Chapitre IV : Services
Partie II : services réseau d'infrastructure

Eric Leclercq

Département IEM
http://ufrsciencestech.u-bourgogne.fr
http://ludique.u-bourgogne.fr/~leclercq

5 mars 2018

Plan du chapitre

Aperçu du protocole DHCP

- Le service DHCP (*Dynamic Host Configuration Protocol*) est un système qui permet d'attribuer dynamiquement une adresse IP à un poste qui se connecte au réseau
- Le serveur DHCP fournit également d'autres informations comme la passerelle par défaut et les serveurs DNS etc.

Dialogue C/S

Le dialogue entre le client et le serveur est décrit de la manière suivante :
1) Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau, il envoie donc une trame `DHCPDISCOVER`, destinée à trouver un serveur DHCP.

- Cette trame est un broadcast. N'ayant pas encore d'adresse IP, il utilise provisoirement l'adresse 0.0.0.0.
- Ce n'est pas avec cette adresse que le DHCP va pouvoir l'identifier, il fournit donc aussi sa *MAC Address* ;

Dialogue C/S

2) Le ou les serveurs DHCP du réseau qui vont recevoir cette trame vont répondre par un `DHCPOFFER`.

- Cette trame, elle aussi en broadcast car il n'est pas encore possible d'atteindre le client qui n'a pas encore d'adresse IP valide.
- Elle contient une proposition de bail et la *MAC Address* du client, avec également l'adresse IP du serveur. Tous les DHCP répondent et le client normalement accepte la première réponse venue ;

Dialogue C/S

3) Le client répond ensuite par un `DHCPREQUEST` toujours en broadcast (donc à tous les serveurs) pour indiquer quelle offre il accepte ;

4) Le serveur DHCP Concerné répond définitivement par un `DHCPACK` qui constitue une confirmation du bail.

L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

Principe du bail

- Un serveur DHCP dispose d'une plage d'adresses à distribuer aux clients. Il tient à jour une table des adresses déjà utilisées et utilisées récement.
- Lorsqu'il attribue une adresse, il le fait par l'intermédiaire d'un bail. Ce bail a normalement une durée limitée dans le temps.
- Sur un réseau d'entreprise où l'on dispose largement d'assez d'adresses pour le nombre de postes et que ces derniers sont en service toute la journée, le bail peut être d'une semaine ou plus encore.
- En pratique, il est recommandé de ne pas créer de baux inutilement courts, ceci entraînant une augmentation significative du broadcast sur le réseau. Le compromis est à trouver entre la durée moyenne de connexion des utilisateurs, la réserve d'adresses IP du serveur, le nombre d'abonnés.

Principe du bail

- Après expiration du bail, ou résiliation par le client, les informations concernant ce bail restent mémorisées dans les tables du serveur pendant un certain temps. Bien que l'adresse IP soit disponible, elle ne sera pas attribuée en priorité à une autre machine. C'est ce qui explique que l'on retrouve souvent la même adresse d'une session à l'autre.
- Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration comme :
  - l'adresse d'un ou de plusieurs DNS (résolution de noms) ;
  - l'adresse de la passerelle par défaut ;
  - l'adresse du serveur DHCP.

Principe du bail

- Lorsque le bail arrive à la moitié de son temps de vie, le client va essayer de renouveler ce bail, cette fois-ci en s'adressant directement au serveur qui le lui a attribué.
- Il n'y aura alors qu'une requête DHCPREQUEST et un DHCPACK.
- Si, au bout des 7/8èmes de la durée de vie du bail en cours, ce dernier n'a pu être renouvelé, le client essayera d'obtenir un nouveau bail auprès d'un DHCP quelconque qui voudra bien lui répondre.
- Il est alors possible que le client change d'adresse IP en cours de session. Normalement, cette situation ne devrait pas se produire, sauf en cas de panne du DHCP.

Packages

Sur Linux Redhat l'installation se fait via le package `dhcpcd-1.3.18pl8-13` ou supérieur. Il y a un seul fichier de configuration : `/etc/dhcpd.conf`.
Il y a deux choses essentielles à configurer :

- la réserve d'adresses dont le serveur pourra disposer pour les attribuer aux clients
- les paramètres optionnels à leur communiquer, comme l'adresse d'un DNS et de la passerelle par défaut.

Il est possible de définir des options globales, qui seront les mêmes pour tous les clients du DHCP, tous sous réseaux confondus et des options propres à chaque sous réseau, celles-ci écrasant les options globales, en cas de conflit.

