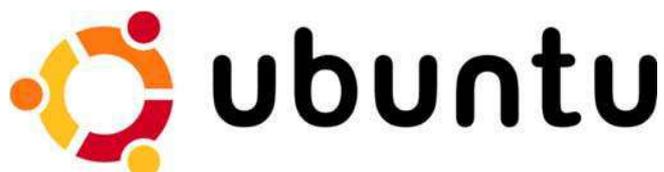


Installation d'un serveur DHCP (Dynamic Host Configuration Protocol) sous Ubuntu Server 12.10

Table des matières



1. Comment le protocole DHCP alloue des adresses IP	3
2. Processus de création d'un bail DHCP	5
3. Processus de renouvellement d'un bail DHCP	6
Installation d'un serveur DHCP (Dynamic Host Configuration Protocol) sous Ubuntu Server 12.10.....	7
1. Topologie Physique et logique du réseau.....	7
2. Installation du serveur DHCP	9
3. Configuration du serveur DHCP	10
4. Configuration des clients.....	15
Mise en œuvre et exploration des Trames avec le logiciel Wireshark.....	16
1. Mise en route du Poste 1	16
2. Analyse des trames avec le logiciel WIRESHARK.....	17
3. Mise en route du Poste 2	23
4. Pour aller plus loin....	24
5. Conclusion.....	27

1. Le protocole DHCP

Le *protocole DHCP* est une norme IP permettant de simplifier la gestion de la configuration IP hôte. La norme DHCP permet d'utiliser les serveurs DHCP pour gérer l'allocation dynamique des adresses IP et des autres données de configuration IP pour les clients DHCP de votre réseau. Pour les réseaux basés sur le protocole TCP/IP, le protocole DHCP simplifie et réduit le travail administratif requis pour la reconfiguration des ordinateurs.

Pour comprendre en quoi le protocole DHCP simplifie la configuration du protocole TCP/IP sur des ordinateurs clients, il est utile de comparer les configurations manuelle et automatique du protocole TCP/IP, la configuration automatique utilisant le protocole DHCP.

Le protocole DHCP est décrit dans la RFC2131.

Lorsque vous configurez les données de configuration IP pour chaque hôte en entrant manuellement les informations, telles que l'adresse IP, le masque de sous-réseau ou la passerelle par défaut, vous pouvez faire des erreurs typographiques. Ces erreurs peuvent créer des problèmes de communication ou des incidents liés aux adresses IP dupliquées. De plus, il en résulte des tâches administratives supplémentaires sur les réseaux où les ordinateurs sont souvent déplacés d'un sous-réseau à l'autre. De même, lorsque vous devez modifier une valeur IP pour plusieurs clients, il vous faut mettre à jour la configuration IP de chaque client.

Lorsque vous configurez le serveur DHCP de manière à ce qu'il prenne en charge les clients DHCP, il fournit automatiquement les informations de configuration aux clients DHCP. Il s'assure également que les clients du réseau utilisent des informations de configuration exactes. En outre, si vous devez modifier les données de configuration IP de plusieurs clients, il suffit de modifier une seule fois le serveur DHCP pour que le protocole DHCP mette automatiquement à jour les informations de configuration des clients.

2. Comment le protocole DHCP alloue des adresses IP

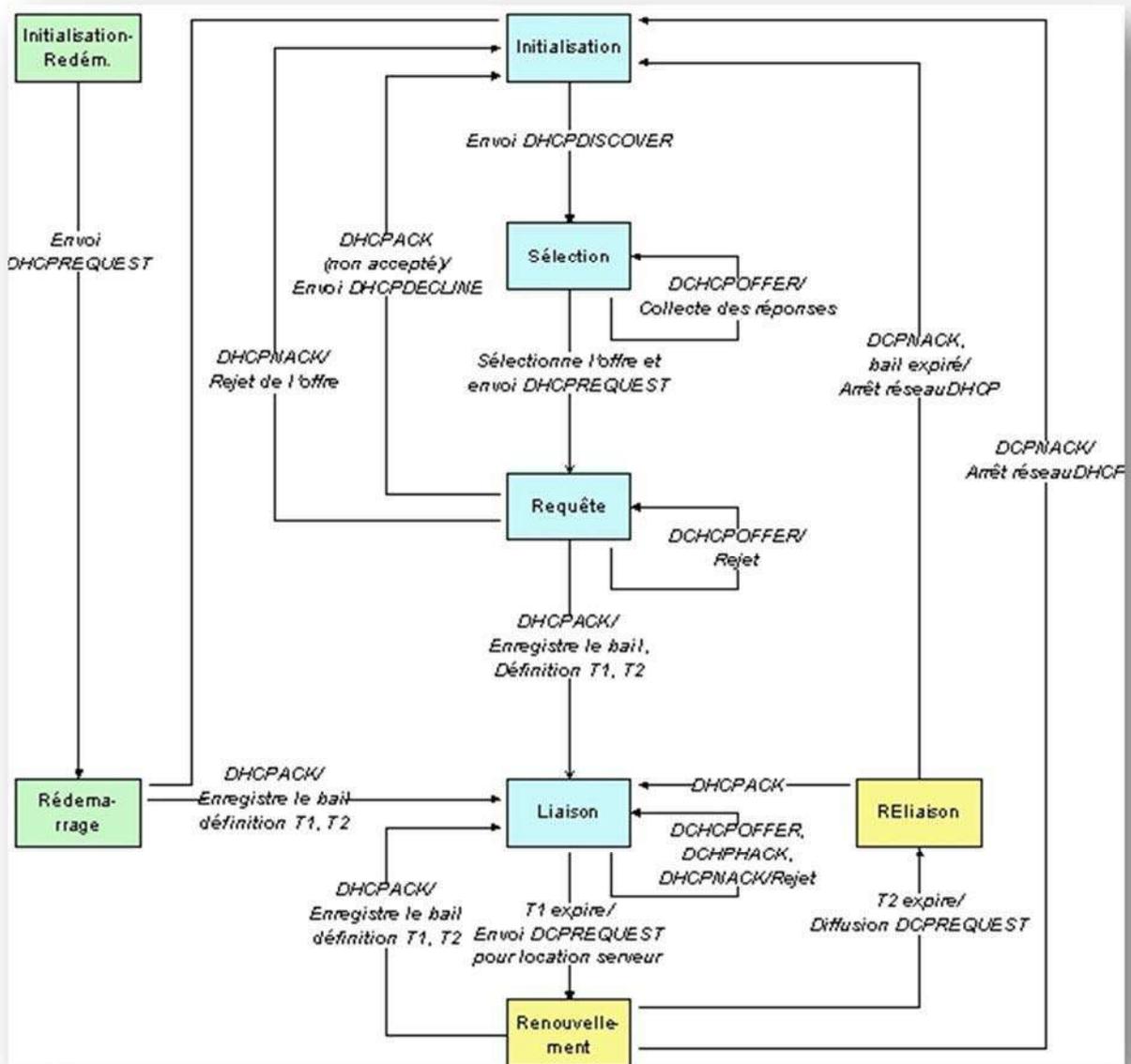
Le protocole DHCP gère l'attribution et la libération des données de configuration d'adresse IP en louant la configuration d'adresse IP au client.

