

D.H.C.P. (Dynamic Host Control Protocol)

1 - D.H.C.P. (Dynamic Host Control Protocol)

2 - Protocole DHCP

2.1 - Problème

2.2 - Théorie

2.3 - Détails sur le serveur DHCP

2.3.1 - Plages d'adresses IP

2.3.2 - Détails sur le bail

2.3.3 - Réseaux multiples

3 - Serveur DHCP

3.1 - Topologie du réseau

3.2 - Installation du serveur DHCP

3.2.1 - Principe de configuration du serveur

3.2.2 - Une configuration basique

4 - Les clients DHCP

4.1 - Configuration des clients DHCP

4.2 - Contrôle et maintenance

4.2.1 - Configuration Windows 95/98

4.2.2 - Configuration Windows NT4/2000/XP

4.2.3 - Configuration Linux

5 - Analyse de trames

5.1 - Capture

5.2 - Note à propos du ping

5.3 - Détail des trames

5.3.1 - Le DHCP Discover

5.3.2 - Le ping

5.3.3 - Offre d'un nouveau bail

5.3.4 - Demande du bail de la part du client

5.3.5 - Confirmation du serveur

5.3.6 - Notes supplémentaires

5.4 - Renouvellement d'un bail en cours de validité

6 - Possibilités supplémentaires du serveur DHCP

6.1 - Adresse IP fixe, via DHCP

6.2 - Mise à jour dynamique du DNS

1 - D.H.C.P. (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.

Plusieurs raisons peuvent conduire à mettre en oeuvre dhcp :

- Lorsqu'il y a des portables à connecter au réseau, typiquement chez soi et sur son lieu de travail et lorsqu'il y a des utilisateurs nomades comme des commerciaux ou des techniciens de maintenance qui sont amenés à se déplacer ;
- Pour organiser chez soi des "Lan parties" avec les machines de vos collègues ;
- Quand le réseau local contient plusieurs dizaines de machines ;
- Pour une meilleure surveillance du réseau et pour une gestion centralisée.

2 - Protocole DHCP

2.1 - Problème

Lorsque l'on souhaite connecter une machine à un réseau Ethernet TCP/IP, cette unité doit disposer pour fonctionner correctement :

- D'une adresse IP unique dans le réseau et appartenant au même réseau logique que toutes les autres machines du réseau en question ;
- D'un masque de sous-réseau, le même pour tous les hôtes du réseau ou du sous-réseau ;
- D'une adresse de DNS pour pouvoir résoudre les noms des hôtes, surtout si le réseau en question est relié au Net ;
- De l'adresse de la passerelle qui permet d'accéder au Net.

Pour configurer les hôtes locaux, il existe deux possibilités :

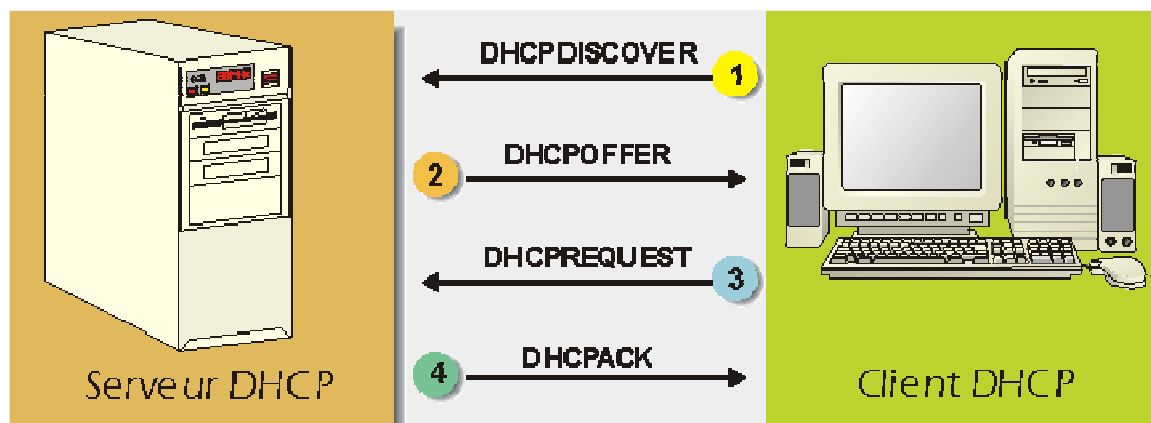
- En intervenant sur chaque machine et en configurant à chaque fois tous les paramètres de la pile IP à la main, en n'oubliant pas de tout référencer sur un support papier ou électronique ;
- En installant un serveur DHCP sur le réseau et en configurant les clients pour qu'ils aillent chercher toute leur configuration IP sur ce serveur.

