Administration et sécurité des réseaux

Chapitre 4

Le Protocole DHCP
(Dynamic Host Configuration Protocol)

Plan

- Objectifs
- Présentation du protocole
- Fonctionnement
- Les types de messages
- Le relais DHCP
- Configuration et options

Rôle d'un service DHCP

- Rôle:
  - Distribue d'une façon dynamique des adresses IP à des clients pour une durée déterminée.
  - Evite l'affectation manuelle à chaque hôte d'une adresse IP statique, ainsi que tous les paramètres dont il a besoin pour utiliser le réseau
- Exemple d'utilisation: chez les FAI.
  - Le fournisseur d'accès alloue une adresse IP de son réseau le temps de la liaison. Cette adresse est libérée, donc de nouveau disponible, lors de la fermeture de la session.
- Contraintes:
  - Tous les nœuds critiques du réseau (serveur de nom, passerelle par défaut, serveur de mail…etc) ont une adresse IP statique sinon problèmes de gestion

Avantage de DHCP

- Configuration fiable et simple de réseaux TCP/IP
- Minimisation du risque de conflits d'adresses
- Les postes itinérants sont plus faciles à gérer (PC portable)
- L'économie des adresses IP:
  - Exemple: Les FAI disposent d'un nombre d'adresses limité.
  - Avec DHCP, seules les machines connectées en ligne ont une adresse IP.
- Contrôle centralisé de l'utilisation des adresses IP.
- Le changement de la valeur d'un paramètre au niveau du serveur DHCP (exemple: passerelle par défaut) est pris en compte par tous les clients du serveur ➔ changement facile
  - Dans le cas de l'adressage statique, il faudrait reconfigurer toutes les machines manuellement .

L'économie des adresses: cas pratique

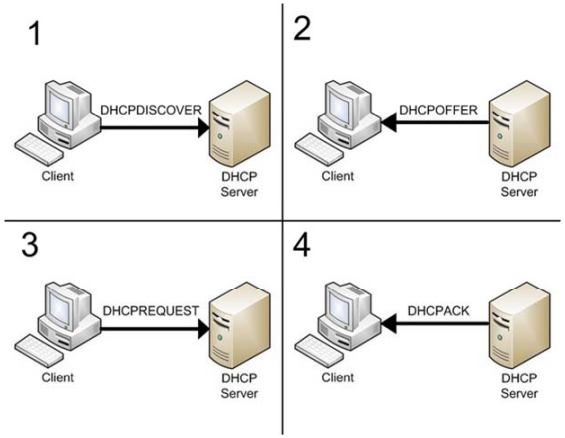
- Un FAI a plus de 1000 clients.
- Il lui faudrait 5 réseaux de classe C pour adresser tous ses clients
- Si on sait que chaque client utilise en moyenne un temps de connexion de 10 min par jour ➔adresser tous les clients avec une seule plage d'adresses de classe C.
- Attribuer des "jetons d'accès" en fonction des besoins des clients.

Le protocole DHCP

- RFC 1533 et 1534
- Extension de BootP
- Se base sur les protocoles UDP et IP
- Fonctionne en mode client serveur
  - Le client demande une adresse IP (une configuration automatique)
  - Le serveur dispose d'une pool d'adresses à louer
  - Le serveur fournit/loue l'adresse IP (configuration) pendant un temps limité appelé bail (lease)

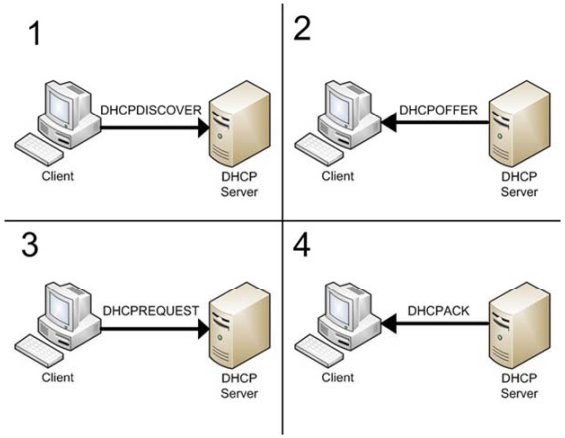
Attribution d'adresse IP

- Le client émet un message de demande de bail IP (DHCPDISCOVER) envoyé par diffusion sur le réseau avec adresse IP source 0.0.0.0, adresse IP destination 255.255.255.255 et son adresse MAC.



