Mise en place du réseau pour une LAN

Aurélien BONNARDON

16/06/2008

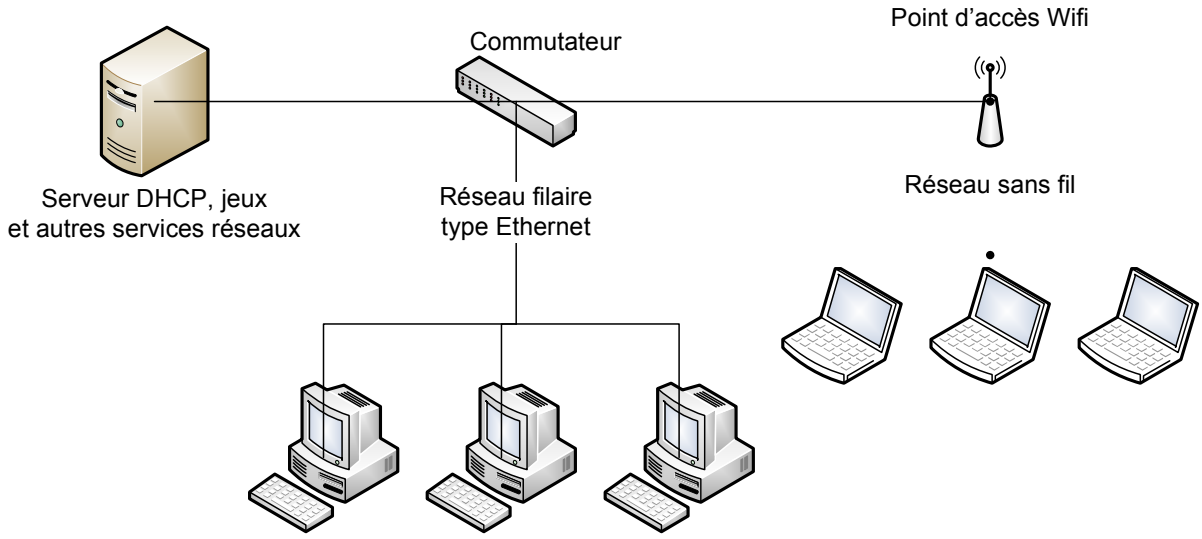
Ce document explique comment mettre en place d'un réseau de base pour l'organisation d'une LAN sans accès à Internet.

Sommaire

Introduction

Ce document détaille la mise en place d'un réseau informatique local pour l'organisation d'évènements visant à rassembler environ 30 personnes. Ce réseau prévoit, matériellement, un commutateur possédant un nombre de ports conséquents, un point d'accès Wifi permettant aux possesseurs de cartes sans fil de se connecter au réseau et un serveur permettant d'offrir les services de bases. Ce document ne traitera pas l'accès à Internet.

Voici un schéma du réseau à réaliser :



1 Matériel

Le choix du matériel est réalisé en fonction des éléments déjà en possession.

1.1 Commutateur

Le commutateur proposé est un 3Com SuperStack 2 3300. Il possède 24 ports et fonctionne avec les normes Ethernet 10 base T et 100 base TX. Il est paramétrable (VLAN, …) mais vu la taille du LAN, cela n'st pas nécessaire.

