- TP 7 -
Translation d'adresse réseau NAT pour IPv4

par Édouard Lumet & [redacted]

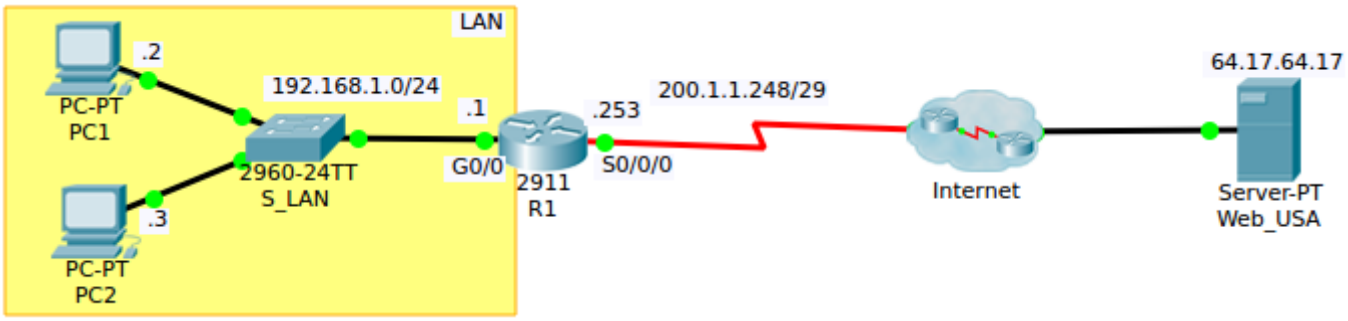
Sommaire

Introduction

Le NAT (**Network Address Translation** dans la langue de Shakespeare, ou **Traduction d'adresses réseau** dans la langue de molière) permet entre autres à un hôte ayant une adresse IP privée d'emprunter l'adresse IP publique du routeur NAT. Différents types de NAT existent pour répondre désormais au manque d'adresses IPv4. En effet, un particulier ou une petite entreprise n'a en général qu'une seule adresse IPv4 pour plusieurs machines… de même pour les grandes entreprises qui peuvent avoir plusieurs adresses IPv4 mais toujours pas autant que de machines dans leur réseau. Il y a donc un besoin d'exploiter au maximum la ou les adresses IPv4 publiques en configurant un NAT statique, dynamique ou NAT overload et PAT en utilisant les ports (couche 4).

1. Configuration de NAT statique, NAT dynamique avec/sans surcharge, de PAT

1.1. Topologie pour cet exercice



M2103_TP7_Topo1_NAT_Stat_Dyn.pkt

1.2. Configuration de NAT statique

Nous allons ici configurer le NAT statique, qui consiste à prêter une adresse publique à une machine, configuration que l'on privilégie pour les serveurs.

- De prime abord, PC1 et le serveur Web_USA ne peuvent pas communiquer ensemble, l'adresse de PC1 étant privé et donc non routable sur Internet :

```
PC>ping 64.17.64.17

Pinging 64.17.64.17 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

*Ping PC1 (192.168.1.2) > Web_USA (64.17.64.17) : **NOK***

- On configure le NAT statique sur le routeur R1 avec les traductions suivantes : 192.168.1.2 ↔ 200.1.1.249 et 192.168.1.3 ↔ 200.1.1.250
  NB : les commandes sont présentes dans la fiche d'intervention jointe

- Avec le bloc d'adresses 200.1.1.248/29, on dispose des adresses hôtes 200.1.1.249 à 200.1.1.254 sachant que les deux dernières sont déjà attribuées aux routeurs. On peut donc configurer 4 hôtes au maximum en NAT statique.

- La commande **#show ip nat translations** permet d'afficher la table NAT :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  200.1.1.249       192.168.1.2        ---                ---
---  200.1.1.250       192.168.1.3        ---                ---
```

- On effectue de nouveau un ping de PC1 vers Web_USA puis de Web_USA vers PC1. Pour ce dernier test de ping, on utilise l'adresse globale interne de PC1 soit 200.1.1.249 :

Voir page suivante

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.249:10    192.168.1.2:10     64.17.64.17:10     64.17.64.17:10
icmp 200.1.1.249:11    192.168.1.2:11     64.17.64.17:11     64.17.64.17:11
icmp 200.1.1.249:12    192.168.1.2:12     64.17.64.17:12     64.17.64.17:12
icmp 200.1.1.249:1     192.168.1.2:1      64.17.64.17:1      64.17.64.17:1
icmp 200.1.1.249:2     192.168.1.2:2      64.17.64.17:2      64.17.64.17:2
icmp 200.1.1.249:3     192.168.1.2:3      64.17.64.17:3      64.17.64.17:3
icmp 200.1.1.249:4     192.168.1.2:4      64.17.64.17:4      64.17.64.17:4
icmp 200.1.1.249:9     192.168.1.2:9      64.17.64.17:9      64.17.64.17:9
---  200.1.1.249       192.168.1.2        ---                ---
---  200.1.1.250       192.168.1.3        ---                ---
```

Table NAT de R1 après pings PC1 > Web_USA / Web_USA > PC1

On peut voir les 8 traductions d'adresses effectuées pour le protocole ICMP, soit les 4 tests de ping PC1 > Web_USA et les 4 pings dans le sens inverse.

- On tente maintenant une requête web depuis PC1 vers le serveur Web_USA avant de réafficher la table NAT :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  200.1.1.249       192.168.1.2        ---                ---
---  200.1.1.250       192.168.1.3        ---                ---
tcp 200.1.1.249:1025   192.168.1.2:1025   64.17.64.17:80     64.17.64.17:80
```

Table NAT après requête web PC1 > Web_USA

On reconnaît l'adresse interne locale (inside local) qui correspond à l'adresse privée de l'hôte PC1 et l'adresse interne globale (inside globale) qui correspond à l'adresse publique prêtée par R1 à PC1.

- La commande **#show ip nat statistics** permet quant à elle de visualiser les statistiques NAT :

```
R1#show ip nat statistics
Total translations: 3 (2 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0
Hits: 14  Misses: 9
Expired translations: 8
Dynamic mappings:
```

Statistiques/Infos NAT du routeur R1

On identifie ici l'interface du réseau interne : gi0/0 (LAN) ; et l'interface du réseau externe : s0/0/0 (Internet)

1.3. Config de NAT dynamique (sans surcharge)

Ici on onfigure le NAT dynamique selon la même logique que précédemment. La différence à noter est que l'on attribue par une adresse par machine mais un pool d'adresses publiques pour un ensemble de machines. Les machines n'emprunteront donc une adresse que pour la durée d'une session.

- On configure alors cette fonction NAT sur le routeur en définissant quel ensemble de machines peut recourir à la fonction NAT, via une ACL. Puis on définit un pool que l'on lie ensuite à l'ACL avant de définir le réseau interne et le réseau externe.

Pour rappel, les commandes sont listées et commentées dans la fiche d'intervention

- On affiche la table NAT et les statistiques NAT :

```
R1#show ip nat translations
R1#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool POOL_NAT refCount 0
 pool POOL_NAT: netmask 255.255.255.248
       start 200.1.1.249 end 200.1.1.252
       type generic, total addresses 4 , allocated 0 (0%), misses 0
```

Traductions et statistiques NAT dynamique sur R1

On peut voir que la table NAT est vide dans le cas du NAT dynamique lorsque aucune traduction n'a été faite. En effet, comme nous l'avons vu, aucune adresse publique n'est prêtée de façon permanente à une machine physique.