Le bail DHCP spécifie la durée pendant laquelle le client peut utiliser les données de configuration IP avant de les restituer au serveur DHCP, puis de les renouveler. Le processus d'attribution des données de configuration d'adresse IP est appelé *processus de création d'un bail DHCP*. Le processus de renouvellement des données de configuration d'adresse IP est appelé *processus de renouvellement d'un bail DHCP*.

La première fois qu'un client DHCP est ajouté au réseau, il demande les données de configuration d'adresse IP au serveur DHCP. Lorsque celui-ci reçoit la requête du client, il sélectionne une adresse IP dans une plage d'adresses définies par l'administrateur dans son étendue. Il propose ces données de configuration d'adresse IP au client DHCP.

Si le client accepte l'offre, le serveur DHCP loue l'adresse IP au client pour une période donnée. Le client utilise ensuite ces données de configuration d'adresse IP pour accéder au réseau.

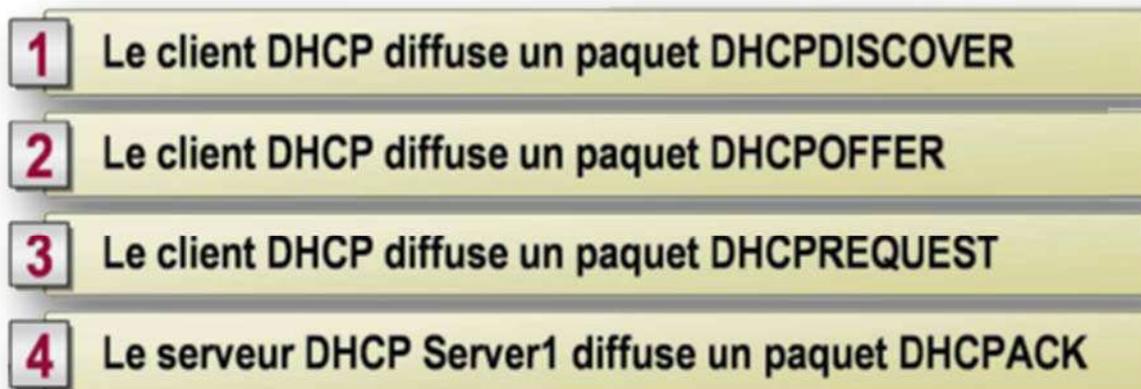
Voici le schéma proposé par la RFC 2131 :



3. Processus de création d'un bail DHCP

Le protocole DHCP utilise un processus en quatre étapes pour louer des informations d'adressage IP aux clients DHCP. Ces quatre étapes sont nommées en fonction des types de paquets DHCP.

1. Découverte DHCP
2. Offre DHCP
3. Requête DHCP
4. Accusé de réception DHCP ou accusé de réception DHCP négatif



Le *processus de création d'un bail DHCP* est le processus permettant au client DHCP de recevoir des données de configuration d'adresse IP du serveur DHCP.

Le client DHCP diffuse un paquet DHCPDISCOVER pour localiser un serveur DHCP. Un paquet DHCPDISCOVER est un message que les clients DHCP envoient lors de leur première tentative de connexion au réseau pour demander des informations d'adresse IP à un serveur DHCP.

Le processus de création d'un bail peut s'effectuer de deux manières : lorsqu'un ordinateur client démarre ou initialise le protocole TCP/IP pour la première fois, ou lorsqu'un client tente de renouveler son bail et que sa requête est refusée. (Par exemple, un client peut se voir refuser sa demande de renouvellement lorsque vous le déplacez vers un autre sous-réseau).

Le serveur DHCP diffuse un paquet DHCPOFFER au client. Un paquet DHCPOFFER est un message utilisé par les serveurs DHCP pour proposer le bail d'une adresse IP à un client DHCP lorsqu'il démarre sur le réseau.

Chaque serveur DHCP qui répond, réserve l'adresse IP proposée, pour ne pas la proposer à un autre client DHCP avant l'acceptation par le client en ayant fait la demande.

Si le client ne reçoit pas d'offre après quatre requêtes, il utilise une adresse IP de la plage réservée comprise entre 169.254.0.1 et 169.254.255.254. Ces adresses préconfigurées permettent de s'assurer que les clients d'un sous-réseau comportant un serveur DHCP non disponible puissent communiquer entre eux. Le client DHCP continue à rechercher un serveur DHCP disponible toutes les cinq minutes. Lorsqu'un serveur DHCP est enfin disponible, les clients reçoivent des adresses IP valides, ce qui leur permet de communiquer avec des hôtes internes ou externes à leur sous-réseau.

Le client DHCP diffuse un paquet DHCPREQUEST. Un paquet DHCPREQUEST est un message envoyé par un client au serveur DHCP pour demander ou renouveler le bail de son adresse IP.

Le client DHCP répond au premier paquet DHCPOFFER qu'il reçoit en diffusant un paquet DHCPREQUEST pour accepter l'offre. Ce paquet contient l'identification du serveur dont il a accepté l'offre. Tous les autres serveurs DHCP retirent alors leur offre et conservent leurs adresses IP pour d'autres demandes de bail IP.

Le serveur DHCP diffuse un paquet DHCPACK au client. Un paquet DHCPACK est un message envoyé par le serveur DHCP à un client pour accuser réception et répondre à sa requête de configuration de bail. Ce message contient un bail valide pour l'adresse IP, ainsi que d'autres données de configuration IP.

Lorsque le client DHCP reçoit l'accusé de réception, le protocole TCP/IP s'initialise avec les données de configuration IP fournies par le serveur DHCP.

Le client associe également le protocole TCP/IP aux services réseau et à la carte réseau, ce qui permet au client de communiquer sur le réseau.

Le serveur DHCP envoie un accusé de réception DHCP négatif (paquet DHCPNAK) si l'adresse IP offerte n'est plus valide ou si elle est utilisée par un autre ordinateur. Le client doit recommencer le processus de création de bail.

4. Processus de renouvellement d'un bail DHCP

Le processus de renouvellement d'un bail DHCP est le processus permettant au client DHCP de renouveler ou de mettre à jour ses données de configuration d'adresse IP à l'aide du serveur DHCP.

Le client DHCP renouvelle ses données de configuration IP avant l'expiration du bail. Si le bail expire avant leur renouvellement, ces données sont perdues et il doit recommencer le processus de création d'un bail DHCP.

