

TP NAT

U6 SISR

SPINELLI Dylan
BTS SIO SISR | PARIS YNOV CAMPUS

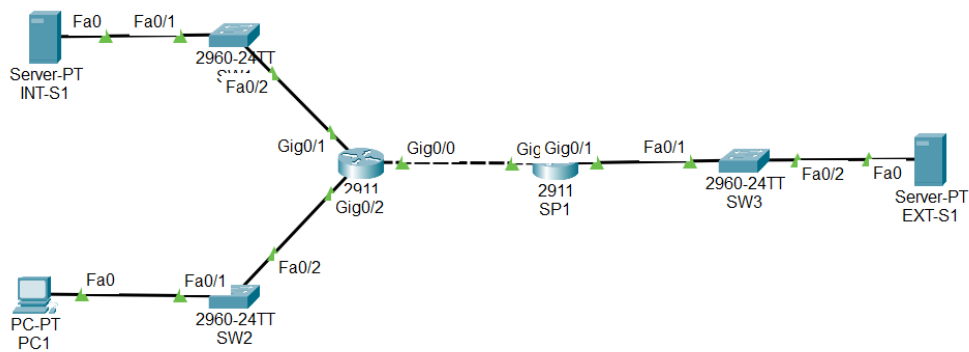
Table des matières

1-	Présentation du TP.....	2
2-	Configuration du NAT Statique	3
3-	Configuration du NAT dynamique	6
4-	Configuration du PAT.....	9

1-Présentation du TP

Dans ce TP nous allons apprendre à configurer le NAT dans un routeur. Dans un premier temps, nous ferons la configuration du NAT statique, puis le NAT dynamique. Nous terminerons par la configuration du PAT (Port Address Translation).

Voici la maquette du réseau qui sera utilisé pour ce TP :



On pense à configurer les routes dans chaque routeur :

```
R1(config)#  
R1(config)#ip route 203.0.113.16 255.255.255.240 203.0.113.1  
R1(config)#  
-----  
SP1(config)#ip route 10.0.1.0 255.255.255.0 203.0.113.2  
SP1(config)#ip route 10.0.2.0 255.255.255.0 203.0.113.2  
SP1(config)#
```

2-Configuration du NAT Statique

INT-S1 est le serveur web de l'entreprise. Il doit être accessible depuis internet. Nous allons donc lui configurer une adresse publique 203.0.113.3 dans le routeur R1 afin que les clients externes puissent y accéder.

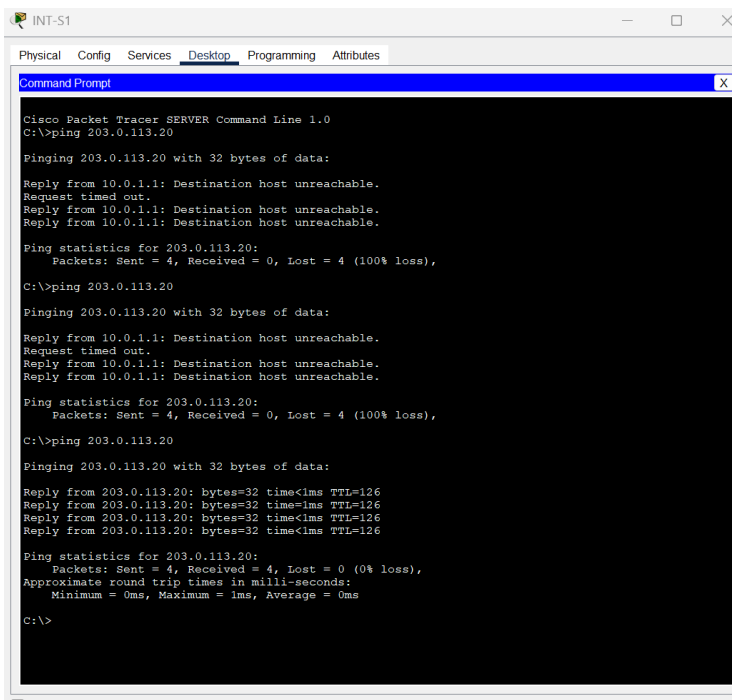
On configure donc le NAT dans R1 :

```
R1(config)#ip nat inside source static 10.0.1.10 203.0.113.3
R1(config)#int G0/1
R1(config-if)#ip nat inside
R1(config-if)#int G0/2
R1(config-if)#ip nat inside
R1(config-if)#int G0/0
R1(config-if)#ip nat outside
R1(config-if)#
```