- On effectue alors les tests de ping vers Web_USA :

```
PC>ping 64.17.64.17

Pinging 64.17.64.17 with 32 bytes of data:

Reply from 64.17.64.17: bytes=32 time=1ms TTL=126
Reply from 64.17.64.17: byt
Reply from 64.17.64.17: byt
Reply from 64.17.64.17: byt
```

Ping PC1 > Web_USA

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.249:3     192.168.1.2:3      64.17.64.17:3      64.17.64.17:3
icmp 200.1.1.249:4     192.168.1.2:4      64.17.64.17:4      64.17.64.17:4
icmp 200.1.1.249:5     192.168.1.2:5      64.17.64.17:5      64.17.64.17:5
icmp 200.1.1.249:6     192.168.1.2:6      64.17.64.17:6      64.17.64.17:6
```

Table NAT suite au ping de PC1 vers Web_USA

L'adresse globale interne ici utilisée est 200.1.1.249, soit la première adresse disponible dans le pool NAT dynamique que nous avons configuré.

- Web_USA ne peut donc pas pinguer les PCs de notre LAN puisque ces derniers n'ont pas d'adresse publique, ils n'en empruntent une que pour initier une connexion de façon dynamique et le temps d'une session sur Internet.
- Après quelques temps, la table NAT se vide à nouveau et il n'y a plus aucune entrée dans celle-ci.
- On tente une connexion web au serveur Web_USA et on affiche la table NAT :

```
R1#show ip nat statistics
Total translations: 17 (0 static, 17 dynamic, 17 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: GigabitEthernet0/0
Hits: 110  Misses: 27
Expired translations: 10
Dynamic mappings:
-- Inside Source
access-list 1 pool POOL_NAT refCount 17
 pool POOL_NAT: netmask 255.255.255.248
       start 200.1.1.249 end 200.1.1.252
       type generic, total addresses 4 , allocated 2 (50%), misses 0
```

Statistiques/Infos NAT sur R1 suite à la connexion Web

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.249:12    192.168.1.2:12     64.17.64.17:12     64.17.64.17:12
icmp 200.1.1.249:13    192.168.1.2:13     64.17.64.17:13     64.17.64.17:13
icmp 200.1.1.249:14    192.168.1.2:14     64.17.64.17:14     64.17.64.17:14
tcp 200.1.1.249:1030   192.168.1.2:1030   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.249:1031   192.168.1.2:1031   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.249:1032   192.168.1.2:1032   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.249:1033   192.168.1.2:1033   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.249:1034   192.168.1.2:1034   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.250:1025   192.168.1.3:1025   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.250:1026   192.168.1.3:1026   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.250:1027   192.168.1.3:1027   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.250:1028   192.168.1.3:1028   64.17.64.17:80     64.17.64.17:80
```

Table NAT suite à la connexion web

On remarque que sur un totale de 4 adresses, 2 adresses ont été allouées (voir statistiques NAT en fin de page précédente). Ensuite, on peut voir dans la table NAT les connexions TCP liées au trafic web depuis PC1 et PC2 vers le serveur Web_USA. On voit que PC1 (192.168.1.2) a emprunté l'adresse globale interne 200.1.1.249 et que PC2 (192.168.1.3) a emprunté l'adresse globale interne 200.1.1.250.

- Avec cette solution NAT, un nombre illimité d'hôtes peut accéder à Internet puisque les adresses globales internes sont réutilisées. Cependant, simultanément 4 hôtes seulement peuvent accéder à Internet (comme on peut le voir dans les statistiques NAT).
- Pour autoriser davantage d'hôtes à accéder simultanément à Internet, il faut configurer le NAT dynamique avec surcharge (NAT overload).

1.4. Surcharge NAT (dynamique) = NAT overload

Le NAT overload consiste à utiliser un pool d'adresses publiques de façon dynamique comme nous l'avons vu dans la partie 1.3, en ajoutant en plus l'utilisation des numéros de port pour exploiter au maximum une même adresse globale interne. Un hôte sera donc identifié par le couple @ globale interne / port source.

- On configure alors le NAT overload sur R1 qui se configure comme le NAT dynamique configuré dans la sous partie précédente. On ajoute seulement le mot-clé **overload** dans une commande. *NB : les commandes sont toujours listées dans la fiche jointe*
- On effectue alors des tests de ping depuis les PCs vers le serveur Web_USA. Ils sont concluants.
- On peut alors afficher la table NAT pour voir les traductions NAT effectuées :

```
      type generic, total addresses 4 , allocated 1 (25%), misses 0
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.249:1024  192.168.1.3:1      64.17.64.17:1      64.17.64.17:1024
icmp 200.1.1.249:1025  192.168.1.3:2      64.17.64.17:2      64.17.64.17:1025
icmp 200.1.1.249:1026  192.168.1.3:3      64.17.64.17:3      64.17.64.17:1026
icmp 200.1.1.249:1027  192.168.1.3:4      64.17.64.17:4      64.17.64.17:1027
icmp 200.1.1.249:1     192.168.1.2:1      64.17.64.17:1      64.17.64.17:1
icmp 200.1.1.249:2     192.168.1.2:2      17.64.17.64:2      17.64.17.64:2
icmp 200.1.1.249:3     192.168.1.2:3      17.64.17.64:3      17.64.17.64:3
icmp 200.1.1.249:4     192.168.1.2:4      17.64.17.64:4      17.64.17.64:4
icmp 200.1.1.249:5     192.168.1.2:5      17.64.17.64:5      17.64.17.64:5
icmp 200.1.1.249:6     192.168.1.2:6      64.17.64.17:6      64.17.64.17:6
icmp 200.1.1.249:7     192.168.1.2:7      64.17.64.17:7      64.17.64.17:7
icmp 200.1.1.249:8     192.168.1.2:8      64.17.64.17:8      64.17.64.17:8
icmp 200.1.1.249:9     192.168.1.2:9      64.17.64.17:9      64.17.64.17:9
```

Table NAT après tests de ping depuis PCs vers Web_USA

En haut de la capture, on voit qu'une seule adresse du pool NAT a été attribuée. En effet, dans la table NAT, on peut voir que seule l'adresse globale interne 200.1.1.249 est utilisée pour PC1 et PC2. Cependant, PC1 (192.168.1.2) est identifié par les ports > 1 et PC2 (192.168.1.3) par les ports > 1024.

- On vide la table NAT à l'aide de la commande **#clear ip nat translation *** avant d'initier une connexion web depuis PC1 et PC2 vers Web_USA. On affiche alors à nouveau la table NAT :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 200.1.1.249:1024   192.168.1.3:1025   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.249:1025   192.168.1.2:1025   64.17.64.17:80     64.17.64.17:80
```

Table NAT après connexion web

On peut voir que PC1 et PC2 ont tous deux emprunté l'adresse globale interne 209.1.1.249, avec le port source 1024 pour PC2 (192.168.1.3) et le port source 1025 pour PC1 (192.168.1.2).

- Dans ce mode, une machine sur Internet ne peut pas initier de connexion avec un serveur situé sur le LAN de l'entreprise, pour les mêmes raisons que pour le NAT dynamique vu dans la partie 1.3.

1.5. Configuration de PAT

Le PAT classique est basé sur le même principe que la NAT overload vu précédemment, que l'on appelle par ailleurs PAT overload. Ici, on n'utilise plus un pool d'adresses globales internes mais une seule adresse. Cette configuration est la configuration la plus courante dans un réseau particulier ou de petite entreprise, soit n'ayant qu'une seule adresse IPv4 publique.

- On configure alors cette fonction sur le routeur en créant une ACL pour indiquer quelles adresses du LAN peuvent recourir au PAT. Puis on lie cette ACL à l'interface ayant l'adresse publique à utiliser et en indiquant **overload**. On identifie également les interfaces interne et externe pour le NAT. *Pour rappel, les commandes sont listées et commentées dans la fiche jointe.*
- On effectue alors des tests de ping depuis les PCs vers le serveur Web_USA et on affiche la table NAT :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.253:1024  192.168.1.3:1      64.17.64.17:1      64.17.64.17:1024
icmp 200.1.1.253:1025  192.168.1.3:2      64.17.64.17:2      64.17.64.17:1025
icmp 200.1.1.253:1026  192.168.1.3:3      64.17.64.17:3      64.17.64.17:1026
icmp 200.1.1.253:1027  192.168.1.3:4      64.17.64.17:4      64.17.64.17:1027
icmp 200.1.1.253:1     192.168.1.2:1      64.17.64.17:1      64.17.64.17:1
icmp 200.1.1.253:2     192.168.1.2:2      64.17.64.17:2      64.17.64.17:2
icmp 200.1.1.253:3     192.168.1.2:3      64.17.64.17:3      64.17.64.17:3
icmp 200.1.1.253:4     192.168.1.2:4      64.17.64.17:4      64.17.64.17:4
```

