Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so FRIBOURG FREIBURG
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz

Bachelor of Science HES-SO in Telecommunications
Technologies de l'information et de la communication

Réseaux IP

- Travail pratique -

Translation d'adresses IPv4 : NAT/PAT

François Buntschu
francois.buntschu@hefr.ch

Haute école d'ingénierie et d'architecture de Fribourg (HEIA-FR)

HES-SO//Fribourg, 19 décembre 2017, v1.6

Table des matières

1. INTRODUCTION

La croissance rapide de l'Internet a étonné la plupart des observateurs. Une raison pour laquelle l'Internet s'est développé tellement rapidement est due à la flexibilité de sa conception. Sans développer de nouvelles méthodologies d'attribution d'adresses IP, cette croissance rapide de l'Internet aurait épuisé l'attribution d'adresses IP. Afin de faire face à un manque d'adresses IP, plusieurs solutions ont été développées. Une solution largement mise en application est la translation d'adresses de réseau (**NAT**=*Network Address Translation* et **PAT**=*Port Address Translation* ou aussi appelé NAT-PT).

NAT/PAT est un mécanisme pour conserver des adresses IP public dans de grands réseaux et simplifier la gestion de l'attribution des adresses IP. Lorsqu'un paquet IP est routé par un équipement réseau, habituellement un routeur ou un firewall, l'adresse IP source est translatée d'une adresse de réseau interne privée à une adresse IP public qui elle est routable.

2. OBJECTIFS

L'objectif de ce travail est d'observer le trafic généré avant et après la translation d'adresse pour découvrir les caractéristiques les plus importantes de ces mécanismes avec un minimum d'informations au départ

3. CONFIGURATION D'EXPÉRIENCE

3.1. Schéma du réseau

Câbler le réseau complet selon le schéma ci-dessous :

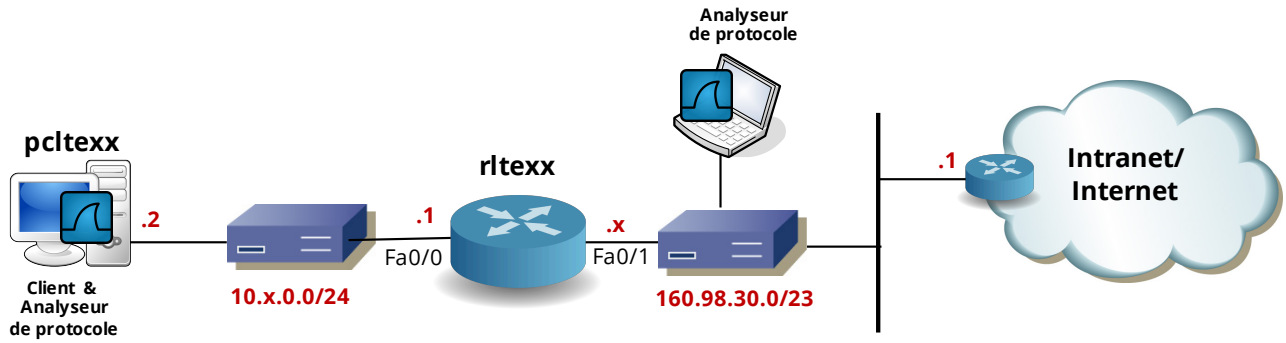

Figure 1 : ***Infrastructure du réseau***

Le PC de chaque place de travail est relié au routeur Cisco 2800 ou 2900 au travers du HUB disponible (ou du switch avec le port « miroir ») à votre place de travail. La deuxième interface du routeur est connectée au LAN du laboratoire de télécommunication au travers d'un second HUB (qui lui sera connecté sur l'interface LAN1 ou LAN2). Les analyseurs de protocole, sont connectés sur la même infrastructure.

3.2. Configuration du PC et du routeur

- Sur le PC, démarrer TeraTerm Pro :

  Start→All Programs→Accessories→Tera Term Pro

- Configurer le terminal comme suit (selon documentation routeur) :

```
Bits per second : 9600
Data bits : 8
Parity : none
Stop bits : 1
Flow control : none
[OK]
```

- Câblez le port Console du routeur avec le câble disponible sur votre place de travail.
- Démarrer le routeur, attendre la fin du *bootstrap* (**répondre «no»** aux questions **si nécessaire**). Attendre le message «Press RETURN», taper RETURN et attendre le prompt «Router».
- Afin d'effacer toute configuration préalable, il est conseillé d'exécuter les commandes suivantes (en mode privilégié)[1] :

```
Router> enable
Router# erase startup-config
Router# reload
```

> **Commentaire**
>
> *Dans la suite du document <x> représente le numéro de la place de travail sur laquelle vous effectuez vos mesures*