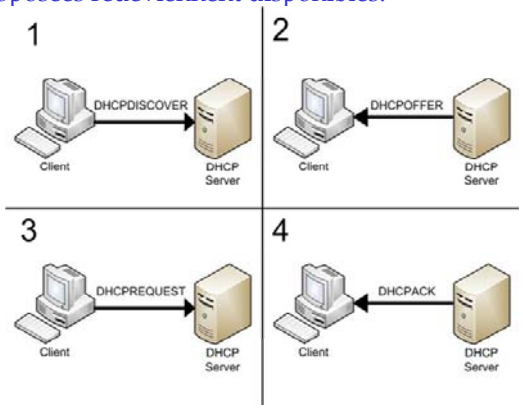
Attribution d'adresse IP

- Les serveurs DHCP répondent en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP (DHCOFFER)



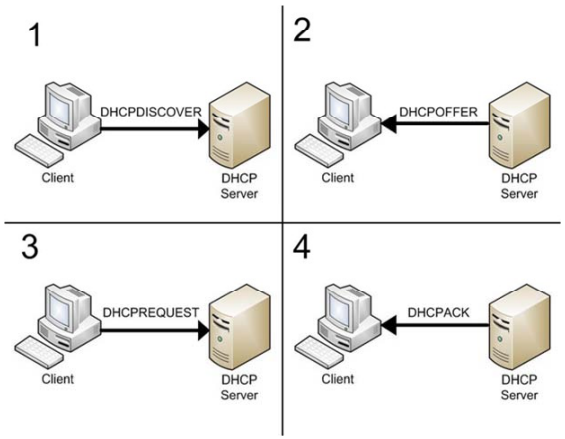
Attribution d'adresse IP

- Le client sélectionne la première adresse IP reçue (s'il y a plusieurs serveurs DHCP) et envoie une demande d'utilisation de cette adresse au serveur DHCP (DHCPREQUEST). Son message envoyé par diffusion comporte l'identification du serveur sélectionné qui est informé que son offre a été retenue ; tous les autres serveurs DHCP retirent leur offre et les adresses proposées redeviennent disponibles.

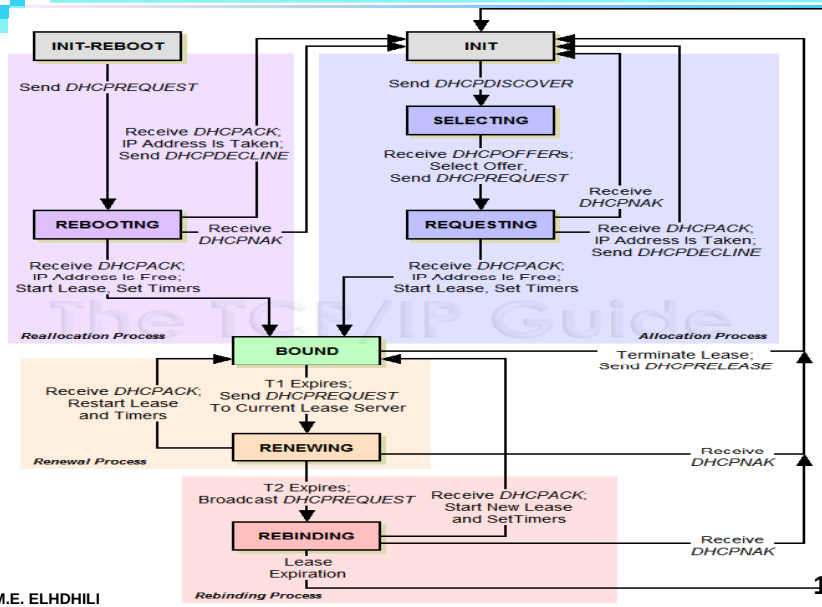


Attribution d'adresse IP

- Le serveur DHCP accuse réception de la demande et accorde l'adresse en bail (DHCPACK), les autres serveurs retirent leur proposition.



