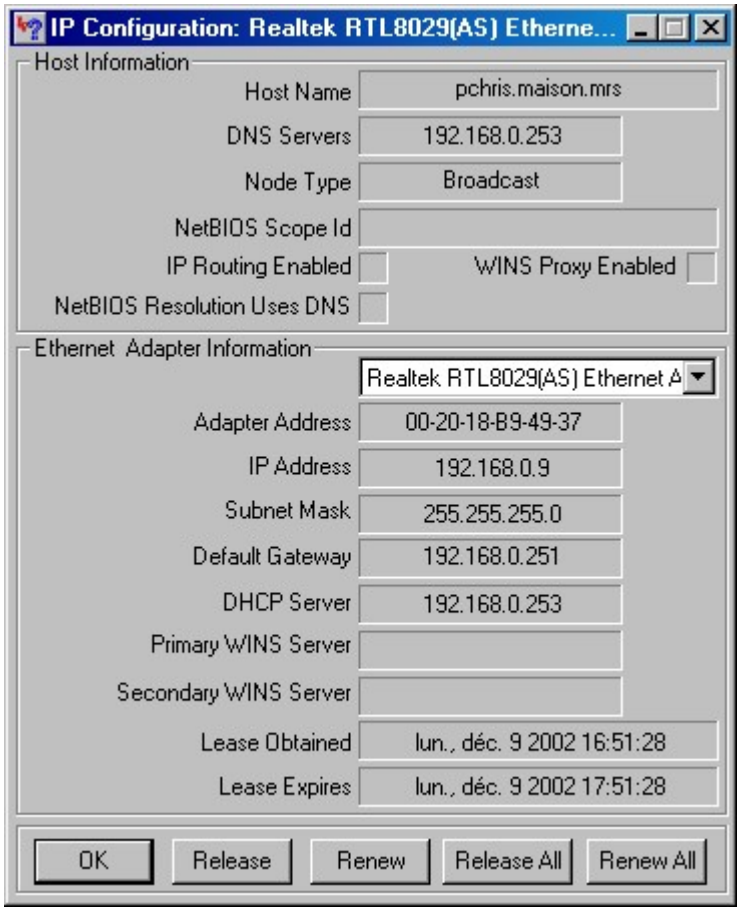
Si vous avez un bail en cours de validité, la commande "winipcfg" vous affiche les choses suivantes:



ATTENTION! Windows 95 et 98 installent également le client PPP dont nous n'avons rien à faire... Ce client apparaît également dans la liste des interfaces réseau.

Vérifiez bien que vous pointez sur votre carte Ethernet et pas sur le client PPP...

Si vous cliquez sur le bouton "Plus d'info>>" :



Ici, c'est le bouton "Renouveler" qui sera votre seul secours en cas de problèmes.

Notez que les rubriques "Bail obtenu" et "Expiration du bail" contiennent des valeurs calculées par votre machine. Le serveur DHCP ne donne que la durée.

