

DHCP - DNS

Master 2 I2L

Année 2009/2010

D. Duvivier

LIL – Université du Littoral Côte d’Opale
duvivier@lil.univ-littoral.fr

1 Préparer son serveur

```
aptitude update
aptitude upgrade
aptitude clean
```

Attention : Comme pour l'installation d'apache, protégez en mode 700 /root, \$home et /usr/src/...

2 Installer DHCP

```
aptitude install dhcp3-server
```

Lors de l'installation, un message d'erreur apparaît ! C'est normal car votre serveur DHCP n'est pas encore configuré (vérifiez les messages d'erreur dans /var/log/syslog). Nous allons le configurer :

```
cp /etc/dhcp3/dhcpd.conf /etc/dhcp3/dhcpd.conf.orig
emacs /etc/dhcp3/dhcpd.conf
```

Pour la suite du document, utilisez le dernier champ de votre adresse IP (utilisez ifconfig si vous avez oublié) pour créer chacun un sous réseau différent. Par exemple, si votre adresse IP est 192.168.22.88 alors, dans toute la suite du document, il faut remplacer **partout** 172.16.0 par 172.16.88.

Pour éviter les « frautes de fappe », basez-vous sur un exemple de configuration déjà présent (et commenté) dans le fichier dhcpd.conf initial. Sur ma version du fichier, l'exemple du sous-réseau 10.5.5.0 est un bon point de départ. Déclarez votre sous-réseau après les options globales. Le fichier /etc/dhcp3/dhcpd.conf sera modifié de manière à contenir les lignes suivantes :

```
# En début de fichier, hors d'une paire d'accolades sont situées
# les options globales (applicables par défaut à tous les sous-réseaux
# Pas d'update DNS
ddns-update-style none;
# On donne le nom du domaine
option domain-name "m2i2l.org";
# Quels sont les DNS par défaut (option globale) :
# mettez les DNS utilisés lors du premier TP si vous voulez
# en séparant leurs adresses IP par une virgule
# ici je mets juste « mon » DNS
option domain-name-servers 172.16.0.1;
# Définition globale de la durée mini/maxi du bail
default-lease-time 600;
max-lease-time 7200;
# Si ce serveur fait autorité (= seul serveur officiel sur le réseau)
# alors décommentez la ligne suivante, s'il existe plusieurs serveurs
# dhcp ne décommentez pas :
#authoritative
# On définit notre sous réseau et le masque réseau associé
subnet 172.16.0.0 netmask 255.255.255.0 {
# Plage d'adresses disponibles pour les clients
# conseil : évitez les adresses terminées par 0, 1, 254 et 255 :-) !
    range 172.16.0.2 172.16.0.253;
# Ici c'est le serveur de nom, le serveur privé,
# il faut aussi mettre le/les DNS
    option domain-name-servers 172.16.0.1;
# On donne le nom du domaine (inutile si c'est le nom global)
# option domain-name "m2i2l.org";
# Les clients auront cette adresse comme passerelle par défaut
    option routers 172.16.0.1;
```

```
# Et l'adresse utilisée pour la diffusion
# Attention à ne pas vous tromper en calculant le broadcast :
option broadcast-address 172.16.0.255
# Le bail a une durée 3600s par défaut, soit 1H
default-lease-time 3600;
# On le laisse avec un maximum de 12H
max-lease-time 43200;
# SURTOUT N'OUBLIEZ PAR L'ACCOLADE CI-DESSOUS :
}
```

Remarque : au niveau du sous-réseau 172.16.0.0 il est possible de ne pas spécifier l'adresse de passerelle si elle a été définie globalement :

```
# Définition du réseau : 172.16.0.0 et de son masque
subnet 172.16.0.0 netmask 255.255.255.0 {
# La plage d'adresses disponibles pour les clients
range 172.16.0.4 172.16.0.253;
# Et l'adresse utilisée pour la diffusion
option broadcast-address 172.16.0.255;
}
```