L'automate de DHCP

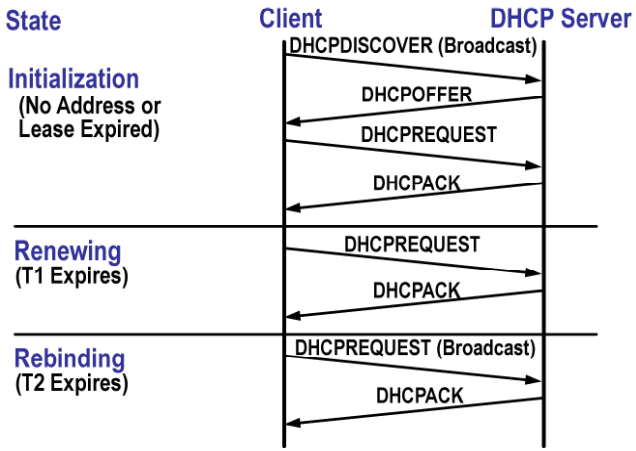


Renouvellement de bail IP

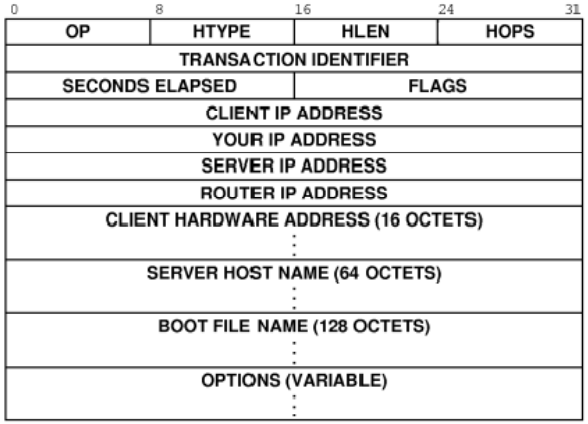
- Lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un DHCPREQUEST.
- En cas d'échec, le client continue à utiliser la même adresse IP s'i le bail n'a pas encore expiré.
- Les clients DHCP d'un serveur DHCP Windows (NT/2000) tentent de renouveler leur bail lorsqu'ils ont atteint 50% de sa durée par un DHCPREQUEST. Si le serveur DHCP est disponible il envoie un DHCPACK avec la nouvelle durée et éventuellement les mises à jour des paramètres de configuration.
- Si à 50% le bail n'a pu être renouvelé, le client tente de contacter l'ensemble des serveurs DHCP (diffusion) lorsqu'il atteint 87,5% de son bail, avec un DHCPREQUEST, les serveurs répondent soit par DHCPACK soit par DHCPNACK (adresse inutilisable, étendue désactivée...).
- Lorsque le bail expire ou qu'un message DHCPNACK est reçu le client doit cesser d'utiliser l'adresse IP et demander un nouveau bail (retour au processus de souscription). Lorsque le bail expire et que le client n'obtient pas d'autre adresse la communication TCP/IP s'interrompt.

- Remarque : Si la demande n'aboutit pas et que le bail n'est pas expiré, le client continue à utiliser ses paramètres IP.

Echange de messages DHCP



Format du message DHCP



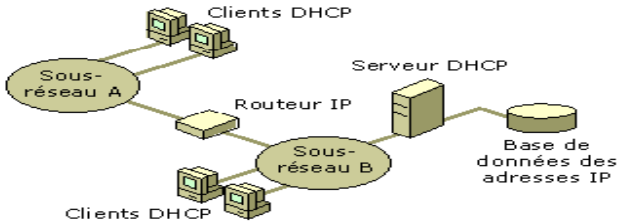
Format du message DHCP

- **op** : vaut 1 pour BOOTREQUEST (requête client), 2 pour BOOTREPLY (réponse serveur)
- **htype** : type de l'adresse hardware (adresse MAC, par exemple. Voir Rfc 1340)
- **hlen** : longueur de l'adresse hardware (en octet). C'est 6 pour une adresse MAC
- **hops** : peut être utilisé par des relais DHCP
- **xid** : nombre aléatoire choisi par le client et qui est utilisé pour reconnaître le client
- **secs** : le temps écoulé (en secondes) depuis que le client a commencé sa requête
- **flags** : flags divers