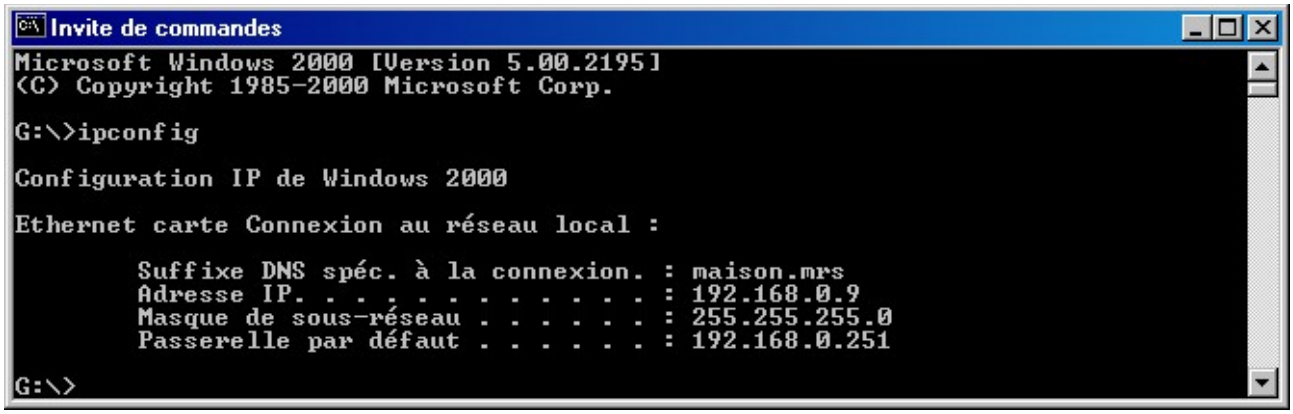
Windows NT4/2000/XP

La configuration

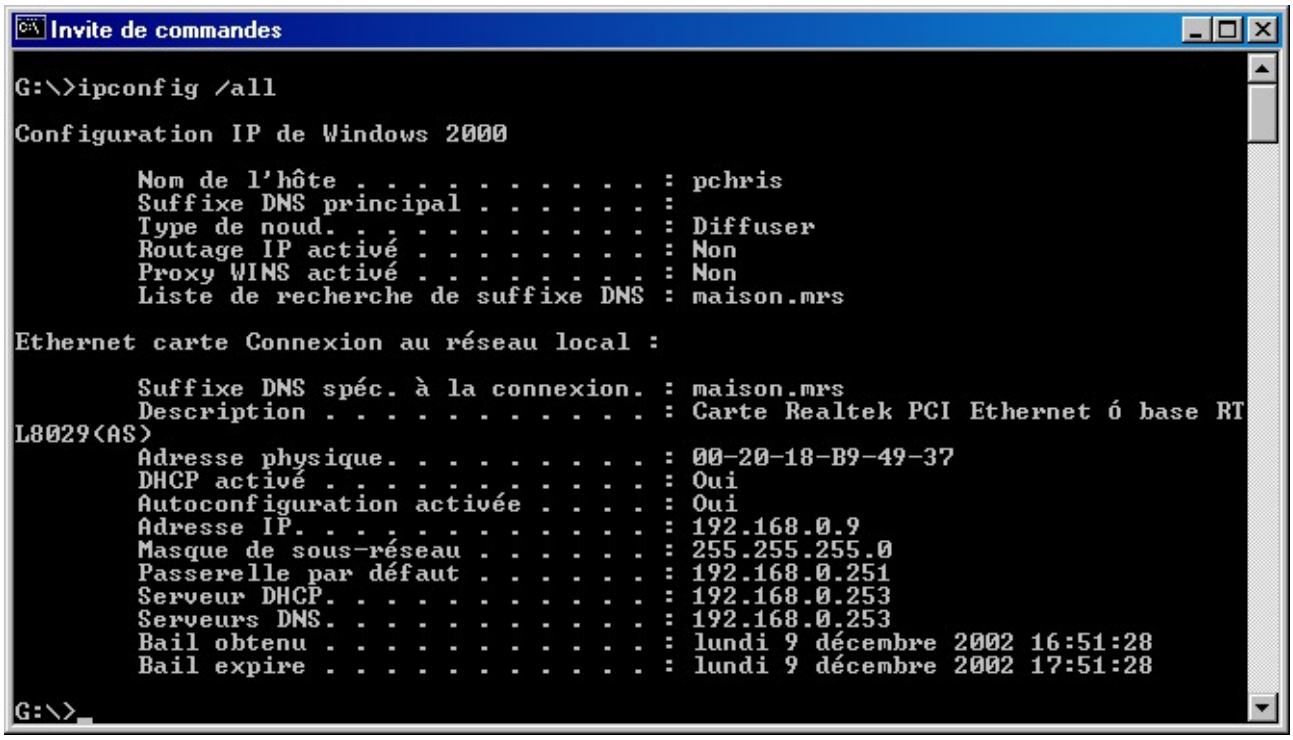
La configuration se fait dans le panneau de configuration, icône "réseau", onglet "protocoles", puis "propriétés" de TCP/IP. Là, vous avez indiqué que la carte doit recevoir une adresse IP dynamiquement.

Vérification

Tapez dans une console, la commande "ipconfig" :



Votre adresse doit être affichée. Si vous voulez tous les détails, utilisez la commande "ipconfig /all" :



La commande "ipconfig" permet également :

- De résilier le bail : "ipconfig /release"
- De renouveler le bail : "ipconfig /renew"

C'est cette commande qui est à utiliser pour essayer de récupérer une adresse IP lorsque vous avez des problèmes.

Notes

- Les rubriques "Bail obtenu" et "Expiration du bail" contiennent des valeurs calculées par votre machine. Le serveur DHCP ne donne que la durée.
- La commande en mode graphique "winipcfg" n'existe pas nativement sous Windows NT mais vous pouvez la récupérer dans le kit de ressources techniques (téléchargeable sur le site MS en cherchant bien :-).
  N'essayez pas d'utiliser celle de Windows 95/98, les dll winsock32 utilisées ici ne sont pas compatibles.

Linux

La configuration

Avec cet OS c'est beaucoup plus compliqué, parce qu'il y a beaucoup plus de configurations possibles.

La configuration utilisée dans l'exposé est la suivante :

- Un portable Compaq équipé d'une carte réseau D-LINK PCMCIA
  - MANDRAKE 8.2
  - Eth0 et configurée avec DHClient.

Notez que DHClient n'est pas le seul client possible. Vous pouvez parfaitement le remplacer par PUMP, DHCPXD ou par DHCPCD. Tous ces clients sont disponibles dans la distribution Mandrake, qui installe d'ailleurs DHCPCD par défaut, et non pas celui que j'utilise.

- DHCPCD semble avoir la préférence du distributeur. Je n'ai jamais rencontré de problèmes avec, mais je ne l'utilise normalement pas pour la raison suivante: Son paramétrage ne se fait que par la ligne de commande, ce qui oblige à aller modifier des scripts pas toujours faciles à trouver si l'on veut par exemple utiliser son propre DNS à la place de celui proposé dans le bail.
- PUMP Fonctionne également sans problèmes, il dispose d'un fichier de configuration /etc/pump.conf dans le quel on peut par exemple spécifier très simplement que l'on ne veut pas modifier le paramétrage du DNS avec l'information récupérée par DHCP. (Le ou les DNS sont inscrits dans le fichier /etc/resolv.conf).
- Je n'ai pas vraiment étudié DHCPXD qui fonctionne lui aussi sans difficultés. Il dispose d'un répertoire /etc/dhcpxd dans lequel vous trouverez quelques fichiers qui vous donneront toutes les indications sur le bail en cours.

- DHCLIENT a ma préférence. Il est écrit par ISC[5] (les auteurs de BIND le fameux DNS et DHCPD que nous utilisons ici, c'est dire qu'ils savent de quoi ils parlent :). Ce client cumule à mon sens tous les avantages :
  - Un fichier de configuration /etc/dhclient.conf, sans doute encore plus performant que celui de PUMP. Notez que ce fichier n'existe pas dans la distribution Mandrake, il vous faudra éventuellement le créer si vous ne voulez pas vous contenter du fonctionnement par défaut.
  - Des scripts optionnels exécutés automatiquement avant l'obtention du bail et après l'obtention du bail, avec à disposition des variables contenant toutes les informations recueillies par le client auprès du serveur. Très pratique par exemple pour vous envoyer par mail l'adresse courante de votre machine si celle-ci change; dans le cas par exemple où vous avez besoin de vous y connecter à distance par telnet ou ssh.
  - Il tient un historique des baux obtenus dans le fichier /var/lib/dhcp/dhclient.leases.

  Son seul inconvénient est sa richesse. Il n'est pas le plus facile à mettre en oeuvre.