Il faut ensuite indiquer sur quelle(s) interface(s) réseau le serveur dhcp est actif en éditant le fichier /etc/default/dhcp3-server :

```
cp /etc/default/dhcp3-server /etc/default/dhcp3-server.orig
emacs /etc/default/dhcp3-server
```

Sur ma configuration, je veux que le serveur dhcp réponde sur l'interface réseau eth0, donc je l'indique dans le fichier /etc/default/dhcp3-server :

```
INTERFACES= "eth0"
```

Le problème c'est que sur vos configuration, vous disposez d'une seule carte réseau accessible via eth0 ! Donc si vous installez le serveur dhcp sur eth0, dites adieu à l'accès au réseau ! Pour éviter cela nous allons utiliser une interface virtuelle « eth0:0 ». Il serait tout à fait possible d'en définir plusieurs (eth0:0, eth0:1, eth0:2, ...). Sur votre configuration, je veux que le serveur dhcp réponde sur l'interface réseau virtuelle eth0:0, pourtant j'indique ceci dans le fichier /etc/default/dhcp3-server :

```
INTERFACES= "eth0"
```

ATTENTION : C'est bien eth0 qu'il faut indiquer ci-dessus et non eth0:0 sinon vous obtenez un message du genre « No subnet declaration for eth0:0 (0.0.0.0) » dans /var/log/syslog et le serveur dhcp est stoppé !

Pour tester, il est possible d'activer temporairement l'interface eth0:0 si cela n'est pas déjà fait automatiquement au démarrage. Sur votre configuration, cela donne la commande suivante :

```
ifconfig eth0:0 172.16.0.1 netmask 255.255.255.0
ifconfig
```

Vous voyez normalement apparaître eth0 et eth0:0. Pour « stopper » cette interface (en cas d'erreur ou de problème), si elle n'a pas été démarrée automatiquement via ifup (cf. ci-dessous) :

```
ifconfig eth0:0 down
ifconfig
```

Sur ma configuration, je dois simplement remplacer eth0:0 par eth0 (car je n'ai pas besoin d'interface réseau virtuelle puisque ma machine possède plusieurs cartes réseau et un seul réseau sur chaque carte).

Si l'interface a été démarrée automatiquement via ifup, il faut utiliser la commande ifdown (cf. man).

Pour effectuer ça de manière durable et utiliser les commandes « de plus haut niveau » ifup et ifdown, il faut modifier le fichier /etc/network/interfaces :

```
cp /etc/network/interfaces /etc/network/interfaces.orig
emacs /etc/network/interfaces &
```

Sur ma configuration moi le fichier /etc/network/interfaces a cet aspect après modification :

```
auto lo eth0
iface lo inet loopback
allow-hotplug eth2
iface eth2 inet dhcp
iface eth0 inet static
    address 172.16.0.1
    netmask 255.255.255.0
```

La première ligne indique les interfaces (lo et eth0) à lancer au boot (via /etc/rcS.d/S15networking qui invoque ifup -a). La connexion de la machine via dhcp à ma « XXBox » gentiment louée auprès de mon provider ☺ se fera plus tard via eth2 lors du boot (via dhcp). La seconde ligne configure le loopback. Les lignes 3 et 4 configurent l'interface eth2 pour une connexion via dhcp (à ma XXBox). Les trois dernières lignes font la même chose que la commande ifconfig invoquée ci-dessus en configurant l'interface eth0 avec une adresse ip fixe (172.16.0.1) et un masque réseau (255.255.255.0).

Si vous devez manipuler des adresses IPv6, vous pouvez installer le paquet ipv6calc.