- Configuration de base du routeur, entrez dans le mode privilégié

```
Router> enable
Router#
```

- Affecter un nom au routeur

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname rlte<x>
rlte<x>(config)# ^Z
rlte<x>#
```

- Les interfaces (*FastEthernet 0/n* pour les Cisco 2800 et *GigaEthernet 0/n* pour les Cisco 2900) peuvent être vérifiées de la manière suivante

```
rlte<x> # show interface FastEthernet 0/0
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is QUICC Ethernet, address is 0010.7bdf.32f1
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  …
```

- Si l'interface est "`administratively down`" il faut l'activer de la façon suivante :

```
rlte<x> # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x> (config)#interface FastEthernet 0/0
rlte<x>(config-if)#no shutdown
rlte<x>(config-if)# ^Z                          (Ctrl+z)
rlte<x>#
```

[1] Nécessaire si vous n'obtenez pas le mode questions/réponses au démarrage du routeur.

- Vérification de l'interface:

```
rlte<x># show interface FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is QUICC Ethernet, address is 0010.7bdf.32f1
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:21, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  …
```

- Vérifier la deuxième interface
- Configuration des adresses IP :

```
rlte<x>#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)#interface FastEthernet 0/0
rlte<x>(config-if)#ip address 10.xx.0.1 255.255.255.0
rlte<x>(config-if)#exit
rlte<x>(config)#interface FastEthernet 0/1
rlte<x>(config-if)#ip address 160.98.30.(200+xx) 255.255.254.0
rlte<x>(config-if)#end
rlte<x>#
```

!! Il faut modifier la configuration IP du PC pour qu'il ait l'adresse IP 10.<x>.0.2 avec le subnet mask = 255.255.255.0 et comme default gateway = 10.<x>.0.1.

- Configuration du routage par défaut :

```
rlte<x>#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)#ip route 0.0.0.0 0.0.0.0 160.98.30.1
rlte<x>(config)#end
rlte<x>#
```

4. NAT (*NETWORK ADDRESS TRANSLATION*)

4.1. NAT Statique

Le NAT Statique permet de définir manuellement la translation d'adresse IP privée en adresse public.

- Configuration du NAT statique :

```
rlte<x>#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)#interface FastEthernet 0/0
rlte<x>(config-if)#ip nat inside
rlte<x>(config-if)#exit
rlte<x>(config)#interface FastEthernet 0/1
rlte<x>(config-if)#ip nat outside
rlte<x>(config-if)#exit
rlte<x>(config)#ip nat inside source static 10.x.0.2 160.98.30.(20+<x>)[2]
rlte<x>(config)#end
rlte<x>#
```

[2] Si vous effectuez ce TP dans le laboratoire C10.12, l'adresse IP pour la translation sera 160.98.31.<x>

Commentaire

Avant l'analyse des trames, n'oubliez pas de tester votre configuration en effectuant un « ping » depuis votre PC sur une machine de l'école, par exemple tlabs.tic.eia-fr.ch (160.98.31.32) ou merlin.tic.eia-fr.ch (160.98.31.207).

- Configurez un filtre de station IP et de protocole IP telnet pour ne retenir que les échanges provenant de votre PC
- Démarrez l'analyseur de protocole sur le LAN du laboratoire et sur votre PC.
- Effectuez un telnet depuis votre PC sur merlin.tic.heia-fr.ch. Sans vous authentifier .
- Les commandes disponibles sur votre routeur sont :

```
show ip nat translation
show ip nat statistics
show ip route
```

- Les commandes disponibles sur le PC sont (dans une fenêtre de commande):

```
telnet
ping
netstat
```

4.2. Analyse des trames observées

Questions :

P1: Quelles adresses MAC & IP source sont utilisées par votre PC pour accéder au serveur merlin.tic.heia-fr.ch (des deux côtés du routeur) ? Commentez !

P2: Quels ports de source et de destination sont utilisés dans les trames échangées, des deux côtés du routeur ? Est-ce les mêmes des deux côtés du routeur ?

P3: Quelle sont les protocoles de couche 2, 3 et 4 utilisé pour le Telnet ?

P4: Est-il possible d'atteindre votre PC depuis le LAN du laboratoire (par un ping par exemple) ? Expliquez **pourquoi**. Quelle(s) adresse(s) utilisez-vous pour le ping ?

4.3. NAT Dynamique

Le NAT Dynamique permet de définir un pool d'adresse IP qui sera utilisé pour la translation d'adresses IP privées en adresses publiques.

- Suppression du NAT statique :