1.2 Point d'accès Wifi

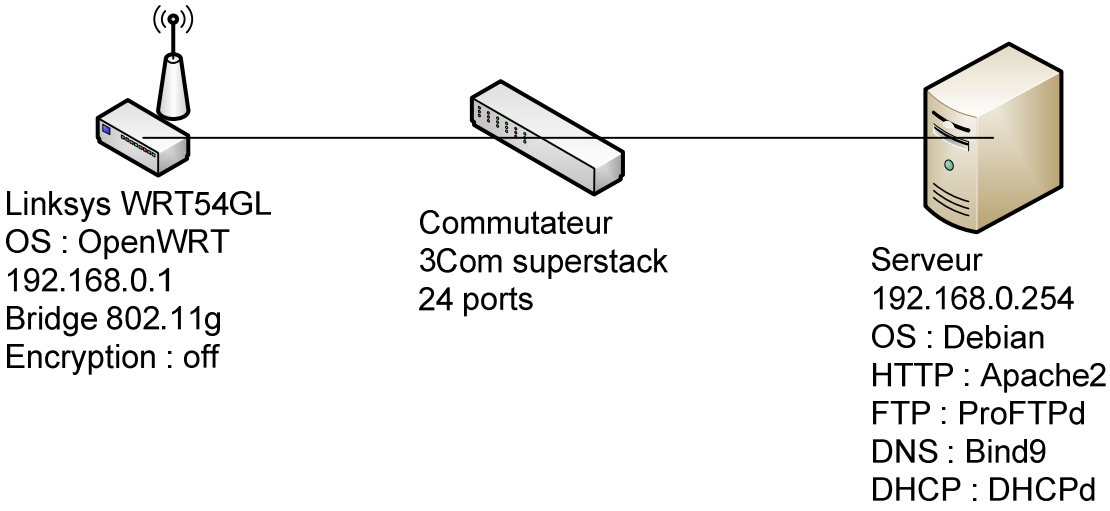
Le point d'accès Wifi doit permettre aux possesseurs de carte compatible de se connecter au réseau. Dans un premier temps, un Linksys WRT54GL sera utilisé. Celui-ci est équipé du firmware alternatif OpenWRT permettant un paramétrage plus aisé.

1.3 Serveur

Le serveur est un PC équipé d'un Pentium 4 2.4 Ghz et de 1 Go de RAM DDR. Il possède un disque dur de 80 Go et est équipé de deux cartes réseaux Ethernet 10/100. Sa puissance et sa capacité de stockage est suffisante pour son utilisation.

2 Plan d'adressage IP

Le réseau fonctionne sur Ethernet/TCP/IP. Le plan d'adressage IP respect la RFC 1918 utilisant des adresses privées. Chaque station possède une adresse IP du réseau 192.168.0.0. Le serveur possède l'adresse 192.168.0.254 et distribue des adresses via son serveur DHCP dans l'intervalle 192.168.0.10-192.168.0.100. Le point d'accès wifi utilise l'adresse IP 192.168.0.1. Le schéma ci-dessous détaille l'architecture et les adresses IP des équipements :



3 Configuration de commutateur

Comme dit précédemment, aucune configuration ne sera apportée au commutateur. Il remplira son rôle de base, c'est-à-dire commuter les paquets vers le bon port.

4 Configuration du point d'accès Wifi

La configuration du routeur demande un peu plus de travail. Le Linksys WRT54G a été équipé d'un firmware alternatif, OpenWRT. Celui-ci est très proche de Linux et propose de multiple paramètre de configuration. Pour plus de détail concernant l'installation de ce firmware, contacter l'auteur.

On se connecte en SSH sur le routeur avec un client quelconque (Putty, …) pour arriver sur une invite de commande. Voici les paramètres de la NVRAM à avoir (la plupart doivent déjà être configurés correctement) :

```
# Configuration du Wifi
nvram set wl0_mode=ap
nvram set wl0_ssid=RootOnLan
# Pas de cryptage
nvram set wl0_wep=disabled
nvram set wl0_akm=open

# Configuration LAN
nvram set lan_ifnames="vlan0 eth1 eth2"
nvram set lan_ipaddr=192.168.0.1
nvram set lan_proto=static
```

```
nvram set wan_ifname=vlan1
```

Il faut ensuite désactiver le serveur DHCP pour les clients du point d'accès passent par celui du serveur. Pour cela, il suffit de retirer les droits d'exécution au script de démarrage :

```
chmod –x /etc/init.d/S60dnsmasq
```

Au niveau des branchements, il faut connecter le commutateur sur le port 1 et il est possible de connecter des stations sur les ports 2,3 et 4. Par contre, le port « Internet » doit rester inutilisé.

