Installer un firmware alternatif sur un Linksys WRT54G v. 5

Aurélien BONNARDON

01/04/2008

Ce document détaille les étapes pour installer un firmware alternatif sur un Linksys WRT54G version 5, malgré que celui-ci possède moins de mémoires que les autres versions.

Introduction

Pendant longtemps, on a cru qu'il était impossible d'installer un firmware alternatif sur un WRT54G version 5 car son firmware d'origine n'était pas basé sur Linux, contrairement aux autres. De plus, ses capacités mémoires sont deux fois inférieures. Il existe pourtant 2 méthodes pour y arriver.

Les méthodes décrites plus bas doivent être suivis rigoureusement. En effet, il y a des risques pour le routeur. Les manipulations ci-dessous sont données à titre d'information et vous êtes seul responsable des dommages qu'elles pourraient causer à votre routeur.

1 Le Linksys WRT54G version 5

Fréquence CPU : 200 MHz
RAM : 8 Mo
Mémoire flash : 2 Mo
Préfixe num de série : CDFB
Chipset : Broadcom BCM5352EKPB
OS : VxWorks

Le WRT54G est un routeur Wifi produit par Linksys. Il permet de partager une connexion Internet vers des ordinateurs via 4 ports Ethernet et une liaison à la norme sans fil IEEE 802.11b/g. Il existe 8 versions. Pour savoir si vous possédez une version 5, il faut regarder le numéro de série au dos de celui-ci. S'il commence par CDFB, alors vous êtes l'heureux propriétaire de la version 5 du routeur.

Contrairement aux autres routeurs de la série, le firmware d'origine n'est pas basé sur Linux. Les firmwares alternatifs tournant tous sous linux, il va falloir flasher le routeur avant d'installer un autre firmware. C'est toute la difficulté de l'opération, contrairement aux autres où il suffit de mettre à jour par le panneau d'administration.

2 Préparatifs

2.1 Configuration du réseau

Pour avoir le plus de chance possible que la manipulation se passe bien, il est conseillé de relier directement le PC au routeur un câble Ethernet. Si vous ne pouvez pas, je ne vous conseille pas d'essayer la 2ème méthode voir même de ne rien essayer du tout. En effet, on va utiliser TFTP pour charger le firmware sur le routeur. Or, ce protocole est basé sur UDP qui n'intègre pas de contrôle des données, donc, si un paquet est corrompu, le firmware ne fonctionnera pas.

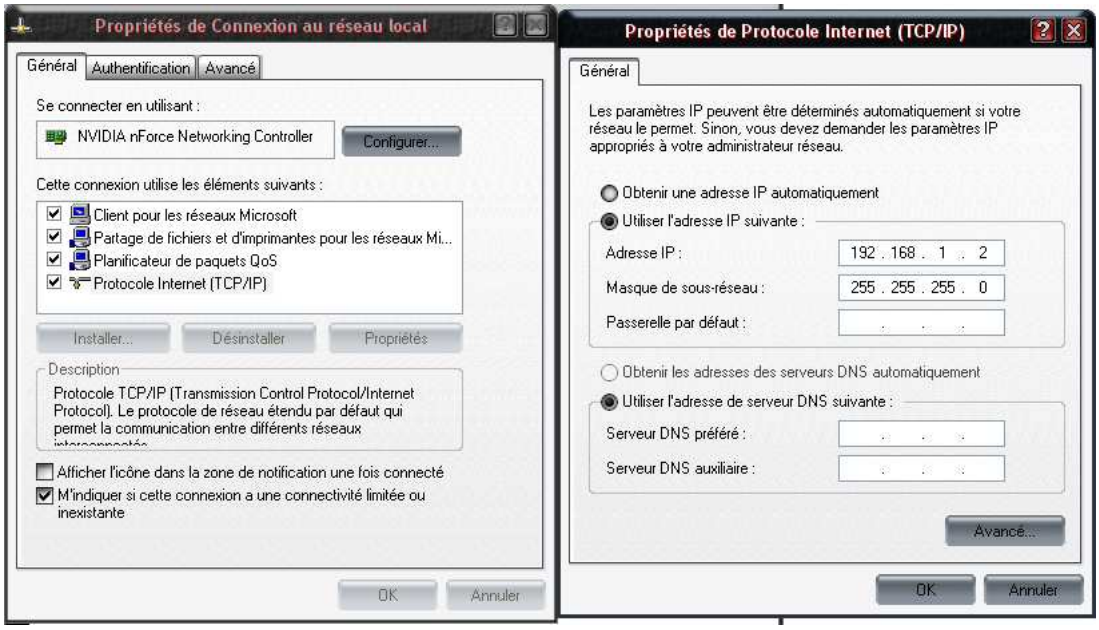
Nous allons utiliser une IP fixe pour le PC, cela augmentera la probabilité de réussir.