2.2 - Théorie

La mise en oeuvre d'une solution dhcp est possible grâce à deux éléments fondamentaux :

- La "MAC Address" écrite "en dur" dans l'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 :



Etape 1 : Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau. Il envoie donc une trame "DHCPDISCOVER" destinée à trouver un serveur DHCP. Cette trame est un "broadcast", donc envoyée à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. comme adresse source. Comme ce n'est pas avec cette adresse que le DHCP va identifier le client, il fournit aussi sa "MAC Address".

Etape 2 : Le ou les serveurs DHCP du réseau qui vont recevoir cette trame DHCPDISCOVER vont répondre par un "DHCPOFFER". Cette trame, elle aussi en "broadcast" car il n'est pas encore possible d'atteindre le client nommément (il n'a pas encore d'adresse IP valide), 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 accepte en principe la première réponse venue.

Etape 3 : Le client répond alors par un DHCPREQUEST à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.

Etape 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.

2.3 - Détails sur le serveur DHCP

2.3.1 - Plages d'adresses IP

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 par qui ce qui explique que l'on récupère souvent la même adresse.

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.

2.3.2 - 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 sur lequel le serveur DHCP a installé la machine) ;
- L'adresse du serveur DHCP ;
- Les adresses des serveurs WINS.

Cette liste est loin d'être complète car il existe une grande quantité d'options qui peuvent être transmises.

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

Si, au bout des 7/8 de la durée de vie du bail en cours, ce dernier n'a pu être renouvelé, le client essaiera 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 serveur DHCP d'origine.

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, ...

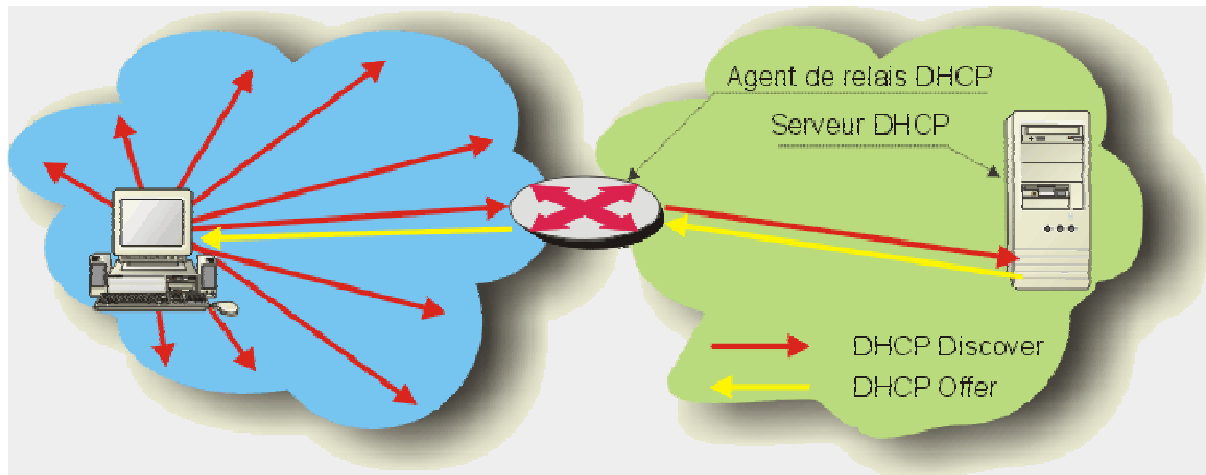
En règle générale, un FAI dispose toujours de moins d'adresses que d'abonnés, parce que tous les abonnés ne se connectent pas en même temps. Une mauvaise analyse des statistiques peut alors entraîner de graves problèmes aux heures de pointe.

2.3.3 - Réseaux multiples

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

Pas nécessairement car le 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.

Le problème de la négociation se pose car normalement, un "broadcast" n'est pas retransmis par les routeurs ! Les requêtes DHCP doivent donc pouvoir atteindre le serveur qui est situé sur un autre réseau logique et pour ce faire elles doivent donc passer les routeurs, ce qui n'est théoriquement pas possible. Il est alors nécessaire d'installer sur un ou plusieurs routeurs ou sur un ou plusieurs hôtes un agent de relais qui interceptera les requêtes en broadcast et les retransmettra à un serveur DHCP connu de cet agent.



L'agent de relais situé sur la passerelle va faire l'intermédiaire et le client réussira tout de même à obtenir une adresse, donnée par un DHCP situé sur un autre réseau, mais relayé par l'agent de relais. Le serveur DHCP est capable d'envoyer des paramètres différents, suivant le sous réseau du client auquel appartient le client.