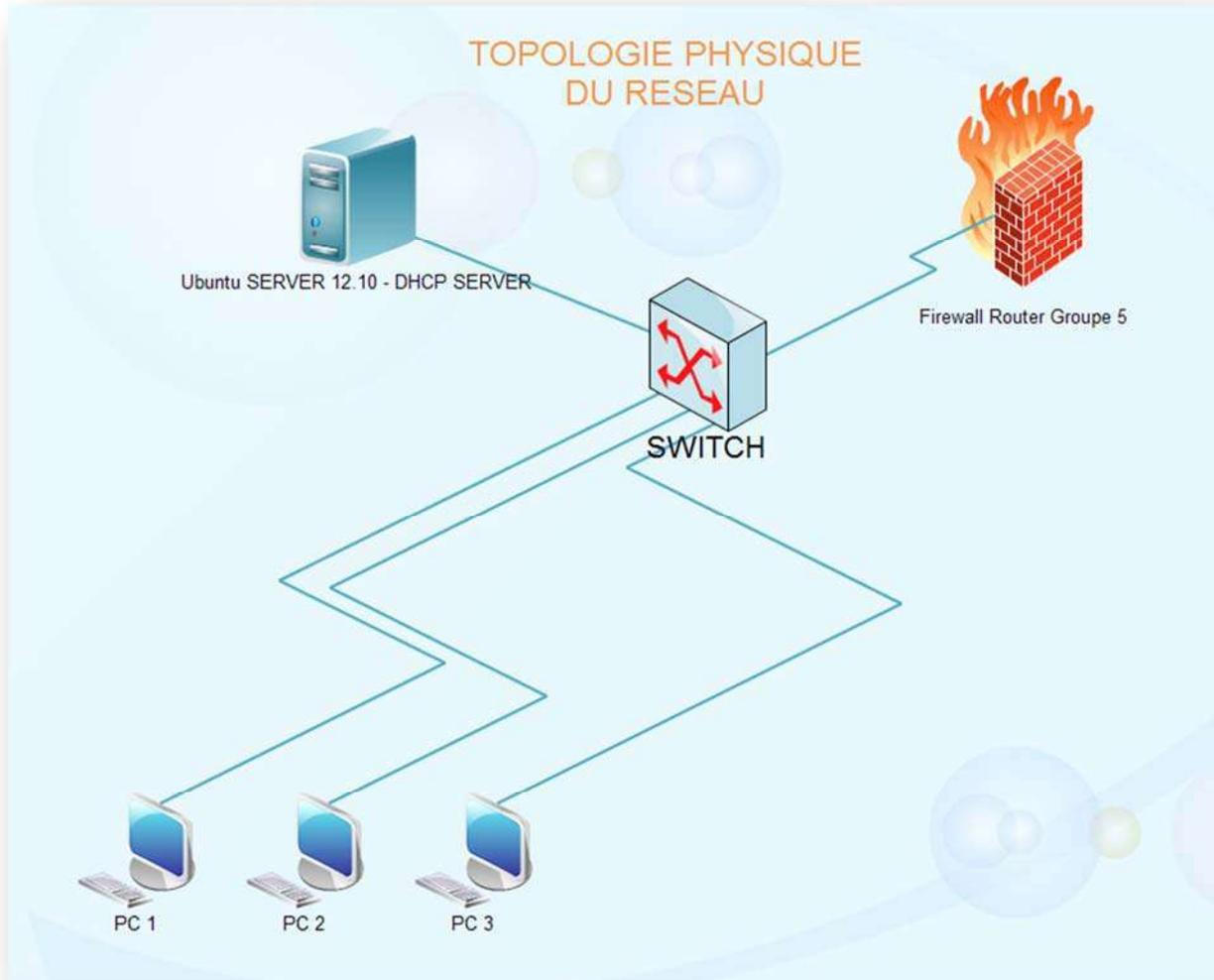
Un client DHCP tente automatiquement de renouveler son bail lorsque sa durée a expiré de 50%. Il essaie également de renouveler son bail d'adresse IP à chaque redémarrage de l'ordinateur. Pour renouveler un bail, le client DHCP envoie un paquet DHCPREQUEST directement au serveur DHCP par lequel il a obtenu le bail précédent.

Si le serveur DHCP est disponible, il renouvelle le bail et envoie au client un paquet DHCPACK contenant la durée du nouveau bail et les paramètres de configuration mis à jour. Le client met à jour sa configuration lorsqu'il reçoit l'accusé de réception. Si le serveur DHCP n'est pas disponible, le client continue à utiliser ses paramètres de configuration en cours.

Si le client DHCP ne parvient pas à renouveler son bail la première fois, il diffuse un paquet DHCPDISCOVER pour mettre à jour son bail d'adresse lorsque 87,5 % de sa durée actuelle a expiré. À ce stade, le client DHCP accepte un bail émis par n'importe quel serveur DHCP.

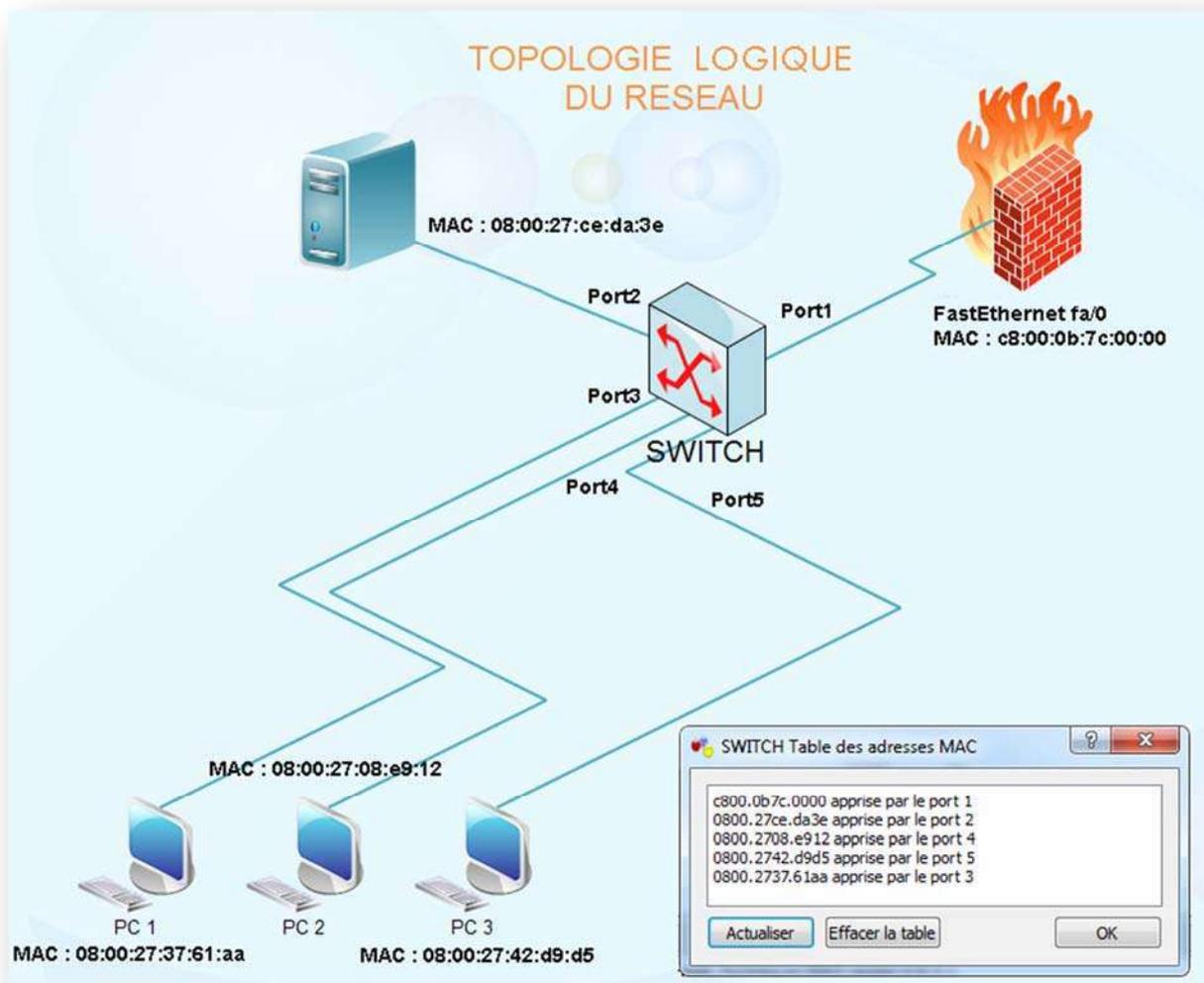
Installation du serveur DHCP et configuration