5 Configuration du serveur

Le serveur du réseau doit fournir les services suivant :

- DHCP : pour distribuer à tous les clients une adresse IP unique qui n'est pas en conflit avec les autres. Elle est distribuée automatiquement ce qui évite à l'utilisateur de devoir configurer les paramètres réseau de son PC. De plus, il permet de fournir d'autres informations telles que le serveur DNS qui nous intéresse dans notre cas.
- HTTP : Le but du serveur HTTP est de permettre aux utilisateurs de télécharger les jeux et de trouver une aide concernant les installations. Le contenu du site ne fait pas débat ici, seule la mise en place du serveur nous concerne.
- FTP : Pour une plus grande rapidité de téléchargement, les jeux sont échangés sur le réseau grâce au protocole FTP. La mise en place d'un serveur anonyme et utilisé par le serveur HTTP semble la solution.
- DNS : Ce serveur n'est pas essentiel, son but est de permettre aux utilisateurs d'accéder au serveur via un nom plutôt qu'une adresse IP.
- Teamspeak : c'est un logiciel de VoIP, son principal usage étant la communication pendant les parties de jeux en réseau.

Dans un souci de facilité de configuration, le serveur est équipé de Linux Debian.

5.1 Configuration réseau

La première étape concerne la configuration du réseau. Le serveur a une adresse IP fixe, 192.168.0.254. Voici les commandes nécessaires :

```
ifconfig eth0 192.168.0.254 netmask 255.255.255.0 up
```

Nous allons modifier le fichier de configuration pour conserver ces paramètres lors des redémarrages. Il s'agit du fichier `/etc/network/interfaces`.

```
auto eth0
iface eth0 inet static
address 192.168.0.254
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.254
dns-nameservers 192.168.0.254
```

5.2 Configuration du serveur DHCP

Il faut commencer par installer le serveur DHCP avec la commande suivante :

```
apt-get install dhcp3-server
```

La configuration se passe ensuite dans le fichier `/etc/dhcp3/dhcpd.conf` :

```
### Configuration des baux
# Durée du bail par défaut, en seconde
default-lease-time 86400;

# Durée maximum d'un bail, en seconde
max-lease-time 172800;

## Configuration du réseau
# Nom du domaine
option domain-name "rootsonlan";

# Masque du réseau
option subnet-mask 255.255.255.0;

# Adresse de broadcast du réseau
option broadcast-address 192.168.0.255;

# Passerelle par défaut
option routers 192.168.0.254;

# Serveurs DNS
option domain-name-servers 192.168.0.254;

# Configuration du réseau et de son masque
subnet 192.168.0.0 netmask 255.255.255.0 {
 # Plage d'adresses disponible pour les clients
 range 192.168.0.10 192.168.0.100;
}
```

Le script de démarrage de Debian ayant un peu de mal, il faut le modifier. Dans le fichier `/etc/init.d/dhcp3-server`, il faut remplacer les lignes :

```
start-stop-daemon --start --quiet --pidfile $DHCPDPID \
                  --exec /usr/sbin/dhcpd3 -- -q $INTERFACES
```

Par :

```
/usr/sbin/dhcpd3 -cf /etc/dhcp3/dhcpd.conf -lf
/var/state/dhcp/dhcps.leases eth0
```

Pour démarrer le serveur, il suffit de taper la commande suivante :

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

Et pour l'arreter :

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

5.3 Configuration du serveur FTP

Il faut commencer par installer le serveur FTP ProFTPd avec la commande suivante :

```
apt-get install proftpd
```

Il faut choisir l'option `standalone`.

