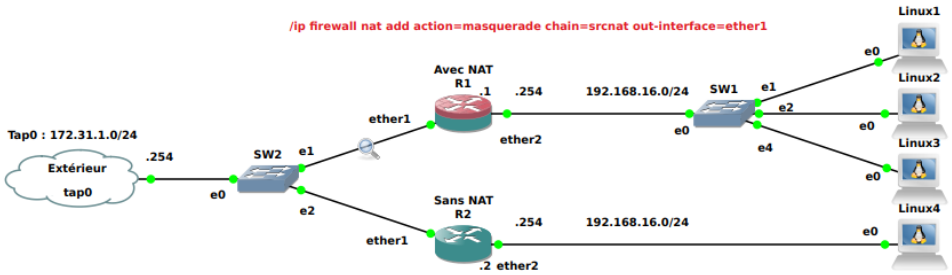
UNIVERSITÉ CAEN NORMANDIE

TP NAT-1

29.01.2023

On masque les @IP privées ☺

Auteur : Pascal Fougeray



Source : Moi ☺

1 Préambule

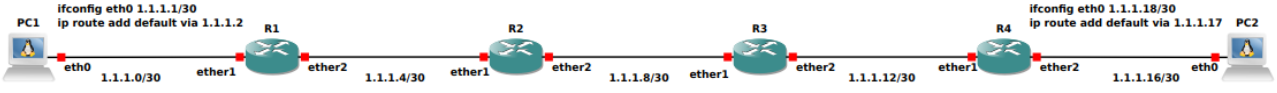
— Ce TP peut être fait chez vous, il n'y a aucune difficulté majeure, il ne va pas vous occuper 2h30 !☺
— On travaille dans la VM et qu'avec les logiciels GNS3 et Wireshark
— Vous devez vous rappeler ce que donne un serveur DHCP à un client.
— **Prenez des notes sur ce que vous comprenez, ces notes vous y aurez le droit de les avoir avec vous au CT !**

2 Introduction

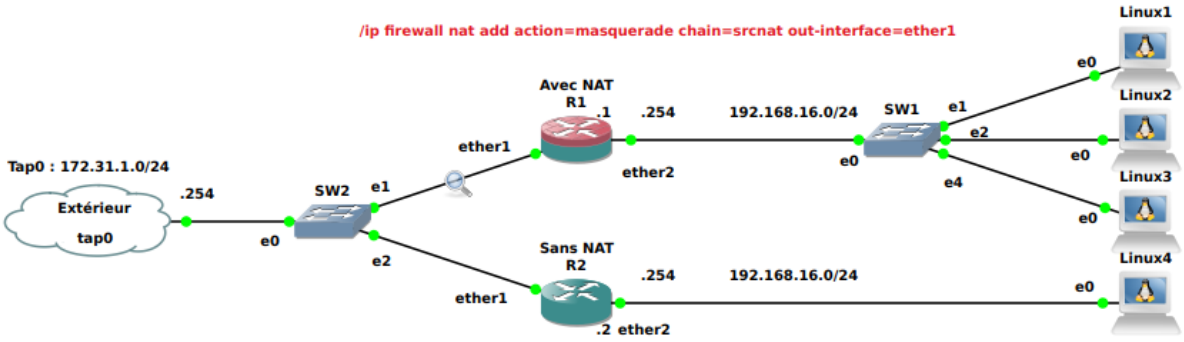
Dans ce TP, je vous propose de **voir** :
— Les adresses IP publiques et privées
— Le principe du NAT et surtout son intérêt !
— etc...

3 L'étude théorique

Soit la structure suivante que nous avons vue au TP intitulé **Ping et traceroute**



1. Si PC1 ping PC2 : Quelles sont les @IP que l'ont relèverait avec wireshark si on mettait une sonde sur chaque câble ?
2. Est-ce toujours la même ?
   Soit la première structure suivante, ☺**/ip firewall nat add action=masquerade chain=srcnat out-interface=ether2**



3. Les 2 réseaux connectés directement aux Linux ont la même valeur 192.168.16.0/24, est-ce que cela pose un problème ?
4. **Sans** le NAT, sachant que la VM représentée ici par l'interface Tap0 ne connaît pas le réseau 192.168.16.0/24 et que sa passerelle n'est pas 172.31.1.2 (Ether1 de R2) peut-elle répondre à un ping de Linux 4.
   Si **non** pourquoi ?
5. **Avec** le NAT, sachant que la VM représentée ici par l'interface Tap0 ne connaît pas le réseau 192.168.16.0/24 et que sa passerelle n'est pas 172.31.1.1 (Ether1 de R1) peut-elle répondre à un ping de Linux 1 à Linux 3.
   Si **oui** pourquoi ?