1. Topologie Physique et logique du réseau



Nous disposons de 4 postes :

- 1 sera configuré comme SERVEUR DHCP
- 3 Clients



2. Installation du serveur DHCP

Sous Debian (Ubuntu), cela s'effectue très simplement en installant le paquetage dhcp3-server.

- Effectuer une mise à jour des paquetages disponibles en mode terminal :

```
root@ubuntu:~# apt-get update
Ign http://fr.archive.ubuntu.com quantal InRelease
Ign http://security.ubuntu.com quantal-security InRelease
Ign http://fr.archive.ubuntu.com quantal-updates InRelease
Atteint http://security.ubuntu.com quantal-security Release.gpg
Lecture des listes de paquets... Fait

root@ubuntu:~# apt-get upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été conservés :
  linux-headers-generic linux-image-generic
Les paquets suivants seront mis à jour :
  apport apt apt-transport-https apt-utils base-files bind9 bind9-doc
  bind9-host bind9utils busybox-initramfs busybox-static coreutils curl
  dnsutils gnupg gpgv kvm libapt-inst1.5 libapt-pkg4.12 libbind9-80
  libboost-iostreams1.49.0 libcurl3 libcurl3-gnutls libdns81 libglib2.0-0
  libgnutls26 libisc83 libisccc80 libiscfg82 liblwres80 libnspr4 libnss3
  libpq5 libvirt-bin libvirt0 libwhoopsie0 libxenstore3.0 libxml2
  libxml2-utils linux-generic lsb-base lsb-release memtest86+ mountall perl
  perl-base perl-modules postfix postgresql-9.1 postgresql-client-9.1
  postgresql-contrib-9.1 postgresql-doc-9.1 python3-apport python3-dbus
  python3-distupgrade python3-gi python3-problem-report python3-update-manager
  python3.2 python3.2-minimal qemu-common qemu-kvm qemu-utils
  ubuntu-release-upgrader-core ufw update-manager-core vim vim-common
  vim-runtime vim-tiny whoopsie
71 mis à jour, 0 nouvellement installés, 0 à enlever et 2 non mis à jour.
Il est nécessaire de prendre 50,8 Mo dans les archives.
Après cette opération, 269 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer [O/n] ?
```

- Vérifier que le paquetage existe bien :

```
root@ubuntu:~# apt-cache search isc-dhcp-server
isc-dhcp-server - ISC DHCP server for automatic IP address assignment
isc-dhcp-server-dbg - ISC DHCP server for automatic IP address assignment (debug
)
isc-dhcp-server-ldap - DHCP server able to use LDAP as backend
tcos-configurator - PyGTK tool to configure some needed services to get a TCOS s
erver
```


Administration Réseau sous Ubuntu SERVER 12.10-Serveur DHCP

Une fois que vous avez choisi l'interface que votre serveur DHCP doit écouter il faut éditer le fichier **dhcpd.conf** qui englobe la configuration de votre serveur.

Dans notre exemple , nous utiliserons les informations de pré configurations suivantes :

- un masque de sous réseau à 255.255.255.0
- une adresse de multi-diffusion à 172.25.205.255
- une adresse de routeur/passerelle à 172.25.205.254
- Le serveur DHCP assignera au client une adresse IP comprise entre 172.25.205.10 et 172.25.205.20
- l'adresse Ip du serveur DHCP sera statique et sera 172.25.205.250

Configuration de l'adresse du serveur dans le fichier **"/etc/network/interfaces"**

Editer le fichier **"/etc/network/interfaces"** avec l'éditeur **"vi"**

```
root@Ubuntu-SERVER-64:~# vi /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
    address 172.25.205.250
    netmask 255.255.255.0
    dns-nameservers 192.168.0.254
```

Dns-nameservers est la passerelle de l'ordinateur hôte dans notre cas (le serveur étant une machine virtuelle sous **VirtualBox**)

Explication des options utilisées :

default-lease-time

Le default-lease-time est la temps en secondes de la validité de la location de l'adresse à moins que le client ne le demande différemment.

max-lease-time

Le max-lease-time est le temps maximum en secondes pendant lequel la location sera assignée.

authoritative

Avec le paramètre "authoritative", le serveur DHCP enverra des messages de DHCPNAK aux clients qui ont obtenu l'adresse d'un serveur légitime de DHCP. Le serveur de DHCP supposera normalement que les informations de configuration sur un segment de réseau donné ne sont pas connues pour être correctes et ne sont pas bien fondées. Ceci signifie que si, par accident ou quelque chose, un autre serveur de DHCP est sur le réseau sans l'autorisation nécessaire, il n'annoncera pas des messages de DHCPNAK aux clients et les clients ne seront pas mis à jour avec des faux baux.

subnet x.x.x.x netmask x.x.x.x

Le paramètre de sous-réseau est employé pour fournir au serveur assez d'information pour indiquer si un IP ADDRESS est sur ce sous-réseau. Il peut également être employé pour fournir des paramètres spécifiques de sous-réseau et pour indiquer quelles adresses peuvent être dynamiquement assignées aux clients étant sur ce sous-réseau. De telles adresses sont indiquées en utilisant la déclaration de range d'adresse.