Par défaut le daemon proftpd se lance avec les privilèges de `root` et cela pose évidemment des problèmes de sécurité. C'est pourquoi je vous conseille d'utiliser un utilisateur sans droits particuliers. Le plus indiqué étant nobody du groupe nobody. Ils existent probablement déjà chez, vous vous pouvez le vérifier par :

```
cat /etc/group | grep nobody
```

Si vous n'aviez aucune réponse, c'est que vous n'avez pas de group nobody, sa création se limite à :

```
groupadd nobody
```

Ensuite :

```
cat /etc/passwd | grep nobody
```

Si vous n'aviez aucune réponse c'est que vous n'avez pas d'utilisateur nobody, sa création et son affectation au groupe nobody se limitent à :

```
useradd nobody -d / -s /bin/false usermod nobody -g nobody
```

Nous allons créer 3 utilisateurs, le premier, `admin` qui sera le login qui permettra de mettre des fichiers sur le serveur. Le second `userftp` sera le login utilisateur.

```
useradd admin -s /bin/false
```

```
useradd userftp -s /bin/false
```

Il faut, bien-sûr leurs affecter des mots de passe :

```
passwd admin
```

```
passwd userftp
```

Dans notre cas, nous utiliserons `admin0` pour l'utilisateur `admin` et `userftp` pour l'utilisateur du même nom.

On crée le répertoire du ftp :

```
mkdir /var/ftp
```

Et on lui donne tous les droits

```
chmod 777 /var/ftp
```

De même, on crée le répertoire devant contenir les pages HTML :

```
mkdir /var/ftp/www
```

```
chmod 777 /var/ftp/www
```

Le fichier `/etc/ftpusers` contient la liste des utilisateurs à exclure du FTP. Pour plus de sécurité, il est important d'y faire figurer tous les utilisateurs de votre système excepté ceux qui utilise le FTP, en particulier l'utilisateur `root`.

La commande suivante facilite la tâche :

```
cat /etc/passwd | cut -d ":" -f 1 > /etc/ftpusers
```

Il suffit ensuite de le nettoyer, en particulier enlever les utilisateurs `admin` et `userftp`.

Le fichier `/etc/proftpd/proftpd.conf` est l'unique fichier de configuration de proftpd. Nous allons le compléter ainsi :

```
# Nom du serveur
ServerName              "Root's on LAN ProFTPD"

# Pas d'IPv6
UseIPv6                         off

# Cela permet que le demon reste en memoire
ServerType              standalone

# Pour les serveurs virtuels
DefaultServer           on

# Port du serveur
Port                    21

# Répertoire ou arrive les utilisateurs
DefaultChdir            /var/ftp/

# Répertoire racine
DefaultRoot             /var/ftp

# Autoriser l'usage de /etc/ftpusers.
UseFtpUsers             on

# Seul le propriétaire d'un fichier peut le modifier.
Umask                   022

# Pour prevenir les attaques DOS,
#on limite le nombre maximum de processus fils au demon.
MaxInstances            80
```

```
# On definit l'utilisateur avec lequel se lance le demon
# nobody permet de securiser la machine
User                    nobody
Group                   nobody

# Nombre maximum de clients simultanes
MaxClients              50

# Nombre maximum de clients ayant le même login
MaxClientsPerHost       50

# Message d'accueil après une connexion réussie
AccessGrantMsg          "Bienvenue sur le serveur FTP de Root's on LAN"

# Fichiers logs des connections et transferts
SystemLog               /var/log/proftpd.log
TransferLog             /var/log/xferlog

# Autoriser la reprise des téléchargements interrompus
AllowStoreRestart       on

# Autoriser l'ecrasement de fichier
AllowOverwrite on

# Pas de shell valide requis et pas de root
<Global>
RequireValidShell off
RootLogin off
</Global>

# Mise en place du repertoire racine du serveur /var/ftp
<Directory /var/ftp>

# Personne ne peut ecrire sauf admin
<Limit WRITE>
AllowUser admin
DenyAll
</Limit>

</Directory>
```

Il faut ensuite lancer le démon proftpd avec la commande suivante :

```
/etc/init.d/proftpd start
```