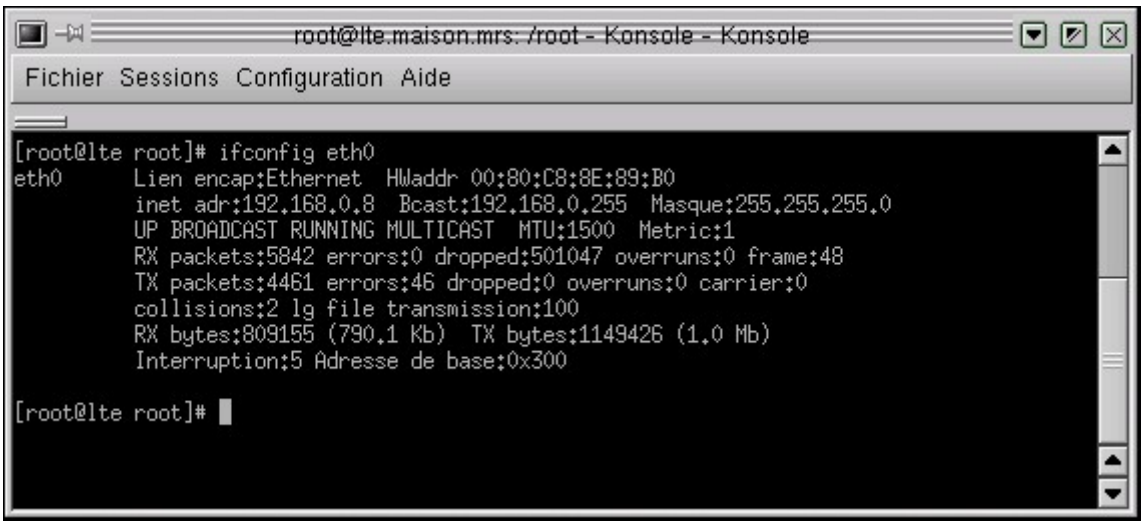
Vérifiez l'état de votre connexion

Dans /etc/sysconfig/network-scripts, il y a un fichier intitulé : ifcfg-eth0. Il doit contenir au moins ces lignes :

```
DEVICE="eth0"
BOOTPROTO="dhcp"
IPADDR=""
NETMASK=""
ONBOOT="yes"
```

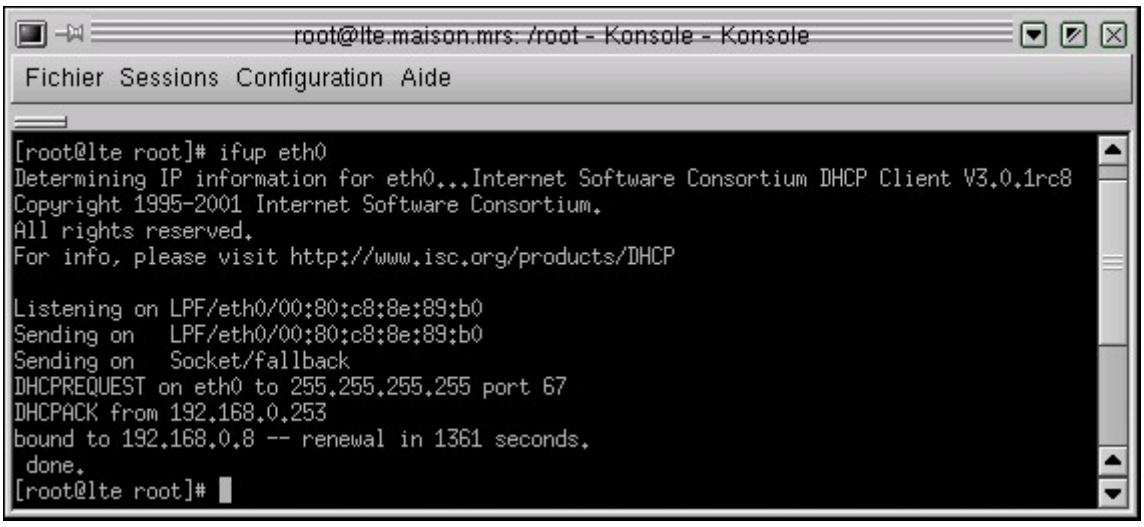
C'est assez parlant pour ne pas nécessiter d'explications particulières.

La commande "ifconfig eth0" devrait vous donner quelque chose comme ceci :



5 ISC : http://www.isc.org/

Si rien n'apparaît, c'est que votre interface n'est pas activée. Essayez alors ifup eth0 :



Cette commande affiche l'état de eth0, mais elle ne donne pas toutes les informations que l'on obtient sous Windows avec winipcfg ou ipconfig. Si vous voulez tout savoir, il faut aller dans le répertoire "/var/lib/dhcp" et regarder le fichier dhclient.leases. Celui-ci contient l'historique des dialogues DHCP :

```
lease {
  interface "eth0";
  fixed-address 192.168.0.8;
  option subnet-mask 255.255.255.0;
  option routers 192.168.0.253;
  option dhcp-lease-time 3600;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.0.253;
  option dhcp-server-identifier 192.168.0.253;
  option domain-name "maison.mrs";
  renew 2 2002/12/10 08:49:42;
  rebind 2 2002/12/10 09:14:05;
  expire 2 2002/12/10 09:21:35;}
```

Notez que ce fichier peut être beaucoup plus long. Cherchez dedans le dernier bail obtenu. Constatez que vous avez bien la trace de toutes les informations que notre serveur DHCP est capable d'envoyer à ses clients.

Particularités du client DHClient

Grâce aux informations conservées dans ce fichier dhclient.leases, ce client adopte un comportement un peu particulier, que l'on ne retrouve pas dans celui de Microsoft, par exemple.

Lorsqu'un hôte a obtenu un premier bail de la part du DHCP, l'adresse du serveur DHCP est conservée et, même après extinction et redémarrage de l'hôte au bout d'un temps bien supérieur à la durée de son bail, le client commencera par envoyer directement un DHCP request au serveur qu'il connaît. Cette particularité peut dérouter lorsque l'on espionne les dialogues DHCP sur le réseau.

Analyse de trames : savoir "Sniffer"

Un "sniffer" n'est pas un outil pour se "shooter", mais pour analyser les données qui se trimbalent sur le réseau. C'est un outil d'administrateur, qui est capable du meilleur comme du pire. Si vous voulez jouer avec, il en existe un tout à fait convenable et gratuit, aussi bien en version Linux que Windows, c'est Ethereal[6]. Il nécessite l'installation de la librairie libpcap, disponible elle aussi sous Linux comme sous Windows.

Nous allons juste ici analyser une capture de trames correspondant au dialogue DHCP, et constater que, lorsque ça va bien, ça se passe comme c'est dit dans les livres, ce qui est un peu réconfortant.

La manipulation est faite avec un client sous Windows XP.