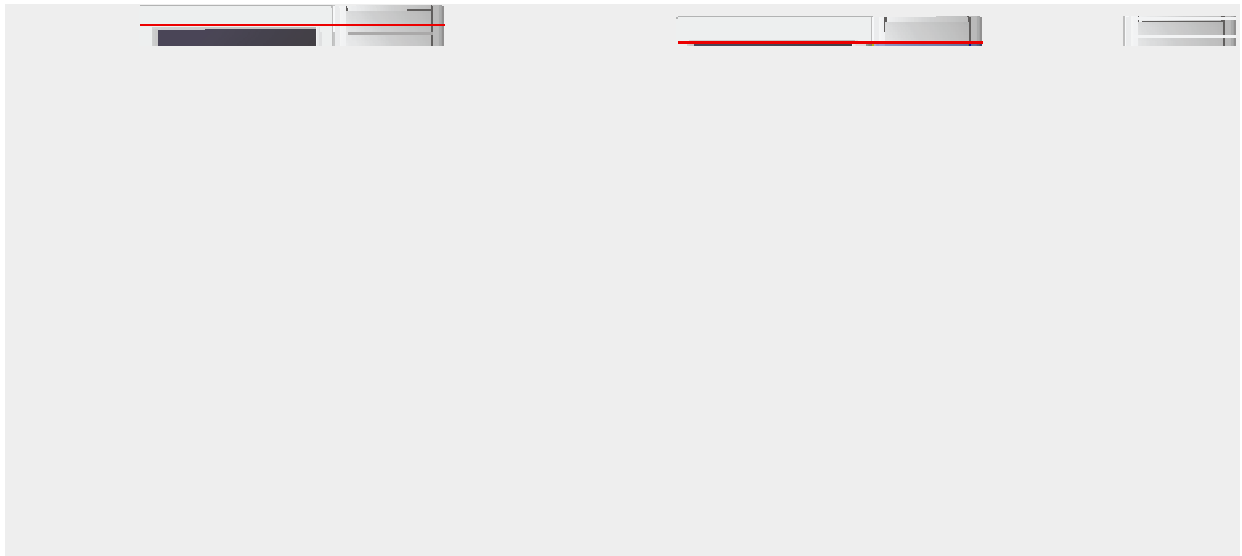
Le relayage utilisant un échange unicast sur IP, le serveur DHCP peut se situer n'importe où sur le réseau ou sur le Net.

.3 - Serveur DHCP

3.1 - Topologie du réseau

Soit le cas d'une configuration simple comportant une machine Linux qui cumulera plusieurs fonctions :

- Passerelle entre le réseau local et l'Internet ;
- Firewall ;
- Serveur DHCP ;
- Serveur DNS.



Un seul serveur DHCP peut 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, il existe une architecture hiérarchique permettant de définir des options globales, qui seront les mêmes pour tous les clients du DHCP (tous sous-réseaux confondus) et également des options propres à chaque sous-réseau, celles-ci écrasant les options globales, en cas de conflit.

Par ailleurs, le démon DHCPd peut créer des groupes distincts de machines dans un même sous-réseau et même gérer des clients de façon individuelle.

3.2.2 - Une configuration basique

Par exemple, pour la mise en place de :

- Un seul réseau, avec des IP choisies dans la classe C privée 192.168.0.0, donc avec un masque 255.255.255.0 ;
- Une passerelle par défaut unique pour tous les hôtes du réseau, par exemple 192.168.0.253 ;
- Un serveur DNS, également unique pour tous les hôtes du réseau et qui se trouve sur la même machine, à savoir 192.168.0.253.

Le "domaine" privé défini sur le réseau local de test s'appelle maison.mrs. Il n'a aucune réalité sur le Net et il n'est donc pas 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.

Il faut toujours garder quelques adresses disponibles pour les machines configurées manuellement, comme les serveurs que l'on place sur le réseau et qu'il n'est pas opportun de déplacer (en terme d'adressage).

Il faudra définir la durée de vie du bail que le serveur DHCP attribuera aux clients. L'un des avantages de DHCP 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 l'emploi du 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).

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 embarrassant s'agissant de réseaux connectés à l'extérieur car il peut s'agir d'un point de faiblesse en terme de sécurité. 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 démarre DHCPd.

Dans le cas d'une Mandrake, il faut éditer le script /etc/rc.d/init.d/dhcpd. Ce script est bien documenté et la variable INTERFACES qu'il faut initialiser avec le nom de la ou des interfaces qui doivent être écoutées est aisément identifiable.

