DHCP

principe et mise en place

EBC Informatique

Centre de compétences UNIX

TABLE DES MATIERES

Notes préliminaires :

Tout en tentant de rester le plus général possible dans cette étude, je tiens à vous informer que la totalité des manipulations UNIX expliquées ont été effectuées sur un serveur fonctionnant sous distribution RedHAT 7.0.

Deux serveurs DHCP ont été testés. Le premier, livré avec la distribution RedHAT 7.0, est suffisant si l'on ne désire pas la prise en charge du DNS dynamique. Le second, téléchargeable sur le site de l'Internet Software Consortium, est obligatoire si l'on désire mettre en place le DNS dynamique. Sa version la plus récente au moment de l'écriture de ces lignes est DHCPd 3.0rc7. Les versions plus récentes ne devraient pas poser de problèmes particulier par rapport aux informations de cette étude.

Le serveur de noms (serveur DNS) utilisé est celui livré avec la distribution RedHAT 7.0. Sa version exacte est : BIND 8.2.2_P5. Les versions plus récentes, téléchargeables sur le site de l'Internet Software consortium http://isc.org/, ne devraient pas poser de problèmes particulier par rapport aux informations de cette étude.

Concernant les systèmes Windows, j'ai testé l'ensemble des configurations réseau décrites avec Microsoft Windows 98 et Microsoft Windows NT 4 (SP 6).

I] Brèves explications et théories sur le DHCP

DHCP (Dynamic Host Configuration Protocol) est un standard TCP/IP qui réduit la complexité et la charge administrative de la gestion des configurations IP des clients réseau. Le service DHCP est exécuté sur un serveur, et permet la gestion automatique et centralisée des adresses IP et des autres paramètres de configuration TCP/IP des ordinateur clients de votre réseau.

L'administrateur du réseau local installe un ou plusieurs serveurs DHCP chargés de gérer les informations de configuration TCP/IP et de fournir aux clients DHCP leurs configurations d'adresses, sous la forme de baux.

Ce processus de baux consiste en un échange de messages de la liste suivante :

Type de message	**Description**
DHCPDiscover (Message de découverte)	La première fois qu'un ordinateur client DHCP tente d'ouvrir une session sur le réseau, il demande des informations d'adresse IP à un serveur DHCP en diffusant un paquet DHCPDiscover. L'adresse IP source de ce paquet est 0.0.0.0 parce que le client n'a pas encore d'adresse IP.
DHCPOffer (Message d'offre)	Chacun des serveurs DHCP qui reçoivent le paquet DHCPDiscover du client répond par un paquet DHCPOffer qui contient une proposition d'adresse IP et des informations supplémentaires de configuration TCP/IP, en particulier le masque de sous-réseau et la passerelle par défaut. Il peut arrive que plusieurs serveurs DHCP répondent de cette manière. Le client accepte le premier paquet reçu.
DHCPRequest (Message de demande)	Lorsqu'un client DHCP reçoit un paquet DHCPOffer, il répond en diffusant un paquet qui contient l'adresse IP offerte et qui indique qu'il accepte cette adresse.
DHCPAck (Accusé de réception)	Le serveur DHCP sélectionné accuse réception du message DHCPRequest du client en envoyant un paquet DHCPAck. A ce stade, le serveur transmet également les paramètres de configuration optionnels. A la réception du paquet DHCPAck, le client peut s'intégrer au réseau TCP/IP et terminer son démarrage.
DHCPNak (Accusé de réception négatif)	Si l'adresse IP ne peut pas être utilisée par le client parce qu'elle n'est plus valide ou bien parce qu'elle est utilisée par un autre ordinateur, le serveur DHCP répond par un paquet DHCPNak ; le client doit alors recommencer le processus d'obtention de bail. Chaque fois qu'un serveur reçoit une demande pour une adresse IP invalide dans les étendues (plage d'adresses IP distribuables aux clients DHCP) pour lesquelles il est configuré, il envoie un message DHCPNak au client.
DHCPDecline (Message de refus)	Si le client DHCP constate que les paramètres de configuration proposés sont invalides, il envoie un paquet DHCPDecline au serveur ; il devra alors recommencer le processus d'obtention d'un bail.
DHCPRelease (Message de libération)	Un client DHCP envoie un paquet DHCPRelease au serveur pour libérer l'adresse IP et annuler le bail en cours.
DHCPInform (Message d'information)	Ce nouveau type de message, est employé par les ordinateurs du réseau pour demander à un serveur DHCP les informations nécessaires à leur configuration locale.

Comment fonctionne le processus des baux ?

La première fois que le client DHCP démarre et tente de se joindre au réseau, il passe automatiquement par un processus d'initialisation qui lui permet d'obtenir un bail auprès d'un serveur DHCP. Ce processus d'obtention de bail se déroule ainsi :

1. Le client DHCP émet une demande d'adresse IP en diffusant un message DHCPDiscover sur le sous-réseau local.
2. Une adresse est alors offerte au client sous la forme d'une réponse DHCPOffer envoyée par un serveur DHCP qui contient une adresse IP et des informations de configuration destinées à constituer un bail pour le client. Si le client ne reçoit aucune réponse, il peut réagir de deux manières différentes :
   - S'il s'agit d'un client Windows 2000 sur lequel l'autoconfiguration IP n'a pas été désactivée, il autoconfigure une adresse IP pour son interface.
   - Si le client n'est pas un client Windows 2000, ou si l'autoconfiguration IP a été désactivée, son initialisation sur le réseau échoue. Le client continue alors à envoyer des messages DHCPDiscover en arrière-plan (4 messages, toutes les 5 minutes) jusqu'à ce qu'il reçoive un message DHCPOffer provenant d'un serveur DHCP.
3. Le client indique qu'il accepte l'offre en sélectionnant l'adresse offerte et en répondant au serveur par un message DHCPRequest.
4. L'adresse est affectée au client, et le serveur DHCP envoie un message DHCPAck pour confirmer le bail. Ce message peut contenir d'autres options de configuration.
5. Une fois que le client a reçu l'accusé de réception, il configure ses paramètres TCP/IP en fonction des informations des options DHCP jointes aux réponses, et il s'intègre au réseau.