range

Ceci définit les adresses IP à employer pour le dhcp. Les IP doivent être sur le même sous-réseau que défini dans la déclaration de sous-réseau.

routers

C'est une option à employer qui indique quel passerelle/routeur les clients doivent employer.

```
root@ubuntu:~# vi /etc/dhcp/dhcpd.conf_ ←
#
# Sample configuration file for ISC dhcpd for Debian
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
#
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
#option domain-name "ghost.fr";
#option domain-name-servers ns1.ghost.fr;

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 local?;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

subnet 172.25.205.0 netmask 255.255.255.0 {
  range 172.25.205.10 172.25.205.20;
  option broadcast-address 172.25.205.255;
  option routers 172.25.205.254;
}

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

#subnet 10.254.239.0 netmask 255.255.255.224 {
#  range 10.254.239.10 10.254.239.20;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
-- INSERTION --
```

Administration Réseau sous Ubuntu SERVER 12.10-Serveur DHCP

Notez qu'il vous est aussi possible d'attribuer un adressage IP spécifique à une adresse MAC d'une machine pour cela il suffit d'ajouter ces lignes dans le fichier dhcpd.conf :

```
host « le nom de la machine » {  
    hardware ethernet « adresse mac de la machine »;  
    fixed-address « adresse ip fixe »;  
}
```

Une fois la configuration du serveur finie, redémarrer celui-ci et lancer le service DHCP avec la commande :

```
root@ubuntu:/# service isc-dhcp-server start  
start: Job is already running: isc-dhcp-server  
root@ubuntu:/# _
```

Vérifions si notre serveur DHCP est opérationnel à l'aide de la commande "ps" qui permet d'afficher les processus en cours.

```
root@ubuntu:/# ps -ef | grep dhcpd  
dhcpd    1043    1  0 09:51 ?        00:00:00 dhcpd -user dhcpd -group dhcpd -  
f -q -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf eth1  
root     2246    2007  0 18:00 tty1    00:00:00 grep --color=auto dhcpd  
root@ubuntu:/# _
```

En cas de problème de configuration ou d'erreurs diverses, la consultation du fichier "syslog" permettra d'examiner les erreurs éventuelles.

```
root@ubuntu:/# cat /var/log/syslog ou vi /var/log/syslog
```

La commande "netstat" permettra de connaître les connexions TCP actives sur le serveur et ainsi de lister l'ensemble des ports TCP et UDP ouverts sur l'ordinateur.

5. Configuration des clients

Ubuntu

Par défaut l'attribution des adresses IP est configurée en DHCP sur les clients.
Pour en être sûr il faudra vérifier le fichier “ /etc/network/interfaces “

```
# la ligne qui suit représente la boucle locale
auto lo
iface lo inet loopback

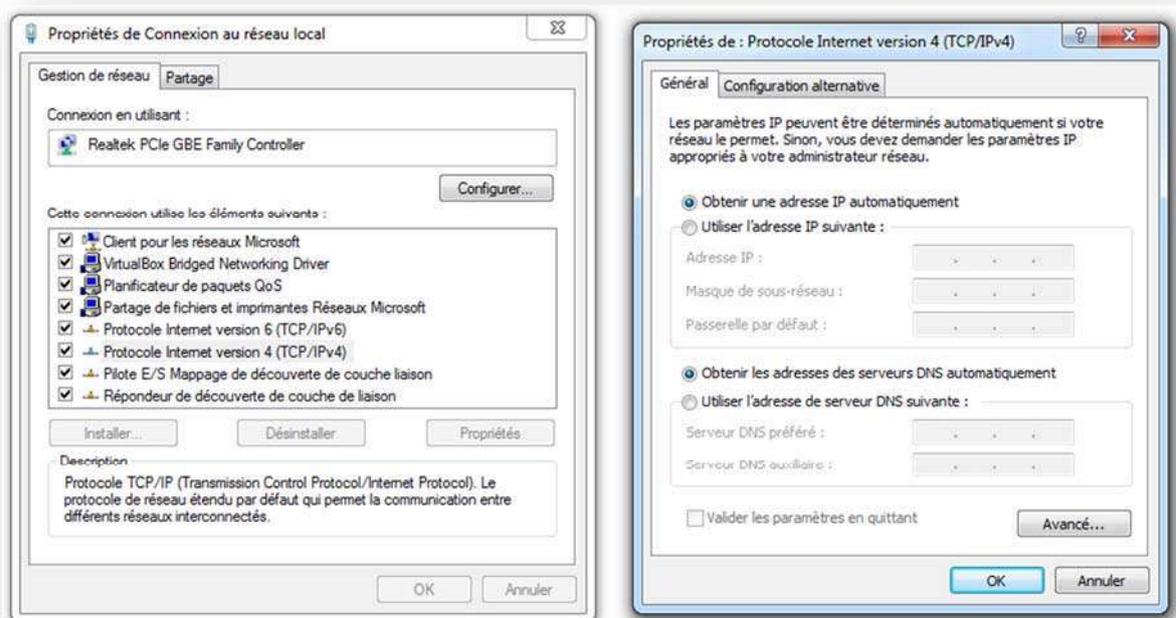
# la ligne qui suit indique que l'adressage de l'interface
# "eth1" est en mode dhcp
auto eth1
iface eth1 inet dhcp

# en mode static la ligne de commande serait la suivante
# iface eth1 inet static
#     address xxx.xxx.xxx.xxx
#     netmask xxx.xxx.xxx.xxx
```

Windows NT4/2000/XP/7

La configuration se fait dans le panneau de configuration, icône réseau, onglet protocoles de la carte réseau, puis propriétés de TCP/IPv4.

Ici, vous devez indiquer que la carte doit recevoir une adresse IP dynamiquement.



Mise en œuvre et exploration des Trames avec le logiciel Wireshark

Vérification du bon adressage du SERVEUR DHCP à l'aide de la commande ifconfig

```
eth1    Link encap:Ethernet  HWaddr 08:00:27:ce:da:3e
        inet adr:172.25.205.250  Bcast:172.25.205.255  Masque:255.255.255.0
        adr inet6: fe80::a00:27ff:fece:da3e/64 Scope:Lien
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        Packets reçus:0 erreurs:0 :0 overruns:0 frame:0
        TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:1000
        Octets reçus:0 (0.0 B) Octets transmis:468 (468.0 B)

lo      Link encap:Boucle locale
        inet adr:127.0.0.1  Masque:255.0.0.0
        adr inet6: ::1/128 Scope:Hôte
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        Packets reçus:31 erreurs:0 :0 overruns:0 frame:0
        TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:0
        Octets reçus:16385 (16.3 KB) Octets transmis:16385 (16.3 KB)
```

