11

NAT

Le NAT (**N**etwork **A**ddress **T**ranslation, ou traduction d'adresses de réseau en français) est une technique utilisée dans les réseaux informatiques pour permettre à plusieurs appareils de partager une seule adresse IP publique.

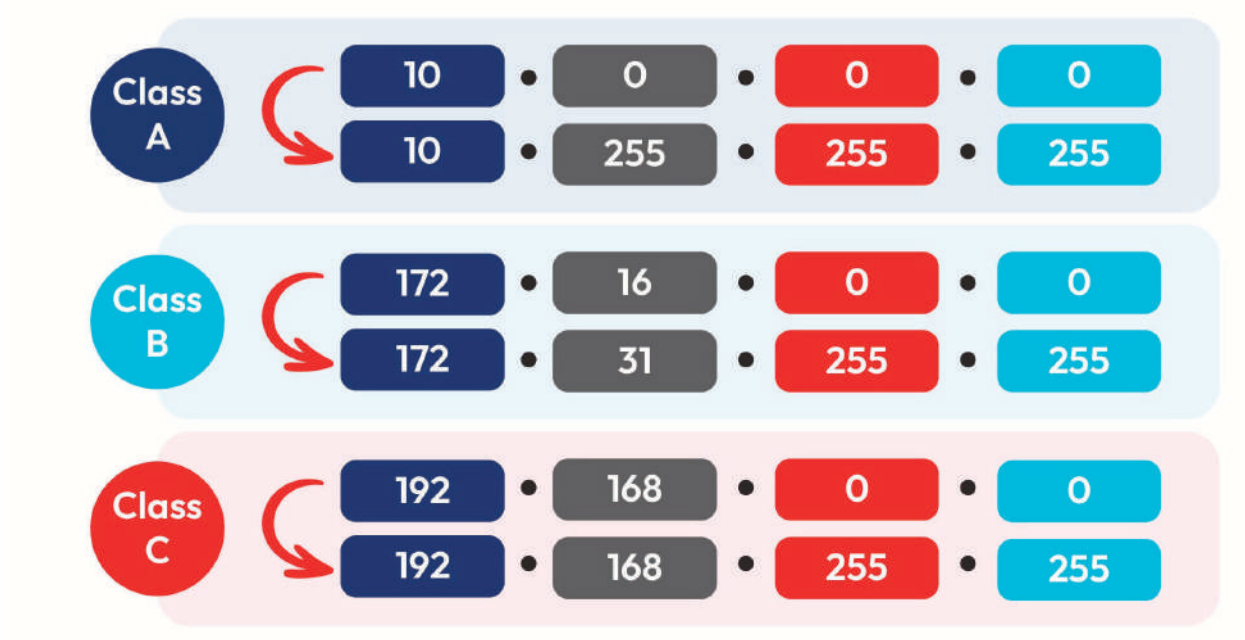
Cela signifie que plusieurs appareils peuvent communiquer avec l'extérieur en utilisant une seule adresse IP publique, ce qui permet de conserver un nombre limité d'adresses IP publiques et de protéger la confidentialité des appareils internes.