Table NAT après tests de ping PCs > Web_USA

Ici, c'est désormais l'adresse de l'interface s0/0/0 (côté Internet) du routeur qui est utilisée par les machines hôtes. De plus, les deux PCs utilisent cette même adresse, mais avec des ports différents comme pour le NAT overload.

- On vide à nouveau la table NAT (**#clear ip nat translation ***) :
- On se connecte au serveur en web depuis les deux PCs puis on consulte la table NAT :

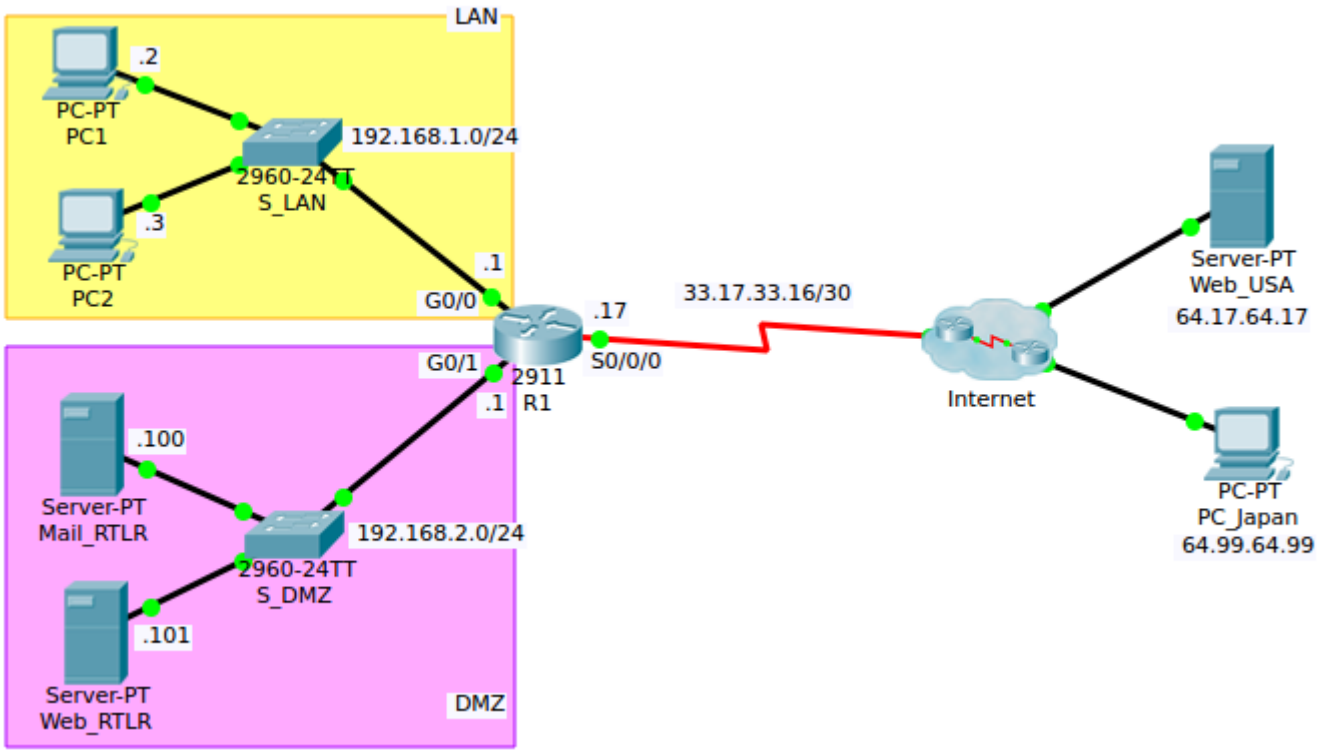
```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 200.1.1.253:1024   192.168.1.3:1025   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.253:1025   192.168.1.2:1025   64.17.64.17:80     64.17.64.17:80
tcp 200.1.1.253:1026   192.168.1.3:1026   64.17.64.17:80     64.17.64.17:80
```

Table NAT suite aux connexions Web

De même que pour les pings, chaque PC est identifié par un port source associé à l'adresse globale interne de R1. Ils utilisent tous les deux cette même adresse.

- Dans ce mode, une machine sur Internet ne peut toujours pas initier de connexion avec une machine de LAN car cette association d'adresse via le port n'est pas permanente. En effet, après quelques dizaines de secondes la table NAT est à nouveau vide.

2. NAT pour topologie réseau avec DMZ



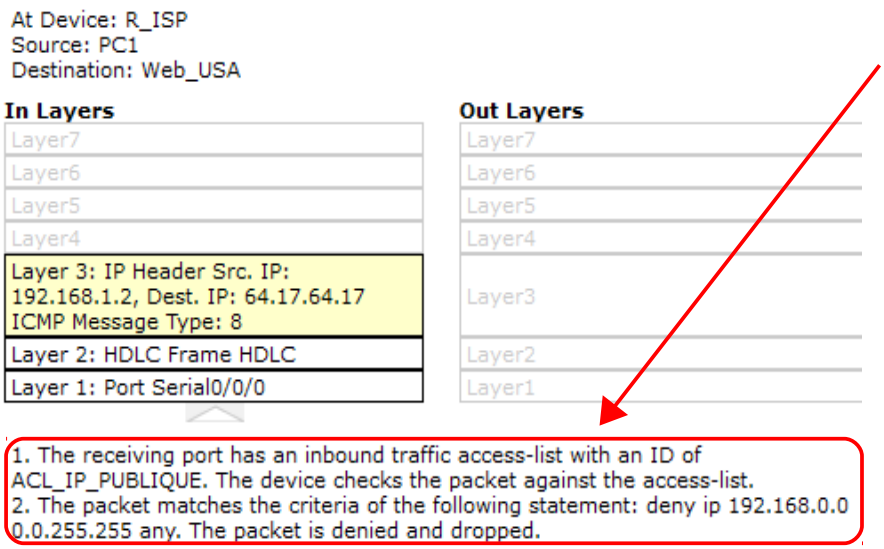
M2103_TP7_Topo3_NAT_DMZ.pkt

Périphérique	Interface	Adresse IPv4 / Longueur préfixe
R1	gi0/0	192.168.1.1/24
	gi0/1	192.168.2.1/24
	s0/0/0	33.17.33.17/30
PC1	NIC	192.168.1.2/24
PC2	NIC	192.168.1.3/24
Mail_RTLR	NIC	192.168.2.100/24
Web_RTLR	NIC	192.168.2.101/24
Web_USA	NIC	64.17.61.17
PC_Japan	NIC	64.99.64.99

2.1. Analyse préalable

- Sans aucune configuration, les tests de ping depuis les PCs vers les machines sur Internet ne sont pas concluants. En effet, les adresses IPv4 privées ne sont pas routables sur Internet :

Voir page suivante



Modèle OSI du paquet ICMP NOK vers Internet

Comme nous l'indique Packet Tracer, une ACL sur le routeur du fournisseur d'accès à Internet interdit les paquets dont l'adresse de destination appartient au réseau 192.168.0.0/16. C'est en effet un des ensembles d'adresses privées non routables sur Inetrnet.