Il arrive (rarement) qu'un serveur DHCP retourne un accusé de réception négatif (DHCPNak) au client. Ceci se produit si un client demande une adresse invalide ou dupliquée. Si un client reçoit un tel accusé de réception négatif, il doit reprendre son processus d'obtention d'un bail à son début.

Redémarrage un client DHCP

Lorsqu'un client qui avait obtenu une adresse IP redémarre, il diffuse un message DHCPRequest plutôt qu'un message DHCPDiscover. Ce message a pour but de redemander l'adresse IP qui lui avait été précédemment allouée.
Si l'adresse demandée peut être utilisée par le client, le serveur DHCP répond par un message DHCPAck. Dans le cas contraire, par exemple si l'adresse est utilisée par un autre client du réseau, le serveur DHCP répond par un message DHCPNak. Dans ce dernier cas, le client doit reprendre le processus d'obtention de bail en totalité.

Renouvellement des baux

Un bail DHCP est défini dans une durée bien déterminée. Lorsque le bail d'un client arrive à expiration, ce dernier doit le renouveler en envoyant une requête de renouvellement au serveur (DHCPRequest). Ce dernier renvoie alors un message d'accusé de réception au client l'informant que son bail est bien renouvelé. Si le serveur DHCP n'est pas accessible, le client renouvelle entièrement son bail courant en recommençant le processus d'obtention de bail du début.

Comment choisir la durée des baux ?

La durée des baux doit être judicieusement choisie selon le comportement des clients sur le réseau sinon, les performances du serveur DHCP risque d'être affectées par une mauvaise configuration.

- Si vous disposez d'un grand nombre d'adresses IP disponibles et si les configurations de votre réseau changent rarement, augmenter la durée de bail pour réduire la fréquence des dialogues de renouvellement entre les clients et les serveurs DHCP. Cela permet de réduire le traffic du réseau.
- SI le nombre de vos adresses IP disponibles est limité et si les configurations des clients sont souvent modifiées, ou si les clients se déplacent souvent sur le réseau, réduisez la durée du bail. Cela permet un retour plus rapide des adresses non utilisées dans le pool d'adresses allouables.

Il n'y a pas de durée idéale, cette dernière est fonction de vos besoins. Une durée de bail d'une journée dans un premier temps paraît judicieux. A votre charge ensuite d'augmenter ou de réduire cette dernière selon le trafic et la dynamique du réseau.

Coopération de plusieurs serveurs DHCP

Pour que la défaillance d'un serveur ne puisse pas empêcher le démarrage des clients DHCP, il sera nécessaire de mettre en place un second serveur DHCP. Cependant, il s'agit d'être très vigilant dans ce cas de figure car il n'existe aucun mécanisme de discussion entre les serveur DHCP, il ne faudra donc jamais se trouver dans le cas de figure ou deux serveurs DHCP ont la possibilité de distribuer des adresses IP d'une étendue commune, il s'ensuivrait des conséquences désastreuse pour le bon fonctionnement du réseau.

La stratégie recommandée par Microsoft dans son système serveur Windows 2000 et l'application de la règle des 80/20. Cette règle est très simple : il s'agit de partager la plage d'adresses IP distribuables en deux parties inégales. Un premier serveur DHCP s'occupera de 80% de cette étendue d'IP distribuables. Ce serveur devra être le plus performant possible, le mieux accessible. Un second serveur DHCP s'occupera des 20% restant. Celui-ci, par contre, devra avoir un temps de réponse inférieur au premier serveur, il devra aussi être situé dans un « recoin » du réseau afin, qu'en priorité, la plupart des machines demandant une adresse IP la reçoivent du premier serveur. Si ce serveur plante, les clients recevront alors la réponse du second serveur qui s'occupera alors de l'affectation des adresses IP jusqu'à ce que le premier soit remis en service.

II] Installation du serveur DHCP

1) Supprimer éventuellement une version existante

Supprimer une version existante du serveur DHCP n'est pas nécessaire, cette action permet seulement de conserver la propreté de son système.

a) Comment savoir si une version est déjà installée ?

Tapez la commande suivante :

```
[root@redhat /etc]# find / -name dhcpd -print
```

Cette commande affiche les différents chemins dans l'arborescence du disque où l'on peut trouver le fichier « dhcpd » qui est l'exécutable du serveur DHCP.

