M2-ESECURE Rezo avancé
TP10: NAT64 et DNS64

Jean Saquet
jean.saquet@unicaen.fr

19/10/2012

1 Introduction

Le but est de mettre en place un réseau uniquement en IPv6 relié à l'Internet, avec la possibilité de communiquer avec les services v4.

Nous allons utiliser les préfixes qui vous sont attribués de manière à :

- Configurer un réseau "v6-only"
- Utiliser ces préfixes connus de DNSTP et routés pour simuler des adresses publiques (et donc ne pas compter sur les réseaux d'interconnexion qui risquent de ne pas être routés).

Nous utiliserons les mécanismes DNS64 et NAT64 pour établir des communications entre notre réseau v6 et le monde v4.

Nous utiliserons un schéma conforme à la figure 1

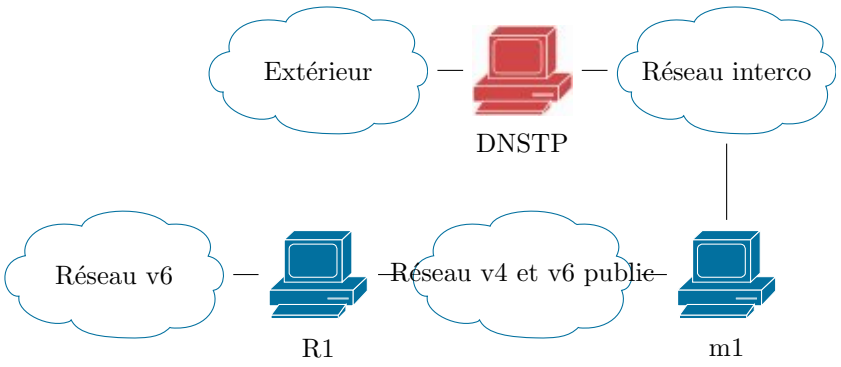

FIGURE 1 – Le principe du réseau

2 Configuration

La machine m1 peut être un Alix ou une machine virtuelle marionnet.
Le réseau d'interconnexion utilise les adresses `2001:660:7101:ffff:10/80` et `192.168.128.0/24` .

Le réseau v4 et v6 “public” utilisera les préfixes qui vous sont fournis : `2001:660:7101:XX::/64` et +192.168.xx.0/24+. (xx entre 16 et 31 pour les marionnet, XX entre 10 et 2F)
En v6, vous pouvez utiliser les deux sous-réseaux disponibles, un pour le “Réseau public”, l'autre pour le “Réseau v6”.

Vous devez positionner des adresses compatibles avec le schéma ci-dessus. Dans le réseau v6 prévoyez deux machines en plus de R1.
Configurez et lancez Quagga sur m1 et sur R1 afin qu'ils échangent leurs routes v6 entre eux et avec DNSTP.
Pour v4, le routage entre le réseau v4 et v6 et DNSTP sera assuré si l'interface de m1 vers le réseau d'interco a la bonne adresse (`192.168.128.xx`)

3 Tests

Testez la connectivité y compris avec l'extérieur. IPv6 est routé mais pas IPv4.

Configurez les resolv.conf des machines du réseau v6 avec l'adresse v6 du serveur de noms de DNSTP.

Essayer alors de consulter, à partir d'une machine du réseau v6, des sites webs (à l'aide de **lynx**) tel que `www.renater.fr`. Essayez maintenant le site `www.microsoft.com`. Que se passe-t-il ? À quoi est dû ce problème ?

Pour le contourner, il serait possible d'utiliser un proxy intermédiaire qui permet de faire le lien entre IPv6 et IPv4. Pour le configurer, vous pourriez utiliser la variable `HTTP_PROXY`, mais on va utiliser une autre méthode.

4 NAT64 et DNS64

Ces deux mécanismes sont indépendants, la seule contrainte est de les configurer avec le même préfixe.

4.1 DNS64

On va installer ce mécanisme sur une machine du réseau v6, autre que le routeur R1. Pour cela, sur la machine choisie :

- Mettez à jour la liste des packages.
- installez le package `totd`.
- Dans le resolv.conf, indiquez “localhost” (ou : :1) comme adresse de serveur de noms.
- Configurez totd.conf, cf annexe A.