En-têtes de trames

```
No. Time       Source          Destination       Protocol Info
  1 0.000000   0.0.0.0         255.255.255.255   DHCP     DHCP Discover - Transaction ID 0x6719436e
  2 0.001182   192.168.0.253   192.168.0.9       ICMP     Echo (ping) request
  3 0.342454   192.168.0.253   192.168.0.9       DHCP     DHCP Offer    - Transaction ID 0x6719436e
  4 0.344405   0.0.0.0         255.255.255.255   DHCP     DHCP Request  - Transaction ID 0x6719436e
  5 0.348264   192.168.0.253   192.168.0.9       DHCP     DHCP ACK      - Transaction ID 0x6719436e
  6 0.353014   CIS_b9:49:37    Broadcast         ARP      Who has 192.168.0.9?  Tell 192.168.0.9
  7 0.571241   CIS_b9:49:37    Broadcast         ARP      Who has 192.168.0.9?  Tell 192.168.0.9
  8 1.571441   CIS_b9:49:37    Broadcast         ARP      Who has 192.168.0.9?  Tell 192.168.0.9
  9 2.580537   192.168.0.9     192.168.0.255     NBNS     Registration NB PCHRIS<00>
 10 2.590265   192.168.0.9     192.168.0.255     NBNS     Registration NB PCHRIS<03>
```

1. Notre client se réveille, il n'a pas d'IP et utilise 0.0.0.0 pour faire un "broadcast général (255.255.255.255)". C'est le DHCP Discover.
2. Notre serveur DHCP, qui a l'intention d'offrir à ce client l'IP 192.168.0.9, fait un ping sur cette adresse, histoire de voir si elle est réellement disponible sur le réseau.
3. Comme il ne reçoit pas de réponse à son ping, il offre cette adresse au client.
4. Le client fait alors un DHCP Request
5. Le serveur accepte.
6. Le client fait un broadcast ARP pour vérifier de son côté que l'IP 192.168.0.9 n'est pas dupliquée sur le réseau.
7. idem
8. idem
9. Là, commence le verbiage propre aux réseaux Microsoft...

Note à propos du ping

Ce ping fait "perdre" une seconde au processus d'attribution d'un bail. En effet, le serveur attend pendant une seconde une éventuelle réponse. Si vous êtes absolument sûr de votre réseau, vous pouvez désactiver ce ping dans le fichier de configuration de DHCPd, mais je ne vous le conseille pas.

6 Ethereal : http://www.ethereal.com/

Détail des trames

Ce qui suit représente l'interprétation exhaustive des trames par le "sniffer". Il est évident qu'en lecture directe sur le réseau, on ne verrait qu'une suite d'octets difficilement interprétable par l'esprit humain.

La lecture en est certes un peu fastidieuse, mais elle est riche d'enseignements... Les points les plus importants sont marqués en gras.

Le DHCP Discover

```
Frame 1 (342 bytes on wire, 342 bytes captured)
    Arrival Time: Dec 10, 2002 10:10:04.658425000
    Time delta from previous packet: 0.000000000 seconds
    Time relative to first packet: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 342 bytes
    Capture Length: 342 bytes
Ethernet II, Src: 00:20:18:b9:49:37, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (Broadcast)
    *** La destination est inconnue, c'est un Broadcast ARP. On cherche un serveur DHCP
    Source: 00:20:18:b9:49:37 (CIS_b9:49:37)
    *** La source, elle, est connue, c'est l'adresse MAC de la machine cliente.
    Type: IP (0x0800)
Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 328
    Identification: 0x4b10
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0xee95 (correct)
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    *** Même chose niveau IP, mais sans adresse, bien entendu.
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
    Checksum: 0xf904 (correct)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6719436e
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client hardware address: 00:20:18:b9:49:37
    Server host name not given
    Boot file name not given
    *** Actuellement, le client ne dispose d'aucune configuration.
Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Discover
```

```
    Unknown Option Code: 251 (1 bytes)
    Option 61: Client identifier
        Hardware type: Ethernet
        Client hardware address: 00:20:18:b9:49:37
    Option 50: Requested IP Address = 192.168.0.9
    *** Mais comme il se souvient de l'IP qu'il avait autrefois,
    *** Il souhaiterait récupérer la même.
    Option 12: Host Name = "pchris"
    *** Il connaît aussi son nom d'hôte et le signale au serveur.
    *** Nous verrons (beaucoup) plus loin que ça peut être utile.
    Option 60: Vendor class identifier = "MSFT 5.0"
    Option 55: Parameter Request List
        1 = Subnet Mask
        15 = Domain Name
        3 = Router
        6 = Domain Name Server
        44 = NetBIOS over TCP/IP Name Server
        46 = NetBIOS over TCP/IP Node Type
        47 = NetBIOS over TCP/IP Scope
        31 = Perform Router Discover
        33 = Static Route
        43 = Vendor-Specific Information
    End Option
    *** La liste des option qui peuvent l'intéresser.
    *** le serveur peut en connaître bien plus...
    *** Notez que le client, d'origine Microsoft, demande pas mal d'informations
    *** sur NetBIOS. Nous ne les lui donnerons pas ici, mais ça peut être utile
    *** de le faire sur un gros réseau Microsoft.
    Padding
```

Un petit ping...

```
Frame 2 (62 bytes on wire, 62 bytes captured)
    Arrival Time: Dec 10, 2002 10:10:04.659607000
    Time delta from previous packet: 0.001182000 seconds
    Time relative to first packet: 0.001182000 seconds
    Frame Number: 2
    Packet Length: 62 bytes
    Capture Length: 62 bytes
Ethernet II, Src: 00:00:b4:bb:5d:ee, Dst: 00:20:18:b9:49:37
    Destination: 00:20:18:b9:49:37 (CIS_b9:49:37)
    Source: 00:00:b4:bb:5d:ee (Edimax_bb:5d:ee)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.253 (192.168.0.253), Dst Addr: 192.168.0.9 (192.168.0.9)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 48
    Identification: 0x0000
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0xb876 (correct)
    Source: 192.168.0.253 (192.168.0.253)
    Destination: 192.168.0.9 (192.168.0.9)
    *** Ping du serveur vers l'adresse 192.168.0.9 supposée disponible...
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xa7db (correct)
    Identifier: 0x5024
    Sequence number: 00:00
    Data (20 bytes)
```

```
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0010  00 00 00 00                                       ....
```

Pas de réponse au ping, on peut continuer tranquille...