Format du message DHCP

- **ciaddr** : adresse IP du client, lorsqu'il en a déjà une
- **yiaddr** : la (future ?) adresse IP du client
- **siaddr** : adresse IP du (prochain) serveur à utiliser
- **giaddr** : adresse IP du relais (passerelle par exemple) lorsque le serveur n'est pas dans le même réseau physique
- **chaddr** : adresse hardware du client
- **sname** : champ optionnel. Nom du serveur
- **file** : nom du fichier à utiliser pour le boot
- **options** : Champ réservé pour les options (RFC 2132).

Le relais DHCP



- Lorsque le serveur DHCP n'est pas sur le même réseau physique que les clients: nécessité d'un relais DHCP
- Le relais fait passer les messages DHCP d'un réseau à un autre
- Un routeur doit être configuré pour jouer le rôle d'un relais DHCP

Les options du protocole

- Le passage de paramètres (nom de la machine...) se fait par l'intermédiaire d'options.
- Les options sont documentées dans la RFC 2132.
- Chaque option porte un numéro qui l'identifie.
- Il est possible d'envoyer plusieurs options dans le même message DHCP.
- Dans tous les cas, on doit toujours finir la zone d'options par une option 255 (end).
- Le format des options est le suivant :

Octet 1	Octet 2	Données
Code de l'option	Longueur champ de données	…

Quelques options utiles

- 1 Masque
- 3 Routeur
- 4 Serveur de temps
- 5 serveur de noms
- 6 serveur du domaine
- 10 serveur d'impression
- 15 nom du domaine
- 28 adresse de diffusion
- 66 serveur TFTP
- 255 end

Inconvénients de DHCP

- Les trames de diffusion pour obtenir les adresses chargent le réseau.
- Risque de graves goulots d'étranglement sur le réseau lors des démarrages synchronisés.

  →L'administrateur doit donc réfléchir à l'organisation de son réseau.
- Nécessité d'un équipement serveur pour chaque zone de diffusion

  → Compromis nombre de serveurs/ zone de diffusion

Config. d'un réseau en DHCP

- Attribuer aux serveurs des adresses IP statiques
- Organiser les clients en catégories
- Affecter à chaque catégorie une pool d'adresses dynamiques
- Configurer le maximum d'options dans le serveur
- Bien dimensionner la durée du bail pour un compromis charge réseau/validité
- Faire le choix entre utiliser un relais ou plusieurs serveurs distincts

Analyse DHCP

DHCP: mise en ouevre

Mise en œuvre DHCP (linux)

- Identité :
  - Type : service standalone
  - Ports : 67 (serveur), 68 (client)
  - Démon : /etc/init.d/dhcpd
  - Fichier de configuration : /etc/dhcpd.conf
  - Fichiers gérés par dhcpd(dans /etc ou /var/state/dhcp):
  - dhcpd.leases → contenant les baux en cours
  - dhcpd.leases~ → contenant les baux précédant .
  - Remarque: Pour certaines versions, ces fichiers ne sont pas créées lors de l'installation → executer:

    touch /var/state/dhcp/dhcpd.leases

Mise en œuvre DHCP

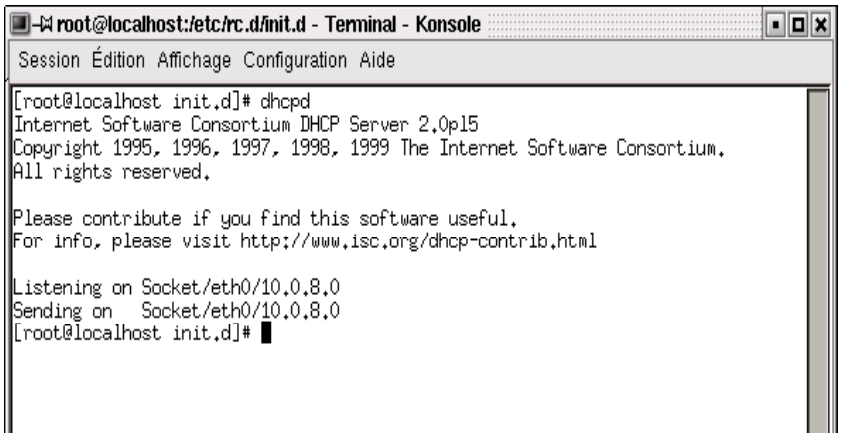
```
# Sample dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

ddns-update-style ad-hoc;

# option definitions common to all supported networks...
option domain-name "linuxhelp.ca";

# Your name servers. You can normally find these in
# your /etc/resolv.conf file. These will be distributed to all DHCP
# clients.
option domain-name-servers 10.1.1.1, 65.39.196.215, 65.39.192.130;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# Configuration for an internal subnet.
subnet 10.1.1.0 netmask 255.255.255.0 {
  range 10.1.1.2 10.1.1.25;
  option domain-name-servers 10.1.1.1, 65.39.196.215, 65.39.192.130;
  option domain-name "linuxhelp.ca";
  option routers 10.1.1.1;
  option broadcast-address 10.1.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```


Mise en œuvre DHCP

- **max-lease-time** : durée maximale du bail que dhcp peut fournir (max une semaine) selon la durée demandée par le client
- **default-lease-time:** durée du bail utilisé (1 jour) si le client ne spécifie pas une durée dans sa demande
- **option subnet-mask** : definie le net mask.
- **option domain-name-servers** : liste des adresse IP des serveurs DNS
- **option domain** : le domaine par défaut
- **option lpr-servers** : liste les adresses des serveurs d'impression
- **option routers** : liste les routeurs du sous réseau du client
- **range** : Definie la plage d'addresses

Mise en œuvre DHCP

- Invoquer le démon /usr/sbin/dhcpd par la commande dhcpd



Commande démon dhcpd

dhcpd [interfce] [-p port] [-f] [-d] [-q] [-cf config-file] [-lf lease-file]

- Options
  - -p: specifier le port udp sur lequel le processus reste en écoute des demandes.
  - -f : le processus dhcpd sera lancer en avant plan.
  - -d : pour lancer le processus en mode deboguage (plus d'information sur le traffic dhcp).
  - -cf :specifier le fichier de configuration.
  - -q: les information d'entete sera omise lors du démarrage du démon(version ,copyright...)
  - -lf :spécifier un fichier .lease

- Pour lancer automatiquement le service dhcp lors de démarage ajouter /etc/sbin/dhcpd dans :

  /etc/rc.d/rc.local

- Lancer avec le script dhcpd sous /etc/rc.d/init.d

  dhcpd [start | stop | status……]

DHCP CLIENT sous linux

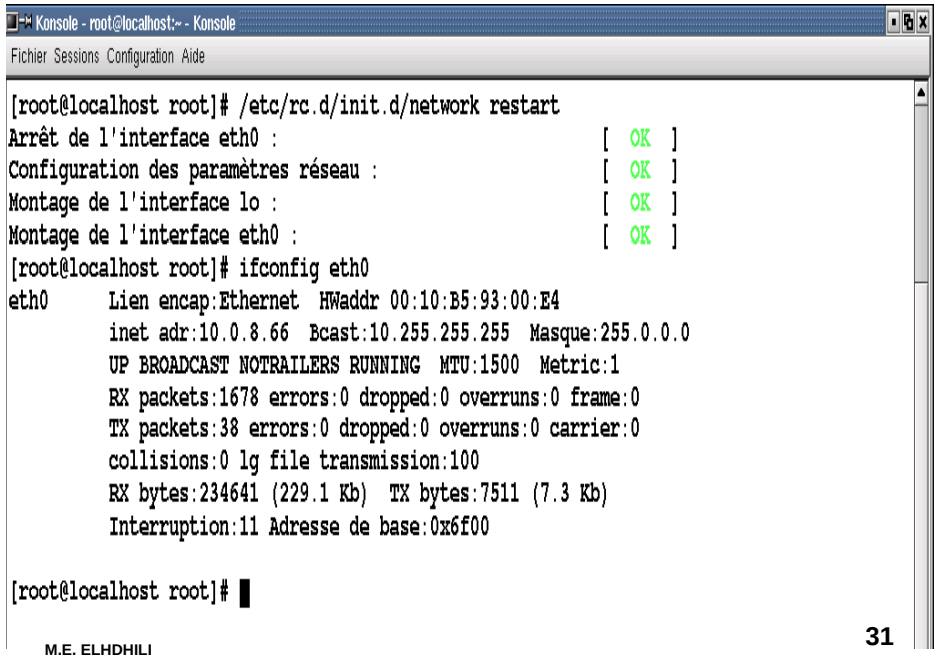
- Configurer le client
  - configurer l'interface eth0 comme client dhcp
    - Modifier: /etc/sysconfig/network-scripts/ifcfg-eth0
    - Relancer les service réseau /etc/rc.d/init.d/network start

Avant

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.255.255.255
IPADDR=10.0.8.4
NETMASK=255.0.0.0
NETWORK=10.0.0.0
ONBOOT=yes
```