11.1. Notion d'adresse publique et d'adresse privée

11.1.1. Caractéristiques :

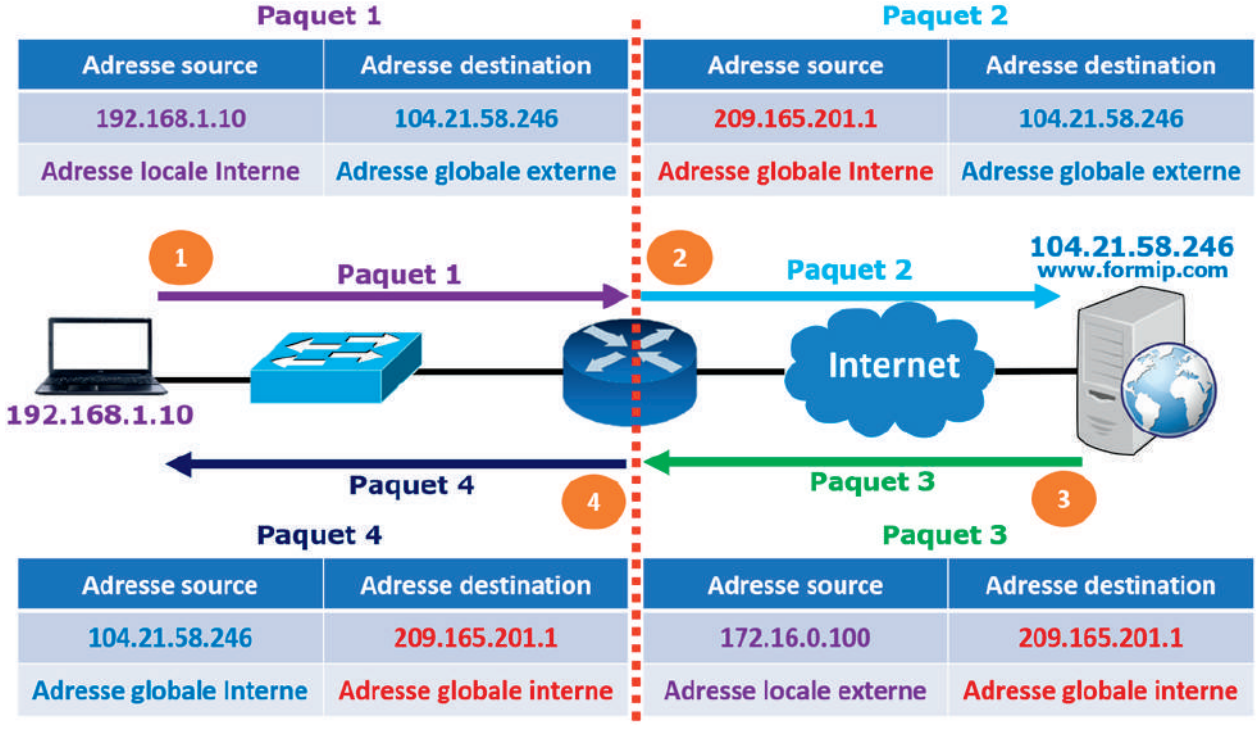
	ADRESSES PRIVÉES	ADRESSES PUBLIQUES
ÉTENDUE	Locales	Globales
FRAIS	Gratuites	Payantes
INTERNET	Non routables sur Internet	Routables sur Internet

11.1.2. La liste des adresses privées :



11.2. Terminologie NAT

- Une adresse locale interne est l'adresse privée du périphérique de votre réseau local.
- Une adresse globale interne est l'adresse publique utilisée pour se connecter au réseau Internet.
- Une adresse locale externe est l'adresse privée d'un serveur dans un autre réseau local externe.
- Une adresse globale externe est l'adresse publique d'un serveur sur Internet.



- Le paquet 1 utilise l'adresse locale interne (privée) comme adresse source et l'adresse globale externe (adresse publique de www.formip.com) comme adresse de destination.
- Le paquet arrive au niveau du routeur d'extrémité.
- Le routeur remplace l'adresse locale interne (privée) par une adresse globale interne (publique) et envoie le nouveau paquet « Paquet 2 » : C'est le NAT