Sur votre configuration, le fichier /etc/network/interfaces doit avoir cet aspect après modification :

```
auto lo eth0:0
iface lo inet loopback
allow-hotplug eth0
iface eth0 inet dhcp
iface eth0:0 inet static
    address 172.16.0.1
    netmask 255.255.255.0
```

La première ligne indique l'interface (lo) à lancer au boot. La connexion à eth0 se fait en dhcp sur ma machine. En salle machine cela peut varier si vous avez une adresse IP fixe sur eth0. En ce cas, ne changez rien pour eth0, ajoutez simplement ce qui concerne eth0:0. A noter que les puristes utiliseront plutôt cette syntaxe (on configure une interface à la fois) :

```
auto lo
iface lo inet loopback
allow-hotplug eth0
iface eth0 inet dhcp
auto eth0:0
iface eth0:0 inet static
    address 172.16.0.1
    netmask 255.255.255.0
```

On active l'interface (→ elle sera automatiquement activée pour les prochains redémarrages) :

```
ifup eth0:0
ifconfig
```

Sur ma configuration, je dois simplement remplacer eth0:0 par eth0. Notez que l'adresse MAC est bien la même pour eth0 et eth0:0 !

Remarque : évitez de mixer les commandes ifup, ifdown avec la commande ifconfig car cette dernière commande est une commande de bas niveau (appelée par ifup et ifdown) ; elle ne met pas à jour certains fichiers utilisés par ifup et ifdown.

On redémarre le serveur dhcp :

```
/etc/init.d/dhcp3-server restart
```

Remarque : il est possible de le faire via une commande kill et le signal SIGHUP.

Les commandes suivantes donnent des indications précieuses sur la « santé » de votre serveur DHCP :

```
/etc/init.d/dhcp3-server status  
tail -50 /var/log/syslog  
cat /var/lib/dhcp3/dhcpd.leases
```

C'est terminé côté serveur DHCP, mais pas du côté client : si le client était déjà actif avant la mise en service du serveur DHCP, il n'a pas récupéré d'adresse IP auprès de votre serveur... [Sur ma machine cliente, l'interface utilisée est eth1, il suffit de lancer la commande suivante pour tester :](#)

```
dhclient3 eth1
```

Sur vos machines, si nous supposons que l'interface utilisée est eth0, il suffit de lancer la commande suivante pour tester :

```
dhclient3 eth0
```

Vous obtenez un certain nombre d'informations : requêtes (DHCPDISCOVER, DHCPOFFER, DHCPREQUEST et DHCPACK) puis informations sur l'adresse IP obtenue et le bail associé → Ça marche !

Il reste à ajouter une route vers le nouveau réseau :

```
route add -net 172.16.0.0 netmask 255.255.255.0 gw 172.16.0.1
```

Comme précédemment ceci n'est qu'un test temporaire et le client ne tentera pas de connexion automatique en dhcp sauf si cela est indiqué dans le fichier /etc/network/interfaces. [Sur ma machine client \(ddrouter\), ce fichier a cet aspect \(après éventuelle modification\) :](#)

```
auto lo  
iface lo inet loopback  
allow-hotplug eth0 eth1  
iface eth0 inet dhcp  
iface eth1 inet dhcp
```

Pensez à ajouter le nom et l'adresse IP et le nom de votre (futur?) serveur de noms dans /etc/hosts selon le format suivant :

```
<IP> [<nom_complet_avec_domaine>] <alias>
```

Lancez la commande « route », puis ajoutez votre [sous-]réseau dans /etc/networks selon le format suivant (par exemple IP_du_sous_reseau = 172.16.0.0, ce qui permet d'utiliser le nom du sous-réseau dans les commandes route & cie :

```
<nom_sous_reseau> <IP_du_sous_reseau>
```

Vous pouvez ensuite relancer la commande « route ».