Exemple

- nous avons un seul réseau, avec des IP choisies dans la classe C privée `10.X.Y.0`, donc avec un masque `255.255.255.0` ;
- nous avons une passerelle par défaut pour tous nos hôtes du réseau, dans l'exemple, ce sera `10.X.Y.1` ;
- nous disposons d'un DNS, unique pour tous les hôtes du réseau, `80.10.246.1` ;
- sur la totalité de la classe C disponible, nous allons réserver les adresses comprises entre `10.X.Y.101` et `10.X.Y.199` pour les clients du réseau. Cette plage constituera la réserve d'adresses que le DHCP pourra fournir aux clients ;
- la durée de vie du bail que le DHCP va attribuer aux clients. Dans l'exemple, nous utiliserons environ 2 heures.

Configuration du serveur NFS

```
default-lease-time 6000;
max-lease-time 72000;
option subnet-mask 255.255.255.0;
option broadcast-address 10.21.19.255;
option routers 10.21.19.1;
option domain-name-servers 80.10.246.1;

subnet 10.21.19.0 netmask 255.255.255.0 {
# range 10.21.19.100 10.21.19.120;
}

host epn-0101 {
      hardware ethernet 00:C0:A8:F4:8B:56;
      fixed-address 10.21.19.101;
      option host-name "poste-0101";
    }
host epn-0102 {
      hardware ethernet 00:C0:A8:F4:9C:11;
      fixed-address 10.21.19.102;
      option host-name "poste-0102";
    }
```

- L'option `domain-name-servers` sert à attribuer aux hôtes une adresse de DNS.
- L'option `domain-name` est optionnelle, elle permet aux clients de savoir dans quel domaine ils sont enregistrés.
- L'option `routers` permet de définir la passerelle par défaut.

Améliorations

- le daemon DHCPd écoute par défaut sur toutes les interfaces réseau actives sur le serveur. Ce n'est pas forcément souhaitable.
- Ce comportement par défaut peut être modifié, non pas dans le fichier de configuration mais dans le script de démarrage.
- Il faut utiliser un paramètre dans la ligne de commande qui va démarrer DHCPd.
- Généralement il faut éditer le script `/etc/sysconfig/dhcpd` et il faut spécifier le nom de la ou des interfaces qui doivent êtres écoutées. Dans notre cas, nous aurons par exemple : `INTERFACES="eth1";`

Améliorations

- il est également possible de ne pas répondre aux clients dont on ne connait pas l'adresse MAC : `deny unknown clients;` ;
- l'historique requêtes DHCP et les messages d'erreur ou d'avertissement sont enregistrés dans `/var/log/messages`. Il est possible de modifier ne fichier de log afin de ne pas le remplir inutilement :
  - dans dhcpd.conf, ajouter la ligne `log-facility dhcpd;`
  - dans `syslog.conf`, ajouter `dhcpd.* /var/log/dhcpd.log`

Fichiers coté client

Utiliser l'interface graphique ou le fichier de configuration pour indiquer au client de se configurer via dhcp (`/etc/sysconfig/network-scripts/ifcfg-eth0` sous RedHat).

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

Modifier le fichier `/etc/network/interfaces` sur les distribution Debian.

Partage de fichiers via NFS

- Le protocole NFS (Network File System) est utilisé à l'intérieur d'un réseau local pour partager les systèmes fichiers entre machines
- Il repose sur UDP et les services RPC
- NFS est développé principalement dans le monde UNIX (NFS v3, NFS v4)
- Serveurs dédiés (*Appliance*)
- Reproches en terme de sécurité et de performances
- Néanmoins des évolutions utilisant du chiffrement (NFS v4 ?)
- Il existe des concurrents AFS par exemple

Configuration du serveur NFS

- Il faut d'abord s'assurer que le service nfs est lancé : `/etc/init.d/nfsd start`. Vérifier aussi qu'il est activé dans les services démarrant au boot (utilitaire `setup` sous les distribution type RedHat).
- Éditer le fichier `/etc/exports` et définir les partages.

```
/home    10.21.7.101(rw) 10.21.7.102(rw) 10.21.7.103(rw)
```

- La commande `exportfs` permet de lister les répertoire partagés, l'option `-a` remet à jour les exportation en cas de changement.
- **Attention :** écrire la liste des machines sur une même ligne, ne pas mettre d'espace avant les parenthèses (risque de se retrouver avec un partage valable pour toute machine de l'internet)

Options de partage

- `ro` : n'autorise que des requêtes en lecture-seule sur ce volume NFS. Le comportement par défaut autorise également les requêtes en écriture, ce que l'on peut également mentionner explicitement en utilisant l'option rw.
- `async` : consulter la documentation de J. Procaccia pour une étude des optimisations `http://www.int-evry.fr/s2ia/user/procacci/Doc/NFS/nfs.pdf`
- `root_squash/no_root_squash` : transforme les requêtes de couple UID/GID 0 (c-à-d root) en UID/GID anonymes (`nobody` par exemple). Ceci ne s'applique pas aux autres couples UID/GID sensibles comme bin.