Dans notre exemple, nous aurons :

```
INTERFACES="eth0"
```

Ce que comportera le fichier texte dhcpd.conf :

```
# Les trois lignes qui suivent doivent être présentes
# même si pour le moment, elles ne servent pas
# Elles concernent la mise à jour dynamique du DNS
# étudiée 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 fournir 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 simple suffit aux besoins d'un petit réseau local.
Dans ce fichier, certaines directives sont obligatoires :

- Les directives `ddns-xxx` serviront ultérieurement, 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 daemon `dhcpcd` puisse démarrer ;
- La directive `allow unknown-clients`. C'est en principe la configuration par défaut. Elle signifie 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 dhcpcd.conf`" indiquant quelle est cette différence.

Certaines options seront dans la pratique des paramètres de configuration optionnels comme :

- L'option `domain-name-servers` qui attribuera aux hôtes une adresse de DNS qui correspond à un serveur DNS local dans l'exemple fourni. S'il n'y a pas de serveur DNS local, il faudra indiquer l'IP du DNS du fournisseur d'accès. Il est éventuellement possible de spécifier plusieurs DNS ;
- L'option `domain-name` permettra aux clients de savoir dans quel domaine ils sont enregistrés ;
- L'option `routers` correspond à 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 et il n'y a ici aucune option d'étendue (de sous-réseau) définie.

Cette configuration doit permettre un fonctionnement dans un contexte de réseau simple.

Il faut lancer ou relancer le serveur :

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

4 - Les clients DHCP

4.1 - Configuration des clients DHCP

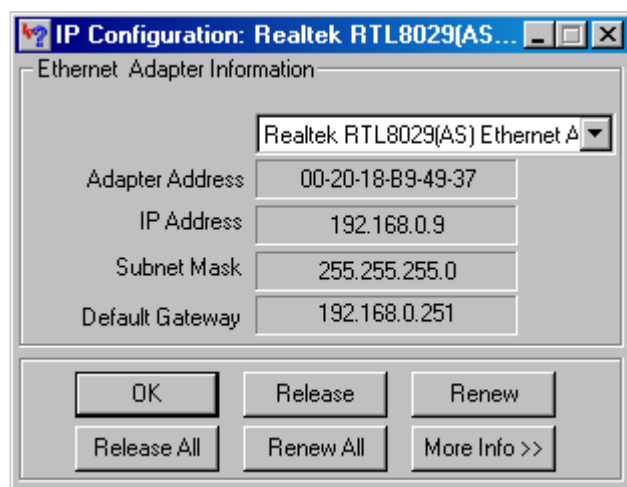