- En revanche, depuis R1, les pings sont fonctionnels vers les deux machines sur Internet comme on peut le voir ici :

```
R1(config)#do ping 64.99.64.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.99.64.99, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/7 ms

R1(config)#do ping 64.17.64.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.17.64.17, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/5/10 ms
```

Pings R1 > PC_Japan puis R1 > Web_USA

- Pour finir, on effectue des test de ping entre les machines du LAN et celles de la DMZ. Ceux-ci sont consluants :

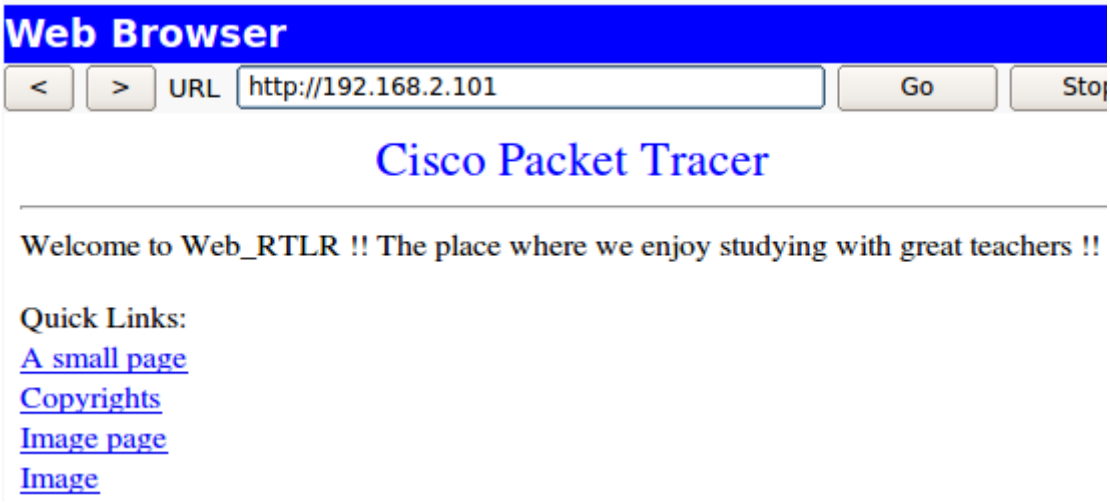
```
PC>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.100: bytes=32 time=0ms TTL=127
Reply from 192.168.2.100: bytes=32 time=0ms TTL=127
Reply from 192.168.2.100: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.2.101

Pinging 192.168.2.101 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.101: bytes=32 time=1ms TTL=127
Reply from 192.168.2.101: bytes=32 time=0ms TTL=127
Reply from 192.168.2.101: bytes=32 time=0ms TTL=127
```

Pings PC1 vers Mail_RTLR puis Web_RTLR

2.2. Configuration de l'accès aux serveurs RTLR

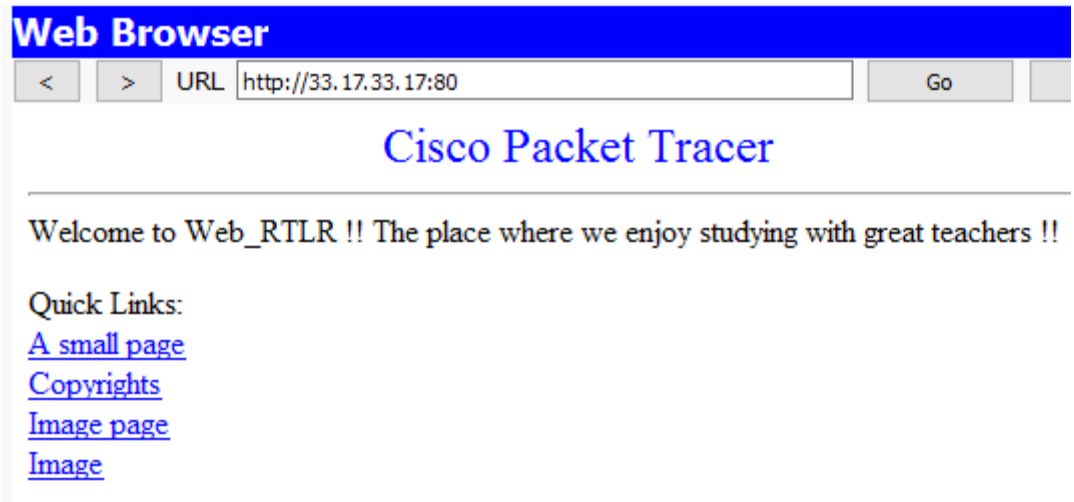
On commence par configurer l'accès aux machines de la DMZ depuis Internet.

- Pour accéder au serveur Web_RTLR depuis PC1 par exemple, il faut composer l'adresse IP du serveur soit 192.168.2.101 dans le navigateur.



Navigateur Web du PC1 (accès au serveur Web_RTLR)

- Les machines sur Internet ne peuvent, elles, pas accéder aux serveurs de la DMZ puisqu'ils disposent d'adresses IPv4 privées.
- La fonctionnalité NAT à implanter est une redirection de ports (port forwarding). Lorsque l'on accède à l'adresse publique du routeur via le port 80 par exemple, la requête sera alors redirigée vers le serveur Web_RTLR (192.168.2.101) sur le même port. Le client sur Internet doit alors saisir l'adresse 33.17.33.17 dans son navigateur Web.
- On configure alors la redirection de ports sur R1 en conséquence (*voir fiche d'intervention*).
- La machine PC_Japan par exemple peut alors accéder au site Web_RTLR entre autres :



Accès web depuis PC_Japan vers Web_RTLR

2.3. Configuration de l'accès du LAN à Internet

Nous allons maintenant permettre aux machines du LAN d'accéder à Internet.