NFS Client

- Sur les clients NFS il suffit juste de modifier le fichier `/etc/fstab` pour monter un répertoire partagé.

```
10.21.7.1:/home      /home      nfs      defaults 0 0
```

- La commande `mount` suivie du point de montage permet de tester la validité de la ligne ajoutée. Le fichier `fstab` sera relu et exécuté complètement au reboot de la machine.
- Les autres options de montage s'appliquent : `noexec`, `nosuid`

Services NIS (1/2)

- NIS signifie Network Information Service
- Utilise des tables (version binaire indéxée des principaux fichiers de configuration)
- Repose sur une notion de domaine (différent du nom de domaine Internet)
- Propose de mécanismes de redondance (serveur escalves)
- Un service RPC nommé `ypserv` est utilisé en conjonction de `portmap` pour distribuer les tables des comptes utilisateur ainsi que d'autres information (sensibles) à n'importe quel machine connectée au domaine NIS.

Services NIS (2/2)

- Un serveur NIS comprend les services suivants :
  - `/usr/sbin/rpc.yppasswdd` pour permettre aux utilisateur de changer leur mot de passe ;
  - `/usr/sbin/yppush` pour propager les tables à des serveurs NIS esclaves ;
  - `/usr/sbin/rpc.ypxfrd` pour transferer les tables au travers du réseau ;
  - `/usr/sbin/ypserv` pour l'authentification.
- Sur les clients NIS, le service symétrique de `ypserv` est `ypbind`.

Configuration du serveur

- Éditer le fichier `/var/yp/securenets` et ajouter les réseaux concernes.
- Le service NIS répond, par défaut, à toutes les requêtes.
- Le paramétrage des éléments de `/var/yp/securenets` se fait sous la forme de couples netmask/network comme par exemple :

  ```
  255.255.255.0 192.168.0.0
  ```

- Cette technique ne peut pas protéger d'attaques de type IP spoofing mais permet déjà une protection simple.

Configuration du serveur

- Éditer le fichier `/etc/sysconfig/network`, il doit contenir la ligne : `NISDOMAIN=mondom`.
- Éditer le fichier `/etc/yp.conf`, il doit contenir la ligne : `domain mondom server localhost` afin de permettre au serveur d'être son propre client.
- Initialiser le domaine NIS : `/usr/lib/yp/ypinit -m`
- Le serveur est intialisé et lancé par : `/etc/init.d/ypserv start`

Configuration du serveur

- Pour créer des utilisateur, il suffit de créer un utilisateur traditionnel et de demander la mise à jour des tables NIS à partir du fichier `/etc/passwd`.
- Si il existe des esclaves il faut forcer make a pousser les tables NIS sur les escalve. Pour cela mettre la ligne `NOPUSH=FALSE` dans le fichier `/var/yp/make`

```
useradd -g user utili
passwd utili
cd /var/yp
make
```

Configuration d'un client

- Éditer le fichier `/etc/sysconfig/network`, il doit contenir la ligne : `NISDOMAIN=nomdom`.
- Éditer le fichier `/etc/yp.conf`, il doit contenir la ligne : `domain nomdom server 194.206.63.99`
- Sur le client les services portmap, ypbind et yppasswd doivent être lancés.
- Remarque : afin de faciliter l'administration des postes client et de les rendre indépendant du serveur NIS, il est possible d'utiliser l'option `broadcast` pour demander une recherche d'un serveur NIS dans le réseau.

Initialisation (ré-) d'un serveur NIS esclave

L'(ré)initialisation d'un serveur NIS suit les étapes :

1. éditer le fichier `/etc/yp.conf` fixer l'adresse du serveur principal (le poste ne doit plus être son propore client) : `domain nomdom server 194.206.63.99`
2. arrêter les services :

```
/etc/init.d/ypbind stop
/etc/init.d/ypserv stop
```

3. effacer les tables : `rm -r /var/yp/nomdom`
4. relancer les services :

```
/etc/init.d/ypbind start
/etc/init.d/ypserv start
```

5. rappatrier les tables depuis le serveur NIS maître et initialiser le serveur NIS escalve :

```
cd /usr/lib/yp/
./ypinit -s nomdom
```

6. ensuite rechanger `/etc/yp.conf` afin que le serveur escalve soit son propre client : `domain nomdom server localhost`