Si vous obtenez comme réponse que le fichier se situe dans un répertoire tel que /bin/, /sbin/, /usr/bin ou encore /usr/sbin/, c'est qu'un serveur DHCP est installé. Il se peut bien sûr que le serveur soit installé dans un autre répertoire d'exécutable si votre système est configuré différemment des standards.

b) Connaître la version du serveur DHCP

Une astuce consiste à afficher l'aide du serveur :

```
[root@redhat /etc]# /usr/sbin/dhcpd --help
Internet Software Consortium DHCP Server V3.0rc7
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
Usage: dhcpd [-p <UDP port #>] [-d] [-f]
             [-cf config-file] [-lf lease-file]
                   [-tf trace-output-file]
                   [-play trace-input-file]
             [-t] [-T] [-s server] [if0 [...ifN]]

If you did not get this software from ftp.isc.org, please
get the latest from ftp.isc.org and install that before
requesting help.

If you did get this software from ftp.isc.org and have not
yet read the README, please read it before requesting help.
If you intend to request help from the dhcp-server@isc.org
mailing list, please read the section on the README about
submitting bug reports and requests for help.

Please do not under any circumstances send requests for
help directly to the authors of this software - please
send them to the appropriate mailing list as described in
the README file.

exiting.
```

Un résultat similaire peut être obtenu en démarrant le serveur DHCP en mode « debug » :

```
[root@redhat /etc]# /usr/sbin/dhcpd -f -d
```

Si un serveur fonctionne déjà en arrière-plan, il devrait se produire une erreur, mais l'information voulu devrait s'afficher quand même.

c) Désinstaller la version existante

Hélas, cette étape dépend de votre distribution et de sa configuration.

Sur la RedHAT 7, pour supprimer le serveur installé par le programme d'installation, il suffit de démarrer l'application graphique « GnomeRPM » ou « GnoRPM », d'effectuer une recherche sur tout les packages contenant « dhcp » dans leurs noms et d'effacer les packages de liste ainsi obtenue. Le programme vous indiquera les éventuelles dépendances existantes et vous proposera de les supprimer elles aussi.

2) Installer un serveur DHCP

a) Télécharger les sources

Le sources sont téléchargeables sur le site de l'Internet Software Consortium : http://www.isc.org/. Il faut rechercher dans la section DHCP où télécharger la dernière version pour finalement la télécharger (normalement, c'est un fichier nommé « dhcpd-latest.tar.gz »). Pour ma part, j'utilise la version 3.0rc7.

b) Installer le logiciel

L'installation du logiciel est une installation type UNIX de base. Il s'agit d'abord de copier l'archive dans le répertoire /usr/local/ (ou tout autre répertoire de votre choix, mais dans mon cas, c'est dans celui-ci), puis de la décompresser à l'aide des commandes suivantes :

```
[root@redhat local]# gunzip dhcpd-latest.tar.gz
[root@redhat local]# tar xvf dhcpd-latest.tar
```

Il nous faut ensuite créer le fichier makefile grâce à la commande suivante :

```
[root@redhat local]# ./configure
```

Pour finalement compiler et installer le programme :

```
[root@redhat local]# make install
[root@redhat local]# make
```

Durant l'installation, les éventuelles erreurs qui surviendront seront affichées à l'écran. Une seule erreur est presque assurée : le programme d'installation va vous demander de créer le fichier « dhcpd.leases » dans le répertoire qu'il indiquera. Pour ce faire, utilisez la commande « touch » :

```
[root@redhat /]# touch /var/state/dhcp/dhcpd.leases
```

c) Restaurer ses fichiers de configuration

Si vous avez précédemment sauvegardé vos fichiers de configuration DHCP, vous pouvez les restaurez en déplaçant le fichier « dhcpd.leases » dans le répertoire que le programme vous a indiqué précédemment ainsi qu'en déplacant le fichier « dhcpd.conf » dans /etc/.

d) Tester son installation

Si votre fichier « dhcpd.conf » restauré n'est pas ou plus viable, il vous faudra attendre le prochain chapitre. Mais si ce dernier est compatible, vous pouvez tester votre installation en procédant comme indiqué dans cette partie.

Veuillez démarrez le serveur DHCP en mode « debug » avec une commande semblable à celle-ci :

```
[root@redhat /etc]# /usr/sbin/dhcpd eth0 -f -d
```

Le serveur s'exécute alors au premier plan et affiche des informations sur les opérations effectuées.

Sur un client NT, exécutez les commandes MS-DOS suivantes :

```
C:\WINNT>ipconfig /all
```

(Notez l'adresse IP de la carte réseau de par laquelle le client est connecté au serveur)

```
C:\WINNT>ipconfig /release
```

(Le serveur DHCP devrait indiquer qu'il a reçu un message DHCPRelease et ne devrait pas afficher d'erreurs)

```
C:\WINNT>ipconfig /renew
```

(Le serveur DHCP devrait afficher les messages émis et reçus correspondant à l'affectation d'un bail IP)

```
C:\WINNT>ipconfig /all
```

(Vérifiez bien que votre client a bien une adresse IP valide, et dans 99% des cas, cette dernière sera identique à celle notée précédemment)

Sur un client Win9X, ces opérations peuvent être effectuée à l'aide du programme « winipcfg » et libérant l'adresse affecté à la carte et en le renouvelant.

Si des erreurs surviennent, il se peut que votre fichier « dhcpd.conf » ne soit plus viable. Il faudra alors le modifier pour le rendre compatible avec la nouvelle version du serveur DHCP.

e) Le client ne trouve pas le serveur DHCP

Si votre client indique qu'il est dans l'impossibilité de trouver un serveur DHCP lors du renouvellement de la phase de test précédente, c'est qu'il ne peut l'atteindre.

Procédons comme suit :

- Vérifions d'abord que votre noyau dispose du support multicast :

```
[root@redhat /]# /sbin/ifconfig -a
eth0    Lien encap:Ethernet  HWaddr 00:50:8B:B4:7F:E0
   inet adr:172.16.100.1  Bcast:172.16.255.255  Masque:255.255.0.0
   UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
   Paquets Reþus:22056070 erreurs:0 jetés:0 débordements:0 trames:1
   Paquets transmis:4770260 erreurs:0 jetés:0 débordements:692 carrier:0
   collisions:0 lg file transmission:100
   Interruption:30 Adresse de base:0x3000

lo      Lien encap:Boucle locale
   inet adr:127.0.0.1  Masque:255.0.0.0
   UP LOOPBACK RUNNING  MTU:3924  Metric:1
   Paquets Reþus:189033 erreurs:0 jetés:0 débordements:0 trames:0
   Paquets transmis:189033 erreurs:0 jetés:0 débordements:0 carrier:0
   collisions:0 lg file transmission:0
```

Si le mot MULTICAST n'apparait pas, vous devez recompiler votre noyau avec le support multicast. Sur la plupart des systèmes, ça ne devrait pas être nécessaire car leurs noyaux sont, par défaut, compilés avec ce support.