Dans le panneau de configuration TCP/IP sous Windows ou sous Linux il faut enlever tout ce qui concerne l'IP, le masque de sous réseau, le DNS et la passerelle et juste indiquer le choix d'une configuration dynamique (DHCP). Relancez les services réseaux, la méthode la plus simple étant le "reboot". Une fois le système redémarré, la configuration automatique a été effectuée.

4.2 - Contrôle et maintenance

Les outils pour contrôler l'état du client DHCP diffèrent suivant le système d'exploitation utilisé.

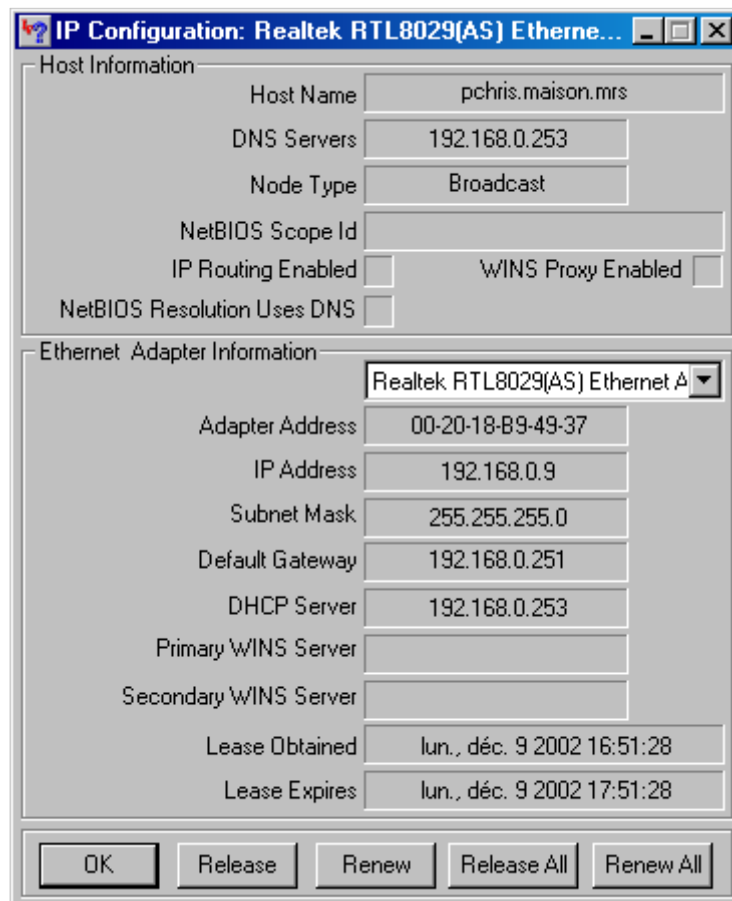
4.2.1 - Configuration Windows 95/98

Par le panneau de configuration, icône "réseau", cliquez sur TCP/IP puis choisir la carte réseau souhaitée. L'adresse IP doit être configurée dynamiquement, c'est d'ailleurs le choix par défaut à l'installation. La vérification peut être effectuée grâce à la commande "winipcfg" qui affiche les informations suivantes :



Windows 95 et 98 installent également le client PPP et il faut vérifier que la carte Ethernet est bien sélectionnée et pas le client PPP.

En cliquant sur le bouton "Plus d'info>>" on obtient :



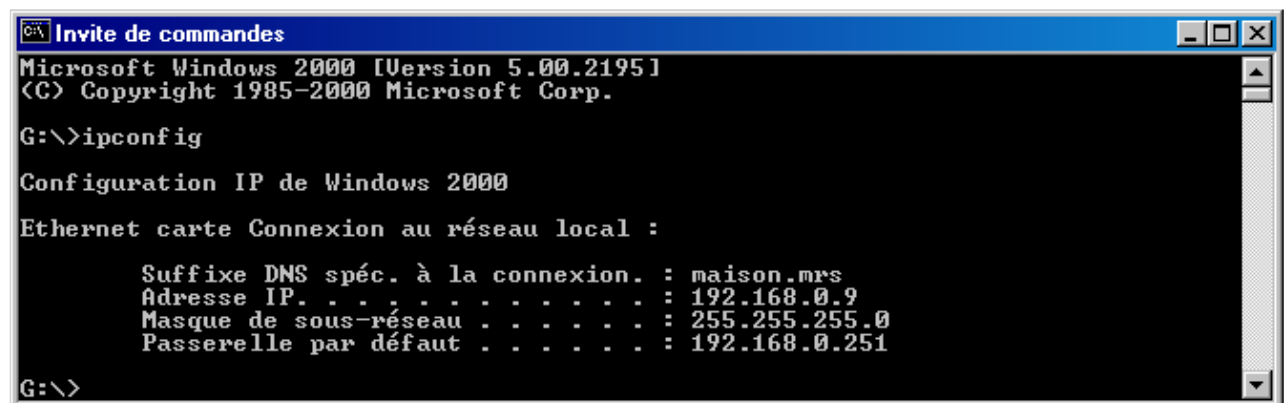
En cas de problème, le bouton "Renouveler" permettra d'effectuer une nouvelle requête auprès du serveur DHCP.

Notez que les rubriques "Bail obtenu" et "Expiration du bail" contiennent des valeurs calculées par le poste local, le serveur DHCP ne donnant que la durée du bail.

4.2.2 - Configuration Windows NT4/2000/XP

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

La vérification peut être effectuée en exécutant dans une fenêtre DOS, la commande "ipconfig" :



L'adresse IP doit être affichée et il est possible d'obtenir plus de détails en utilisant la commande "ipconfig /all" :

