Chapitre 11 : traduction d'adresse réseau pour IPv4

Routage et commutation

Cisco | Networking Academy®
Mind Wide Open™

Chapitre 11

11.0 Introduction

11.1 Fonctionnement de la NAT

11.2 Configuration de la traduction d'adresses réseau (NAT)

11.3 Dépannage de la NAT

11.4 Résumé

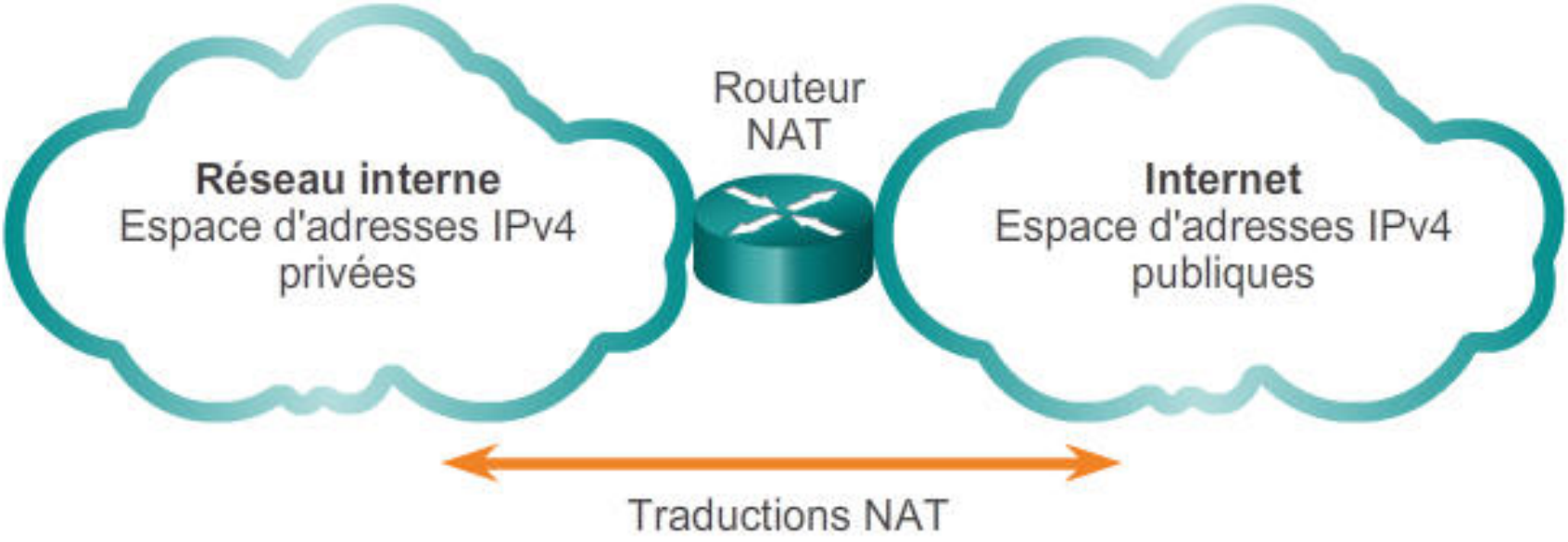
Chapitre 11 : objectifs

- Décrire les caractéristiques de la NAT
- Décrire les avantages et les inconvénients de la NAT
- Configurer la NAT statique à l'aide de l'interface en ligne de commande
- Configurer la NAT dynamique à l'aide de l'interface en ligne de commande
- Configurer la PAT à l'aide de l'interface en ligne de commande
- Configurer la redirection à l'aide de l'interface en ligne de commande
- Configurer la NAT-PT (v6 à v4)
- Utilisez les commandes show pour vérifier le fonctionnement de la NAT

Espace d'adressage privé IPv4

- L'espace d'adressage IPv4 est trop restreint pour accommoder tous les périphériques à connecter à Internet
- Les adresses privées des réseaux sont décrites dans la RFC 1918 et sont conçues pour être utilisées dans une organisation ou un site uniquement.
- Elles ne sont pas routées par les routeurs Internet, contrairement aux adresses publiques.
- Elles peuvent pallier la pénurie d'adresses IPv4, mais comme elles ne sont pas routées par les périphériques Internet, elles doivent d'abord être traduites.
- C'est le rôle de la fonction NAT.