Notez que ce ping est facultatif, il n'est pas demandé par la norme DHCP.

Offre d'un nouveau bail

```
Frame 3 (342 bytes on wire, 342 bytes captured)
    Arrival Time: Dec 10, 2002 10:10:05.000879000
    Time delta from previous packet: 0.341272000 seconds
    Time relative to first packet: 0.342454000 seconds
    Frame Number: 3
    Packet Length: 342 bytes
    Capture Length: 342 bytes
Ethernet II, Src: 00:00:b4:bb:5d:ee, Dst: 00:20:18:b9:49:37
    Destination: 00:20:18:b9:49:37 (CIS_b9:49:37)
    Source: 00:00:b4:bb:5d:ee (Edimax_bb:5d:ee)
    *** Le serveur ne répond pas ici en Broadcast Ethernet. C'est rendu possible
    *** par le fait que le client, lors du "Discover" a transmis son adresse MAC
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.253 (192.168.0.253), Dst Addr: 192.168.0.9 (192.168.0.9)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
        0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 328
    Identification: 0x0000
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 16
    Protocol: UDP (0x11)
    Header checksum: 0x273f (correct)
    Source: 192.168.0.253 (192.168.0.253)
    Destination: 192.168.0.9 (192.168.0.9)
    *** Notez que le serveur fait comme si le client disposait déjà de son adresse IP
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
    Length: 308
    Checksum: 0xb216 (correct)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6719436e
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.9 (192.168.0.9)
    *** Confirmation de l'IP du client.
    Next server IP address: 192.168.0.253 (192.168.0.253)
    *** IP du serveur DHCP qui répond
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    *** Il n'y a pas d'agent de relais DHCP
    Client hardware address: 00:20:18:b9:49:37
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Offer
    Option 54: Server Identifier = 192.168.0.253
    Option 51: IP Address Lease Time = 1 hour
```

```
    Option 1: Subnet Mask = 255.255.255.0
    Option 15: Domain Name = "maison.mrs"
    Option 3: Router = 192.168.0.253
    Option 6: Domain Name Server = 192.168.0.253
    End Option
    *** Voilà tout ce que le serveur DHCP peut indiquer au client
    Padding
```

Le serveur DHCP vient de proposer une configuration au client.

Demande du Bail de la part du client

Il faut aussi, maintenant que le client fasse une demande explicite pour ce bail. N'oublions pas qu'il pourrait y avoir plusieurs DHCP qui répondent, il faut donc qu'il y ait une confirmation au serveur choisi par le client.

```
Frame 4 (349 bytes on wire, 349 bytes captured)
    Arrival Time: Dec 10, 2002 10:10:05.002830000
    Time delta from previous packet: 0.001951000 seconds
    Time relative to first packet: 0.344405000 seconds
    Frame Number: 4
    Packet Length: 349 bytes
    Capture Length: 349 bytes
Ethernet II, Src: 00:20:18:b9:49:37, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (Broadcast)
    Source: 00:20:18:b9:49:37 (CIS_b9:49:37)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 335
    Identification: 0x4b12
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0xee8c (correct)
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 315
    Checksum: 0xe94b (correct)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6719436e
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client hardware address: 00:20:18:b9:49:37
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
```

```
    Option 61: Client identifier
        Hardware type: Ethernet
        Client hardware address: 00:20:18:b9:49:37
    Option 50: Requested IP Address = 192.168.0.9
    Option 54: Server Identifier = 192.168.0.253
    Option 12: Host Name = "pchris"
    ***
    *** Bien que très similaire à la trame DHCP Discover, notez la
    *** subtile différence, principalement sur l'option 54
    *** qui ne figurait pas dans le Discover, et pour cause.
    ***
    Option 81: Client Fully Qualified Domain Name (10 bytes)
    Option 60: Vendor class identifier = "MSFT 5.0"
    Option 55: Parameter Request List
        1 = Subnet Mask
        15 = Domain Name
        3 = Router
        6 = Domain Name Server
        44 = NetBIOS over TCP/IP Name Server
        46 = NetBIOS over TCP/IP Node Type
        47 = NetBIOS over TCP/IP Scope
        31 = Perform Router Discover
        33 = Static Route
        43 = Vendor-Specific Information
    End Option
```

C'est presque fini, il ne reste plus au serveur qu'à confirmer l'attribution de ce bail.

Le serveur est d'accord

```
Frame 5 (342 bytes on wire, 342 bytes captured)
    Arrival Time: Dec 10, 2002 10:10:05.006689000
    Time delta from previous packet: 0.003859000 seconds
    Time relative to first packet: 0.348264000 seconds
    Frame Number: 5
    Packet Length: 342 bytes
    Capture Length: 342 bytes
Ethernet II, Src: 00:00:b4:bb:5d:ee, Dst: 00:20:18:b9:49:37
    Destination: 00:20:18:b9:49:37 (CIS_b9:49:37)
    Source: 00:00:b4:bb:5d:ee (Edimax_bb:5d:ee)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.253 (192.168.0.253), Dst Addr: 192.168.0.9 (192.168.0.9)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00)
        0001 00.. = Differentiated Services Codepoint: Unknown (0x04)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 328
    Identification: 0x0000
    Flags: 0x00
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 16
    Protocol: UDP (0x11)
    Header checksum: 0x273f (correct)
    Source: 192.168.0.253 (192.168.0.253)
    Destination: 192.168.0.9 (192.168.0.9)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
    Length: 308
    Checksum: 0xaf16 (correct)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6719436e
```

```
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.9 (192.168.0.9)
    Next server IP address: 192.168.0.253 (192.168.0.253)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client hardware address: 00:20:18:b9:49:37
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 192.168.0.253
    Option 51: IP Address Lease Time = 1 hour
    Option 1: Subnet Mask = 255.255.255.0
    Option 15: Domain Name = "maison.mrs"
    Option 3: Router = 192.168.0.251
    Option 6: Domain Name Server = 192.168.0.253
    End Option
    Padding
```

Pas besoin de regarder de près ce qu'il se passe dans les broadcasts ARP que le client fait par la suite.