11.3. Types et configuration de NAT

11.3.1. NAT statique

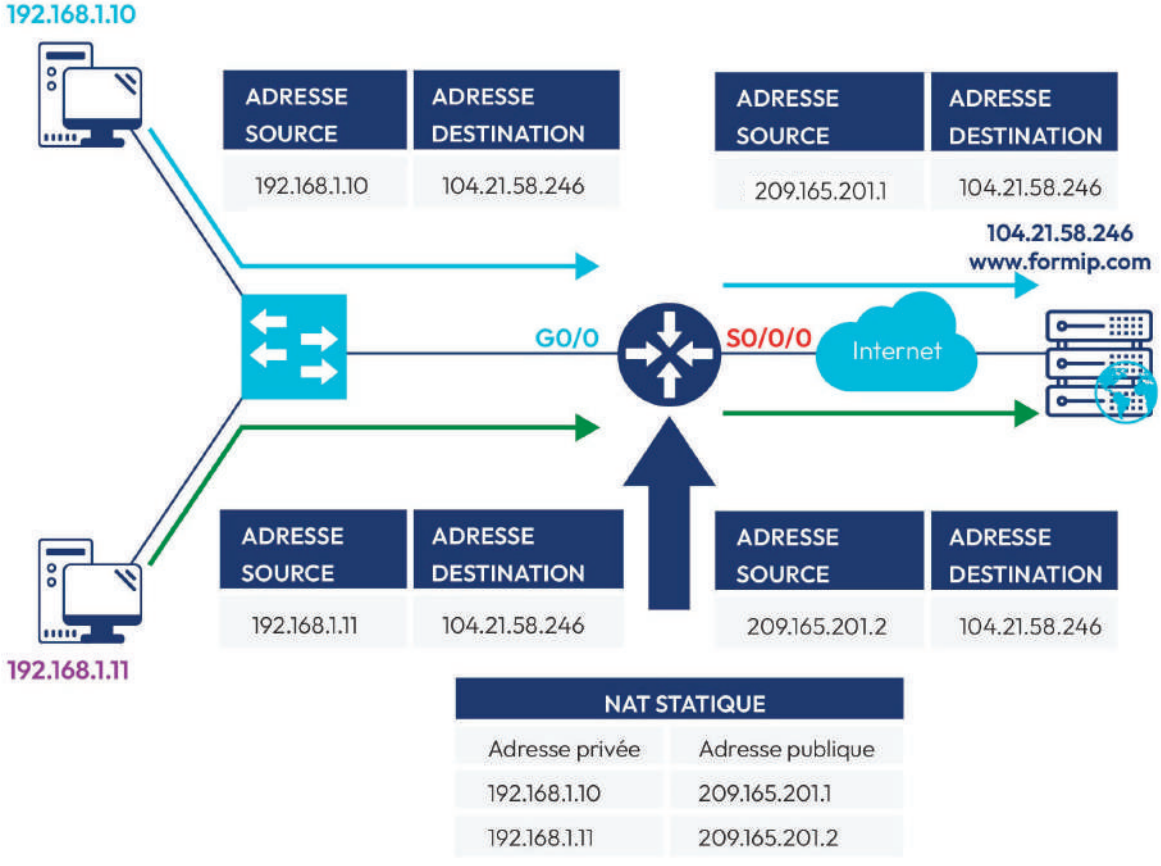
NAT STATIQUE	
Adresse privée	Adresse publique
192.168.1.10	209.165.201.1
192.168.1.11	209.165.201.2

PRINCIPE DU NAT STATIQUE :

Le NAT statique associe à chaque adresse IP locale interne (privée) une adresse globale interne (publique).
Dans cet exemple :

- L'adresse locale interne 192.168.1.10 est associée avec l'adresse globale interne 209.165.201.1
- L'adresse locale interne 192.168.1.11 est associée avec l'adresse globale interne 209.165.201.2

CONFIGURATION DU NAT STATIQUE :



NAT STATIQUE	
Adresse privée	Adresse publique
192.168.1.10	209.165.201.1
192.168.1.11	209.165.201.2

Étape 1 : Association des adresses locales internes aux adresses globales internes :

```
R1(config)#ip nat inside source static 192.168.1.10 209.165.201.1
R1(config)#ip nat inside source static 192.168.1.11 209.165.201.2
```

Étape 2 : Activation du NAT sur les interfaces du routeur :

```
R1(config)#interface G0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface S0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

Vérification de la configuration du NAT statique :

Avant l'envoi d'un paquet ICMP :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.201.1     192.168.1.10       ---                ---
---  209.165.201.2     192.168.1.11       ---                ---
R1#
```

Après l'envoi d'un paquet ICMP :