```
rlte<x>#configure termina
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)#no ip nat inside source static 10.<x>.0.2 160.98.30.(20+<x>)[3]
rlte<x>(config)#end
rlte<x>#
```

- Configuration du NAT dynamique :

```
rlte<x>#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)# ip nat pool public-access 160.98.30.<a> 160.98.30.<a+3> netmask
255.255.254.0
rlte<x>(config)# access-list 1 permit 10.<x>.0.0 0.0.0.255
rlte<x>(config)# ip nat inside source list 1 pool public-access
rlte<x>(config)#end
rlte<x>#
```

[3] Si vous effectuez ce TP dans le laboratoire C10.12, l'adresse IP pour la translation sera 160.98.31.xx

Avec a = 212 pour la table LTE02
a = 216 pour la table LTE03
a = 220 pour la table LTE04
a = 224 pour la table LTE05
a = 228 pour la table LTE06
a = 232 pour la table LTE07
a = 236 pour la table LTE08
a = 240 pour la table LTE09
a = 244 pour la table LTE10

- Configurez un filtre de station IP et de protocole IP telnet pour ne retenir que les échanges provenant de votre PC
- Démarrez l'analyseur de protocole sur le LAN du laboratoire et sur votre PC.
- Effectuez un telnet depuis votre PC sur merlin.tic.heia-fr.ch (160.98.31.207). Sans s'authentifier.
- Les commandes à utiliser sont les mêmes qu'à la mesure précédente.

Questions :

P5: Quelle adresse IP source est utilisée par votre PC pour accéder au serveur merlin.tic.heia-fr.ch (des deux côtés du routeur) ? Commentez.
P6: Quels ports de source et de destination sont utilisés dans les trames échangées, des deux côtés du routeur ? Est-ce les mêmes des deux côtés du routeur ?

- Modifiez l'adresse de votre PC avec l'adresse : 10.<x>.0.3/24.

P7: Est-il possible d'atteindre votre PC depuis le LAN du laboratoire (par un ping par exemple) ? Expliquez pourquoi. Quelle(s) adresse(s) utilisez-vous pour le ping ?
P8: Expliquer les avantages/inconvénients du NAT statique par rapport au NAT dynamique.

- Relancez les mesures (analyseur de protocole, telnet, …)

P9: Quels sont les adresses IP utilisées et libres dans le pool d'adresse *public-access* ?

5. PAT

Le PAT (*Port Address Translation*) permet de partager une adresse IP public avec plusieurs adresses IP privées utilisées dans votre réseau internet.

- Suppression du NAT dynamique :

```
rlte<x>#clear ip nat translation *
rlte<x>#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)# no ip nat pool public-access 160.98.30.<a> 160.98.30.<a+3>
rlte<x>(config)# no ip nat inside source list 1 pool public-access
rlte<x>(config)#end
rlte<x>#
```

Avec a = 212 pour la table LTE02
a = 216 pour la table LTE03
a = 220 pour la table LTE04
a = 224 pour la table LTE05
a = 228 pour la table LTE06
a = 232 pour la table LTE07
a = 236 pour la table LTE08
a = 240 pour la table LTE09
a = 244 pour la table LTE10

- Configuration du PAT :