On active le débogage ICMP sur le routeur :

```
R1>
R1>en
R1#debug ip icmp
ICMP packet debugging is on
R1#
```

Nous arrivons bien à effectuer un ping vers le serveur EXT-S1 depuis INT-S1 :



```
INT-S1
Physical Config Services Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 203.0.113.20
Pinging 203.0.113.20 with 32 bytes of data:
Reply from 10.0.1.1: Destination host unreachable.
Request timed out.
Reply from 10.0.1.1: Destination host unreachable.
Reply from 10.0.1.1: Destination host unreachable.
Ping statistics for 203.0.113.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 203.0.113.20
Pinging 203.0.113.20 with 32 bytes of data:
Reply from 10.0.1.1: Destination host unreachable.
Request timed out.
Reply from 10.0.1.1: Destination host unreachable.
Reply from 10.0.1.1: Destination host unreachable.
Ping statistics for 203.0.113.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 203.0.113.20
Pinging 203.0.113.20 with 32 bytes of data:
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Ping statistics for 203.0.113.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Observons la réponse au ping envoyée par EXT-S1 :

PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

At Device: R1
Source: INT-S1
Destination: EXT-S1

In Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 203.0.113.20, Dest. IP: 203.0.113.3
ICMP Message Type: 0
- Layer 2: Ethernet II Header
0009.7C45.4301 >> 00D0.9759.0E01
- Layer 1: Port GigabitEthernet0/0

Out Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 203.0.113.20, Dest. IP: 10.0.1.10
ICMP Message Type: 0
- Layer 2: Ethernet II Header
00D0.9759.0E02 >> 0060.3E50.0AC7
- Layer 1: Port(s): GigabitEthernet0/1

1. The packet is coming from an outside network. The device looks up its NAT table for necessary translations.
2. The NAT table has a matched dynamic entry for source and destination global addresses.
3. The device translates the packet from global to local addresses with the matched entry.
4. The device looks up the destination IP address in the CEF table.

Challenge Me << Previous Layer Next Layer >>

On voit que le ping est bien renvoyé à l'adresse IP publique 203.0.113.3

Ensuite le routeur va modifier l'adresse IP de destination pour la remplacer par l'IP privée 10.0.1.10

Faisons un test de connexion telnet vers 203.0.113.3 sur le port 80 pour s'assurer que les clients externes pourront bien se connecter :

```
EXT-S1
Physical Config Services Desktop Programming Attributes
Command Prompt
Pinging 203.0.113.3 with 32 bytes of data:
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Ping statistics for 203.0.113.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>203.0.113.3
Invalid Command.
C:\>ping 203.0.113.3
Pinging 203.0.113.3 with 32 bytes of data:
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Ping statistics for 203.0.113.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 203.0.113.3
Pinging 203.0.113.3 with 32 bytes of data:
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Reply from 203.0.113.3: bytes=32 time=126ms TTL=126
Ping statistics for 203.0.113.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>telnet 203.0.113.3 80
Trying 203.0.113.3 ...Open
```

La connexion est réussie.

On peut vérifier la table d'adresses NAT dans R1 :