Notes supplémentaires

Que se serait-il passé, si l'adresse proposée par le serveur (ici 192.168.0.9) avait été déjà utilisée par un autre noeud du réseau ?

Je ne vous assommerai pas encore une fois avec un sniff, croyez-moi sur parole, j'ai fait la manip pour vérifier.

Dans ce cas, le serveur recevra un "echo reply" de la part du noeud utilisant cette IP et ne répondra pas au Discover. Le client, ne recevant pas de réponse, enverra un nouveau discover et le serveur lui proposera une autre IP.

Et si le client qui a pris l'IP 192.168.0.9 ne répond pas aux pings ?

Ce sera la catastrophe annoncée. Le bail sera alloué et il y aura une duplication de l'IP sur le réseau. Mais les broadcast ARP fait par le client qui a reçu l'IP dupliquée mettra à jour cette duplication et la configuration échouera.

Cette situation ne devrait pas se produire sur un réseau proprement configuré. Elle ne devrait apparaître que s'il y a un utilisateur malveillant sur le réseau, qui force une configuration statique quand il ne le faut pas et qui bloque volontairement les échos ICMP.

Pour ceux qui n'ont pas peur de se plonger dans les RFCs, vous trouverez celle qui traite du protocole DHCP ici (RFC 2131)[7].

Renouvellement d'un bail en cours de validité

Lorsque la durée du bail est inférieure à " l'uptime" du client, autrement dit, si votre client reste connecté plus longtemps que la durée de validité de son bail, il va devoir le renouveler.

7 RFC 2131 en français : http://abcdrfc.free.fr/rfc-vf/rfc2131.html

Pour visualiser cette procédure, nous faisons un petit test, en diminuant la durée de vie du bail à quatre minutes, et nous sniffons :

Quand ça se passe bien...

```
No. Time        Source          Destination     Protocol Info
  1 0.000000    0.0.0.0         255.255.255.255 DHCP     DHCP Discover - Transaction ID 0xe84b4f54
  2 0.001347    192.168.0.253   192.168.0.7     ICMP     Echo (ping) request
  3 0.837995    192.168.0.253   192.168.0.7     DHCP     DHCP Offer    - Transaction ID 0xe84b4f54
  4 0.839967    0.0.0.0         255.255.255.255 DHCP     DHCP Request  - Transaction ID 0xe84b4f54
  5 0.848485    192.168.0.253   192.168.0.7     DHCP     DHCP ACK      - Transaction ID 0xe84b4f54
...
 75 120.629525  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0xc1494f49
 76 120.632278  192.168.0.253   192.168.0.7     DHCP     DHCP ACK      - Transaction ID 0xc1494f49
```

Ca semble suffisamment parlant, au bout d'environ 120 secondes, soit 50% de la durée de vie du bail, le client essaye de le renouveler. Ca se passe bien, puisque le serveur répond toute de suite et ça repart pour 4 minutes. Inutile de regarder le détail des trames.

Et quand ça se passe mal

Nous allons faire la même chose, mais en simulant une panne de serveur DHCP :

```
No. Time        Source          Destination     Protocol Info
*** Premier bail, le serveur est en route, tout va bien...
  1 0.000000    0.0.0.0         255.255.255.255 DHCP     DHCP Discover - Transaction ID 0xe1fc342
  2 0.001302    192.168.0.253   192.168.0.7     DHCP     DHCP Offer    - Transaction ID 0xe1fc342
  3 0.003157    0.0.0.0         255.255.255.255 DHCP     DHCP Request  - Transaction ID 0xe1fc342
  4 0.006847    192.168.0.253   192.168.0.7     DHCP     DHCP ACK      - Transaction ID 0xe1fc342
...
*** Mi temps, tentative de renouvellement, mais le démon DHCP est stoppé
399 119.949192  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0xe220dc2e
*** Comme la machine est polie, elle prévient au moyen d'ICMP qu'il y a un problème
*** voyez qu'ICMP peut avoir du bon...
400 119.949376  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
401 123.951521  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0xe220dc2e
402 123.951733  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
...
*** Ca va durer comme ça un petit moment...
405 130.953962  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0xe220dc2e
406 130.954174  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
407 178.960775  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0x95759f13
408 178.960990  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
409 181.963368  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0x95759f13
410 181.963582  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
411 189.966027  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0x95759f13
412 189.966201  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
...
415 209.972090  192.168.0.7     192.168.0.253   DHCP     DHCP Request  - Transaction ID 0x8229871
416 209.972305  192.168.0.253   192.168.0.7     ICMP     Destination unreachable
*** Le client commence à s'affoler, il multiplie les requêtes...
417 213.975068  192.168.0.7     255.255.255.255 DHCP     DHCP Request  - Transaction ID 0x8229871
418 220.976509  192.168.0.7     255.255.255.255 DHCP     DHCP Request  - Transaction ID 0x8229871
419 235.983200  192.168.0.7     255.255.255.255 DHCP     DHCP Request  - Transaction ID 0x6851e126
420 240.984665  192.168.0.7     255.255.255.255 DHCP     DHCP Request  - Transaction ID 0x6851e126
421 248.986247  192.168.0.7     255.255.255.255 DHCP     DHCP Request  - Transaction ID 0x6851e126
*** Le client est désespéré, il cherche un nouveau serveur DHCP
422 265.041026  0.0.0.0         255.255.255.255 DHCP     DHCP Discover - Transaction ID 0xc7517868
423 269.041902  0.0.0.0         255.255.255.255 DHCP     DHCP Discover - Transaction ID 0xc7517868
*** Comme on n'est pas chien, on remet le démon en service...
424 278.042746  0.0.0.0         255.255.255.255 DHCP     DHCP Discover - Transaction ID 0xc7517868
425 278.044686  192.168.0.253   192.168.0.7     ICMP     Echo (ping) request
426 279.052019  192.168.0.253   192.168.0.7     DHCP     DHCP Offer    - Transaction ID 0xc7517868
427 279.053983  0.0.0.0         255.255.255.255 DHCP     DHCP Request  - Transaction ID 0xc7517868
428 279.058503  192.168.0.253   192.168.0.7     DHCP     DHCP ACK      - Transaction ID 0xc7517868
*** Et l'histoire finit bien.
```

Mais elle aurait pu mal finir, si ça avait été une bonne, vraie, grosse panne du serveur. En effet, une fois le bail expiré, le client perd bel et bien son IP et est éjecté de fait du réseau... Du temps où les câblés Wanadoo fonctionnaient sur ce système, ils n'ont pas manqué d'assister quelques fois à ce désolant spectacle.