- Si cela ne fonctionne toujours pas, il faut ajouter une route pour le BROADCAST.

Exécutez la commande suivante :

```
[root@redhat /]# route add -host 255.255.255.255 dev eth0
```

Si vous voyez un message d'erreur:

```
"255.255.255.255: Unknown host"
```

essayez d'ajouter la ligne suivante à votre fichier /etc/hosts:
255.255.255.255 tout-le-monde

Ensuite, essayez:

```
[root@redhat /]# route add -host tout-le-monde dev eth0
```

ou

```
[root@redhat /]# route add 255.255.255.255 dev eth0
```

Supprimez ensuite l'entrée précédemment ajoutée du fichier /etc/hosts.

eth0 désigne bien sûr l'interface réseau que vous utilisez. Si vous en utilisez une autre, faites les modifications nécessaires.

III] Configuration du serveur DHCP

La configuration du serveur DHCP se fait en paramétrant le fichier /etc/dhcpd.conf, puis en redémarrant le serveur DHCP.

Pour redémarrer son serveur DHCP, il faut d'abord fermer le processus du serveur DHCP existant :

```
[root@redhat /]# killall dhcpd
```

puis ensuite démarrez le serveur :

```
[root@redhat /]# /usr/sbin/dhcpd eth0 -f -d
```

1) La configuration de base pour un réseau local

Vous avez un réseau local et vous désirez allouer dynamiquement les informations TCP/IP à chaque client de votre réseau. Voici une configuration type de ce genre de situation : on alloue à chaque client des adresses du type 10.0.100.x ou 10.0.101.x, on lui fournit aussi d'autres informations tel que le serveur DNS du réseau, la passerelle, le serveur WINS, …

```
#
# Fichier de configuration du serveur DHCPd : /etc/dhcpd.conf
#

# Durée par défaut du bail IP en secondes (0 = infini)
default-lease-time 3600;

# Durée maximale de bail IP possible en secondes
# (Si le client demande une durée de bail plus importante)
max-lease-time 7200;

# Demande de non-prise en charge du DNS dynamique
ddns-update-style none;

# Déclaration de sous-réseau 10.0.0.0
# Il faut obligatoirement déclarer chaque sous-réseau auxquels le
# serveur DHCP sera connecté
subnet 10.0.0.0 netmask 255.0.0.0 {

    # Masque de sous-réseau du client
    option subnet-mask 255.0.0.0;

    # Adresse de broadcast préférentielle
    option broadcast-address 10.255.255.255;

    # Nom de domaine auxquels appartiendront les clients
    option domain-name "unix.ebc-informatique.com";

    # Adresses IP des serveurs de noms par ordre croissant de préférence
    option domain-name-servers 10.0.0.1;

    # Adresses IP des routeurs par ordre croissant de préférence
    option routers 10.0.0.1;
```

```
    # Adresses IP des serveurs WINS par ordre croissant de préférence
    option netbios-name-servers 10.0.0.1;

    # Etendue des adresses IP distribuables
    range 10.0.100.2 10.0.100.254;
    range 10.0.101.2 10.0.101.254;
}

# Affectation d'une adresse IP fixe à un client
host patron {

    # Adresse ETHERNET de la carte réseau du client
    hardware ethernet 08:00:2b:4c:59:23;

    # Adresse IP associée
    fixed-address 192.168.1.222;
}
```

2) Une configuration avec prise en charge du DNS dynamique

La machine qui supporte le serveur DHCP est également le serveur DNS du réseau. Dans la configuration suivante, le serveur DHCP côtoie le serveur DNS maître du domaine « ebc-informatique.com. ». Ce serveur comprend deux interfaces réseaux : eth0 qui est connecté au réseau « ebc-informatique.com. » (adresses IP du style 172.16.x.x) et eth1 qui est connecté au sous-réseau dynamique « unix.ebc-informatique.com. » (adresses IP du style 10.x.x.x). Le serveur DHCP, cette fois-ci à l'écoute de la seule interface eth0, devra donc informer le serveur DNS de l'arrivée d'un client sur le sous-réseau 10.0.0.0 afin que celui-ci modifie les correspondances DNS en conséquences. Voici la configuration générale que vous pourrez aisément transformer selon les caractéristiques de votre réseau :

```
#
# Fichier de configuration du serveur DHCPd : /etc/dhcpd.conf
#

# Durée par défaut du bail IP en secondes (0 = infini)
default-lease-time 3600;

# Durée maximale de bail IP possible en secondes
# (Si le client demande une durée de bail plus importante)
max-lease-time 7200;

# Demande de prise en charge du DNS dynamique
ddns-update-style ad-hoc;

# Déclaration d'une clé de protection pour les MAJ du DNS
# (ATTENTION : il faudra configurer le serveur DNS en conséquence)
key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;
    secret pRP5FapFoJ95JEL06sv4PQ==;
}
```

```
# Déclaration d'informations DNS spécifiques à certaines zones
# (Comme par exemple la clé de MAJ à transmettre)
zone ebc-informatique.com. {

    # Serveur primaire du domaine
    primary 127.0.0.1;

    # Clé de cryptage
    key DHCP_UPDATER;
}

zone 10.in-addr.arpa. {
    primary 127.0.0.1;
    key DHCP_UPDATER;
}

# Déclaration de sous-réseau 10.0.0.0
subnet 10.0.0.0 netmask 255.0.0.0 {

    # Masque de sous-réseau du client
    option subnet-mask 255.0.0.0;

    # Adresse de broadcast préférentielle
    option broadcast-address 10.255.255.255;

    # Nom de domaine auxquels appartiendront les clients
    option domain-name "unix.ebc-informatique.com";

    # Adresses IP des serveurs de noms par ordre croissant de préférence
    option domain-name-servers 10.0.0.1;

    # Adresses IP des routeurs par ordre croissant de préférence
    option routers 10.0.0.1;

    # Adresses IP des serveurs WINS par ordre croissant de préférence
    option netbios-name-servers 10.0.0.1;

    # Etendue des adresses IP distribuables
    range 10.0.100.2 10.0.100.254;
    range 10.0.101.2 10.0.101.254;
}

# Affectation d'une adresse IP fixe à un client
host patron {

    # Adresse ETHERNET de la carte réseau du client
    hardware ethernet 08:00:2b:4c:59:23;

    # Adresse IP associée
    fixed-address 192.168.1.222;
}
```

