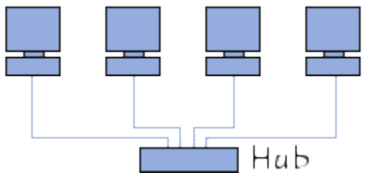
Formation réseau pour tous [Samedi 4 Juin 2005]

1. Le TCP/IP

a. Le principe

Pour créer un réseau local en **RJ45** (type de cables), il faut adopter une structure dite "en étoile", dans laquelle les ordinateurs sont chacun connecté au hub/switch (collecteur) par l'intermédiaire d'un câble RJ45. Un hub/switch est un boîtier auquel on connecte chacun des PC et qui se charge d'acheminer les données d'un PC à un autre. Le choix du hub/switch se fera donc en fonction du nombre d'ordinateurs connectés afin d'avoir assez de prises sur celui-ci.
La structure d'un tel réseau ressemble à ceci:



b. Les adresses

Sur Internet, chaque ordinateur doit avoir sa propre adresse, il existe donc un organisme, l'INTERNIC, qui est chargé d'allouer des adresses IP aux ordinateurs qui sont connectés sur Internet.

Si votre réseau n'est pas connecté à Internet vous pouvez mettre les adresses IP que vous désirez aux ordinateurs du réseau local.

Si votre réseau est connecté à Internet (c'est généralement pour cette raison que l'on installe le protocole TCP/IP sur un réseau local), il existe des adresses réservées par l'INTERNIC, c'est-à-dire des adresses que vous pouvez utiliser à loisir sur votre réseau local car elles ne seront pas prises en compte par les routeurs sur Internet et ne gêneront donc personne.

Il s'agit des adresses suivantes:

- **10.0.0.0 à 10.255.255.255 sous-masque : 255.0.0.0**
- **172.16.0.0** à **172.31.255.255 sous-masque : 255.255.0.0**
- **192.168.0.1** à **192.168.255.255 sous-masque : 255.255.0.0**

Les ordinateurs sont donc identifiés par une adresse TCPIP, ainsi que par une adresse MAC (identifiant unique de la carte réseau). Afin de trouver une machine sur un réseau, il faut donc son adresse IP, ou avoir un serveur de nom (DNS) qui, comme son nom l'indique, fournis les IP des machines en fonction d'un nom. Cela s'appelle la résolution de nom de domaine. Ces serveurs DNS doivent être renseigné auprès de votre machine, afin que celle-ci puisse contacter le serveur de noms en cas de besoin.

Exemple : host www.google.fr retourne l'IP du serveur www.google.fr

c. Mise en pratique

Installation du matériel : lspci, modconf, discover, mdetect

Configuration tcpip : ifconfig eth0 10.1.0.41 netmask 255.255.252.0

Dns : vi /etc/resolv.conf - nameserver 10.1.0.41

d. Les services (Ssh, Telnet, Ftp, etc)

Sur un hôte TCPIP, vous avez la possibilité de faire tourner des services, qui répondront aux demandes des machines “voisines”.

Exemple : Un serveur de mail, installé chez votre fournisseur d'accès à l'Internet, fait tourner plusieurs services afin de pouvoir acheminer correctement votre courrier électronique :

- Le service SMTP (logiciel Postfix, Sendmail, Exim, etc) permet d'envoyer du courrier,
- Le service POP3 ou IMAP (logiciel Cyrus, uw-*, etc) permet de récupérer son courrier.

Ces services sont également appelé démons.

Chaque service possède un port d'exécution. (Comme dans un building à plusieurs étages, chaque étage correspond à un service.) La liste des services est consultables dans /etc/services.

Les services peuvent tourner en mode indépendant (ou automome), ou en mode inetd (ou xinetd)

/etc/inetd.conf

e. Routage, Brodcasting, Vlan, etc...

Si nous reprenons le principe du TCPIP, votre ordinateur ne peut communiquer qu'avec des ordinateurs dans le même réseau que lui (10.0.0.1 à 10.0.0.255 par exemple si son sous-masque est 255.255.255.0). Pour “sortir” de ce réseau, vous devez passer par une passerelle (Gateway) qui acheminera vos demandes à l'extérieur de votre réseau.

Cette manipulation se fait en ajoutant une route... Vous pouvez ajouter plusieurs routes afin de joindre plusieurs réseaux distincts.

route add -net 10.1.0.0 netmask 255.255.255.0 gw 10.0.0.254
route add default gw 10.0.0.250

Les passerelles sont des machines qui acheminent les paquets TCPIP d'un réseau A vers un réseau B. Ceux-ci doivent donc être identifiés clairement (type Unicast : une machine PC1 envoi un paquet IP vers le PC2 via la passerelle A).