1. Mise en route du Poste 1

Après démarrage complet du poste 1 , effectuer la commande “ifconfig“ en mode terminal.

```
eth1    Link encap:Ethernet  HWaddr 08:00:27:37:61:aa
        inet adr:172.25.205.10  Bcast:172.25.205.255  Masque:255.255.255.0
        adr inet6: fe80::a00:27ff:fe37:61aa/64 Scope:Lien
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        Packets reçus:20 erreurs:0 :0 overruns:0 frame:0
        TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:1000
        Octets reçus:2610 (2.6 KB) Octets transmis:17496 (17.4 KB)

lo      Link encap:Boucle locale
        inet adr:127.0.0.1  Masque:255.0.0.0
        adr inet6: ::1/128 Scope:Hôte
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        Packets reçus:120 erreurs:0 :0 overruns:0 frame:0
        TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 lg file transmission:0
        Octets reçus:10197 (10.1 KB) Octets transmis:10197 (10.1 KB)
```

Nous pouvons vérifier que notre poste a bien une adresse IP correspondant à la plage programmée au niveau du serveur DHCP : 172.25.205.10

Relevons maintenant l'adresse MAC de notre interface "eth1" du poste 1 : 08:00:27:37:61:aa

2. Analyse des trames avec le logiciel WIRESHARK

Nous allons maintenant analyser les trames enregistrées par Wireshark correspondant aux requêtes DHCP.

Au niveau du serveur , nous relevons 4 lignes importantes notées 1-2-3-4:

No.	Time	Source	Destination	Protocol	Length	Info
100	205.712594	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
101	205.990269	fe80::a00:27ff:fe37:61aa	ff02::fb	MDNS	415	Standard query response TXT, cache flush AAAA, c
102	206.075919	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xd7ae2450
103	207.279159	fe80::a00:27ff:fe37:61aa	ff02::fb	MDNS	383	Standard query response PTR _udisks-ssh_tcp.loc
104	208.006434	fe80::a00:27ff:fe37:61aa	ff02::fb	MDNS	415	Standard query response TXT, cache flush AAAA, c
105	208.213129	fe80::a00:27ff:fe37:61aa	ff02::2	ICMPV6	70	Router Solicitation from 08:00:27:37:61:aa
106	208.721416	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
107	209.720500	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
108	210.720675	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
109	212.221674	fe80::a00:27ff:fe37:61aa	ff02::2	ICMPV6	70	Router Solicitation from 08:00:27:37:61:aa
110	212.649702	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xd7ae2450
111	213.727697	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
112	214.109914	fe80::a00:27ff:fe37:61aa	ff02::16	ICMPV6	90	Multicast Listener Report Message v2
113	214.724707	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
114	215.724800	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
115	218.733754	CadmusCo_ce:da:3e	Broadcast	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
1	116	219.465697	0.0.0.0	DHCP	342	DHCP Discover - Transaction ID 0xd7ae2450
2	117	219.732340	CadmusCo_ce:da:3e	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
2	118	220.732449	CadmusCo_ce:da:3e	ARP	60	who has 172.25.205.254? Tell 172.25.205.250
3	119	223.738891	172.25.205.250	DHCP	342	DHCP Offer - Transaction ID 0xd7ae2450
3	120	223.739230	172.25.205.250	DHCP	342	DHCP offer - Transaction ID 0xd7ae2450
3	121	223.739449	172.25.205.250	DHCP	342	DHCP offer - Transaction ID 0xd7ae2450
3	122	223.739774	172.25.205.250	DHCP	342	DHCP offer - Transaction ID 0xd7ae2450
4	123	223.739990	0.0.0.0	DHCP	342	DHCP Request - Transaction ID 0xd7ae2450
4	124	223.742668	172.25.205.250	DHCP	342	DHCP ACK - Transaction ID 0xd7ae2450

Details for Frame 116:

- Frame 116: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
- Ethernet II, Src: CadmusCo_37:61:aa (08:00:27:37:61:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: CadmusCo_37:61:aa (08:00:27:37:61:aa)
 - Type: IP (0x0800)
- Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x10 (DSCP 0x04: unknown DSCP; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 - Total Length: 328
 - Identification: 0x0000 (0)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: UDP (17)
 - Header checksum: 0x3996 [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)
- Bootstrap Protocol

1 – A la ligne 116 de la capture Wireshark nous notons une découverte DHCP ou **DHCP Discover** : le Client envoie une trame de diffusion MAC (avec l'adresse 08:00:27:37:61:aa) sur le réseau, lui permettant de localiser les serveurs DHCP présents sur le réseau sur le (port DP 67 ou serveur BOOTP).

2 – A la ligne 119 , le serveur DHCP avec l'adresse IP 172.25.205.250 envoie une offre DHCP (**DHCP OFFER**)



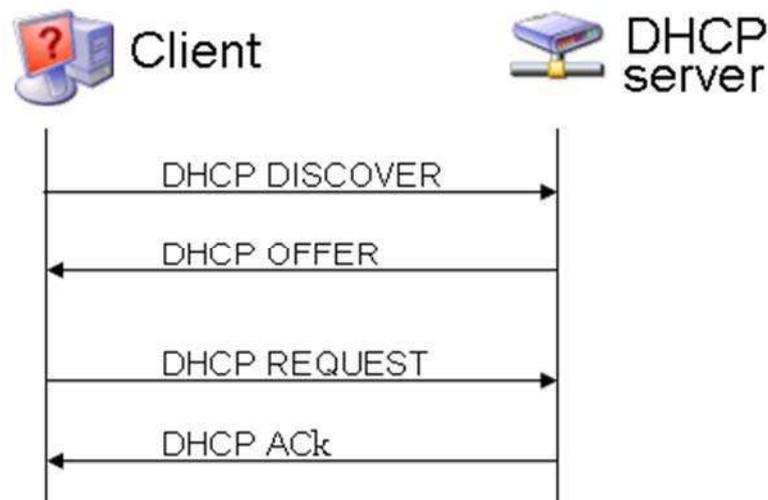
Administration Réseau sous Ubuntu SERVER 12.10-Serveur DHCP

3 – A la ligne 123 , le poste répond **DHCP REQUEST** qui va lui d’obtenir de la part du serveur DHCP une adresse IP.