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.201.1:3   192.168.1.10:3     104.21.58.246:3    104.21.58.246:3
icmp 209.165.201.2:2   192.168.1.11:2     104.21.58.246:2    104.21.58.246:2
---  209.165.201.1     192.168.1.10       ---                ---
---  209.165.201.2     192.168.1.11       ---                ---
R1#
```

11.3.2. NAT dynamique

PRINCIPE DU NAT DYNAMIQUE :

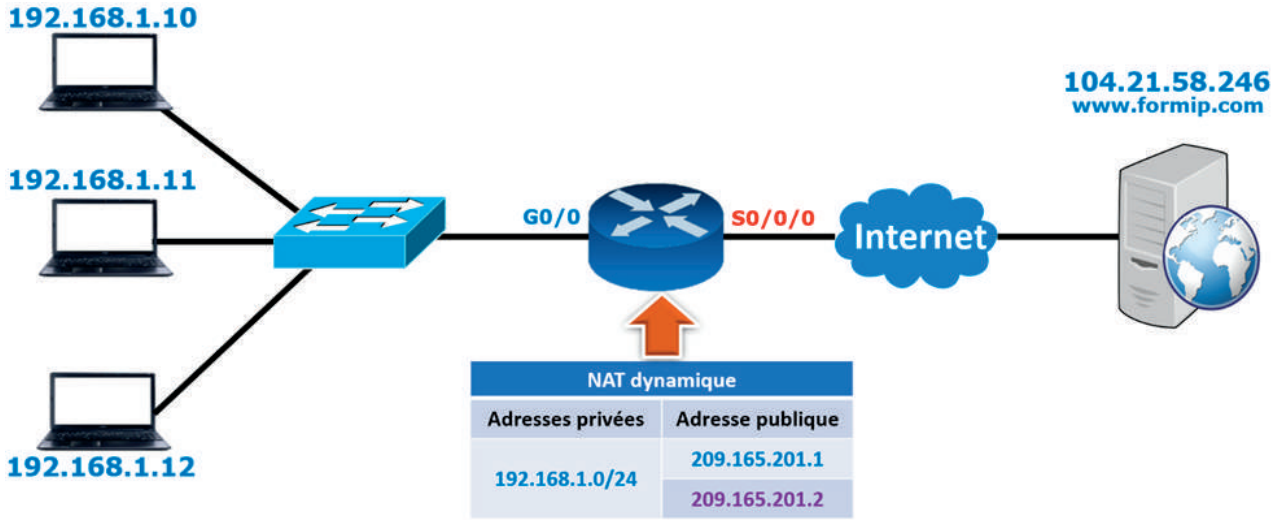
Le NAT dynamique associe à plusieurs adresses IP locales internes une plage d'adresses globales internes.

Dans cet exemple :

On a associé à toutes les adresses du réseau : 192.168.1.0/24
Et deux adresses globales internes : 209.165.201.1 et 209.165.201.2

NAT STATIQUE	
Adresse privée	Adresse publique
192.168.1.0/24	209.165.201.1
	209.165.201.2

CONFIGURATION DU NAT DYNAMIQUE :



Étape 1 : Création d'une ACL des adresses locales internes :

```
R1(config)#ip access-list standard LAN
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

Étape 2 : Création d'un pool NAT :

```
R1(config)#ip nat pool NAT 209.165.201.1 209.165.201.2 netmask 255.255.255.252
```

Étape 3 : Association de l'ACL au pool :

```
R1(config)#ip nat inside source list LAN pool NAT
```

Étape 4 : Activation du NAT sur les interfaces du routeur :

```
R1(config)#interface G0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface S0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

Vérifi cation du fonctionnement NAT :