2.1.1 Windows

Rendez-vous dans « Panneau de Configuration » (Démarrer -> Panneau de configuration) puis cliquez sur « Connexions réseaux ». Faites un clic droit sur votre carte réseau Ethernet, puis sélectionnez « Propriétés ». Dans la liste qui se présente à vous, double-cliquez sur « Protocole Internet (TCP/IP) ». Cochez la case « Utiliser l'adresse IP suivante » puis remplissez les champs comme ceci:

- Adresse IP : *192.168.1.2*
- Masque de sous-réseaux : *255.255.255.0*

Validez avec « Ok » pour fermer les 2 fenêtres, cela peu prendre un peu de temps.



2.1.2 Linux

Si votre routeur est connecté à la carte eth0, utilisez la commande suivante :

$ ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up

2.2 Activer le boot_wait

Pour pouvoir réussir au mieux les manipulations suivantes, il faut mettre le routeur en mode boot_wait. Il s'agit d'un mode dans lequel le routeur attend quelques secondes avant de démarrer sur l'OS. Par défaut, sa valeur est à off. Pour pouvoir l'activer, il faut utiliser une faille dans le firmware d'origine qui permet de modifier les variables de la NVRAM. Connectez vous sur l'interface Web du routeur (http://192.168.1.1 dans votre navigateur) et allez dans « Administation » puis « Dagnostics » et enfin « Ping ». Dans la fenêtre qui s'ouvre entrez les commandes suivantes une par une:

```
;cp${IFS}*/*/nvram${IFS}/tmp/n
;*/n${IFS}set${IFS}boot_wait=on
;*/n${IFS}commit
;*/n${IFS}show>tmp/ping.log
```

La dernière commande doit vous afficher les variables de la NVRAM et vous devez voir vers la fin de cette liste « boot_wait=on ». Pour vérifier s'il est effectivement activé, il faut redémarrer le routeur et si la LED power clignote au démarrage, alors c'est bon.

3 Installer un firmware alternatif

3.1 1ére méthode : en utilisant les outils proposés pas DD-WRT

3.1.1 Flasher le routeur

Les développeurs de DD-WRT, en plus de fournir un très bon firmware pour WRT54G, propose sur leur site des outils pour flasher une version 5. Le premier s'appelle vxworks_prep, il s'agit d'un « faux » firmware qui peut être installé à partir de l'interface Web de Linksys. Vous le trouverez à cette adresse :

http://www.dd-wrt.com/dd-wrtv2/downloads/others/wrt54gv5%20flashing/vxworks_prep_v03.zip

Une fois le fichier téléchargé et extrait, rendez-vous sur l'interface Web du routeur et suivez le chemin « Administration -> Firmware -> Update ». Il est conseillé d'utiliser Internet Explorer version inférieure à 7. Lancez la mise à jour en sélectionnant vxworks_prep.bin et attendez. Surtout, ne redémarrez pas votre routeur ! Un fois qu'un message confirme la mise à jour, débranchez la prise et attendez environ 30 secondes avant de rebrancher celle-ci. L'adresse IP doit normalement rester la même (192.168.1.1) mais sur certaines versions, elle est changée en 192.168.1.145. Testez par un ping.

Connectez-vous à nouveau avec un navigateur Web. La page qui s'affichera sera différente, elle vous permettra uniquement de sélectionner un fichier. Il ne s'agit pas encore du nouveau firmware, mais d'un outil dont le but est de flasher complètement la mémoire du routeur. Vous le trouverez également sur le site DD-WRT à l'adresse suivante :

http://www.dd-wrt.com/dd-wrtv2/downloads/others/wrt54gv5%20flashing/vxworks_killer_v04.bin

Il vous suffit de sélectionner ce fichier dans l'interface Web. Une fois le message de succès affiché, débranchez le routeur quelques secondes. Par la suite, inutile d'essayer d'accéder à l'interface Web, il n'y a plus rien pour le moment.

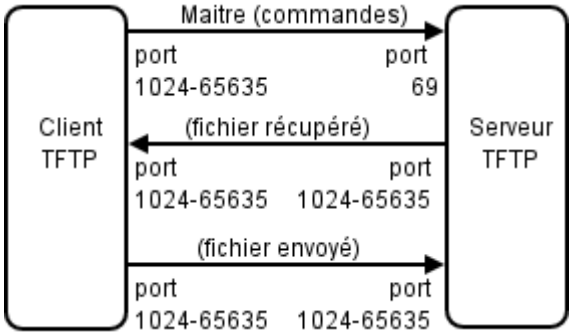
3.1.2 Installer le nouveau firmware

Votre routeur et maintenant prêt à accueillir un nouveau firmware, reste à choisir celui-ci. Personnellement, je vous conseille DD-WRT si vous n'avez pas de connaissance poussées en Linux. En effet, il permet d'avoir une interface Web malgré le manque de mémoire sur le routeur. La version standard est la mieux adaptée :

http://www.dd-wrt.com/dd-wrtv2/downloads/stable/dd-wrt.v23/dd-wrt.v23.std.zip

Il y a plusieurs firmwares différents, pour la version 5 du WRT54G, il faut utiliser la version « generic ».