```
Invite de commandes

G:\>ipconfig /all

Configuration IP de Windows 2000

    Nom de l'hôte . . . . . : pchris
    Suffixe DNS principal . . . . . :
    Type de noud. . . . . : Diffuser
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche de suffixe DNS : maison.mrs

Ethernet carte Connexion au réseau local :

    Suffixe DNS spéc. à la connexion. : maison.mrs
    Description . . . . . : Carte Realtek PCI Ethernet ó base RT
L8029(AS)
    Adresse physique. . . . . : 00-20-18-B9-49-37
    DHCP activé . . . . . : Oui
    Autoconfiguration activée . . . . . : Oui
    Adresse IP. . . . . : 192.168.0.9
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 192.168.0.251
    Serveur DHCP. . . . . : 192.168.0.253
    Serveurs DNS. . . . . : 192.168.0.253
    Bail obtenu . . . . . : lundi 9 décembre 2002 16:51:28
    Bail expire . . . . . : lundi 9 décembre 2002 17:51:28

G:\>
```

La commande "ipconfig" permet également :

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

Il s'agit d'une commande utilisable pour essayer de récupérer une adresse IP lorsque le système connaît des problèmes.

Remarques :

- Les rubriques "Bail obtenu" et "Expiration du bail" contiennent des valeurs calculées par l'hôte local, le serveur DHCP ne donnant que la durée du bail ;
- La commande en mode graphique "winipcfg" n'existe pas nativement sous Windows NT mais il est possible de la récupérer dans le kit de ressources techniques (téléchargeable sur le site MS). Celle de Windows 95/98 n'est pas compatible à cause de la dll winsock32 qui est différente.

4.2.3 - Configuration Linux

Avec cet OS la configuration s'avère un peu plus compliquée car il y a beaucoup plus de possibilités. La configuration utilisée dans l'exemple est la suivante :

- Un portable Compaq équipé d'une carte réseau D-LINK PCMCIA ;
- Une MANDRAKE 8.2 ;
- Une carte Ethernet Eth0 et configurée avec DHClient. L'application DHClient n'est pas le seul client possible. Il est possible d'utiliser PUMP, DHCPXD ou par DHCPD. Tous ces clients sont disponibles dans la distribution Mandrake, qui installe d'ailleurs DHCPD par défaut.

DHCPD semble avoir la préférence du distributeur. Son paramétrage ne se fait qu'en lignes 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 lequel il est possible par exemple de spécifier très simplement que l'on ne souhaite pas modifier le paramétrage du DNS avec l'information récupérée par DHCP. Le ou les DNS sont inscrits dans le fichier `/etc/resolv.conf`.

DHCPXD fonctionne lui aussi sans difficultés. Il dispose d'un répertoire `/etc/dhcpd` dans lequel se trouvent quelques fichiers qui donnent toutes les indications sur le bail en cours.

DHCLIENT a été écrit par ISC (les auteurs de BIND correspondant au DNS et au DHCPD utilisé dans l'exemple). Ce client cumule les avantages suivants :

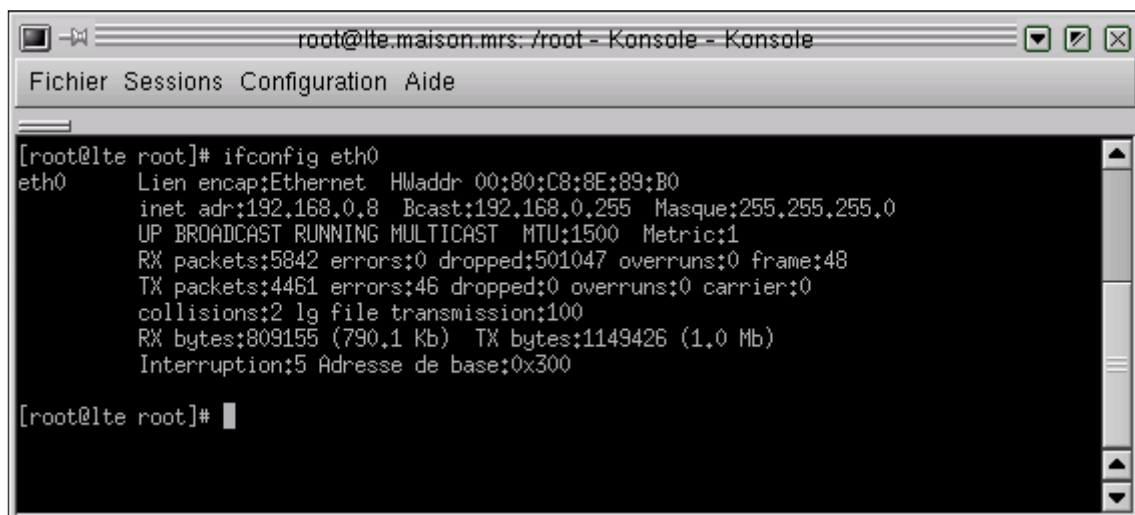
- Un fichier de configuration `/etc/dhclient.conf`, plus performant que celui de PUMP. Il faut noter que ce fichier n'existe pas dans la distribution Mandrake et il faudra éventuellement le créer si l'on souhaite aller au-delà du fonctionnement par défaut ;
- Des scripts optionnels exécutés automatiquement 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. Ceci est très pratique par exemple pour envoyer par mail l'adresse courante de la machine si celle-ci change. C'est utile lorsque l'on souhaite s'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 car il n'est pas le plus simple à mettre en oeuvre.

La vérification de l'état de la connexion peut être effectuée par l'intermédiaire d'un script. Dans `/etc/sysconfig/network-scripts`, il y a un fichier nommé `ifcfg-eth0`.

Il doit contenir au moins ces lignes :

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

La commande `"ifconfig eth0"` devrait fournir les indications suivantes :

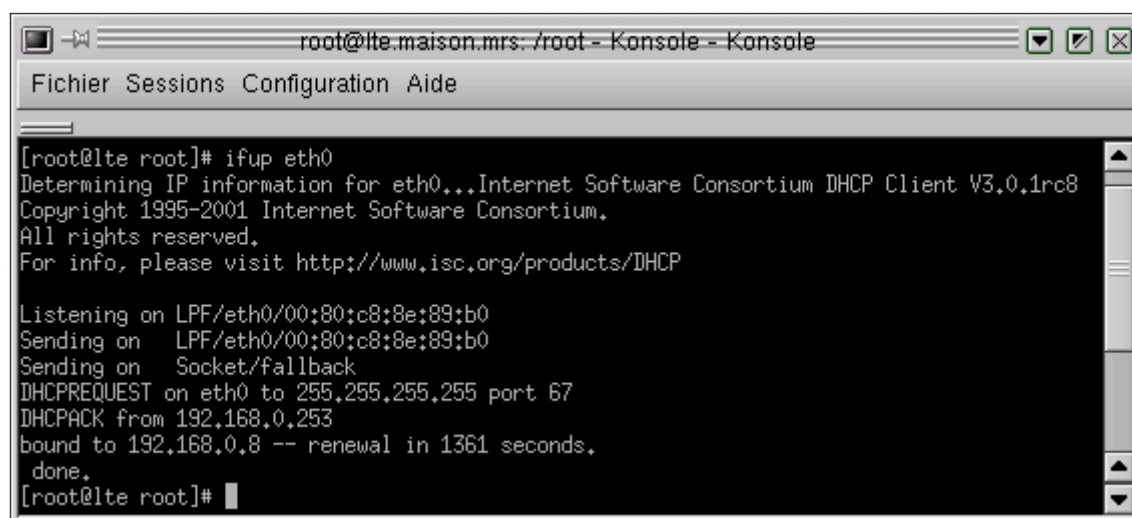