- Afin de ce faire, on peut configurer sur R1 la fonctionnalité PAT classique puisque nous ne disposons que d'une seule adresse publique.
- On configure R1 en conséquence. *Pour rappel, les commandes sont dans la fiche d'intervention*
- Les pings depuis les PCs vers Internet sont désormais fonctionnels :

```
PC>ping 64.17.64.17

Pinging 64.17.64.17 with 32 bytes of data:

Request timed out.
Reply from 64.17.64.17: bytes=32 time=1ms TTL=126
Reply from 64.17.64.17: bytes=32 time=1ms TTL=126
Reply from 64.17.64.17: bytes=32 time=1ms TTL=126

Ping statistics for 64.17.64.17:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

PC>ping 64.99.64.99

Pinging 64.99.64.99 with 32 bytes of data:

Request timed out.
Reply from 64.99.64.99: bytes=32 time=1ms TTL=126
Reply from 64.99.64.99: bytes=32 time=1ms TTL=126
Reply from 64.99.64.99: bytes=32 time=1ms TTL=126
```

Pings PC1 > Web_USA puis PC1 > PC_Japan

- Ensuite, on effectue quelques tests plus approfondis afin de saisir le fonctionnement. En mode simulation filtré sur TCP, on effectue une requête Web depuis PC1 vers Web_USA (64.17.64.17).
  - En amont de R1 :

Adresse source	Port source	Adresse destination	Port destination
192.168.1.2	1025	64.17.64.17	80

  - En aval de R1 :

Adresse source	Port source	Adresse destination	Port destination
33.17.33.17	1025	64.17.64.17	80

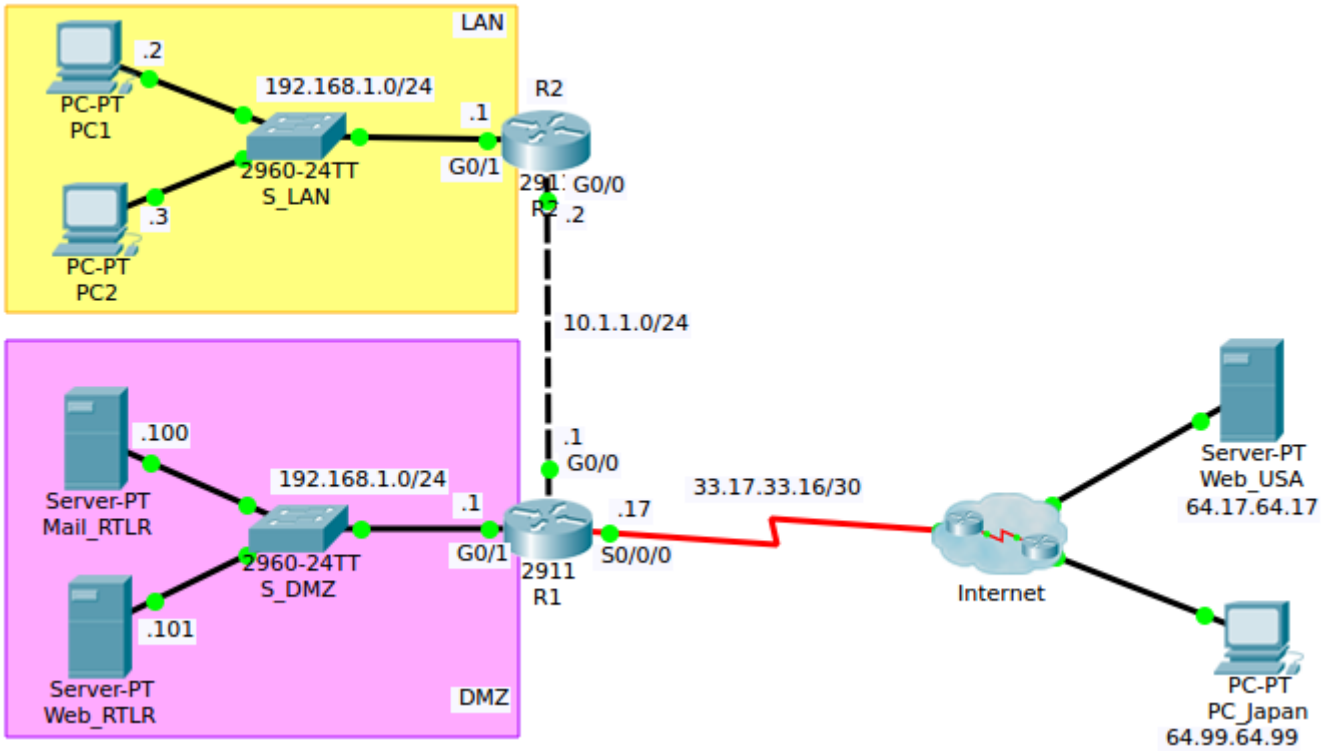
Comme nous l'avons vu précédemment (partie 1.5), PC1 emprunte l'unique adresse IP publique avec un numéro de port source retenu dans la table NAT du routeur car c'est le moyen, pour le PAT classique, d'identifier le trafic lié à au PC1.

- Conformément à la conclusion de la partie 1.5, il n'est pas possible d'accéder à PC1 par exemple depuis Internet puisque l'adresse 33.17.33.17 n'est empruntée que temporairement.

- Les machines sur Internet peuvent évidemment toujours accéder aux serveurs situés sur la DMZ, la redirection de ports étant toujours effective.
- Les machines de la DMZ peuvent aussi initier une connexion vers le réseau interne, ce qui peut poser problème du fait que ça soit la zone démilitarisée et donc avec une faible protection et étant directement accessible depuis Internet.

2.4. Modification de la topologie

- Le fait d'attribuer la même adresse réseau sur la DMZ et sur le LAN permet de cloisonner intégralement ces deux zones entre elles. En effet, lorsqu'une machine du LAN ou de la DMZ envoie un message à destination d'une adresse du réseau 192.168.1.0/24, elles ne contacteront pas la passerelle puisque c'est le même réseau. Le message ne sortira donc en aucun cas.



M2103_TP7_Topo4_NAT_DMZ.pkt

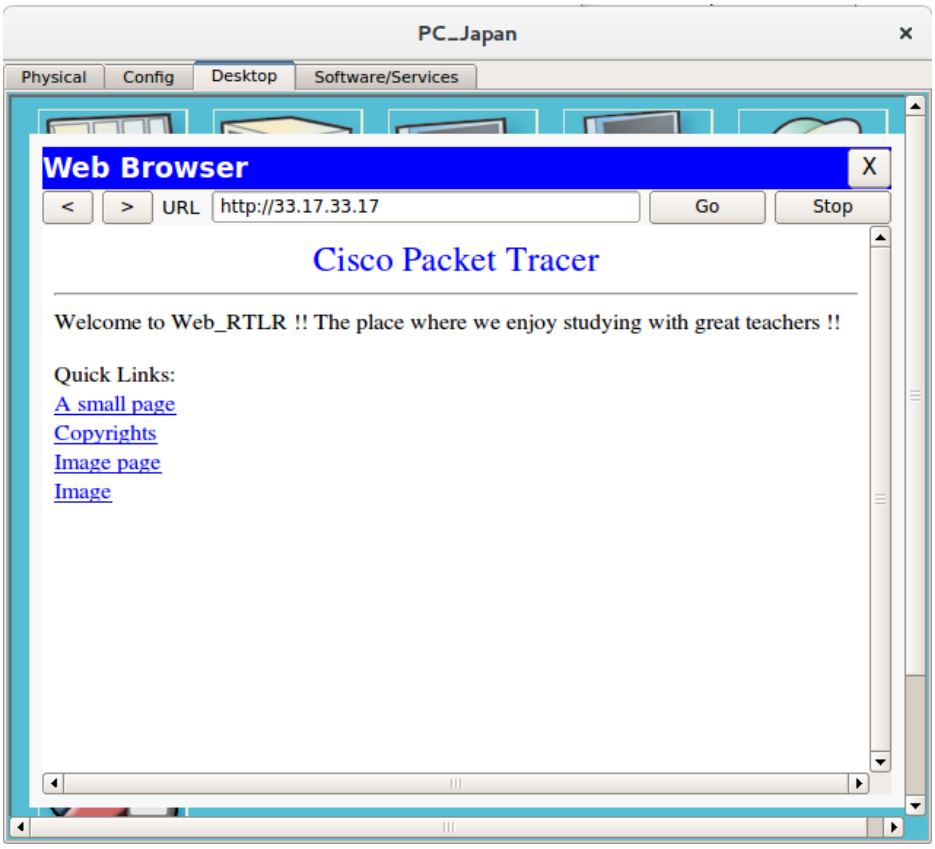
2.5. Configuration des routes par défaut