Généralement, les passerelles n'acheminent pas les paquets Broadcast (recherche d'un serveur de domaine Windows par inondation du réseau, recherche d'un serveur Dhcp, etc), car cela génèrerait trop de traffic “inutile”.

Des solutions “paliatives” existent tout de même : mise en place de serveur Wins pour les clients Windows, mise en place de Relay DHCP, etc.

Mais passons aux choses sérieuses.....

2. Serveur DHCP

a. Pourquoi ?

L'attribution des adresses IP se fait de manière manuelle. Toutefois, en cas de gros réseau, la gestion de ces adresses devient vite problématique.

Un serveur DHCP s'occupe d'attribuer les adresses IP, les masques de sous-réseau, les serveurs et suffixes DNS, les passerelles et les serveurs Wins.

Au démarrage de la connexion réseau, la machine recherche un serveur DHCP sur le réseau (mode BroadCast : si votre serveur DHCP est derrière une passerelle, il vous faut un serveur relais DHCP), et lui demande de lui attribuer une IP non utilisée.

b. Configuration

Si vous souhaitez que votre serveur DHCP mette à jour votre serveur DNS automatiquement, il faut tout d'abord générer une clef d'identification commune aux 2 services. En effet, donner le droit au serveur DHCP de modifier le serveur DNS est extrêmement pratique. Lors de l'attribution de l'IP à un PC (exemple : hobbes.G3L), le DNS sera automatiquement mis à jour. Ainsi, tout systême recherchant calvin.G3L arrivera à le joindre.

dnssec-keygen -a HMAC-MD5 -r /dev/urandom -b 512 -n zone rndc-key

Le serveur est configuré très simplement : /etc/dhcp3/dhcpd.conf

ddns-domainname "G3L";
ddns-updates off;
ddns-update-style interim;
ignore client-updates;

option domain-name "G3L";
option domain-name-servers 10.1.0.41;

default-lease-time 2592000;
max-lease-time 2592000;

authoritative;

log-facility local7;

```
# Site ETOILE
subnet 10.1.0.0 netmask 255.255.252.0 {
        range 10.1.0.201 10.1.0.250;
        range 10.1.1.1 10.1.1.250;
        range 10.1.2.1 10.1.2.100;

        option domain-name-servers 10.1.0.41;
        option domain-name "G3L";
        option subnet-mask 255.255.252.0;

        option routers 10.1.0.4;
        option netbios-name-servers 10.1.0.41;

        authoritative;
        ddns-updates on;
}
key DHCP_UPDATER {
      algorithm hmac-md5;
      secret "03uKV+lWBMwH52mv91GkUQ==";
};

zone G3L. {
        primary 127.0.0.1;
        key DHCP_UPDATER;
}

zone 1.10.in-addr.arpa. {
        primary 127.0.0.1;
        key DHCP_UPDATER;
}
```

c. Les relais Dhcp

Encore plus simple : il suffit de paramétrer l'ip du serveur DHCP. Ainsi, lorsque cette machine recoit une demande DHCP, elle s'occupe de relayer cette demande auprès du serveur spécifié. On peut donc passer des passerelles qui ne gèrent pas le BroadCast. (/etc/default/dhcp3-relay)

3. Serveur DNS

a. Pourquoi ?

Comme on l'a vu plus haut, le serveur DNS permet de mettre en relation des noms de machines et des adresses IP.

On spécifie le serveur DNS de la machine dans le fichier /etc/resolv.conf

domain G3L

search G3L

nameserver 10.1.0.41

b. Configuration : Bind

Un serveur DNS sert les noms des machines d'un ou plusieurs domaines donnés. Il se peut que vous souhaitiez rediriger les requêtes pour les autres domaines vers d'autres serveurs. Dans ce cas, modifier le fichier /etc/bind/named.conf.options et mettre les ip des serveurs DNS aux lignes forwarders.

Modifier le fichier /etc/bind/named.conf.local

```
zone "G3L" {
        type master;
        file "/etc/bind/db.dyn.g3l";
        allow-update { key DHCP_UPDATER; };
};

zone "1.10.in-addr.arpa" {
        type master;
        file "/etc/bind/db.1.10";
        allow-update { key DHCP_UPDATER; };
};
```

Ainsi, nous mettons en place le DNS pour le domaine G3L (exemple : calvin.G3L donnera l'ip 10.1.0.41) et pour la recherche inversée (exemple : l'ip 10.1.0.41 donnera le nom de machine calvin.G3L)

Le fichier /etc/bind/db.dyn.g3l

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
calvin  IN      A       10.1.0.41
```

Le fichier /etc/bind/db.1.10

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
41.0    IN      PTR     calvin.
```

Attention : dans les serveurs DNS, les IP sont représentées dans l'ordre inverse.