```
root@lfe.maison.mrs: /root - Konsole - Konsole
Fichier Sessions Configuration Aide

[root@lfe root]# ifconfig eth0
eth0      Lien encap:Ethernet  HWaddr 00:80:C8:8E:89:B0
          inet adr:192.168.0.8  Bcast:192.168.0.255  Masque:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5842 errors:0 dropped:501047 overruns:0 frame:48
          TX packets:4461 errors:46 dropped:0 overruns:0 carrier:0
          collisions:2 lg file transmission:100
          RX bytes:809155 (790.1 Kb)  TX bytes:1149426 (1.0 Mb)
          Interruption:5 Adresse de base:0x300

[root@lfe root]#
```

Si rien n'apparaît, c'est que l'interface n'est pas activée. Il faut alors effectuer `ifup eth0` :



```
root@lte.maison.mrs: /root - Konsole - Konsole
Fichier Sessions Configuration Aide

[root@lte root]# ifup eth0
Determining IP information for eth0...Internet Software Consortium DHCP Client V3.0.1rc8
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP

Listening on LPP/eth0/00:80:c8:8e:89:b0
Sending on LPP/eth0/00:80:c8:8e:89:b0
Sending on Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.253
bound to 192.168.0.8 -- renewal in 1361 seconds.
done.
[root@lte root]#
```

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. Pour obtenir plus d'informations il faut aller dans le répertoire `/var/lib/dhcp` et visualiser 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;}
```

Il faut noter que ce fichier peut être beaucoup plus long. En cherchant dans ce fichier le dernier bail obtenu, on constate qu'il y a bien la trace de toutes les informations que le serveur DHCP est capable d'envoyer à ses clients. Particularités du client DHCP.

Grâce aux informations conservées dans le fichier `dhclient.leases`, le client adopte un comportement particulier que l'on ne retrouve pas dans celui de Microsoft. Lorsqu'un hôte a obtenu un premier bail de la part du serveur 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.

5 - Analyse de trames

5.1 - Capture

L'analyse d'une capture de trames correspondant au dialogue DHCP lors d'une manipulation faite avec un client sous Windows XP donne ceci :

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>

Les étapes suivantes se déroulent :

- Le client qui démarre ne possède pas d'IP et utilise 0.0.0.0 pour faire un "broadcast général (255.255.255.255)". C'est le DHCP Discover ;
- Le serveur DHCP qui a l'intention d'offrir à ce client l'IP 192.168.0.9, fait un ping sur cette adresse afin de vérifier si elle est réellement disponible sur le réseau ;
- Comme il ne reçoit pas de réponse à son ping, il offre cette adresse au client ;
- Le client exécute alors un DHCP Request ;
- Le serveur accepte ;
- Le client exécute à trois reprises un broadcast ARP pour vérifier de son côté que l'IP 192.168.0.9 n'est pas dupliquée sur le réseau ;
- Ensuite commence le verbiage propre aux réseaux Microsoft.

5.2 - Note à propos du ping

Le ping initial exécuté par le serveur dhcp fait perdre une seconde au processus d'attribution d'un bail. En effet, le serveur attend pendant une seconde une éventuelle réponse. Si le réseau est absolument sûr, il est possible de désactiver le ping initial dans le fichier de configuration de DHCPd.

5.3 - Détail des trames

Ce qui suit représente l'interprétation exhaustive des trames par le "sniffer".

5.3.1 - 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

```

5.3.2 - Le 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 00
0010 00 00 00 00

```

Pas de réponse au ping !

5.3.3 - 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)
  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: 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.

5.3.4 - Demande du bail de la part du client

Il faut aussi 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

```

5.3.5 - Confirmation du serveur

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
 .. = 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

```

5.3.6 - Notes supplémentaires

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

Dans ce cas, le serveur recevra un "echo reply" de la part du nœud 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 adresse IP.