```
rlte<x>#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rlte<x>(config)# ip nat inside source list 1 interface FastEthernet 0/1 overload
rlte<x>(config)#end
rlte<x>#
```

Commentaire

Avant l'analyse des trames, n'oubliez pas de tester votre configuration en effectuant un « ping » depuis votre PC sur une machine de l'école, par exemple tlabs.tic.heia-fr.ch (160.98.31.32) ou merlin.tic.heia-fr.ch (160.98.31.207)

- Configurez un filtre de station IP et de protocole IP telnet pour ne retenir que les échanges provenant de votre PC
- Démarrez l'analyseur de protocole sur le LAN du laboratoire et sur votre PC.
- Effectuez un telnet depuis votre PC sur merlin.tic.heia-fr.ch (160.98.31.207). Sans vous authentifier.
- Les commandes à utiliser sont les mêmes qu'à la mesure précédente.

Questions :

P10: Quelle adresse IP source est utilisée par votre PC pour accéder au serveur merlin.tic.heia-fr.ch (des deux côtés du routeur) ?

P11: Quels ports de source et de destination sont utilisés dans les trames échangées, des deux côtés du routeur ? Est-ce les mêmes des deux côtés du routeur ? Commentez.

- Modifiez l'adresse de votre PC, configurez à nouveau 10.<x>.0.2/24.
- Relancez les mesures (wireshark, telnet, …)

Questions :

P12: Est-il possible d'atteindre votre PC depuis le LAN du laboratoire (par un ping par exemple) ? Expliquez pourquoi.

P13: Quelle adresse IP source est utilisée par votre PC pour accéder au serveur merlin.tic.heia-fr.ch (des deux côtés du routeur) ?

P14: Quels ports de source et de destination sont utilisés dans les trames échangées, des deux côtés du routeur ? Est-ce les mêmes des deux côtés du routeur ? Comparez vos résultats avec la question P11.

P15: Que trouvez-vous comme informations dans la table de translation du routeur ? (avec la commande « `show ip nat translation` »

P16: Expliquer les avantages/inconvénients du PAT par rapport au NAT.

6. RÉFÉRENCES / DOCUMENTATIONS

[1] RFC 3022 (NAT)
[2] D. Comer, TCP/IP vol. 1. Prentice-Hall.
[3] T. Martinson/F. Buntschu, Notes de cours Réseaux IP

7. TEMPS À DISPOSITION ET RAPPORT

La séance dure 4 périodes. Un rapport contenant mesures et explications doit être rendu au plus tard 7 jours après la réalisation du TP. Le rapport insistera plus sur ce qui a été observé que sur l'exactitude absolue des réponses.

ANNEXE : MODE DE CONFIGURATION DES ROUTEURS CISCO

La figure ci-dessous présente les différents modes d'exploitation des routeurs Cisco 2600 ainsi que la manière de passer d'un mode à l'autre. Les pages qui suivent présentent les fonctions disponibles dans chacun des modes.

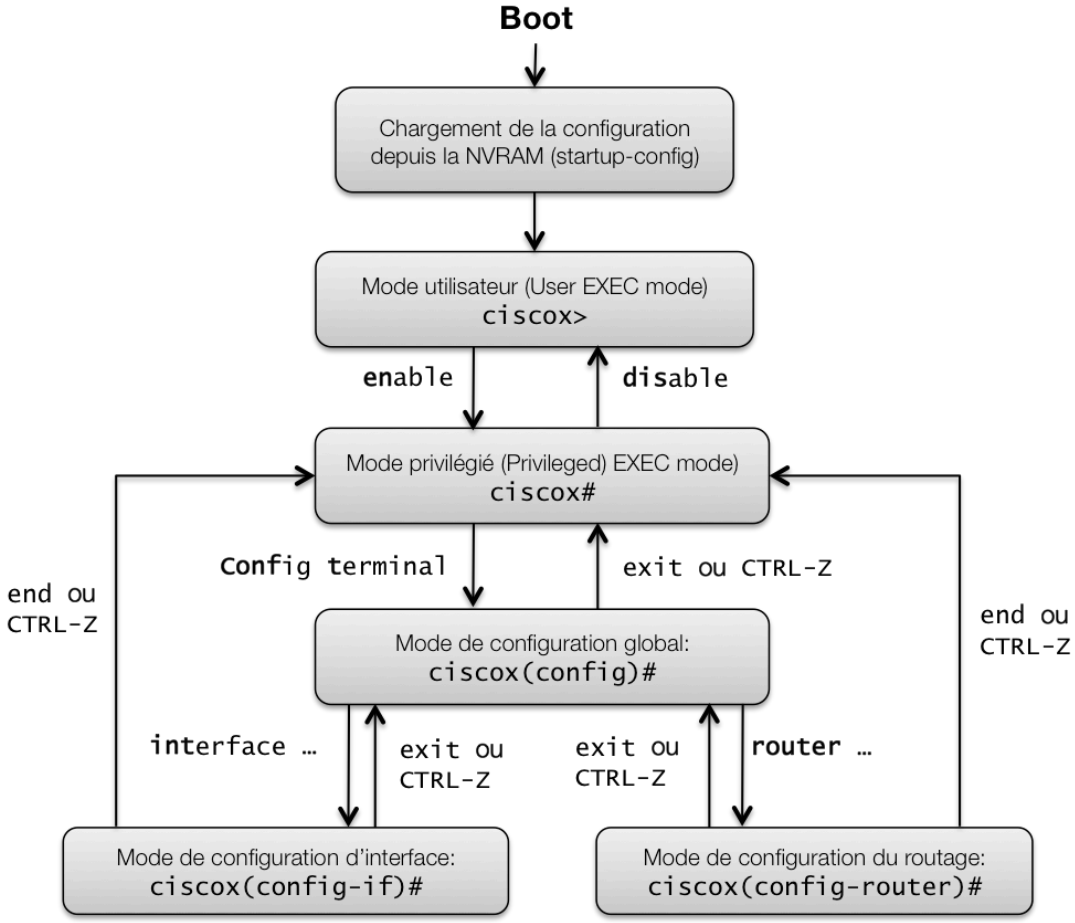

Figure 2 ***: Mode de configuration***