4 L'étude pratique

Pour se loguer sur un routeur, le login est admin et il n'y a pas de MDP donc on valide

1. **Récupérez** sur ecampus le Projet **TP-NAT-1**
2. **Ouvrez**-le dans GNS3
3. **Lancez** toutes les machines**.**
4. **Relevez** les @IP de Linux1 à Linux4
5. **Expliquez**, en regardant la conf de R1 et/ou de R2 comment les Linux1 à Linux4 ont obtenu ces IP
6. **Relevez** le contenu du fichier **/etc/resolv.conf** de Linux1 à Linux4
7. Comment les Linux1 à Linux4 ont obtenu ce contenu ?
8. Sur Linux1 à Linux4, **lancez** la commande ***ip route ls***
   Quelle est leur route par défaut ?
   Comment les Linux1 à Linux4 ont obtenu cette route par défaut ?
9. **Mettez** une sonde wireshark sur les 2 câbles entre les 2 routeurs et le **switch SW2**
10. **Sélectionnez** un filtre de manière à ne voir que de l'**ICMP**
11. Sur la machine Linux4 **lancez** la commande ***ping 172.31.1.254 -c 4***
12. Quelle est l'adresse source et l'adresse destination ?
    Est-ce logique par rapport au TP sur Ping et ICMP ?
    OUI ! ! !
13. Sur les machines Linux1 à Linux3 **lancez** la commande ***ping 172.31.1.254 -c X*** *avec*
    (a) X = 1 pour Linux1,
    (b) X = 2 pour Linux2
    (c) X = 2 pour Linux3
14. **Relevez** sur la capture wireshark, l'@IP source et l'@IP destination des 6 paquets.
15. Est-ce conforme aux adresses relevées à la question 4 : **Relevez** les @IP de Linux1 à Linux4 ?
    Si non **expliquez** pourquoi !

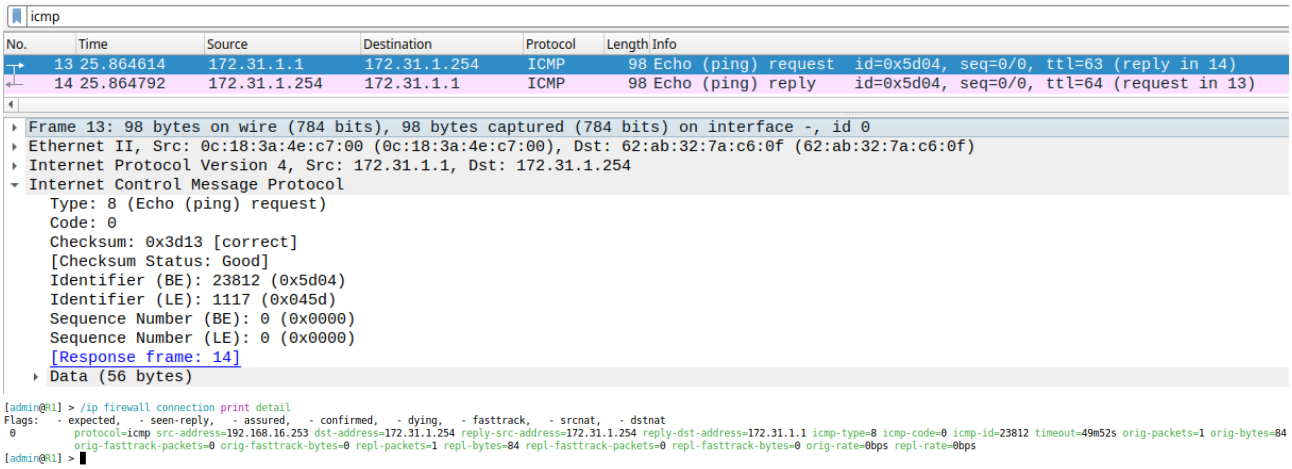
16. Comment peut-on différencier les 3 Linux1 à 3 sur les captures ?
    ATTENTION le cache n'est que de quelques secondes donc au bout de ces quelques secondes on perd les connexions.
    J'ai modifié cela en lançant sur le routeur la commande
    /ip firewall connection tracking set enabled=yes icmp-timeout=300
    Ce qui vous laisse 5mn pour lancer la commande ***/ip firewall connection print detail*** et voir les connexions
17. Sur le routeur R1, **lancez** la commande ***/ip firewall connection print detail***
    Vous devez obtenir quelque chose comme cela

```
[admin@R1] /ip firewall connection> print detail
Flags:   - expected,   - seen-reply,   - assured,   - confirmed,   - dying,   - fasttrack,   - srcnat,   - dstnat
 0          protocol=icmp src-address=192.168.16.253 dst-address=172.31.1.254 reply-src-address=172.31.1.254 reply-dst-address=172.31.1.1 icmp-type=8 icmp-code=0 icmp-id=14852 timeout=42s orig-packets=1 orig-bytes=84
            orig-fasttrack-packets=0 orig-fasttrack-bytes=0 repl-packets=1 repl-bytes=84 repl-fasttrack-packets=0 repl-fasttrack-bytes=0 orig-rate=0bps repl-rate=0bps

 1          protocol=icmp src-address=192.168.16.252 dst-address=172.31.1.254 reply-src-address=172.31.1.254 reply-dst-address=172.31.1.1 icmp-type=8 icmp-code=0 icmp-id=11268 timeout=45s orig-packets=2 orig-bytes=168
            orig-fasttrack-packets=0 orig-fasttrack-bytes=0 repl-packets=2 repl-bytes=168 repl-fasttrack-packets=0 repl-fasttrack-bytes=0 orig-rate=0bps repl-rate=0bps

 2          protocol=icmp src-address=192.168.16.251 dst-address=172.31.1.254 reply-src-address=172.31.1.254 reply-dst-address=172.31.1.1 icmp-type=8 icmp-code=0 icmp-id=12548 timeout=49s orig-packets=3 orig-bytes=252
            orig-fasttrack-packets=0 orig-fasttrack-bytes=0 repl-packets=3 repl-bytes=252 repl-fasttrack-packets=0 repl-fasttrack-bytes=0 orig-rate=1344bps repl-rate=1344bps
[admin@R1] /ip firewall connection>
```