Pour envoyer le fichier sur le routeur, il faut utiliser le protocole TFTP. TFTP (pour Trivial File Transfert Protocol ou Protocole simplifié de transfert de fichiers) est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP. L'utilisation d'UDP, protocole "non fiable", implique que le client et le serveur doivent gérer eux-mêmes une éventuelle perte de paquets.Les principales simplifications visibles du TFTP par rapport au FTP est qu'il ne gère pas le listage de fichiers, et ne dispose pas de mécanismes d'authentification, ni de chiffrement. Il faut connaître à l'avance le nom du fichier que l'on veut récupérer. De même, aucune notion de droits de lecture/écriture n'est disponible en standard. TFTP est très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu, etc.). La dernière version de ce protocole est la version 2, définie dans RFC 1350.



3.1.2.1 Windows

Il existe un utilitaire graphique développé par Linksys pour envoyer un firmware via TFTP, mais nous utiliserons les commandes pour cela. Il est disponible à l'adresse suivante :

ftp://ftp.linksys.com/pub/network/tftp.exe

Il faut lancer une invite de commande (Démarrer -> Tous les programmes -> Accessoire) dans laquelle vous commencerez par faire un ping vers le routeur pour être sur que celui-ci est actif :

ping 192.168.1.1

Puis exécutez la commande suivante :

tftp –i 192.168.1.1 PUT firmware.bin

L'option –i spécifie que le fichier doit être transféré en mode binaire (et non caractère). Un message doit vous informer du bon fonctionnement du transfert (si ce n'est pas le cas, recommencez celui-ci).

3.1.2.2 Linux

Il faut tout d'abord vérifier qu'un client TFTP est installé. Pour cela tapez simplement « tftp » dans une console. Si vous obtenez une erreur de type « command not found », il vous faudra installer un client TFTP. Il est généralement présent dans la liste des paquets disponible via le gestionnaire, selon votre distribution, exécutez :

- apt-get install tftp (Debian)
- sudo apt-get install tftp (Ubuntu)
- emerge tftp (Gentoo)
- …

Dans un shell, il faut exécuter la commande suivante pour transférer le fichier via TFTP :

```
echo -e "binary\nrexmt 1\ntimeout 60\ntrace\nput firmware.bin\n" | tftp 192.168.1.1
```

Le routeur doit ensuite rebooter tout seul. L'installation est terminée !

3.2 2ème méthode : en utilisant le boot_wait

La méthode suivante est moins conseillée, utilisez la uniquement si la première ne fonctionne pas ou si votre routeur est bloqué. Elle consiste à se servir de l'option boot_wait du routeur. En effet, pendant un court instant avant de démarrer sur l'OS, celui-ci va regarder si on essaye de lui transférer un firmware via TFTP. Le problème est que cet instant est très court et qu'il faut souvent plusieurs essais avant d'arriver à transférer le firmware.

3.2.1 Windows

Vous aurez besoin de deux invites de commandes. La première aura pour rôle de faire des ping en continu sur le routeur au déterminer le moment exact où il répond. La seconde servira à exécuter la commande de transfert TFTP.

La commande ping est la suivante, les options ont pour rôle de la rendre continue et de réduire le délai entre chaque commande :

```
ping –t –w 1 192.168.1.1
```

La commande de transfert TFTP est la même que dans la première méthode :

```
tftp –i 192.168.1.1 PUT firmware.bin
```

3.2.2 Linux

De la même manière, vous aurez besoin de deux consoles. Dans l'une exécutez la commande suivante :

```
ping –i 0.1 192.168.1.1
```

Et dans l'autre préparez la commande de transfert TFTP :

```
echo -e "binary\nrexmt 1\ntimeout 60\ntrace\nput firmware.bin\n" | tftp 192.168.1.1
```

Lancez le ping, puis débranchez la prise du routeur quelques secondes. Au moment EXACT où le routeur répond au ping, il faut exécuter la commande TFTP. Il vous faudra plusieurs essais, surement une dizaine, mais ne désespérez pas, ça fonctionne. Quand le transfert fonctionne, la commande TFTP rend la main avec un message de succès, le routeur devrait alors redémarrer tout seul. Le firmware est désormais installé.

Source

- « Remplacement du firmware d'un WRT54G », http://petaramesh.org
- « Installing OpenWrt via TFTP », http://wiki.openwrt.org/OpenWrtDocs/Installing/TFTP
- Wiki DD-WRT, http://www.dd-wrt.com/wiki/index.php/Main_Page
- TFTP, http://fr.wikipedia.org/wiki/TFTP