Si vous utilisez simultanément des adresses « définies localement » (via /etc/hosts) et un serveur de nom, il faut préciser au système la manière de « résoudre » les adresses IP en fonction des noms. Pour cela il faut indiquer les deux lignes suivantes dans le fichier /etc/host.conf (« multi on » permet d'autoriser plusieurs adresses IP pour un même nom de machine dans /etc/hosts ; enlevez le mot clef « bind » si vous n'utilisez pas de serveur de noms) :

```
order hosts,bind  
multi on
```

Pensez à ajouter le nom et l'adresse IP et le nom de votre (futur?) serveur de noms dans /etc/resolv.conf, attention, ceci est un exemple d'un extrait de ce fichier (il n'est pas nécessairement complet) :

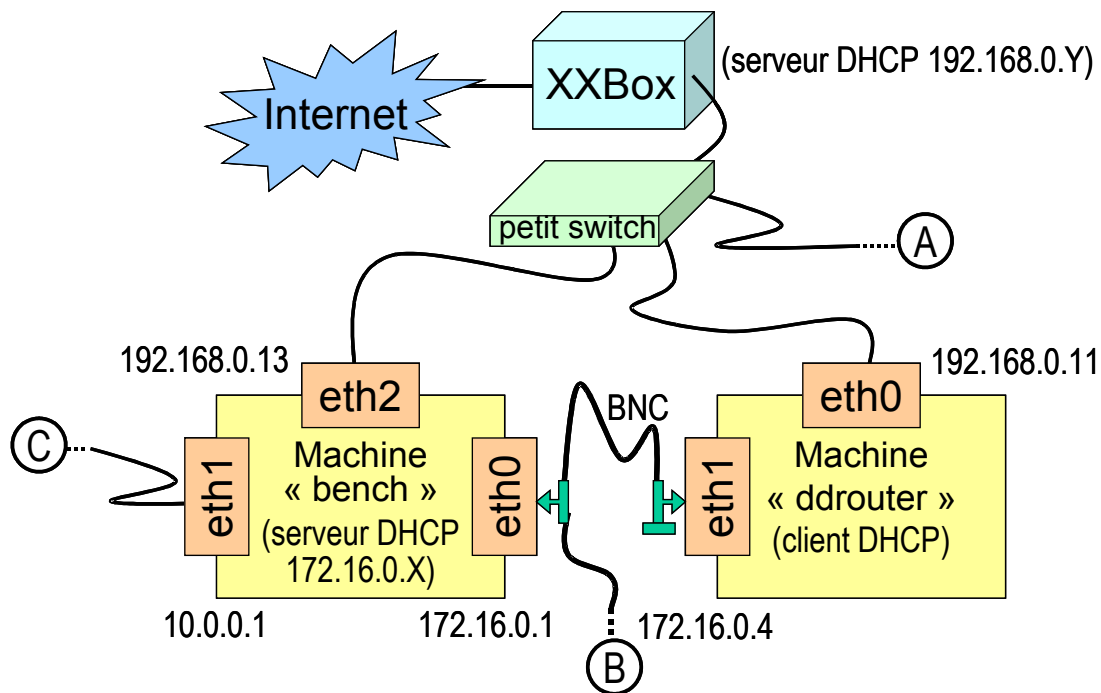
```
domain m2i21.org  
search m2i21.org  
nameserver 172.16.0.1
```

ATTENTION : ceci se fait via la commande « resolvconf »

Pour la suite du TP, il peut être « intéressant » de regarder les options du genre « gateway », « dns-nameservers », « dns-search » et de les ajouter au fichier /etc/network/interfaces (?). [Voici un exemple « bidon »](#) :

```
iface eth0 inet static
    address 192.168.3.3
    netmask 255.255.255.0
    gateway 192.168.3.1
    dns-nameservers 192.168.3.45 192.168.3.10
    dns-search foo.org bar.com
```

Chez-moi, la configuration de test est la suivante :



3 Quelques outils autour de DHCP...

```
aptitude install dhcping dhcpdump
```

Ceci installe les outils dhcping, dhcpdump et tcpdump → **A ne pas mettre entre toutes les mains !!!**

Exemple : testez « dhcpdump -i eth0 » sur le serveur DHCP pendant la connexion d'un client au serveur DHCP !

Pour les accros aux interfaces graphiques ☹ :

```
aptitude install wireshark
```

Installe un outil de monitoring réseau (il y en a bien d'autres).