- Sur R1, on configure une route par défaut directement connectée via s0/0/0, soit vers Internet. Sur R2, on configure une route par défaut directement connectée via gi0/0, soit vers R1 le prochain saut vers Internet. Lors de la configuration de la seconde route, un message d'avertissement nous prévient qu'il n'est pas judicieux de ne pas préciser d'adresse de prochain saut pour une route vers un réseau à accès multiple. Cependant, ici c'est bien une connexion point à point. *Pour rappel, ces configurations sont commentées dans la fiche d'intervention*

2.6. Accès aux serveurs de la DMZ depuis Internet

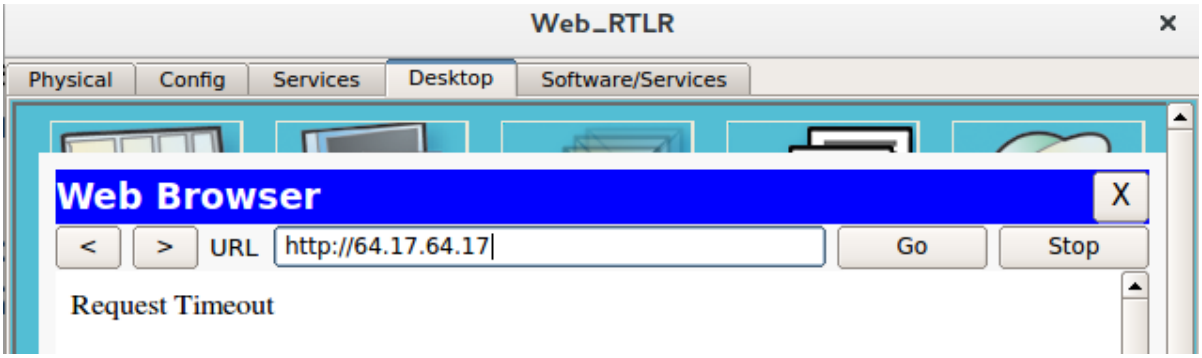
Dans un premier temps, on va permettre aux clients situés sur Internet d'accéder aux serveurs de la DMZ.

- Pour remplir ce premier objectif, nous devons configurer une redirection de ports comme pour la partie 2.2. On implémente alors cette fonctionnalité sur R1, le réseau interne pour le routeur NAT étant la DMZ (*voir fiche ci-jointe*).
- L'adresse à utiliser par un client sur Internet pour consulter le site Web_RTLR est alors l'adresse globale interne de R1 soit 33.17.33.17 :



Connexion web PC_Japan > Web_RTLR

- Les machines de la DMZ quant à elles ne peuvent pas initier de connexion vers les machines sur Internet car nous avons configuré pour la DMZ, une redirection de ports uniquement. Ces machines n'ont donc pas d'adresses publiques leur permettant d'accéder à Internet.



Test de connectivité web depuis Web_RTLR (DMZ) vers Web_USA (Internet)

2.7. Accès Internet pour le réseau 10.1.1.0/24

- Dans l'état actuel, aucun équipement du réseau 10.1.1.0/24 ne peut accéder à Internet car il n'y a pas de configuration NAT pour ce réseau d'adresses privées.
- Pour ce faire, il faut configurer la fonction PAT classique sur R1 afin de permettre à un grand nombre de machines d'accéder simultanément à Internet avec une seule adresse publique.

Voir la fiche d'intervention jointe pour la configuration

- Le ping de R2 vers PC_Japan est alors concluant :

```
R2#ping 64.99.64.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.99.64.99, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/2 ms
```

On peut désormais configurer l'accès à Internet pour le LAN via le réseau 10.1.1.0/24 qui bénéficie du PAT classique par R1.

2.8. Configuration de l'accès à Internet pour le LAN

- Pour l'instant, les PC du LAN ne peuvent pas accéder à Internet pour les mêmes raisons que le réseau 10.1.1.0/24 ne pouvait pas y accéder avant la partie 2.7.
- Pour donner un accès à Internet aux machines du LAN, il faut configurer sur R2 du NAT dynamique dont le pool d'adresses NAT est l'ensemble des adresses du réseau 10.1.1.0/24 disponibles. En effet, ce réseau dispose désormais d'un accès à Internet.

Voir la fiche d'intervention

- Une machine sur Internet ne peut pas initier une connexion avec du machine du LAN. Effectivement, entre le LAN et Internet, il y a deux traductions d'adresses dont un NAT dynamique et un PAT classique. Ces types de NAT ne permettent pas l'initialisation d'une connexion dans le sens réseau externe → réseau interne.

2.9. Configuration de l'accès à la DMZ pour le LAN

Pour finir la configuration, nous devons permettre aux machines du LAN d'initier une communication vers la DMZ.

- Actuellement, les PCs du LAN ne peuvent pas accéder aux serveurs de la DMZ car ils ont le même adressage. Si PC1 envoie un ping vers 192.168.1.100, il n'enverra pas sa requête à sa passerelle mais directement à cette machine via une requête ARP pour connaître son emplacement sur le réseau.
- On configure alors sur R2 des règles NAT statiques de substitution d'adresse de destination remplaçant l'adresse 192.168.2.100 par ex par 192.168.1.100 avant l'envoi sur la route par défaut. Cela permet de faire croire aux PCs du LAN que les machines de la DMZ ne sont pas dans le même réseau, envoyant à la passerelle.

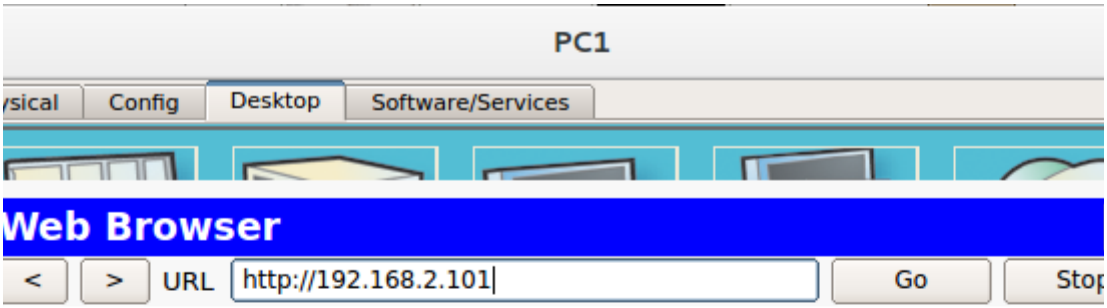
NB : voir la fiche d'intervention pour la configuration

- PC1 doit donc utiliser l'adresse 192.168.2.101 pour effectuer un test de ping vers Web_RTLR par exemple. Le ping est concluant.

```
PC>ping 192.168.2.101

Pinging 192.168.2.101 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.101: bytes=32 time=0ms TTL=126
Reply from 192.168.2.101: bytes=32 time=0ms TTL=126
Reply from 192.168.2.101: bytes=32 time=5ms TTL=126

Ping statistics for 192.168.2.101:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms
```

Ping PC1 > Web_RTLR

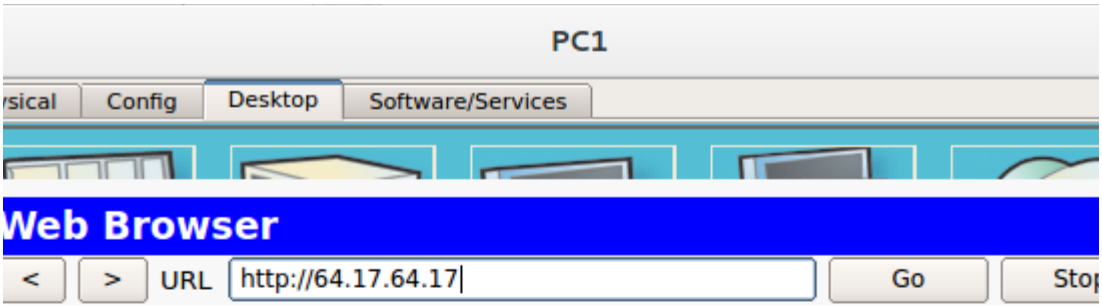
- On teste maintenant l'accès web, pour le « fun », l'accès web vers Web_RTLR puis Web_USA, permettant de vérifier nos configurations :



Cisco Packet Tracer

Welcome to Web_RTLR !! The place where we enjoy studying with great teachers !!