ANNEXE

liste non exhaustive des paramètres du fichier dhcpd.conf

1. Les déclarations

La déclaration shared-network (réseau partagé)

shared-network nom {
[paramètres]
[déclarations]
}

La déclaration shared-network indique au serveur DHCP que des sous réseaux IP partagent le même réseau physique. Tous les sous-réseaux du réseau partagé doivent être indiqués dans cette déclaration. Les paramètres seront utilisés lors du démarrage du client à moins qu'ils ne soient remplacés par ceux des déclarations du sous-réseau ou de l'hôte. Si des sous-réseaux disposent d'adresses à allouer dynamiquement, celles-ci sont rassemblées dans un pot commun et distribuées aux clients du réseau partagé, à la demande. Il n'y a pas de moyen de savoir sur quel sous-réseau du réseau partagé démarre le client.
Le nom est celui du réseau partagé. Il est utilisé à l'affichage des messages de débogage, donc il doit être aussi descriptif que possible. Il doit avoir la même syntaxe que les noms de domaines (même s'il n'est jamais utilisé en tant que tel) ou bien sous forme libre entre guillemets.

La déclaration subnet (sous-réseau)

subnet numéro netmask masque {
[paramètres]
[déclarations]
}

La déclaration subnet sert à dhcpd à avoir suffisament d'informations pour déterminer si une adresse IP est ou pas sur un réseau. Elle peut aussi être utilisée pour indiquer des paramètres propres au sous-réseau ainsi que des adresses à allouer dynamiquement aux clients qui démarrent dessus. Ces adresses sont spécifiées à l'aide de la déclaration range.
Le numéro est une adresse IP ou un nom qui correspond au sous-réseau en cours de description. De même, le masque est soit une adresse IP soit un nom qui correspond au sous-réseau en cours de description. Le numéro de sous-réseau associé au masque est suffisant pour déterminer si une adresse IP appartient au sous-réseau.
Bien que le masque doive être donné avec chaque déclaration, il est recommandé d'utiliser une option subnet-mask pour chaque sous-réseau car elle remplace le masque indiqué dans la déclaration du sous-réseau.
Dans le cas où les masques sous-réseau d'un site sont amenés à changer, il est préférable d'utiliser une option subnet-mask (voir dhcp-options(5) <../man5/dhcp-options.5.html>) pour chaque sous-réseau plutôt que de l'indiquer ici dans chaque déclaration puisque les valeurs de cette option remplacent celles de la déclaration.

La déclaration range (plage d'adresses)

range [dynamic-bootp] adresse-mini [adresse-maxi];

Il doit exister au moins une plage d'adresses pour les réseaux à adressage dynamique. La déclaration indique la plus petite et la plus grande adresse IP de la plage. Toutes celles-ci doivent appartenir au sous-réseau dans lequel elles sont déclarées. L'option dynamic-bootp peut être indiquée dans le cas où les adresses dynamiques correspondent indifféremment aux clients BOOTP ou DHCP. Si la déclaration ne contient qu'une seule adresse, celle maximum peut être omise.

La déclaration host (Hôte)

host nom d'hôte {
[paramètres]
[déclarations]
}

Il doit exister au moins une déclaration host pour chaque client BOOTP à servir. De même pour les clients DHCP bien que ça ne soit pas obligatoire tant que le démarage n'est autorisé que pour les hôtes connus.
Si vous voulez autoriser un client DHCP ou BOOTP à démarrer sur plus d'un sous-réseau avec des adresses fixes, plus d'une adresse peuvent être inscrites dans le paramètre fixed-address ou bien plus d'une déclaration host peuvent être spécifiées.
Si des paramètres spécifiques au client ont à changer suite à des modifications sur le réseau, plusieurs déclarations host peuvent alors être utilisées.
Si un client est amené à démarrer avec une adresse fixe si possible et dynamique sinon, une déclaration host doit être spécifiée sans la clause fixed-address. Le nom d'hôte est celui qui identifie l'hôte. S'il n'y a pas d'option hostname, c'est celui-ci qui est utilisé.
Une déclaration host correspond à un client DHCP ou BOOTP lorsque l'option dhcp-client-identifier de la déclaration correspond à celle donnée par le client. Si l'une des deux n'est pas pas fournie, c'est la pramètre hardware qui est comparé à l'adresse réseau matérielle fournie par le client. Notez que les clients BOOTP ne fournissent normalement pas de dhcp-client-identifier, donc c'est l'adresse matérielle qui est systématiquement utilisée par le protocole BOOTP.