Espace d'adressage privé IPv4



Les adresses Internet privées sont définies dans la RFC 1918 :

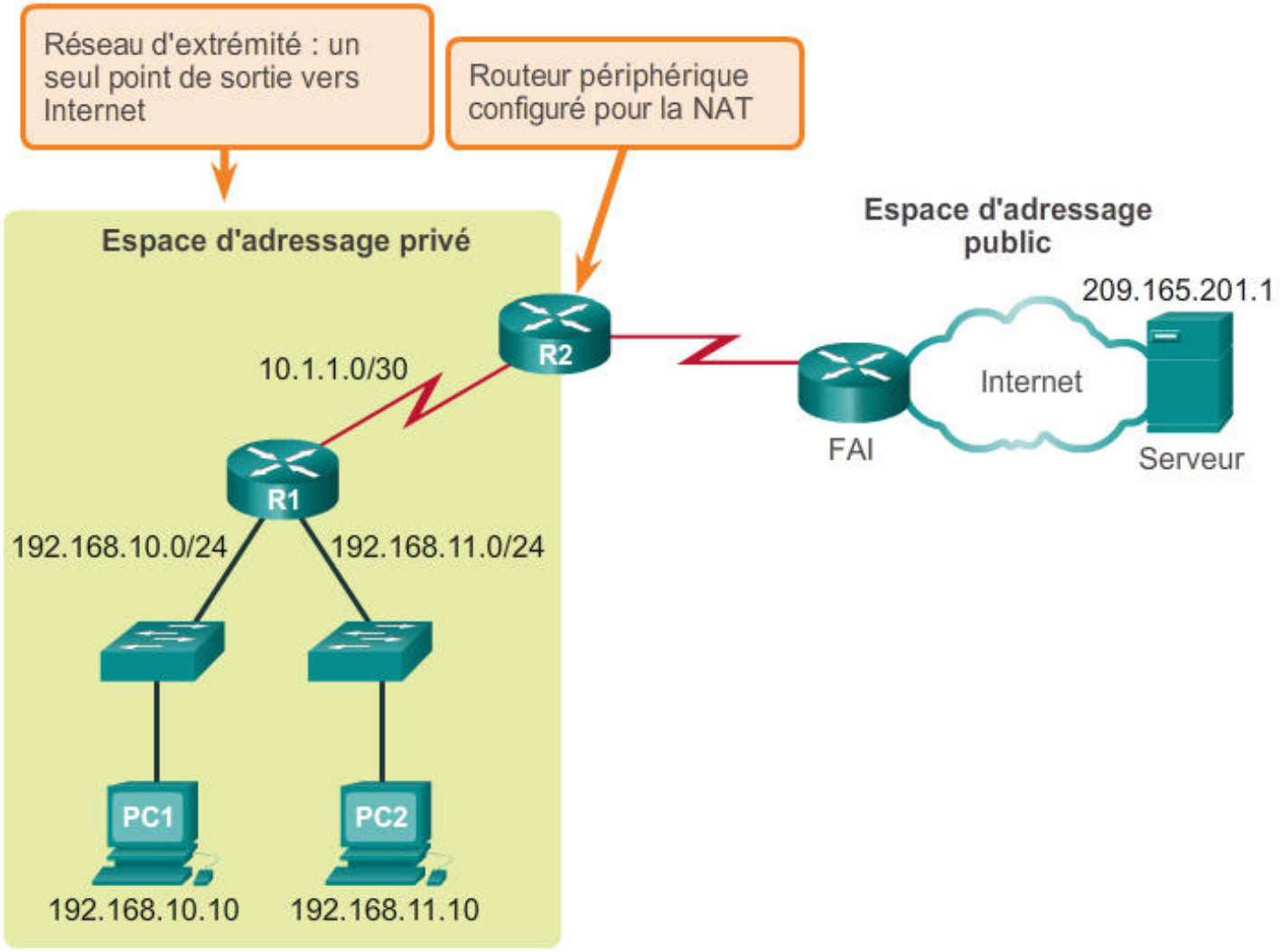
Classe	Plage d'adresses internes RFC 1918	Préfixe CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Qu'est-ce que la NAT ?