```
R1#show ip nat translations
Pro     Inside global     Inside local       Outside local      Outside global
icmp    209.165.201.1:4   192.168.1.10:4     104.21.58.246:4    104.21.58.246:4
icmp    209.165.201.2:1   192.168.1.12:1     104.21.58.246:1    104.21.58.246:1
icmp    209.165.201.2:2   192.168.1.12:2     104.21.58.246:2    104.21.58.246:2
```

11.3.3. NAT dynamique avec surcharge ou PAT

PRINCIPE DU NAT DYNAMIQUE AVEC SURCHARGE :

Le NAT dynamique avec surcharge associe à plusieurs adresses IP locales internes (privées) une plage d'adresses globales internes en utilisant un critère distinctif qui est le numéro de **port TCP ou UDP**.

On a deux possibilités :

- **Association de plusieurs adresses locales internes à une plage d'adresses globales internes :**

Dans cet exemple :

On a associé à toutes les adresses du réseau 192.168.1.0/24 à deux adresses globales internes : 209.165.201.1 et 209.165.201.2

PAT= NAT DYNAMIQUE AVEC SURCHARGE	
Adresse privée	Adresse publique
192.168.1.10: 1721	209.165.201.1: 1721
192.168.1.11: 1722	209.165.201.2: 1722
92.168.1.12: 1723	209.165.201.1: 1723
192.168.1.13: 1724	209.165.201.2: 1724

- **Association de plusieurs adresses locales internes à l'adresse globale interne de l'interface WAN :**

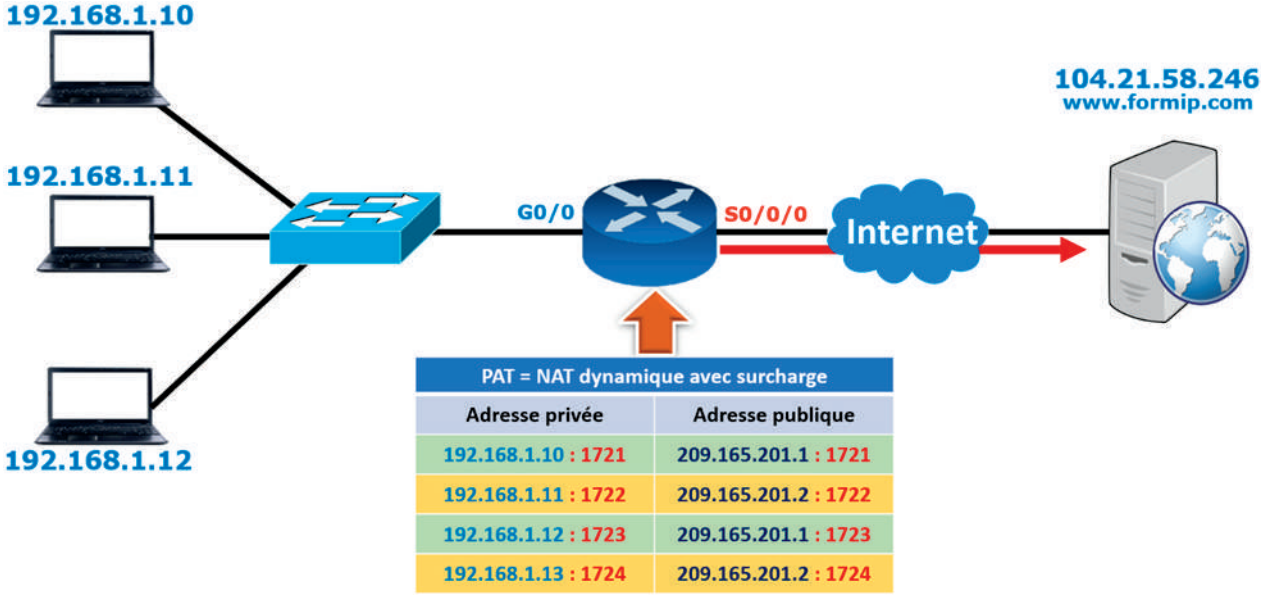
Dans cet exemple :

On a associé à toutes les adresses du réseau 192.168.1.0/24 de l'interface WAN S0/0/0

PAT= NAT DYNAMIQUE AVEC SURCHARGE	
Adresse privée	Adresse publique
192.168.1.10: 1721	@S0/0/0: 1721
192.168.1.11: 1722	@S0/0/0: 1722
192.168.1.12: 1723	@S0/0/0: 1723
192.168.1.13: 1724	@S0/0/0: 1724

CONFIGURATION DU NAT DYNAMIQUE AVEC SURCHARGE :

1re méthode : Utilisation d'un pool d'adresses globales internes



PAT = NAT dynamique avec surcharge	
Adresse privée	Adresse publique
192.168.1.10 : 1721	209.165.201.1 : 1721
192.168.1.11 : 1722	209.165.201.2 : 1722
192.168.1.12 : 1723	209.165.201.1 : 1723
192.168.1.13 : 1724	209.165.201.2 : 1724

Étape 1 : Création d'une ACL des adresses locales internes :