La déclaration group (groupe)

group {
[paramètres]
[déclarations]
}

La déclaration group est simplement utilisée pour appliquer un ou plusieurs paramètres à un ensemble de déclarations. Elle peut être utilisée pour grouper des hôtes, des réseaux partagés, des sous-réseaux et même d'autre groupes.

2. ALLOW and DENY (permettre et empêcher)

Les déclarations allow (permettre) et deny (empêcher) sont utilisées pour contrôler le comportement de dhcpd à diverses requètes.

Le mot clef unknown-clients (clients inconnus)

allow unknown-clients;
deny unknown-clients;

Ceci est utilisé pour indiquer à dhcpd s'il faut ou non donner dynamiquement une adresse à un client inconnu. Par défaut, l'assignation est permise (allow).

Le mot clef bootp

allow bootp;
deny bootp;

Ceci est utilisé pour indiquer à dhcpd s'il doit ou non répondre aux requètes bootp. Par défaut, dhcpd y répond (allow).

Le mot clef booting (démarrer)

allow booting;
deny booting;

Ceci est utilisé pour indiquer à dhcpd s'il faut ou non répondre aux requètes d'un client particulier. Cette déclaration n'a de sens que si elle apparait dans le paramètrage d'un hôte. Par défaut, le démarrage est permis (allow) mais s'il est empêché (deny), le client ne pourra pas avoir d'adresse par ce serveur DHCP.

3. Paramètres

La déclaration default-lease-time (durée de bail par défaut)

default-lease-time durée;

La durée, en secondes, est le temps pendant lequel le bail est cédé au client si celui-ci n'en demande pas de particulière.

La déclaration max-lease-time (durée maximum de bail)

max-lease-time durée;

La durée, en secondes, est la durée maximum du bail que dhcpd peut céder à client qui en demande une spécifique.

La déclaration hardware (matériel)

hardware type-matériel adresse-matérielle;

Pour qu'un client bootp soir reconnu, son adresse réseau matérielle doit être déclarée dans la clause hardware de la déclaration host. Le type-matériel est le nom du type d'interface physique. Actuellement, seuls les types ethernet et token-ring sont reconnus bien que le support de fddi (et d'autres) soit désirable. l'adresse-matérielle est une suite d'octets hexadéciamux (nombres de 0 à ff) séparés par les deux points. Cette déclaration peut aussi exister pour les clients DHCP.

La déclaration filename (nom de fichier)

filename "nom de fichier";

Elle sert à indiquer quel est le fichier qu'un client doit charger afin de démarrer. Le nom de fichier doit être un nom reconnu par tout protocole que le client est susceptible d'utiliser.

La déclaration server-name (nom de serveur)

server-name "nom";

Elle est utilisée pour informer le client du nom du serveur sur lequel il démarre. Le nom est celui envoyé au client.

La déclaration next-server (serveur suivant)

next-server nom de serveur;

Elle sert à indiquer sur quel serveur se trouve le fichier de démarrage, indiqué par la déclaration filename, à télécharger. Le nom de serveur peut être une adresse IP numérique ou bien un nom de domaine. Si elle n'est pas spécifiée pour un client, c'est l'adresse du serveur DHCP qui est utilisée.

La déclaration fixed-address (adresse fixe)

fixed-address adresse [, adresse ...];

Cette déclaration sert à affecter une ou plusieurs adresses fixes à un client. Elle ne doit donc apparaitre que dans une déclaration host. Si plus d'une adresse lui est réservée, le client, au démarrage, acquerra celle qui correspond au réseau sur lequel il démarre. Si aucune adresse de fixed-address ne correspond à ce réseau, le client ne correspond pas à la définition host en question. Chaque adresse peut être une adresse IP ou un nom de domaine pointant sur une ou plusieurs adresses IP.

La déclaration dynamic-bootp-lease-cutoff (suspension de bail)

dynamic-bootp-lease-cutoff date;

Elle permet de définir une date à partir de laquelle les baux bootp dynamiques ne seront plus cédés. Comme les clients BOOTP n'ont pas les moyens de renouveler un bail ni de savoir que celui-ci expire, dhcpd donne une date infine par défaut. Cependant, certaines situations peuvent demander un arrêt des baux (par exemple à la fin d'une période scolaire ou la nuit lorsque le service est fermé et que les machines doivent être éteintes).
La date est celle à laquelle plus aucun bail BOOTP n'est cédé. Elle doit être sous la forme :
S AAAA/MM/JJ HH:MM:SS
S est le jour de la semaine de zéro (dimanche) à 6 (samedi). AAAA est l'année sur quatre chiffres (siècle inclus). MM le mois de 1 à 12. JJ le jour du mois à partir de 1. HH est l'heure de 0 à 23.

MM les minutes et SS les secondes. L'heure est toujours celle de Greenwitch (GMT), jamais l'heure locale.

La déclaration dynamic-bootp-lease-length (durée de bail bootp)

dynamic-bootp-lease-length durée;

Cette déclaration sert à définir la durée du bail cédé aux clients BOOTP. Dans certains cas, on suppose que le bail n'est plus utilisé si son possesseur n'a pas utilisé BOOTP ou DHCP pour demander son adresse dans une certaine période. Celle-ci est définie par durée en nombre de secondes. Si un client redémarre en utilisant BOOTP pendant la période de dépassement, la durée du bail est remise à durée. Ainsi, un client qui redémarre assez souvent ne perdra jamais son bail. Bien entendu, ce paramètre doit être ajusté avec d'extrèmes précautions.