Le luxe du luxe

Toujours plus...

Puisque l'on est dans le luxe, autant y aller carrément. Nous pouvons faire bien plus de choses encore.

Adresse IP fixe, via DHCP

DHCP est avant tout conçu pour configurer dynamiquement les stations, en exploitant au mieux une réserve d'adresses IP, distribuées aux clients du réseau.

Nous avons vu que le système s'arrangeait, autant que possible, pour attribuer toujours la même adresse à un hôte, mais ce n'est pas une obligation. Si la réserve d'IP est limitée, voire inférieure au nombre de clients du réseau, situation que l'on peut admettre si, par exemple, de nombreux portables peuvent venir se connecter, mais jamais tous en même temps, il est clair que l'attribution d'IP deviendra plus ou moins aléatoire.

Il peut être nécessaire pourtant que certains hôtes puissent être assurés d'avoir une IP immuable. DHCP peut gérer cette situation.

Pourquoi alors, passer par DHCP plutôt que de configurer la machine directement ? Il y a au moins deux bonnes raisons :

- Vous pouvez le faire de façon centralisée, sans avoir à vous déplacer de poste en poste,
- toutes les options : DNS, passerelle etc. restent configurées dynamiquement, ce qui vous évitera d'avoir à intervenir sur les machines si vous changez la topologie de votre réseau.

Comment faire ?

Il faut déjà connaître l'adresse MAC de la machine à qui l'on souhaite attribuer une IP fixe, ainsi que son nom.

Par exemple, ma machine s'appelle pchris, dispose de l'adresse MAC 00:20:18:B9:49:37, et je veux lui attribuer l'adresse 192.168.0.10.

Il suffira d'ajouter à la fin du fichier /etc/dhcpd.conf le paragraphe suivant :

```
host pchris
    {
    hardware ethernet 00:20:18:B9:49:37 ;
    fixed-address 192.168.0.10 ;
    }
```

Attention aux accolades et aux point-virgules.

Bien entendu, il faudra choisir des adresses IP en dehors de la plage d'adresses que DHCP peut fournir dynamiquement. (de 192.168.0.1 à 192.168.0.9 dans notre exemple).

Mise à jour dynamique du DNS

Microsoft, depuis Windows 2000 "server edition" et supérieures, a mis en place un système d'identification des stations du réseau par DNS, délaissant son antique système WINS. Nous pouvons très simplement, avec un contrôleur de domaine Windows 2000 installer un serveur DNS et un serveur DHCP. Les stations du domaine qui reçoivent une configuration dynamique via DHCP sont également enregistrées automatiquement sur le DNS.

La solution est élégante et efficace, mais onéreuse. Nous allons voir que nous pouvons faire la même chose avec Linux, Bind et DHCPd, mais de façon infiniment mois onéreuse, puisque c'est gratuit. Notez tout de même que la solution, si elle fonctionne, ne semble pas être entièrement stabilisée. A mon sens, le problème du DNS mis à jour dynamiquement ne sera définitivement et proprement résolu que lorsque DNS et DHCP seront deux services fournis par le même soft, et qu'ils utiliseront pour ce faire une vraie base de données commune.

Dans l'état actuel des choses, si vous souhaitez mettre en production une telle solution sur un réseau sur lequel il faut compter, je vous conseille la plus extrême prudence et un maquettage rigoureux de la solution finale sur un réseau expérimental. En effet, les surprises peuvent être nombreuses, et pas toujours bonnes.

Là encore, pourquoi faire ?

Si votre réseau est un petit réseau constitué de quelques machines toutes sous WIndows, ça ne présentera pas grand intérêt.

En revanche, c'est un moyen extrêmement élégant de retrouver simplement l'IP d'une machine de votre réseau, même si elle est attribuée dynamiquement, rien qu'en connaissant son nom d'hôte. Et puis, ça ne coûte rien et ça fait passer le temps...

Quelques mots sur le principe

Attention, cette méthode est expérimentée avec DHCPd 3.0 et BIND 9.2

Il y a en réalité, deux moyens de le faire. Soit c'est le client qui va s'annoncer au DNS, une fois qu'il aura récupéré son bail, ça présente deux inconvénients :

- Tous les clients DHCP ne savent pas le faire,
- ça oblige à ce que tous les hôtes du réseau soient autorisés à effectuer des modifications sur le DNS, ce qui est loin d'être une solution sûre.

Soit, c'est le DHCP qui sera chargé d'effectuer les mises à jour sur DNS, à chaque attribution d'un bail. C'est bien plus sûr, on est certain que ça fonctionnera avec tous les clients, ça augmente juste un peu la charge du serveur. Nous allons choisir cette seconde solution.

Cette méthode, qui est bien entendu très intéressante lorsque l'adressage est dynamique, c'est à dire que l'IP d'un hôte est susceptible de changer dans le temps, l'est moins si l'on a choisi d'attribuer une IP fixe à un ou plusieurs hôtes. D'ailleurs, par défaut, la mise à jour du DNS ne s'effectuera pas dans ces cas. Il y a cependant une clause qui permet de forcer cette mise à jour et nous allons l'utiliser.

Du côté de BIND

Il faut lui indiquer que les zones de notre domaine peuvent être mise à jour par le serveur DHCP. Il

existe une méthode sécurisée consistant à utiliser des clés MD5 pour l'authentification, nous ne l'utiliserons pas ici, mais suivant le cas de figure, ça peut être très vivement conseillé.

Nous allons juste signaler l'adresse IP nécessaire : 127.0.0.1, puisque les deux services tournent sur la même machine.