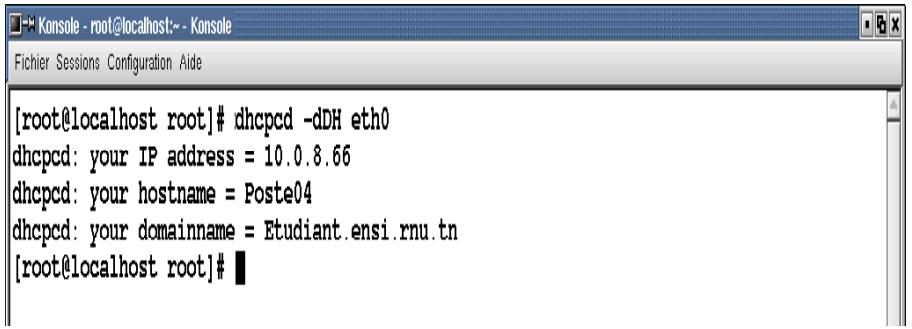
Aprés

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

Démon client dhcpcd

- Permet d'intéragir avec le serveur dhcpd
- invoquer le démon /usr/sbin/dhcpcd par la commande dhcpcd



Commande client dhcpcd

dhcpcd [-dknrBCDHRT] [-t timeout] [-c filename] [-h hostname] [-l leasetime] [-s [ipaddr]] [interface]

- Options

-k : mettre à fin le bail .

-n : renouvellement .

-B : demander une réponse par le serveur en broadcast

-t timeout : temps d'attente d'une réponse du serveur (par défaut 60seconde).

Commande client dhcpcd (suite)

-c filename : pour que dhcpcd exécute le fichier après avoir configurer l'interface .

-H : forcer dhcpcd à affecter au hostname celui reçu par le serveur .

-D : forcer dhcpcd à affecter à domainename celui reçu par le serveur .

-l leasetime : la durée du bail recommandée par le client .

Démon client dhcpcd (suite)

- Le démon dhcpcd gère et créé des fichiers tels que:

✓ **/var/run/dhcpcd-eth0.pid :** image mémoire contient le pid du processus dhcpcd .

✓ **/etc/dhcp/dhcpcd-eth0.info :** contient les information obtenus par le serveur dhcp (avec eth0 est l'interface cliente dhcp) .

Démon client dhcpcd (suite)

✓ **/etc/resolv.conf :** ce fichier est crée par dhcpcd quand le client reçoit **dns** et **domainename options** ,l'ancien fichier renommé en **/etc/resolv.con.sv** pour restauration en cas de problème dû à dhcpcd.

✓ **/etc/dhcp :**contient les fichiers que crées le démon dhcpcd .