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

Ce sera problématique car le bail sera alloué et il y aura une duplication de l'adresse IP sur le réseau. Mais les broadcasts ARP exécutés 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 correctement 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.

La RFC qui traite du protocole DHCP est la RFC 2131.

5.4 - Renouvellement d'un bail en cours de validité

Lorsque la durée du bail est inférieure à l'uptime du client, autrement dit, si le client reste connecté plus longtemps que la durée de validité de son bail, celui-ci devra le renouveler.

Voici l'analyse d'un renouvellement de bail limité à 4 minutes :

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

Quand tout se passe bien, au bout d'environ 120 secondes, soit 50% de la durée de vie du bail, le client essaye de le renouveler. Le serveur répond tout de suite et le bail repart pour 4 minutes.

Il arrive qu'il y ait des problèmes lorsque, par exemple, il y a une panne du 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
*** 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
*** 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 vraie panne du serveur. En effet, une fois le bail expiré, le client perd son adresse IP et est éjecté du réseau.

6 - Possibilités supplémentaires du serveur DHCP

6.1 - 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. Le système s'arrange, 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'adresses IP deviendra plus ou moins aléatoire.

Il peut être nécessaire pourtant que certains hôtes puissent être assurés d'avoir une IP fixe. DHCP peut gérer cette situation. Pourquoi alors, passer par DHCP plutôt que de configurer la machine directement ? Il y a au moins deux raisons :

- Cette opération s'effectue de façon centralisée, sans avoir à se déplacer de poste en poste ;
- Toutes les options : DNS, passerelle, etc... restent configurées dynamiquement, ce qui évite d'avoir à intervenir sur les machines en cas de changement de la topologie du réseau.

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

Par exemple, la machine qui s'appelle pchris, dispose de l'adresse MAC 00:20:18:B9:49:37, et on souhaite lui attribuer l'adresse 192.168.0.10.

Il suffit 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 ;

}
```

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

6.2 - 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. Avec un contrôleur de domaine Windows 2000 il est aisé d'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. Il est possible de réaliser la même chose avec Linux, Bind et DHCPd, mais de façon infiniment moins onéreuse, puisque c'est gratuit. Il faut tout de même noter que la solution, si elle fonctionne, ne semble pas être entièrement stabilisée. 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.

Cette configuration constitue un moyen de retrouver simplement l'IP d'une machine du réseau même si elle est attribuée dynamiquement, rien qu'en connaissant son nom d'hôte.

Il y a deux moyens de réaliser cette opération :

- Soit le client s'annonce au DNS, une fois qu'il aura récupéré son bail. Cette méthode présente deux inconvénients à savoir que tous les clients DHCP ne savent pas le faire, et 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 le DHCP est chargé d'effectuer les mises à jour sur le serveur DNS, à chaque attribution d'un bail. Cette solution est plus sûre, et il est certain que ça fonctionnera avec tous les clients, en augmentant toutefois un peu la charge du serveur.

Cette seconde méthode est très intéressante lorsque l'adressage est dynamique, c'est à dire que l'IP d'un hôte est susceptible de changer dans le temps.

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 indiquer que les zones du domaine peuvent être mises à jour par le serveur DHCP. Il existe une méthode sécurisée consistant à utiliser des clés MD5 pour l'authentification.

Dans l'exemple précédent, il faut juste signaler l'adresse IP 127.0.0.1, puisque les deux services tournent sur la même machine.

Il faut 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 machines ont une configuration fixe et sont référencées dans le serveur DNS, il faut supprimer 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.

Il faut redémarrer le service bind.

Du côté de DHCPd 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;
}
```

Il faut relancer le service DHCPd.

La mise à jour dynamique de DNS nécessite de connaître le nom de l'hôte qui vient de récupérer un bail, surtout pour 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. Il se peut dans ce cas que les machines reçoivent bien leurs baux mais que la mise à jour DNS ne s'effectue pas.

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

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

Pour procéder aux vérifications dans /var/named, à la première attribution d'un nouveau bail, on doit voir apparaître deux nouveaux fichiers de zone, avec le même nom que les zones du domaine, mais avec un suffixe .jnl. Ces fichiers constituent la preuve que tout fonctionne car ce sont des journaux. Ils sont illisibles car en mode binaire. Plus tard, il sera possible de constater que les fichiers de zone ont eux aussi été modifiés. De nouveaux enregistrements RR de type A sont apparus, suivis d'un enregistrement TXT. L'enregistrement TXT 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 permettent de vérifier les réponses du DNS.

Remarques diverses.

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.

Cependant, la version 3.0 permet de créer un système redondant, en créant deux serveurs qui utilisent une réserve d'adresses commune.

Exemple de configuration pour DHCPd.

Le réseau local dispose de cinq clients "habituels", auxquels des IP fixes sont attribuées. 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;
}

```