Il existe d'autres outils, vérifiez notamment avec la commande :

```
apt-cache search ^dhcp
```

ou

```
aptitude search ^dhcp
```

4 Recherche de paquets en vue d'installer un DNS

Il existe plusieurs variantes de serveurs DNS (pdns/powerDNS, bind...).

Vous pouvez jeter un œil aux paquets suivants : bind9, bind9-doc, bindgraph, bind9utils

Question : nous souhaitons vérifier de quel paquet provient « nslookup », où il est installé et où est la page du manuel (man) correspondante, comment faire :

```
dpkg-query --search nslookup
```

Vérifiez si c'est installé et installez le paquet correspondant sinon (dnsutils a priori). Il est également possible d'installer le paquet dlocate pour accélérer et améliorer ce genre de « recherche », mais ceci ajoute une tâche journalière (/etc/cron.daily/dlocate) et une base de données contenant la liste des paquets installés. Nous installons le paquet dlocate et nous forçons la rotation des journaux et la création de la base en lançant la commande « logrotate » :

```
aptitude install dlocate
/usr/sbin/logrotate -vf /etc/logrotate.conf
dlocate -S nslookup
```

Pour simplement connaître le paquet relatif à une commande, il suffit parfois d'utiliser apt-cache search :

```
apt-cache search nslookup
```

Indique « dnsutils »

Par contre, la commande suivante :

```
apt-cache search ^bind
```

Donne une liste de réponses parmi lesquelles bind9, bind9-doc, bind9utils, bindgraph...

En revanche, avec les commandes « dig » ou « host » cela fonctionne beaucoup moins bien ☹ !!!

Si la commande cherchée (dig, host ou ...) est installée, on retrouve les informations (paquet auquel appartient la commande...) en se rappelant qu'elle est forcément précédée de « / » et apparaît en fin de ligne, à l'aide des commandes suivantes :

```
dpkg-query --search dig | grep '/dig$'
dpkg-query --search host | grep '/host$'
```

Remarque : il existe d'autres commandes et des interfaces graphiques pour faire ça, je sais ☺ !

Si elles ne sont pas installées, on peut ajouter des mots-clés lors de la recherche via apt-cache search sachant que l'on demande à ce que tous les mots indiqués apparaissent dans la réponse :

```
apt-cache search dig dns lookup
```

Là c'est beaucoup mieux !

Le paquet apt-file et la commande du même nom peuvent également aider :

```
aptitude install apt-file
apt-file update
```

Puis :

```
apt-file --search dig | grep '/dig$'
```

Voilà, nous avons la liste des paquets à installer via les commandes suivantes :

```
aptitude clean
aptitude update
aptitude upgrade
aptitude install bind9 bind9-doc bind9utils bindgraph dnsutils
```

5 Installer un DNS

Comme dans le cours, il est possible de jouer un peu avec la commande `nslookup`, en mode interactif, il suffit de taper la commande suivante (attention au « . » en fin de certaines commandes/adresses) :

```
nslookup
```

Nous passons en mode interactif avec un prompt « > », il suffit de tester les commandes vues en cours (je n'indique pas les réponses aux différentes commandes, à vous de tester sur votre configuration...

```
> server
... retourne le ou les DNS par défaut ...
> server g.root-servers.net
... voir le cours ...
> set q=ns
> fr.
... voir le cours ...
> server e.ext.nic.fr
... voir le cours ...
> univ-reunion.fr.
... voir le cours ...
exit
```

Exemple en mode non interactif (*cf.* cours) :

```
nslookup www.univ-littoral.fr
```

Nous obtenons le nom réel de la machine qui fait office de serveur DNS, son adresse IP et les alias.

Pour les autres manipulations de `nslookup`, voir le cours...

Les fichiers de configurations sont dans le répertoire `/etc/bind`. Il faut tout particulièrement étudier le fichier `/etc/bind/named.conf.options` pour les options et le fichier `/etc/bind/named.conf` pour « le reste ».