

M2-secure Rezo

TP5: NAT64 DNS64

Gaétan Richard, Jean Saquet
Gaetan.richard@unicaen.fr

10/2016

1 Introduction

Pour la suite des TPs de réseaux, nous allons construire progressivement une architecture réseaux complète en utilisant les switch disponibles dans la salle, les machines Alix ainsi que des réseaux virtuels via *marionnet*.

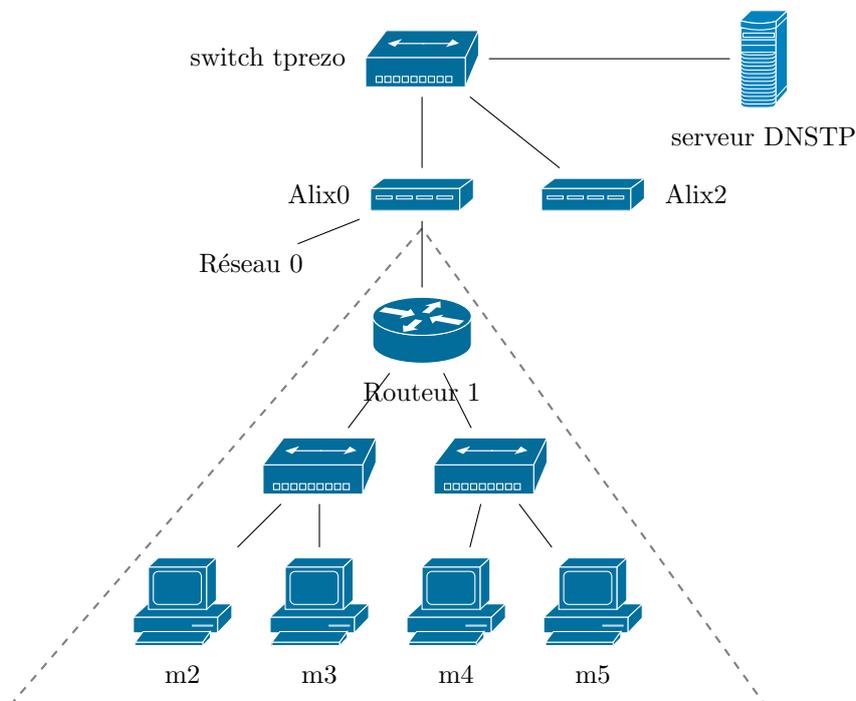


FIGURE 1 – Le réseau avec les ALIX

- Interconnexion Alix - Routeur : $192.168.128+48+x.0/24$, $2001:660:7101:ffff:3X::/80$;
- Réseau m2 / m3 : $192.168.32+x.0/24$, $2001:660:7101:2X::/64$;
- Réseau m4 / m5 : $192.168.16+x.0/24$, $2001:660:7101:1X::/64$.

Dans un premier temps, vérifier la configuration de votre alix et modifier là en conséquence (on prendra l'adresse 1 dans les réseaux d'interconnexion avec les marionnets).

2 Configuration IPv6

On configurera le réseaux IPv6 de *m2* et *m3* (en mettant du ripng sur l'alix pour obtenir la connexion).

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.fr`. 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.

3 NAT64 et DNS64

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

3.1 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.fr`.

3.2 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.fr` 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\dots1 port 53 ;
; Préfixe à utiliser
prefix 3ffe:1234:5678:cafe\dots (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.

Il faut penser à natter ces adresses qui sont privées pour accéder à l'internet v4. Ici on nattera sur l'alix 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 :

```
; choisir 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\dots/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\dots2 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\dots/96 dev nat64
tayga
```

Natter R1 sur l'alix.