4 – A la ligne 124 , le client reçoit enfin un **DHCP ACK** : acquittement qui est un signal logique indiquant que la demande d’adresse IP a bien été prise en compte et lui fournit l’adresse IP **172.25.205.10**

```
Frame 124: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: CadmusCo_ce:da:3e (08:00:27:ce:da:3e), Dst: CadmusCo_37:61:aa (08:00:27:37:61:aa)
  Destination: CadmusCo_37:61:aa (08:00:27:37:61:aa)
  Source: CadmusCo_ce:da:3e (08:00:27:ce:da:3e)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 172.25.205.250 (172.25.205.250), Dst: 172.25.205.10 (172.25.205.10)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x10 (DSCP 0x04: Unknown DSCP; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 328
  Identification: 0x0000 (0)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x465d [correct]
  Source: 172.25.205.250 (172.25.205.250)
  Destination: 172.25.205.10 (172.25.205.10)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
```

Nous retrouvons donc bien le processus DHCP au complet décrit ci-dessous :



Pour une meilleure compréhension de la procédure DHCP, examinons en détail le protocole Bootstarp

DHCP DISCOVER :

```
[-] Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xd7ae2450
  Seconds elapsed: 10
  [+ Bootp flags: 0x0000 (Unicast)
  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 MAC address: CadmusCo_37:61:aa (08:00:27:37:61:aa)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  [+ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  [+ Option: (t=50,l=4) Requested IP Address = 172.25.205.10
  [+ Option: (t=12,l=26) Host Name = "francoisbernier-VirtualBox"
  [+ Option: (t=55,l=13) Parameter Request List
  End option
  Padding
```

Nous constatons que :

- La demande provient bien de l'adresse MAC **08 :00 :27 :37 :61 :aa**
- Que le type de message DHCP est bien un DHCP DISCOVER
- Et nous retrouvons le nom d'hôte du client "francoisbernier-Virtualbox"

DHCP OFFER :

```
[-] Bootstrap Protocol
  Message type: Boot Reply (2)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xd7ae2450
  Seconds elapsed: 0
  [+ Bootp flags: 0x0000 (unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 172.25.205.10 (172.25.205.10)
  Next server IP address: 172.25.205.250 (172.25.205.250)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: cadmusCo_37:61:aa (08:00:27:37:61:aa)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  [+ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  [+ Option: (t=54,l=4) DHCP Server Identifier = 172.25.205.250
  [+ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  [+ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  [+ Option: (t=28,l=4) Broadcast Address = 172.25.205.255
  [+ Option: (t=3,l=4) Router = 172.25.205.254
  [+ Option: (t=15,l=8) Domain Name = "ghost.fr"
  End Option
  Padding
```

Nous constatons dans cette partie :

- Le serveur DHCP **172.25.205.250** offre une adresse **172.25.205.10** au client **0.0.0.0**
- Que le type de message DHCP est bien un DHCP OFFER
- Et nous retrouvons en détail tous les paramètres de notre réseau configurés dans le fichier `/etc/dhcp/dhcpd.conf` du **serveur DHCP**

DHCP REQUEST :

```
[-] Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xd7ae2450
  Seconds elapsed: 17
  [-] Bootp flags: 0x0000 (unicast)
  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 MAC address: CadmusCo_37:61:aa (08:00:27:37:61:aa)
  Client hardware address padding: 00000000000000000000
  server host name not given
  Boot file name not given
  Magic cookie: DHCP
  [-] Option: (t=53,l=1) DHCP Message Type = DHCP Request
    option: (53) DHCP Message Type
    Length: 1
    value: 03
  [-] Option: (t=54,l=4) DHCP Server Identifier = 172.25.205.250
    option: (54) DHCP Server Identifier
    Length: 4
    value: ac19cdfa
  [-] Option: (t=50,l=4) Requested IP Address = 172.25.205.10
    option: (50) Requested IP Address
    Length: 4
    value: ac19cd0a
  [-] Option: (t=12,l=26) Host Name = "francoisbernier-virtualBox"
    option: (12) Host Name
    Length: 26
    value: 6672616e636f69736265726e6965722d566972747475616c42...
  [-] Option: (t=55,l=13) Parameter Request List
  End option
  Padding
```

Nous constatons dans cette partie :

- Que le type de message DHCP est bien un DHCP REQUEST
- Provenant du serveur DHCP 172.25.205.250
- Demandant l'adresse IP 172.25.205.10 par le nom d'Hôte "francoisbernier-Virtualbox" ayant l'adresse MAC 08 :00 :27 :37 :61 :aa

DHCP ACK :

```
⊞ Frame 124: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: CadmusCo_ce:da:3e (08:00:27:ce:da:3e), Dst: CadmusCo_37:61:aa (08:00:27:37:61:aa)
⊞ Internet Protocol Version 4, Src: 172.25.205.250 (172.25.205.250), Dst: 172.25.205.10 (172.25.205.10)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
  Source port: bootps (67)
  Destination port: bootpc (68)
  Length: 308
  ⊞ Checksum: 0x56fc [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  ⊞ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd7ae2450
    Seconds elapsed: 17
    ⊞ Bootp flags: 0x0000 (unicast)
      Client IP address: 0.0.0.0 (0.0.0.0)
      Your (client) IP address: 172.25.205.10 (172.25.205.10)
      Next server IP address: 172.25.205.250 (172.25.205.250)
      Relay agent IP address: 0.0.0.0 (0.0.0.0)
      Client MAC address: CadmusCo_37:61:aa (08:00:27:37:61:aa)
      Client hardware address padding: 00000000000000000000
      Server host name not given
      Boot file name not given
      Magic cookie: DHCP
    ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
    ⊞ Option: (t=54,l=4) DHCP Server Identifier = 172.25.205.250
    ⊞ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
    ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
    ⊞ Option: (t=28,l=4) Broadcast Address = 172.25.205.255
    ⊞ Option: (t=3,l=4) Router = 172.25.205.254
    ⊞ Option: (t=15,l=8) Domain Name = "ghost.fr"
    End option
    Padding
```

Voici donc notre dernière trame N° 124 vue précédemment.

Nous constatons dans cette partie :

- Que le type de message DHCP est bien un DHCP ACK
- A destination du serveur DHCP **172.25.205.250**
- Délivrant l'adresse **IP 172.25.205.10** au client ayant l'adresse MAC **08 :00 :27 :37 :61 :aa**
- Pour un bail de 10 min (600sec configuré sur le serveur : default-lease-time 600)
- Sur le réseau configuré au niveau du serveur DHCP

3. Mise en route du Poste 2

```
59 79.676577 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request - Transaction ID
60 79.676619 172.25.205.250 172.25.205.11 DHCP 342 DHCP Offer - Transaction ID
61 79.677149 172.25.205.250 172.25.205.11 DHCP 342 DHCP Offer - Transaction ID
62 79.681329 172.25.205.250 172.25.205.11 DHCP 342 DHCP ACK - Transaction ID
63 79.744878 172.25.205.11 224.0.0.22 ICMP 54 v2 Membership Report / Join ...

* Frame 62: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
* Ethernet II, Src: CadmusCo_ce:da:3e (08:00:27:ce:da:3e), Dst: cadmusCo_42:d9:d5 (08:00:27:42:d9:d5)
* Internet Protocol Version 4, Src: 172.25.205.250 (172.25.205.250), Dst: 172.25.205.11 (172.25.205.11)
* User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
* Bootstrap Protocol
  Message type: Boot Reply (2)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xd2fac27e
  Seconds elapsed: 17
  * Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 172.25.205.11 (172.25.205.11)
  Next server IP address: 172.25.205.250 (172.25.205.250)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: CadmusCo_42:d9:d5 (08:00:27:42:d9:d5)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  * Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  * Option: (t=54,l=4) DHCP Server Identifier = 172.25.205.250
  * Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  * Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  * Option: (t=28,l=4) Broadcast Address = 172.25.205.255
  * Option: (t=3,l=4) Router = 172.25.205.254
  * Option: (t=15,l=8) Domain Name = "ghost.fr"
  End option
  Padding
```

Nous constatons dans cette partie :

- La présence des 3 requêtes DHCP (DHCP REQUEST – DHCP OFFER – DHCP ACK)
- A destination du serveur DHCP **172.25.205.250**
- Délivrant l'adresse IP **172.25.205.11** au client ayant l'adresse MAC **08 :00 :27 :42:d9 :d5**
- Pour un bail de 10 min (600sec configuré sur le serveur : default-lease-time 600)
- Sur le réseau configuré au niveau du serveur DHCP

Notre serveur DHCP fonctionne donc correctement.