18. Dans la réponse précédente selon vous quelle champ permet au routeur vers quelle Linux 1-2-3 envoyer la réponse ?
    Je vous laisse chercher seul-e ? ☺
    Allez je vous aide ?



    Réponse : 5d04 en base 16 fait 23812 en base 10 ☺
19. Vous pouvez aussi lancer la commande ***/ip firewall connection print append***

```
[admin@R1] /ip firewall connection> print append
Flags:   - expected,   - seen-reply,   - assured,   - confirmed,   - dying,   - fasttrack,   - srcnat,   - dstnat

0         icmp    192.168.16.252      172.31.1.254                4m30s          0bps      0bps          2          2          168          168
1         icmp    192.168.16.251      172.31.1.254                4m35s          0bps      0bps          3          3          252          252
2         icmp    192.168.16.253      172.31.1.254                4m26s          0bps      0bps          1          1           84           84
```

    Remarque on ne voit pas les FLAGS, cela est dû à un bug de la console ! ! !
20. **Passez** votre souris dessus et vous les verrez

```
[admin@R1] /ip firewall connection> print detail
Flags:   - expected,   - seen-reply,   - assured,   - confirmed,   - dying,
 0  S C  s  protocol=icmp src-address=192.168.16.253 dst-address=172.31.1.254
          orig-fasttrack-packets=0 orig-fasttrack-bytes=0 repl-packets=1 repl

 1  S C  s  protocol=icmp src-address=192.168.16.252 dst-address=172.31.1.254
          orig-fasttrack-packets=0 orig-fasttrack-bytes=0 repl-packets=2 repl

 2  S C  s  protocol=icmp src-address=192.168.16.251 dst-address=172.31.1.254
          orig-fasttrack-packets=0 orig-fasttrack-bytes=0 repl-packets=3 repl
[admin@R1] /ip firewall connection>
```

21. Que **comprenez-vous** dans cette commande de configuration du routeur R1 ?
    /ip firewall nat add action=masquerade chain=srcnat out-interface=ether2
22. Questions de logique
    (a) À quoi sert le NAT ?
    (b) **Pensez**-vous que votre Box chez vous fait du NAT ?

5 Conclusion

Le NAT a permis qu'avec pas assez d'@IP on connecte beaucoup de gens avec une seule IP ! ! !

Chaque paquet IP que vous envoyez sur internet a un identifiant et c'est cet identifiant qui permet de savoir si c'est Pierre, Paul ou Jacques qui a contacté tel ou tel serveur !

Dans le prochain TP sur le NAT intitulé **TP-NAT-2 le retour** ☺, je vous propose de cacher le serveur Web de la FAC !