La déclaration get-lease-hostnames (recherche du nom de domaine)

get-lease-hostnames option;

Cette déclaration indique à dhcpd s'il faut ou non rechercher le nom de domaine correspondant à l'adresse IP de chaque adresse de la réserve de baux et de l'utiliser pour l'option hostname de DHCP. Si option est true (vrai) cette recherche est effectuée pour toutes les adresses actuellement utilisées. Par défaut ou si option est false (faux), aucune recherche n'est effectuée.

La déclaration use-host-decl-names (utiliser le nom d'hôte déclaré)

use-host-decl-names option;

Si le paramètre de use-host-decl-names est vrai pour dans un espace donné, alors, pour chaque hôte de cet espace, le nom déclaré sera fourni au client qui l'utilisera comme nom d'hôte. Par exemple :
group {
use-host-decl-names on;
host joe {
hardware ethernet 08:00:2b:4c:29:32;
fixed-address joe.fugue.com;
}
}
est équivalent à :

host joe {
hardware ethernet 08:00:2b:4c:29:32;
fixed-address joe.fugue.com;
option host-name "joe";
}
La ligne option host-name d'une déclaration d'hôte remplace le nom de la déclaration (ici joe).

La déclaration authoritative (autorisé)

authoritative;
not authoritative;

Normalement, le serveur DHCP suppose que les informations sur un réseau donné sont correctes et autorisées. Donc si un client demande une adresse IP sur un sous-réseau que le serveur sait invalide, ce dernier répondra par DHCPNAK, le client oubliera son adresse et en demandera une autre.
Si un serveur DHCP est configuré par une autre personne que l'administrateur système et qui n'a donc pas ce niveau d'autorisations, l'option " not authoritative" (non autorisé) doit être inscrite à l'endroit approprié du fichier de configuration.
Habituellement, inscrire "not authoritative" au début du fichier est suffisant. Cependant, si le serveur DHCP est amené à gérer des réseaux sur lesquels il est autorisé et d'autres sur lesquels il ne l'est pas, il est sans doute plus approprié de faire cette déclaration pour chaque réseau.
Le concept d'autorisation est plus particulièrement adapté aux réseaux physiques (un réseau partagé ou un sous-réseau non-inclus dans un réseau partagé). Il n'est en revanche pas adapté pour dire que le serveur est autorisé sur certains sous-réseaux d'un réseau partagé et pas sur d'autres ni pour certains hôtes et pas d'autres.
La déclaration use-lease-addr-for-default-route (adresse de bail comme route)
use-lease-addr-for-default-route option;
Si ce paramètre est vrai dans un espace donné, alors, au lieu d'envoyer la valeur indiquée par l'option routers (ou au lieu de ne rien envoyer du tout), c'est l'adresse IP du bail cédé qui est envoyée. Celà inciterait les machines Windows95 à utiliser ARP pour toute adresse IP, ce qui est utile si votre routeur est configuré pour un proxy ARP.
Si use-lease-addr-for-default-route est activé et qu'une option "routers" existe au même endroit, cette dernière sera préférée. La raison est que, si vous voulez utiliser cette caractéristique, vous voulez probablement l'appliquer à un ensemble de machines Windows95 et vous voulez qu'elle soit remplacée pour d'autres. Si c'est malheureusement le contraire qui se passe, cette option est certainement désactivée.

La déclaration always-reply-rfc1048 (réponse rfc1048)

always-reply-rfc1048 option;

Certains clients BOOTP attendent une réponse conforme au RFC1048 alors que leurs requètes ne le sont pas. Vous pouvez dire qu'un client a un problème lorsqu'il ne reçoit pas les options que vous lui destiniez et si le message "(non-rfc1048)" apparait à chaque BOOTREQUEST enregistré dans le fichier log.
Si vous voulez envoyer des options rfc1048 à ces clients, indiquez l'option always-reply-rfc1048 dans leur déclaration host. Le serveur répondra alors conformément aux spécifications. Cette option peut être placée à n'importe quel endroit et affectera tous les clients concernés.

La déclaration server-identifier (Identifiant serveur)

server-identifier hôte;

Cette déclaration est utilisée pour définir la valeur envoyée par le serveur dans un espace donné. Cette valeur doit être une adresse IP du serveur et doit être accessible à tous les clients de l'espace. L'utilisation de server-identifier n'est pas recommandée. La seule raison de le faire est de forcer une valeur autre que celle par défaut dans le cas où celle-ci serait incorrecte. La valeur par défaut est la première adresse IP associée à l'interface réseau sur laquelle arrive la requète.

Le cas le plus courrant est lorsque l'interface physique possède plus d'une adresse IP et que celle envoyée par défaut n'est pas appropriée pour certains clients. Un autre cas est si un alias est défini pour avoir une adresse IP de serveur cohérante et que les clients doivent utiliser cette adresse pour contacter le serveur.d
Donner une valeur à l'option "dhcp-server-identifier" est équivalddent à donner une valeur à la déclaration server-identifier.

4. Les options

Les options DHCP commencent toujours par le mot-clé *option*.