```
R1>
R1>
R1>en
R1#show ip nat translation
Pro  Inside global      Inside local      Outside local     Outside global
---  203.0.113.3        10.0.1.10        ---              ---
tcp  203.0.113.3:80    10.0.1.10:80    203.0.113.20:1025 203.0.113.20:1025
tcp  203.0.113.3:80    10.0.1.10:80    203.0.113.20:1026 203.0.113.20:1026
R1#
```

On retrouve bien nos deux adresses publiques et privées

3-Configuration du NAT dynamique

On configure le NAT dynamique sur R1 :

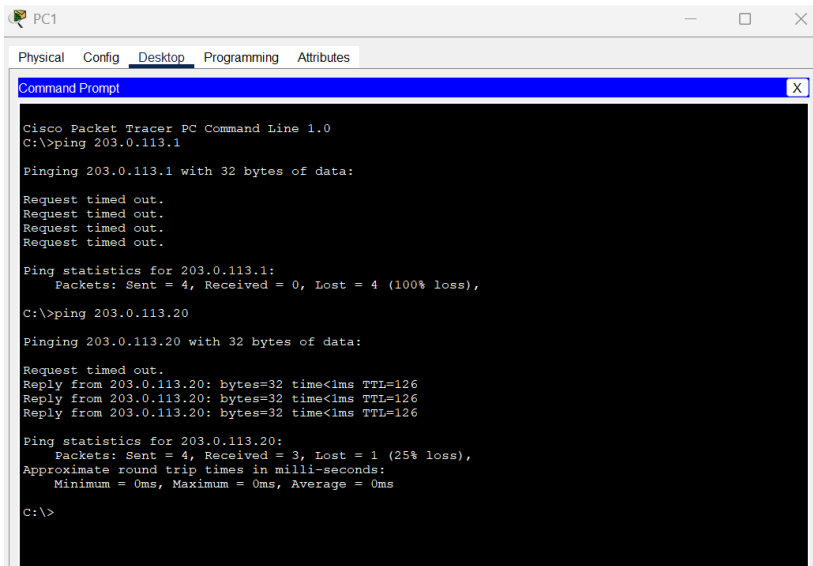
```
R1(config)#ip nat pool POOL-DYN 203.0.113.4 203.0.113.12 netmask 255.255.255.240
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
R1(config)#ip nat inside source list 1 pool POOL-DYN
R1(config)#
```

On configure donc le NAT Dynamique sur le sous-réseau 10.0.2.0/24 avec une plage de 203.0.113.4 à 203.0.113.12

On active ensuite le débogage NAT sur R1 :

```
R1(config)#ip nat pool POOL-DYN 203.0.113.4 203.0.113.12 netmask 255.255.255.240
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
R1(config)#ip nat inside source list 1 pool POOL-DYN
R1(config)#
R1(config)#
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
debug ip nat
IP NAT debugging is on
R1#
```

Test ping de PC1 vers EXT-S1 :



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.1
Pinging 203.0.113.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 203.0.113.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 203.0.113.20
Pinging 203.0.113.20 with 32 bytes of data:
Request timed out.
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Reply from 203.0.113.20: bytes=32 time<1ms TTL=126
Ping statistics for 203.0.113.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

On voit au niveau de R1 que l'adresse IP de PC1 : 10.0.2.10 est devenue 203.0.113.4 à la sortie du routeur

PDU Information at Device: R1

OSI Model Inbound PDU Details Outbound PDU Details

At Device: R1
Source: PC1
Destination: EXT-S1

In Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 10.0.2.10, Dest. IP: 203.0.113.20 ICMP Message Type: 8
- Layer 2: Ethernet II Header 00E0.B021.9510 >> 00D0.9759.0E03
- Layer 1: Port GigabitEthernet0/2

Out Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 203.0.113.4, Dest. IP: 203.0.113.20 ICMP Message Type: 8
- Layer 2: Ethernet II Header 00D0.9759.0E01 >> 0009.7C45.4301
- Layer 1: Port(s): GigabitEthernet0/0

1. GigabitEthernet0/2 receives the frame.

Challenge Me << Previous Layer Next Layer >>

L'adresse globale assignée à PC1 est 203.0.113.4

On voit bien la configuration dans la table de traduction NAT sur R1 :

```
R1#
NAT: s=10.0.2.10->203.0.113.4, d=203.0.113.20 [14]
NAT: s=10.0.2.10->203.0.113.4, d=203.0.113.20 [15]
NAT*: s=203.0.113.20, d=203.0.113.4->10.0.2.10 [38]
NAT: s=10.0.2.10->203.0.113.4, d=203.0.113.20 [16]
NAT*: s=203.0.113.20, d=203.0.113.4->10.0.2.10 [39]
NAT: s=10.0.2.10->203.0.113.4, d=203.0.113.20 [17]
NAT*: s=203.0.113.20, d=203.0.113.4->10.0.2.10 [40]
NAT: s=10.0.2.10->203.0.113.4, d=203.0.113.20 [18]
NAT*: s=203.0.113.20, d=203.0.113.4->10.0.2.10 [41]
NAT: expiring 203.0.113.4 (10.0.2.10) icmp 14 (14)
NAT: s=10.0.2.10->203.0.113.4, d=203.0.113.20 [19]
NAT*: s=203.0.113.20, d=203.0.113.4->10.0.2.10 [42]
NAT: expiring 203.0.113.4 (10.0.2.10) icmp 15 (15)
NAT: expiring 203.0.113.4 (10.0.2.10) icmp 16 (16)
NAT: expiring 203.0.113.4 (10.0.2.10) icmp 17 (17)