Nous allons modifier le fichier /etc/named.conf comme suit :

```
...

# La zone directe du domaine
zone "maison.mrs" {
        type master;
        file "/var/named/maison.mrs.hosts";
        allow-update {
                127.0.0.1;
                };
        };

# La zone de recherche inverse
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/var/named/0.168.192.in-addr.arpa.rev";
        allow-update {
                127.0.0.1;
                };
        ...
        }
```

Si certaines de vos machines avaient une configuration fixe et étaient référencées dans votre DNS, détruisez leurs enregistrements aussi bien dans la zone directe que dans la zone inverse, sinon, la mise à jour dynamique échouera pour ces noms d'hôtes.

Côté Bind, c'est tout ce qu'il y a à faire, dans notre cas. Il ne faut ,bien entendu, pas oublier de redémarrer le service.

Du côté de DHCPd

Là, il y a plus de travail. Il faut modifier le fichier /etc/dhcpd.conf de la manière suivante :

```
# méthode de mise à jour du DNS :
ddns-update-style interim;

# mise à jour autorisée
ddns-update on;

# ici, on force la mise à jour par le serveur DHCP
ignore client-updates;

# on force également la mise à jour des IP fixes
update-static-leases on;
```

Bien que ça puisse parfois fonctionner sans, il vaut tout de même mieux prendre la précaution d'ajouter en fin de fichier, ceci afin de définir clairement quel DNS doit être mis à jour pour ces zones :

```
zone maison.mrs. {
    primary 127.0.0.1;
    }

zone 0.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    }
```

A aménager, bien entendu, en fonction de votre propre configuration. Faites bien attention à la syntaxe. N'oubliez aucun point dans les noms des zones, refermez les accolades et finissez vos directives par un point-virgule.

Relancez le service DHCPd, ça devrait maintenant fonctionner.

Mise en garde

La mise à jour dynamique de DNS nécessite de connaître le nom de l'hôte qui vient de récupérer un bail, surtout si vous voulez conserver une cohérence entre les noms d'hôtes attribués localement et les noms DNS.

Il faut savoir que si le client DHCP de Windows envoie le nom d'hôte lors de la requête DHCP, les clients Linux comme dhcp client et même dhcpcd ne le font pas par défaut. Si vous n'y prenez garde, vos machines recevront bien leur bail, mais la mise à jour DNS ne s'effectuera pas.

Avec dhcp client, il faut créer un fichier /etc/dhclient.conf qui contiendra au moins la ligne :

```
send host-name "lenomdelamachine" ;
```

Consultez la doc de dhcp client pour savoir tout ce que l'on peut configurer par l'entremise de ce fichier.

Vérifications

Dans /var/named, à la première attribution d'un nouveau bail, vous devez voir apparaître deux nouveaux fichiers de zone, avec le même nom que les zones de votre domaine, mais avec un suffixe .jnl. Ces fichiers constituent la preuve que ça fonctionne, ce sont des journaux. N'essayez pas de les lire, ils sont en mode binaire. Beaucoup plus tard, vous pourrez constater que les fichiers de zone ont eux aussi été modifiés. De nouveaux enregistrements A sont apparus, suivis d'un enregistrement TXT. Ne modifiez plus ces enregistrements, surtout, n'enlevez pas l'enregistrement TXT, il permet d'indiquer si le champ précédent est issu d'une mise à jour dynamique ou non, et son utilité est primordiale pour les mises à jour futures.

Les outils classiques, host sous Linux, nslookup sous Windows 2000/XP vous permettront de vérifier les réponses de votre DNS.

Remarques diverses

Il faudrait étudier avec soin toute la documentation de bind et de dhcpd pour maîtriser parfaitement le mécanisme de mise à jour dynamique, j'avoue ne pas encore avoir eu le courage de le faire.

Vous risquez des ennuis si vous faites une mise à jour de la partie statique de votre zone. Après redémarrage de bind, il se peut que la zone ne fonctionne plus. Observez le journal /var/log/messages, vous aurez probablement une alerte vous indiquant que les journaux ne sont plus exploitables. Dans ce cas, détruisez les fichiers jnl et relancez named. Bien entendu, vous aurez sans doute perdu quelques mises à jour dynamiques, mais ça devrait rentrer dans l'ordre lorsque les baux seront renouvelés.

Du "failover" avec DHCP

L'un des problèmes majeur de DHCP, c'est qu'il n'est normalement pas possible de faire de la

tolérance de pannes. Tout au plus pouvons nous mettre deux DHCP sur le même réseau, mais distribuant des adresses dans des réserves disjointes, ce qui n'est guère commode.

Sachez que la version 3.0 permet de créer un système redondant, en créant deux serveurs qui utiliseront une réserve d'adresse commune. Je vous laisse jouer avec, pour ma part, ce sera peut-être pour plus tard.

Ma configuration actuelle pour DHCPd

Pour finir, à titre d'exemple, voici mon fichier de configuration. Mon réseau local dispose de cinq clients "habitués", auxquels j'attribue des IP fixes. Une plage dynamique est prévue pour les "invités".

```
# Les directives de configuration
ddns-update-style interim;
ddns-updates on;
ignore client-updates;
update-static-leases on;
ddns-domainname "maison.mrs";
max-lease-time 3600;
default-lease-time 3600;

# Les options globales
option domain-name-servers 192.168.0.253;
option subnet-mask 255.255.255.0;
option routers 192.168.0.253;


# Un seul sous réseau...
subnet 192.168.0.0 netmask 255.255.255.0 {

#       Adresses dynamiques pour les invités
        range 192.168.0.64 192.168.0.127;

#       Et les clients habituels, en IP fixe.
        host pchris {
                hardware ethernet 12:05:4D:47:F8:C9;
                fixed-address 192.168.0.100;
                }
        host pdaniel {
                hardware ethernet 05:20:18:2f:a7:5e;
                fixed-address 192.168.0.101;
                }
        host pdaniel2 {
                hardware ethernet 05:20:18:2a:fE:50;
                fixed-address 192.168.0.102;
                }
        host premi {
                hardware ethernet 05:20:18:2b:fE:5B;
                fixed-address 192.168.0.103;
                }
        host pmichele {
                hardware ethernet 52:54:C5:1C:2D:03;
                fixed-address 192.168.0.104;
                }
        }

# Pour la mise à jour dynamique du DNS local
allow unknown-clients;
zone maison.mrs. {
        primary 127.0.0.1;
        }
zone 0.168.192.in-addr.arpa. {
        primary 127.0.0.1;
        }
```