4. Pour aller plus loin....

DHCP RELEASE

Lorsqu'un client quitte le réseau, il envoie une requête DHCP RELEASE au serveur lui ayant attribué son adresse IP, lui notifiant qu'il libère l'adresse réseau et annule le bail

```
775 1567.90680 172.25.205.10 172.25.205.250 DHCP 342 DHCP Release - Transaction ID 0xdb6d7a11
Ethernet II, Src: CadmusCo_37:61:aa (08:00:27:37:61:aa), Dst: CadmusCo_ce:da:3e (08:00:27:ce:da:3e)
Internet Protocol Version 4, Src: 172.25.205.10 (172.25.205.10), Dst: 172.25.205.250 (172.25.205.250)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xdb6d7a11
  Seconds elapsed: 0
  Bootp flags: 0x0000 (unicast)
  Client IP address: 172.25.205.10 (172.25.205.10)
  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 MAC address: CadmusCo_37:61:aa (08:00:27:37:61:aa)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Release
  Option: (t=54,l=4) DHCP Server Identifier = 172.25.205.250
  Option: (t=12,l=26) Host Name = "francoisbernier-virtualBox"
  End option
  Padding
```

Nous constatons dans cette partie :

- Que le type de message DHCP est bien un DHCP RELEASE
- A destination du serveur DHCP **172.25.205.250**
- Provenant du client avec l'adresse IP **172.25.205.10** et l'adresse MAC **08 :00 :27 :37 :61 :aa**

Il peut arriver que cette adresse ne soit pas libérée et subsiste avec un bail au niveau du serveur DHCP (ex :à cause d'un plantage du client).

Le serveur stocke les baux attribués dans le fichier “ /var/lib/dhcp/dhcpd.leases “.

On y retrouve des informations essentielles comme l'adresse IP distribuée à une adresse MAC, le nom de la machine qui a fait cette demande DHCP, l'heure de début et de fin du bail...

Au cas ou le serveur DHCP n'attribuerait plus les adresses dans l'ordre et sauterait une certaine adresse , il faudra alors modifier manuellement ce fichier et supprimer les valeurs correspondant à cette adresse .



Explications :

Le serveur DHCP conserve une base de données persistante des concessions attribuées. Cette base de données est un fichier texte ASCII sans contraintes de forme contenant une série de déclarations de concessions. Chaque fois qu'une concession est attribuée, renouvelée ou libérée, sa nouvelle valeur est enregistrée à la fin du fichier des concessions. Aussi si plus d'une déclaration apparaît pour une concession donnée, la dernière valeur du fichier est la valeur courante.

Quand DHCPD est installé pour la première fois, il n'y a pas de base de données de concessions. Cependant, DHCPD requiert une base de données de concessions pour démarrer. Pour créer la base de données des concessions initiales, il convient de créer simplement un fichier vide de nom `“/var/lib/dhcp/dhcpd.leases“`.

Pour éviter que la base de données ne devienne trop grande, le fichier est réécrit de temps en temps. Premièrement, une base de données temporaire de concessions est créée et toutes les concessions connues sont écrites dedans. Puis la vieille base de données est renommée `“/var/lib/dhcp/dhcpd.leases~“` et finalement la nouvelle base de données la remplace.

Il y a une fenêtre de vulnérabilité quand le processus dhcpd est tué ou si le système plante. Après que la vieille base de données a été renommée mais avant que la nouvelle n'ait été déplacée à sa place, il n'y aura pas de fichier `“/var/lib/dhcp/dhcpd.leases“`.

Dans ce cas DHCPD, refusera de démarrer et nécessitera une intervention manuelle. **IL NE FAUT PAS** se contenter de créer un nouveau fichier de concessions, sinon vous perdrez la trace des concessions attribuées et ce sera le chaos.

À la place, renommez `/var/lib/dhcp/dhcpd.leases~` en `“/var/lib/dhcp/dhcpd.leases“`, pour restaurer l'ancien fichier de concessions et redémarrez DHCPD. Ceci garantit qu'un fichier de concessions valide sera restauré.

Voici un aperçu du fichier que vous pouvez afficher et modifier avec la commande :

→ Vi /var/lib/dhcp/dhcp.leases

```
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.2.4

lease 172.25.205.10 {
  starts 6 2013/02/16 17:46:44;
  ends 6 2013/02/16 17:56:44;
  tstp 6 2013/02/16 17:56:44;
  cltt 6 2013/02/16 17:46:44;
  binding state free;
  hardware ethernet 08:00:27:37:61:aa;
}
lease 172.25.205.11 {
  starts 6 2013/02/16 17:48:00;
  ends 6 2013/02/16 17:58:00;
  tstp 6 2013/02/16 17:58:00;
  cltt 6 2013/02/16 17:48:00;
  binding state free;
  hardware ethernet 08:00:27:42:d9:d5;
}
server-uid "\000\001\000\001\030\2627\252\010\000'\316\332>";

lease 172.25.205.10 {
  starts 6 2013/02/16 18:15:18;
  ends 6 2013/02/16 18:25:18;
  cltt 6 2013/02/16 18:15:18;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:37:61:aa;
}
"/var/lib/dhcp/dhcpd.leases" 143L, 4035C 2,1 Haut
```

Il faudra également supprimer les fichiers de baux situés sur le client dans le répertoire :

→ Vi /var/lib/dhcp/

```
francoisbernier@francoisbernier-VirtualBox:~$ ls /var/lib/dhcp/
dhclient-aae2729c-90eb-4846-a305-f5cef02c222a-eth0.lease temp
dhclient.eth1.leases
francoisbernier@francoisbernier-VirtualBox:~$
```

5. Conclusion

Nous avons vu l'installation et la configuration d'un serveur DHCP sous Ubuntu SERVER. Le protocole DHCP représente un avantage majeur dans la configuration des réseaux, en simplifiant la tâche administrative de distribution des adresse IP.

De plus ISC-DHCP-SERVER permet de configurer rapidement et facilement un serveur DHCP tout en proposant une gamme de paramètres qui se veut très complète.