Quick Links:
A small page
Copyrights
Image page
Image



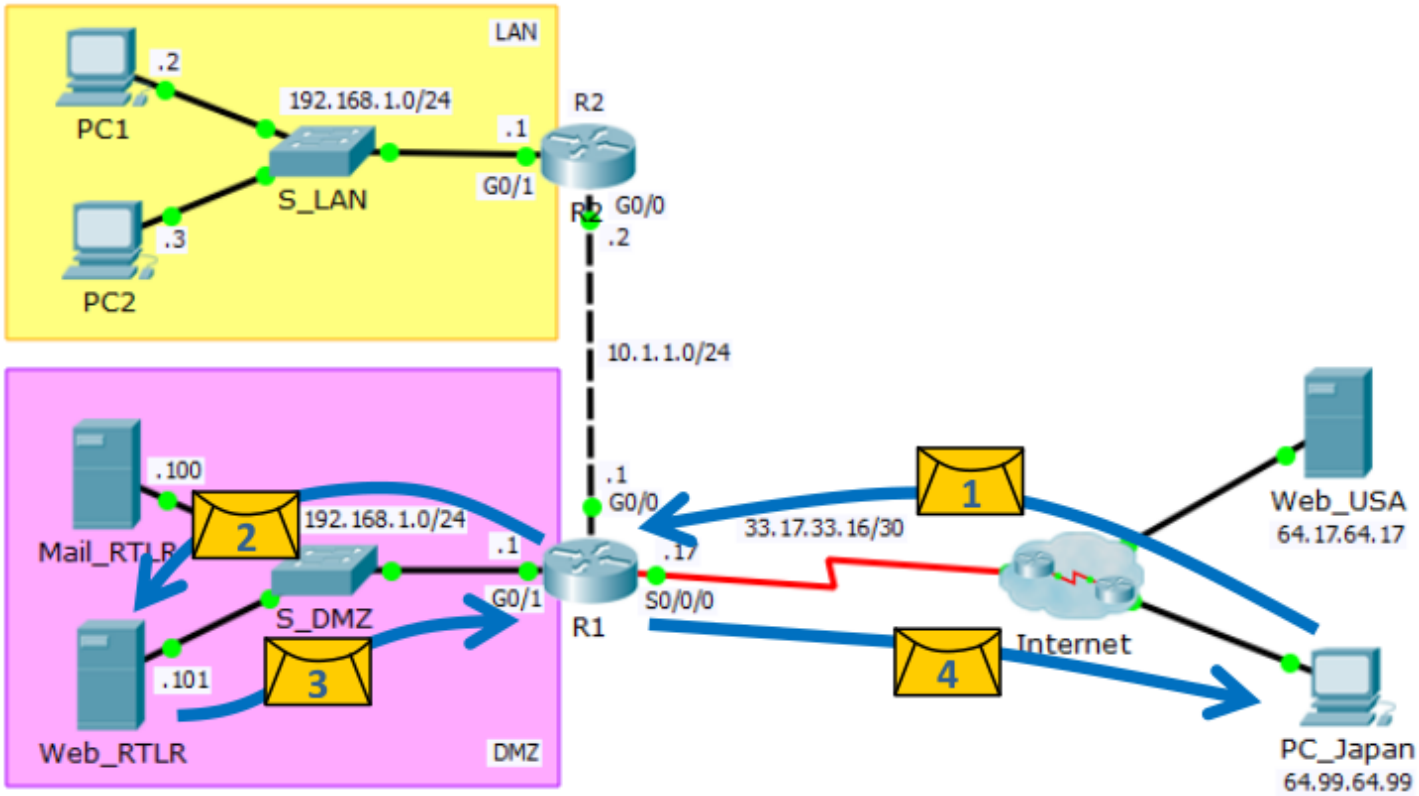
Cisco Packet Tracer

Welcome to Web_USA !! Please don't forget this famous french quote : "RT un jour, RT toujours ! A RT La Rochelle, soit fidèle !!"

Quick Links:
A small page
Copyrights
Image page
Image

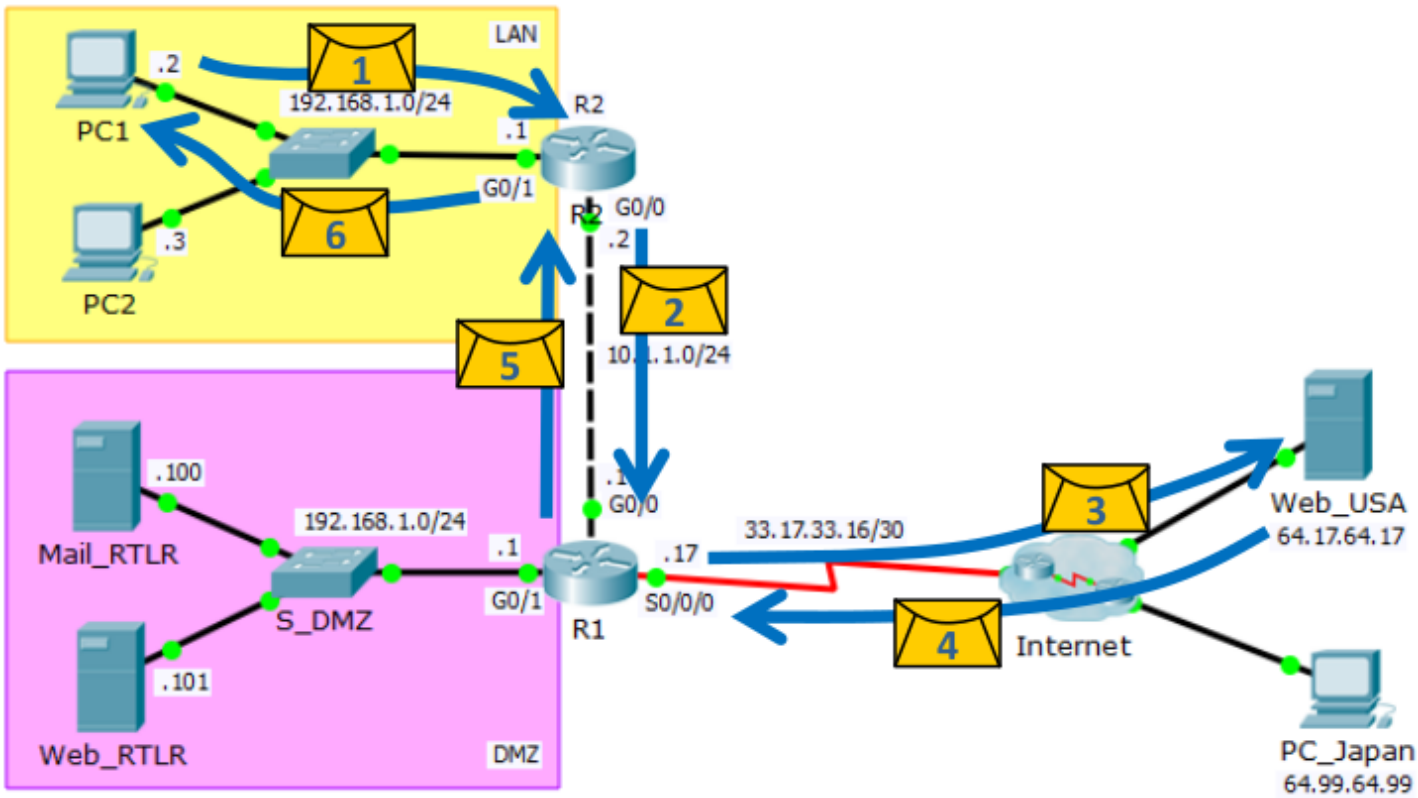
2.10. Synthèse sur les translations NAT

- On analyse dans un premier temps une requête web de PC_Japan vers Web_RTLR :