```
R1(config)#ip access-list standard LAN
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

Étape 2 : Création d'un pool NAT :

```
R1(config)#ip nat pool NAT 209.165.201.2 209.165.201.2 netmask 255.255.255.252
```

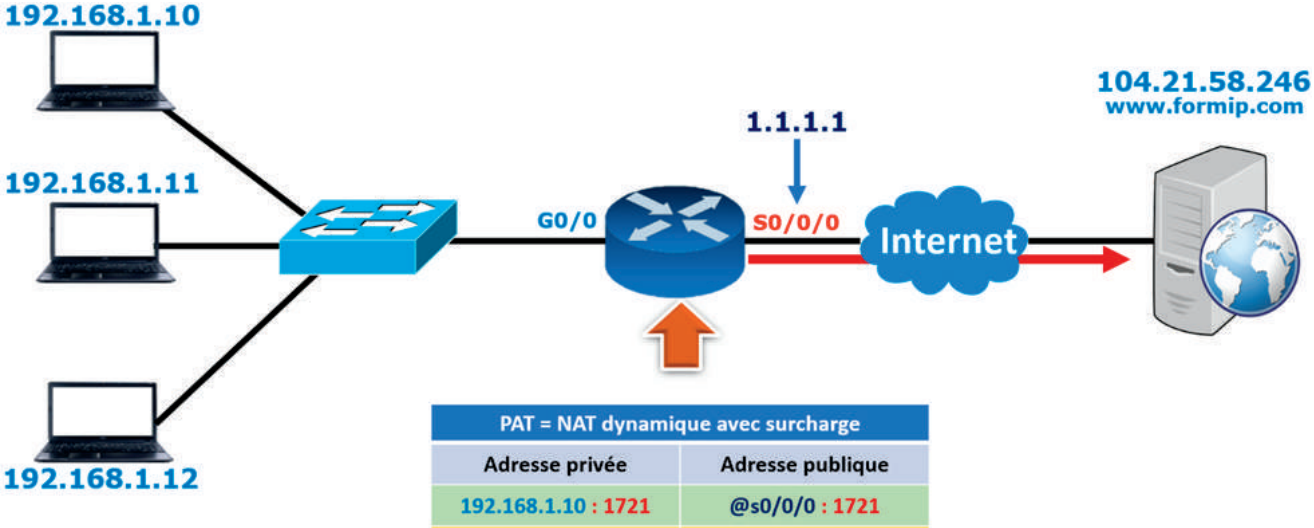
Étape 3 : Association de l'ACL au pool avec surcharge :

```
R1(config)#ip nat inside source list LAN pool NAT overload
```

Étape 4 : Activation du NAT sur les interfaces du routeur :

```
R1(config)#interface G0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface S0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

2e méthode : Utilisation de l'adresse de l'interface série WAN



PAT = NAT dynamique avec surcharge	
Adresse privée	Adresse publique
192.168.1.10 : 1721	@s0/0/0 : 1721
192.168.1.11 : 1722	@s0/0/0 : 1722
192.168.1.12 : 1723	@s0/0/0 : 1723
192.168.1.13 : 1724	@s0/0/0 : 1724

Étape 1 : Création d'une ACL des adresses locales internes :

```
R1(config)#ip access-list standard LAN
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

Étape 2 : Association de l'ACL à l'adresse de l'interface :

```
R1(config)#ip nat inside source list LAN interface S0/0/0 overload
```