Et l'arrêter avec la commande :

```
/etc/init.d/proftpd stop
```

5.4 Configuration du serveur HTTP

Il faut commencer par installer le serveur HTTP apache2 avec la commande suivante :

```
apt-get install apache2
```

Il suffit ensuite de commenter du caractère # la ligne suivante dans le fichier /etc/apache2/sites-available/default :

```
RedirectMatch ^/$ /apache2-default/
```

De plus, en accord avec la configuration du serveur FTP, il faut modifier le dossier contenant les pages HTML. Pour cela, il suffit de remplacer « /var/www » par « /var/ftp/www » dans le fichier précédent.

On lance le serveur avec la commande :

```
/etc/init.d/apache2 start
```

Et on l'arrete avec :

```
/etc/init.d/apache2 stop
```

Les pages sont à placer dans le répertoire /var/www.

5.5 Configuration du serveur DNS

Il faut commencer par installer le serveur DNS bind9 avec la commande suivante :

```
apt-get install bind9
```

Après avoir installé BIND, nous commençons par indiquer dans le fichier /etc/bind/named.conf.local que notre serveur est le serveur principal pour la zone rootsonlan.com. Nous ajoutons donc au fichier de configuration les lignes suivantes :

```
## zone rootsonlan - primaire
zone "rootsonlan" {
        type master ;
        file"/etc/bind/rootsonlan.db";
        notify yes;
};
```

Et nous créons le fichier /etc/bind/rootsonlan.db, qui est pour l'instant vide.
Nous allons le compléter avec les lignes suivantes :

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@    IN    SOA    rootsonlan. root.lyon. (
                  1         ; Serial
             604800         ; Refresh
              86400         ; Retry
            2419200         ; Expire
604800 )    ; Negative Cache TTL
;
@    IN     NS     tryx

tryx    IN      A       192.168.0.254

Jah     IN     A     192.168.0.1

rootsonlan    IN    A    192.168.0.254
```

Il nous suffit ensuite de lancer le serveur avec la commande suivante :

```
/etc/init.d/bind9 start
```

Et on l'arrete avec :

```
/etc/init.d/ bind9 stop
```

5.6 Configuration du serveur Teamspeak

Teamspeak serveur ne fait pas parti des paquets propose par l'outil `apt` de Debian. Il va donc falloir le télécharger les sources sur site officiel. On va utiliser pour cela la commande `wget` :

```
wget
ftp://ftp.freenet.de/pub/4players/teamspeak.org/releases/ts2_server_rc2_202
01.tar.bz2
```

On extrait ensuite le contenu de l'archive avec la commande suivante :

```
tar -xjf ts2_server_rc2_202319.tar.bz2
```

(Si erreur, `apt-get install bzip2`)

Rentrez dans le dossier créé (tss2_rc2) et exécutez la commande suivante :

```
./teamspeak2-server_startscript start
```

Il faut maintenant observer le contenu du fichier `server.log` pour connaitre les mots de passe, en particulier celui du `superadmin`.

Le reste de la configuration se fait via l'interface web. Pour se connecter, on utilise l'URL suivante dans un navigateur quelconque :

```
http://ipduserveur:14534
```

Pour plus d'ergonomie, on va déplacer les fichiers dans le dossier /usr/local/. Pour cela :

cp -r ~/tss2_rc2 /usr/local

Le script de démarrage suivant est à mettre dans le dossier /etc/init.d :

```
#!/bin/sh

start() {
    /usr/local/tss2_rc2/teamspeak2-server_startscript start
}
stop() {
    echo "TS server is stopping.."
    /usr/local/tss2_rc2/teamspeak2-server_startscript stop
}

case "$1" in
    "start")
        start
        ;;

    "stop")
        stop
```

```
        ;;

    "restart")
        stop
        start
        ;;

    *)
        echo "Utilisation : $0 [start | stop]"
        exit 1
        ;;
esac
```