R1#
R1# show ip nat translation
Pro Inside global      Inside local      Outside local     Outside global
icmp 203.0.113.4:118  10.0.2.10:18      203.0.113.20:18  203.0.113.20:18
icmp 203.0.113.4:19  10.0.2.10:19      203.0.113.20:19  203.0.113.20:19
--- 203.0.113.3       10.0.1.10         ---              ---
tcp 203.0.113.3:80    10.0.1.10:80      203.0.113.20:1025 203.0.113.20:1025
tcp 203.0.113.3:80    10.0.1.10:80      203.0.113.20:1026 203.0.113.20:1026
tcp 203.0.113.3:80    10.0.1.10:80      203.0.113.20:1027 203.0.113.20:1027
tcp 203.0.113.3:80    10.0.1.10:80      203.0.113.20:1028 203.0.113.20:1028

R1#
```

Copy Paste

Top

Lorsque toutes les adresses du pool 203.0.113.4 à 203.0.113.12 ont été allouées et qu'un nouveau PC tente d'envoyer du trafic vers un hôte externe, il sera impossible d'attribuer une IP publique à ce nouveau PC. Ce PC ne pourra donc pas se connecter à internet.

On active donc le PAT dans R1 pour remédier à ce problème :

```
R1(config)#ip nat inside source list 1 pool POOL-DYN overload
R1(config)#ipnat_remove_dynamic_cfg: id 1, flag 9, range 0

ipnat_add_dynamic_cfg: id 1, flag 11, range 0

poolstart 203.0.113.4 poolend 203.0.113.12

id 1, flags 0, domain 0, lookup 0, aclnum 1 ,
    aclname 1 , mapname idb 0
```

Il faut ajouter « overload » à la commande « ip nat inside source »

On peut voir ici la configuration complète :

```
R1#show run | section nat
ip nat outside
ip nat inside
ip nat inside
ip nat pool POOL-DYN 203.0.113.4 203.0.113.12 netmask 255.255.255.240
ip nat inside source list 1 pool POOL-DYN overload
ip nat inside source static 10.0.1.10 203.0.113.3
R1#show access-list
Standard IP access list 1
    10 permit 10.0.2.0 0.0.0.255 (12 match(es))

R1#
```

Pour la suite de ce TP, on supprime toute la configuration NAT dans R1 :

```
R1#clear ip nat translation *
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip nat inside source list 1 pool POOL-DYN overload
R1(config)#no ip nat inside source static 10.0.1.10 203.0.113.3
R1(config)#
ipnat_remove_static_cfg: id 1, flag A

R1(config)#no ip nat pool POOL-DYN
R1(config)#ipnat_addrpool_notify_api: id , flags 11, range 0

ipnat_addrpool_notify_api: id , flags 11, range 0

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show run | section nat
ip nat outside
ip nat inside
ip nat inside
R1# show ip nat translation
R1#
```

4-Configuration du PAT

On configure le NAT du réseau 10.0.2.0/24 sur R1 :

```
R1>
R1>
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255
R1(config)#ip nat inside source list 1 interface G0/0 overload
R1(config)#ipnat_add_dynamic_cfg: id 2, flag 5, range 0