Étape 3 : Activation du NAT sur les interfaces du routeur :

```
R1(config)#interface G0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface S0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

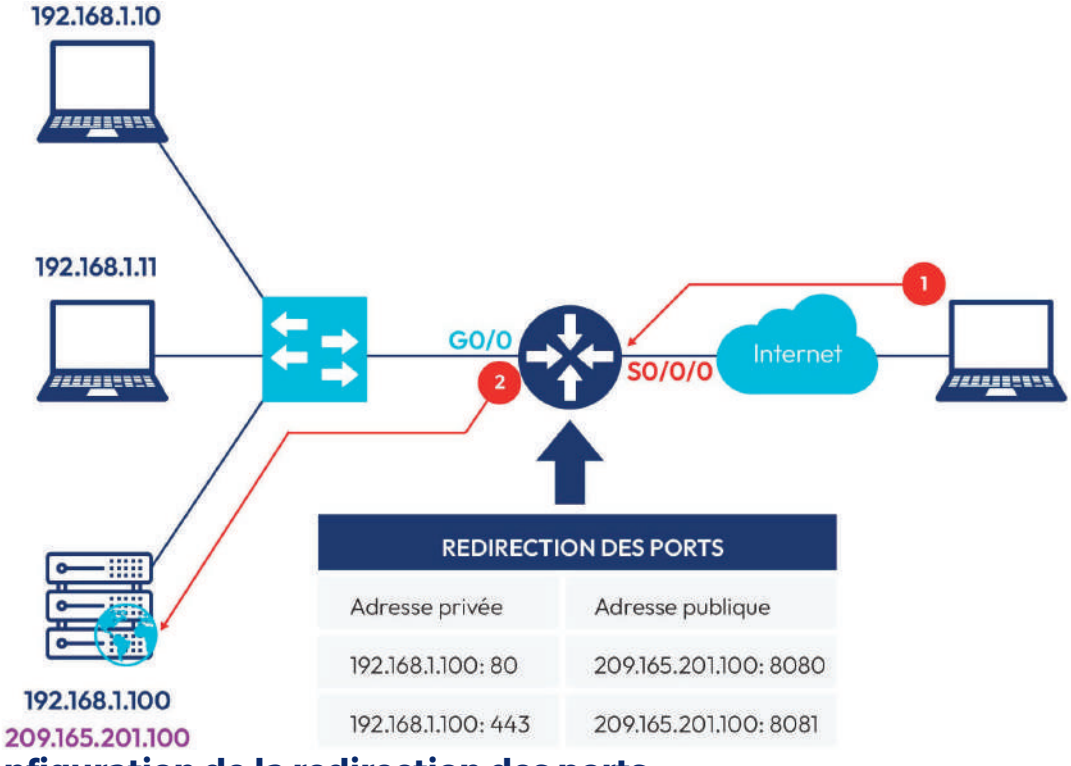
Vérification du fonctionnement NAT :

```
R1#show ip nat translations
Pro     Inside global   Inside local       Outside local      Outside global
icmp    1.1.1.1:4       192.168.1.12:4     104.21.58.246:4    104.21.58.246:4
icmp    1.1.1.1:5       192.168.1.11:5     104.21.58.246:5    104.21.58.246:5
icmp    1.1.1.1:6       192.168.1.10:6     104.21.58.246:6    104.21.58.246:6
```

11.4. Redirection des ports :

11.4.1. Principe de la redirection des ports :

La redirection des ports permet aux utilisateurs externes d'accéder aux serveurs locaux en utilisant une adresse IP publique (Globale interne) et un numéro de port.



11.4.2. Configuration de la redirection des ports :

```
R1(config)#ip nat inside source static tcp 192.168.1.100 80 209.165.201.100 8080
R1(config)#ip nat inside source static tcp 192.168.1.100 443 209.165.201.100 8081
```

- **192.168.1.100**: Adresse locale interne du serveur Web
- **209.165.201.100**: Adresse globale interne du serveur Web
- **TCP** : Le protocole utilisé avec le Web
- **80** : Port local interne (Port http)
- **8080** : Port global interne
- **443** : Port local interne (Port Https)
- **8081** : Port global interne.