Sur la ou les autres machines du réseau v6, modifiez le resolv.conf pour pointer vers cette machine ainsi configurée avec `totd`.

`totd` est un relais DNS qui intercepte les requêtes de type AAAA pour générer également une requête de type A et transformer la réponse avec le préfixe configuré si la machine demandée ne possède pas d'adresse v6.

Essayez un host ou un dig sur `www.renater.fr` et `www.microsoft.com`.

4.2 NAT64

Afin de pouvoir utiliser les adresses v4 transformées v6 avec le préfixe configuré, il faut installer un NAT64 sur le routeur R1, qui transformera les datagrammes v6 provenant d'une machine du réseau V6 en datagrammes v4 ayant comme adresse source l'adresse réputée publique v4 de R1 (en fait ici une adresse privée mais qui sera nattée par DNSTP ou autre machine du réseau du département).

Pour installer ce NAT64 il faut :

- Ajouter dans le fichier `/etc/apt/sources.list` un accès à "testing main" sur le serveur de debian.
- Mettre à jour la base de données des packages (`apt-get update`).
- Installer le package `tayga`
- Configurer R1 pour l'utilisation de tayga (cf. Annexe B)

Vous devriez alors pouvoir consulter `www.microsoft.com` à partir d'une machine v6 ! (bon, avec **lynx**, ce ne sera pas génial)

A Configuration de totd

Fichier totd.conf :

```
; DNS à interroger
forwarder 2001:660:7101:ffff:10::1 port 53 ;
; Préfixe à utiliser
prefix 3ffe:1234:5678:cafe:: (par exemple)
; the port totd listens on for incoming requests
port 53
; the pidfile to use (default: /var/run/totd.pid)
pidfile /var/run/totd.pid
```

B Configuration de tayga

Tayga utilise une plage d'adresses IPv4 pour relayer les requêtes issues des machines v6, ainsi qu'une adresse v4 pour des envois éventuels d'erreurs ICMP, qu'on peut prendre dans la même plage.

L'exemple ci-dessous utilise une plage de deux machines seulement pour simplifier et à cause du bug de ARP, voir ci-dessous.

Il faut penser à natter ces adresses qui sont privées pour accéder à l'internet v4. Ici on nattera sur la machine m1 dont l'adresse en 192.168.128.xx est elle-même nattée par DNSTP.

NB : les adresses 192.168.xx.0/24 sont routées, mais uniquement en interne, sauf demande spéciale aux admins. En les nattant par 192.168.128.xx, on permet l'accès à l'Internet.

Utilisez la commande suivante pour créer la table de correspondance entre adresses v6 et v4 :

```
mkdir -p /var/db/tayga
```

Modifiez le fichier tayga.conf :

```
; chosir la bonne interface
tun-device nat64
; Donner une adresse pour taïga
; (this is TAYGA's IPv4 address, not your router's address)
ipv4-addr 192.168.xx.64
prefix 3ffe:1234:5678:cafe::/96  ;(replace with an unused /96 prefix)
; plage d'adresses v4 pour forward sur Internet
; (ici plage de 2 machines prises dans votre plage d'adresses)
dynamic-pool 192.168.xx.64/31 ;
; fichier de mémorisation des correspondances en cours
data-dir /var/db/tayga
```

Enfin, utilisez les commandes suivantes pour utiliser la bonne interface et configurer le routage :

```
tayga --mktun
ip link set nat64 up
ip addr add 192.168.xx.2 dev nat64
;(replace with your router's IPv4 address)
ip addr add 2001:660:7101:XX::2 dev nat64
;(replace with your router's IPv6 address)
ip route add 192.168.xx.64/31 dev nat64
ip route add 3ffe:1234:5678:cafe::/96  dev nat64
tayga
```

Natter 192.168.xx.0/24 sur la machine m1.

Reste un détail ... la machine m1 va faire une requête ARP pour 192.168.xx.65 qui n'aura pas de réponse ... pourquoi ? mystère ... mettre à la main la correspondance ARP pour l'interface eth0 de R1