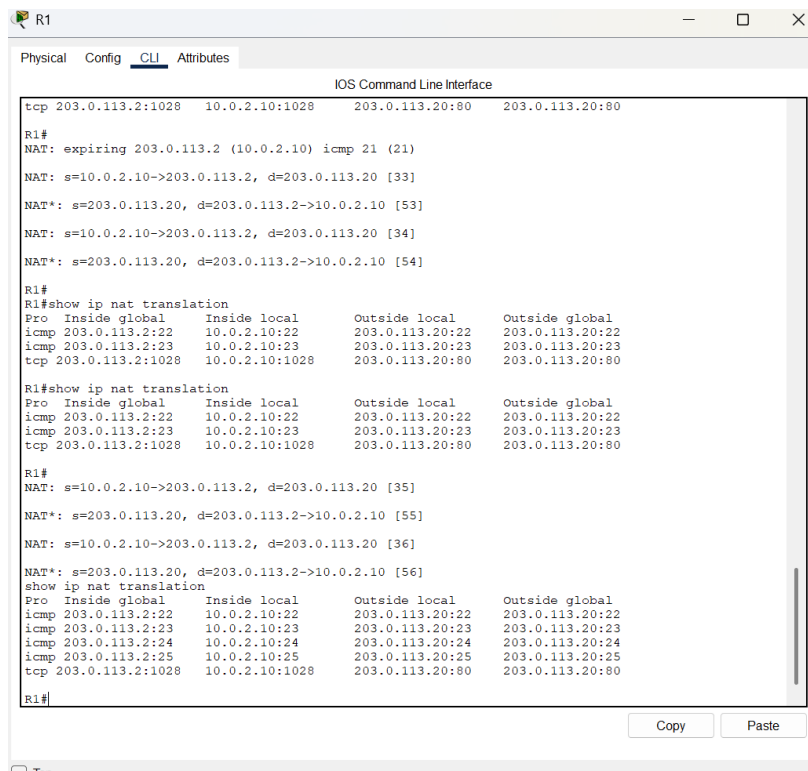
id 2, flags 0, domain 0, lookup 0, aclnum 1 ,

        aclname 1 , mapname idb 5286E006

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#debug ip nat
IP NAT debugging is on
R1#
```

On autorise plusieurs PC à partager l'adresse IP de l'interface G0/0



```
R1
Physical Config CLI Attributes
IOS Command Line Interface

tcp 203.0.113.2:1028 10.0.2.10:1028 203.0.113.20:80 203.0.113.20:80

R1#
NAT: expiring 203.0.113.2 (10.0.2.10) icmp 21 (21)
NAT: s=10.0.2.10->203.0.113.2, d=203.0.113.20 [33]
NAT*: s=203.0.113.20, d=203.0.113.2->10.0.2.10 [53]
NAT: s=10.0.2.10->203.0.113.2, d=203.0.113.20 [34]
NAT*: s=203.0.113.20, d=203.0.113.2->10.0.2.10 [54]

R1#
R1#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 203.0.113.2:22 10.0.2.10:22 203.0.113.20:22 203.0.113.20:22
icmp 203.0.113.2:23 10.0.2.10:23 203.0.113.20:23 203.0.113.20:23
tcp 203.0.113.2:1028 10.0.2.10:1028 203.0.113.20:80 203.0.113.20:80

R1#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 203.0.113.2:22 10.0.2.10:22 203.0.113.20:22 203.0.113.20:22
icmp 203.0.113.2:23 10.0.2.10:23 203.0.113.20:23 203.0.113.20:23
tcp 203.0.113.2:1028 10.0.2.10:1028 203.0.113.20:80 203.0.113.20:80

R1#
NAT: s=10.0.2.10->203.0.113.2, d=203.0.113.20 [35]
NAT*: s=203.0.113.20, d=203.0.113.2->10.0.2.10 [55]
NAT: s=10.0.2.10->203.0.113.2, d=203.0.113.20 [36]
NAT*: s=203.0.113.20, d=203.0.113.2->10.0.2.10 [56]
show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 203.0.113.2:22 10.0.2.10:22 203.0.113.20:22 203.0.113.20:22
icmp 203.0.113.2:23 10.0.2.10:23 203.0.113.20:23 203.0.113.20:23
icmp 203.0.113.2:24 10.0.2.10:24 203.0.113.20:24 203.0.113.20:24
icmp 203.0.113.2:25 10.0.2.10:25 203.0.113.20:25 203.0.113.20:25
tcp 203.0.113.2:1028 10.0.2.10:1028 203.0.113.20:80 203.0.113.20:80

R1#
```

On voit ici que sur chaque ping, un port différent est utilisé pour la communication

Le PAT est donc bien configuré.

Désormais, chaque connexion utilisera un port différent. Le PAT permet d'utiliser une unique adresse IP publique, ce qui permet de réduire les coûts.