4. Samba

a. Pourquoi ?

Le serveur Samba permet de remplacer un serveur Windows (serveur de fichiers, d'impression, d'authentification pour des clients Windows).

Samba peut être paramétré de plusieurs manières :

- Partage de fichiers ou d'imprimantes simple.
- Contrôleur de domaine de réseau Windows.

b. Serveur de fichiers simple

Le client Windows pourra consulter votre partage par un simple voisinnage réseau.

Fichier /etc/samba/smb.conf

```
[global]
workgroup = G3L
netbios name = calvin
server string = Serveur Samba
security = share
[public]
comment = Repertoire public
browseable = yes
guest ok = yes
writable = yes
path = /home/partage
create mask = 0777
directory mask = 0777
[prive]
comment = Repertoire prive total
browseable = no
guest ok = yes
writable = no
path = /home2/prive
create mask = 0777
directory mask = 0777
```

c. Serveur de domaine

Dans ce cas, le client Windows devra être attaché au domaine G3L et identifié par un code utilisateur et un mot de passe. Seul ces utilisateurs auront alors le droit d'accéder aux partages de votre serveur.

Fichier /etc/samba/smb.conf

```
# Global parameters
[global]
netbios name = calvin
workgroup = G3L
server string = Serveur PDC G3L GNU/Linux
passdb backend = tdbsam
wins support = Yes
time server = Yes
load printers = Yes
printing = cups
add user script = /usr/sbin/adduser --system --home /dev/null --no-create-home --force-badname %u
add group script = /usr/sbin/groupadd '%g'
add user to group script = /usr/sbin/usermod -G `/usr/bin/id -G '%U' | /bin/sed 's/ /,/g'`,'%g' '%U'
add machine script = /usr/sbin/adduser --system --home /dev/null --no-create-home --force-badname %
u
logon script = %U.bat
logon path =
domain logons = Yes
os level = 340000
lm announce = Yes
preferred master = Yes
domain master = Yes
dns proxy = No
security=user
ldap ssl = no
panic action = /usr/share/samba/panic-action %d
create mask = 0777
directory mask = 0777
log level = 1

nt acl support = Yes


# [homes]
```

 # browsable = no
 # map archive = yes
 # guest ok = no

[Printers]
path=/tmp
read only = no
create mask = 0700
guest ok = yes
printable = Yes
browseable = Yes

[netlogon]
comment = Fichiers Scripts de Login
path = /home/netlogon
browseable = no
read only = Yes
write list = erival, guenole, Administrateur, root

[public]
comment = Repertoire public
path = /home/partage
read only = No
guest ok = Yes

[guenole]
comment = Repertoire utilisateur Guenole
path = /home/users/guenole
browseable = No
read only = Yes
valid users = root, erival, Administrateur, guenole
write list = root, erival, Administrateur, guenole

Création d'un utilisateur :

adduser guenole

pdbedit -a -u guenole

pdbedit -L pour lister les utilisateurs Réseau

d. Insertion d'un serveur Samba dans un domaine.

Installer le Winbind, afin que le serveur Samba aille chercher les SID sur un autre serveur (le pdc)

vi /etc/nsswitch.conf

passwd: compat winbind
group: compat winbind

Pour joindre le serveur au domaine : *net join -S G3L -U root%passwd*

[global]
workgroup = G3L
netbios name = hobbes
server string = Serveur Samba Esclave
security = domain
password server = calvin
nt acl support = Yes

idmap uid = 10000-20000
idmap gid = 10000-20000
winbind separator = /

create mask = 0777
directory mask = 0777

wins server = 10.1.0.41

[guenole]
comment = Repertoire Guenole
path = /home/dossiers/guenole
browseable = yes
read only = no
inherit acls = yes
inherit permissions = yes
valid users = G3L/guenole, G3L/erival, G3L/root, G3L/Administrateur

5. Cups

a. Pourquoi ?

Cups permet d'installer des imprimantes sur votre machine Linux. Ces imprimantes peuvent être local (Parallèle, Usb, Série) ou bien “réseau” (Lpd, Smb, JetDirect, etc). Une fois l'imprimante installé sur votre Linux, celle-ci est automatiquement partagé via Samba (*print = cups*)

b. Configuration

L'installation de Cups est très simple.

Une fois installé, il suffit de lancé votre navigateur sur la page http://localhost:631/ Une simple connexion en root/password permet d'ajouter une imprimante, d'en gérer les jobs, les options, etc.

On peut également modifier le fichier de configuration /etc/cups/cupsd.conf afin d'autoriser d'autres postes à “administrer” Cups. Etudier prudemment les lignes Allow From.