Les options standards sont :

option subnet-mask ip-address;

Cette option spécifie le masque de sous-réseau du client. Si aucun masque de sous-réseau n'est renseigné dans la portée en cours, dhcpd va utiliser le masque de sous-réseau de la déclaration du masque de sous-réseau pour le réseau. Sinon, la première déclaration d'option du type ci-dessus sera prise en compte.

option time-offset int32;

Cette option permet de définir l'offset du sous-réseau des clients en secondes du temps unniversel coordonné (UTC).

option routers ip-address [, ip-address...];

Cette option spécifie la liste des adresses IP d'un routeur sur le sous-réseau des clients. Les routeurs sont listés par ordre de préférence.

option time-servers

Cette option permet de définir une liste des serveurs de temps (décrit dans le RFC 868) disponibles pour le client. Les serveurs sont listés par ordres de préférence.

option ien116-name-servers ip-adress [, ip-adress...];

Cette option permet de définir une liste de serveurs de noms IEN 116 disponibles disponibles. Les serveurs sont listés par ordre de préférence.

option domain-names-servers ip-adress [, ip-adress...];

Définit la liste des serveurs de noms DNS (STD 13, RFC 1035) accessibles par ordre de préférence.

option log-servers ip-adress [, ip-adress...];

Définit la liste des serveurs de log MIT-LCS UDP accessibles par le client par ordre de préférence.

option cookie-servers ip-adress [, ip-adress...];

Définit la liste des serveurs de cookies (RFC 865) accessibles par le client par ordre de préférence.

option lpr-servers ip-adress [, ip-adress...];

Définit la liste des serveurs d'impression (RFC 1179) accessibles par le client par ordre de préférence.

option impress-servers ip-adress [, ip-adress...];

Définit la liste des serveurs "Imagen Impress" accessibles par le client par ordre de préférence.

option resource-location-servers ip-adress [, ip-adress...];

Définit la liste des serveurs de location de ressources accessibles par le client par ordre de préférences.

option host-name string;

Cette option définit le nom du client. Ce nom peut être suffixé par le nom de domaine, mais il est préférable de définir le nom de domaine avec l'option domain-name.

option boot-size uint16;

Cette option définit la taille en bloc de 512 octets de l'image de boot par défaut du client.

option meri-dump string;

Cette option spécifie le chemin vers un fichier dans lequel l'image core du client devrait être copiée dans le cas où ce dernier crasherait.

option domain-name string;

Définit le nom de domaine que le client utilisera lors de la résolution des noms de machines via le DNS.

option swap-servers ip-adress [, ip-adress...];

Définit les adresses IP du serveur de swap du client.

option roo-path string;

Cette option permet de définir le chemin qui contiend le disque root du client.

option ip-forwarding flag;

Spécifie si le client doit configurer sa couche IP pour la retransmission de paquets. Une valeur de 0 signifie sa désactivation alors qu'ne valeur de 1 signifie le contraire.

option non-local-source-routin flag

Spécifie si le client doit configurer sa couche IP pour permettre la retransmission de paquet avec des routes d'origine non locale.

option policy-filter ip-adress [, ip-adress...];

Définit les filtres pour la politique de routage non local. Le filtre consiste en une liste d'adresses IP et de masques de sous-réseau.

option max-dgram-reassembly uint16;

Cette option définit la taille maximale des paquets que le client est susceptible de réassemblé. La valeur légale minimale ets 576.

option default-ip-ttl uint8

option path-mtu-aging-timeout uint32;

Définit le délai (en secondes) à utiliser lorsqu'il y a découverte par le mécanisme définit dans le RFC 1191 d'un MTU obsolète.

option path-mtu-plateau-table uint16 [, uint16...];

option interface-mtu uint16;

Définit le MTU à utiliser sur cette interface. Le minimum légal est de 68.

option all-subnets-local flag

Définit si le client considère si tout les sous-réseau du réseau IP auxquel le client est connecté utilise le même MTU que le sous-réseau du réseau auquel le client est directement connecté.

option broadcast-adress ip-adress [, ip-adress...];

option perform-mask-discovery flag;

Cette option indique si le client doit ou non découvrir son masque de sous-réseau en utilisant ICMP.

option mask-supplier flah;

Définit si le client doit répondre à des demandes de masque de sous-réseau en utilisant ICMP.

option router-discovery flag;

Définit si le client doit rechercher les routeurs en utilisant le mécanisme de détection des routeurs définit dans le RFC (1256).

option router-soliciation-address ip-adress [, ip-adress...];

Définit à quel adresse le client doit transmettre ses demandes de sollicitations de routeurs.

option static-routes ip-adress ip-adresse [, ip-adress ip-adress...];

Définit une liste de routes que le client doit installer dans son cache de routage. Elles sont classées par ordre de priorité décroissante.

option trailer-encapsulation flag;

Définit si lors de l'utilisation du protocole ARP, le client doit négocier l'utilisation de trailers (RFC 893 [4]).

option arp-cache-timeout uint32;

option ieee802-3-encapsulation flag;

option default-tcp-ttl uint8;

option tcp-keepalive-interval uint32;

option tcp-keepalive-garbage flag;

option nis-domain string;

Définit le nom du domaine NIS (Sun Network Information Services) du client.

option nis-servers ip-adress [, ip-adress...];

option ntp-servers ip-adress [, ip-adress...];

option netbios-name-servers ip-adress [, ip-adress...];

option netbios-dd-server ip-adress [, ip-adress...];

option netbios-node-type uint8;

option netbios-scope string;

option font-servers ip-adress [, ip-adress...];

option x-display-manager ip-adress [, ip-adress...];

option dhcp-client-identifier data-string;

option nisplus-servers ip-adress [, ip-adress...];

option tftp-servers-name string;

option bootfile-name string;

option mobile-ip-home-agent ip-adress [, ip-adress...];

option smtp-server ip-adress [, ip-adress...];

option pop-server ip-adress [, ip-adress...];

option nntp-server ip-adress [, ip-adress...];

option www-server ip-adress [, ip-adress...];

option finger-server ip-adress [, ip-adress...];

option irc-server ip-adress [, ip-adress...];

option streettalk-server ip-adress [, ip-adress...];

option streettalk-directory-assistance-server ip-adress [, ip-adress...];