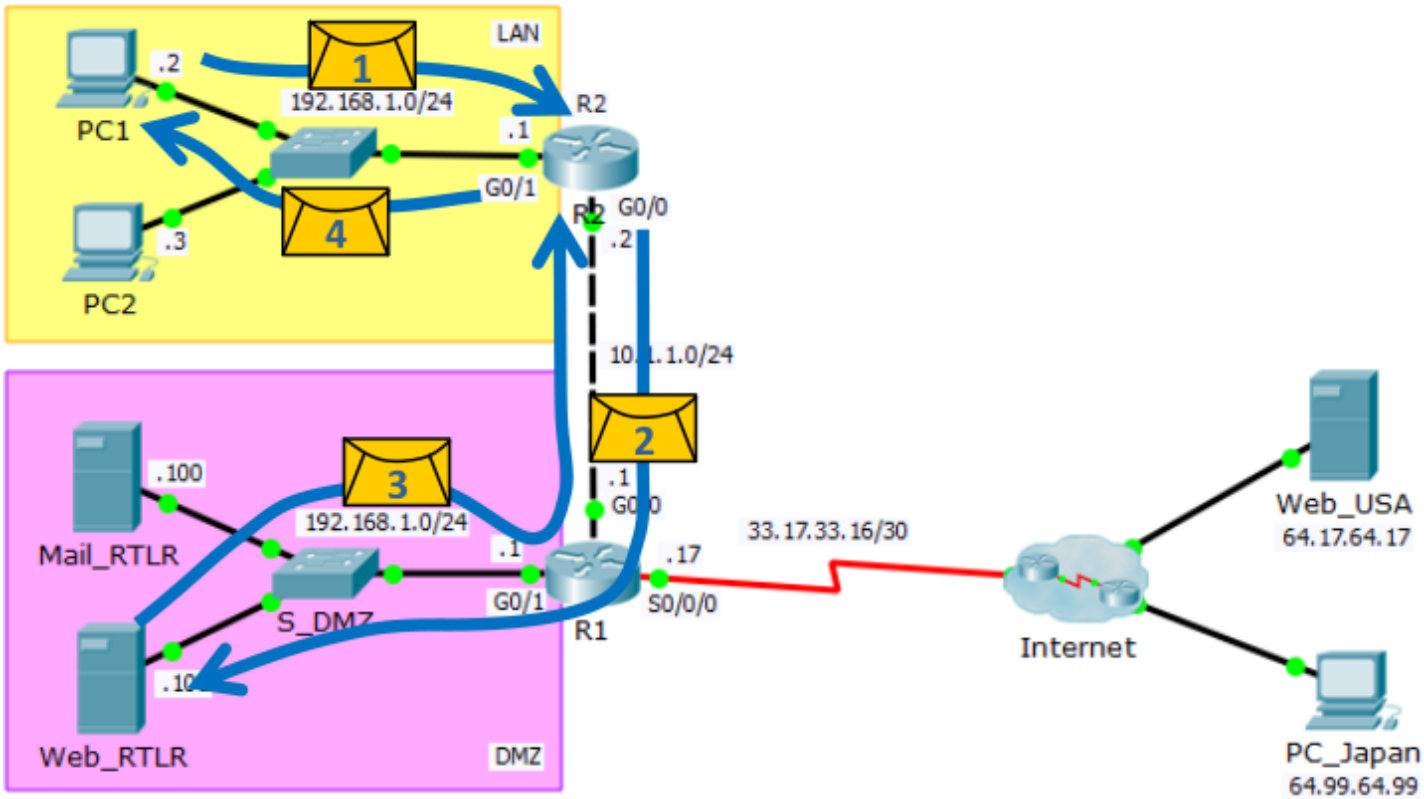
N° paquet	Adresse source		Adresse de destination	
	Type @ NAT pour R1	Valeur @ : n° port	Type @ NAT pour R1	Valeur @ : n° port
1	globale externe	1027	globale interne	80
2	locale externe	1027	locale interne	80
3	locale interne	80	locale externe	1027
4	globale interne	80	globale externe	1027

- On analyse ensuite une requête web de PC1 vers Web_USA :



N° paquet	Adresse source		Adresse de destination	
	Type @ NAT	n° port	Type @ NAT	n° port
1	pour R2 : locale interne	1027	pour R2 : globale externe	80
2	pour R2 : locale externe	1027	pour R2 : globale externe	80
	pour R1 : locale interne		pour R1 : locale externe	
3	pour R1 : globale interne	1027	pour R1 : globale externe	80
4	pour R1 : globale externe	80	pour R1 : locale externe	80
5	pour R1 : locale externe	80	pour R1 : locale interne	1027
	pour R2 : globale externe		pour R2 : locale externe	
6	pour R2 : globale externe	80	pour R2 : locale interne	1027

- Enfin, on analyse une requête web de PC1 vers Web_RTLR :



N° paquet	Adresse source		Adresse de destination	
	Type @ NAT pour R1	Valeur @ : n° port	Type @ NAT pour R1	Valeur @ : n° port
1	locale interne	1028	locale externe	80
2	globale interne	1028	globale externe	80
3	globale externe	80	globale interne	1028
4	locale externe	80	locale interne	1028

Conclusion

Très concrètement, nous avons donc appris dans ce TP à configurer les différents types de NAT sur routeur Cisco dans différentes configurations, afin de répondre au mieux au besoin de la topologie. Cela nous a également permis d'avoir une illustration pour chaque type de NAT.

Nous avons pu également comparer les types de NAT dont nous pouvons dresser un tableau de comparaison :

Type de NAT	Caractéristiques	Avantages	Inconvénients
NAT statique	une @ publique par hôte de façon permanente	possibilité de joindre la machine depuis l'extérieur	besoin d'autant d'@ publique que d'hôtes
NAT dynamique	une @ publique par hôte affectée temporairement	un nombre illimité d'hôtes peut avoir une adresse publique	le nb d'hôtes connectés simultanément est = au nb d'adresses du pool
NAT overload	une @ publique par hôte affectée temporairement associée à un port	le grand nombre d'hôtes pouvant accéder à Internet simultanément	besoin de disposer de plusieurs @ publiques
PAT classique	une @ publique pour tous les hôtes, identifiés par un port	ne nécessite qu'une @ publique	le nombre de connexions simultanées est un peu plus faible
Redirection de ports	le port destination définit quelle machine est visée	possibilité de joindre la machine depuis l'extérieur	permet de faire du NAT pour certains protocoles seulement