- La NAT est le procédé utilisé pour traduire les adresses réseau.
- Sa fonction première est d'économiser les adresses IPv4 publiques.
- Elle est généralement mise en œuvre sur les périphériques réseau situés à la périphérie, tels que les pare-feu ou les routeurs.
- Ainsi, les réseaux peuvent utiliser des adresses privées en interne, et les traduire en adresses publiques uniquement lorsque c'est nécessaire.
- Les équipements de l'entreprise peuvent recevoir des adresses privées et fonctionner avec des adresses uniques en local.
- Lorsque les données doivent être échangées avec d'autres organisations ou Internet, le routeur de périphérie traduit les adresses en adresses publiques et globalement uniques.

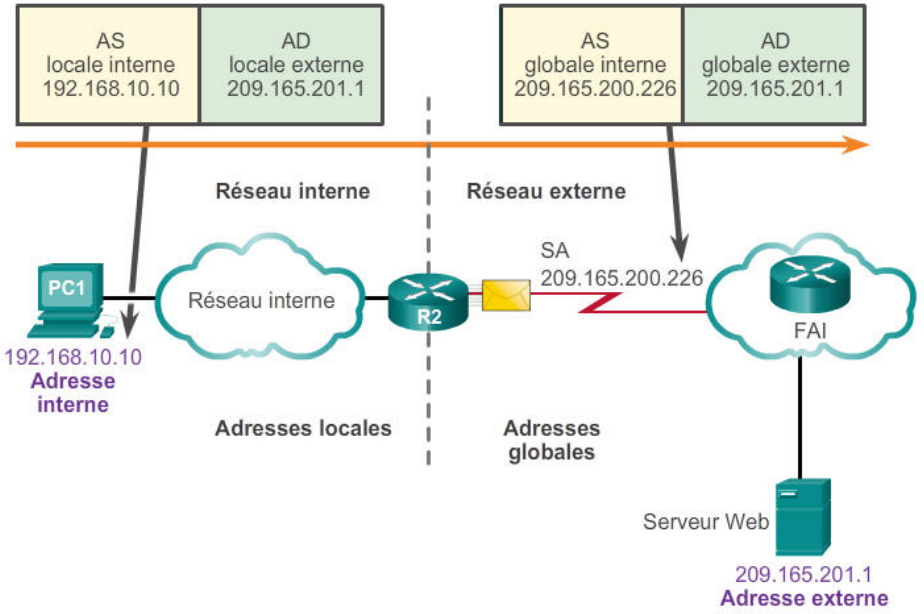
Caractéristiques de la NAT

Qu'est-ce que la NAT ?



Terminologie NAT

- Dans la terminologie NAT, le réseau interne est l'ensemble des périphériques qui utilisent des adresses privées. Les réseaux externes sont tous les autres réseaux.
- La NAT inclut 4 types d'adresse :
  - Adresse locale interne
  - Adresse globale interne
  - Adresse locale externe
  - Adresse globale externe



Terminologie NAT

- Les termes, à l'intérieur et à l'extérieur, sont combinés avec les termes locaux et globaux pour désigner des adresses spécifiques.
- Adresse locale interne
- Adresse globale interne
- Adresse globale externe
- Adresse locale externe

Fonctionnement de la NAT

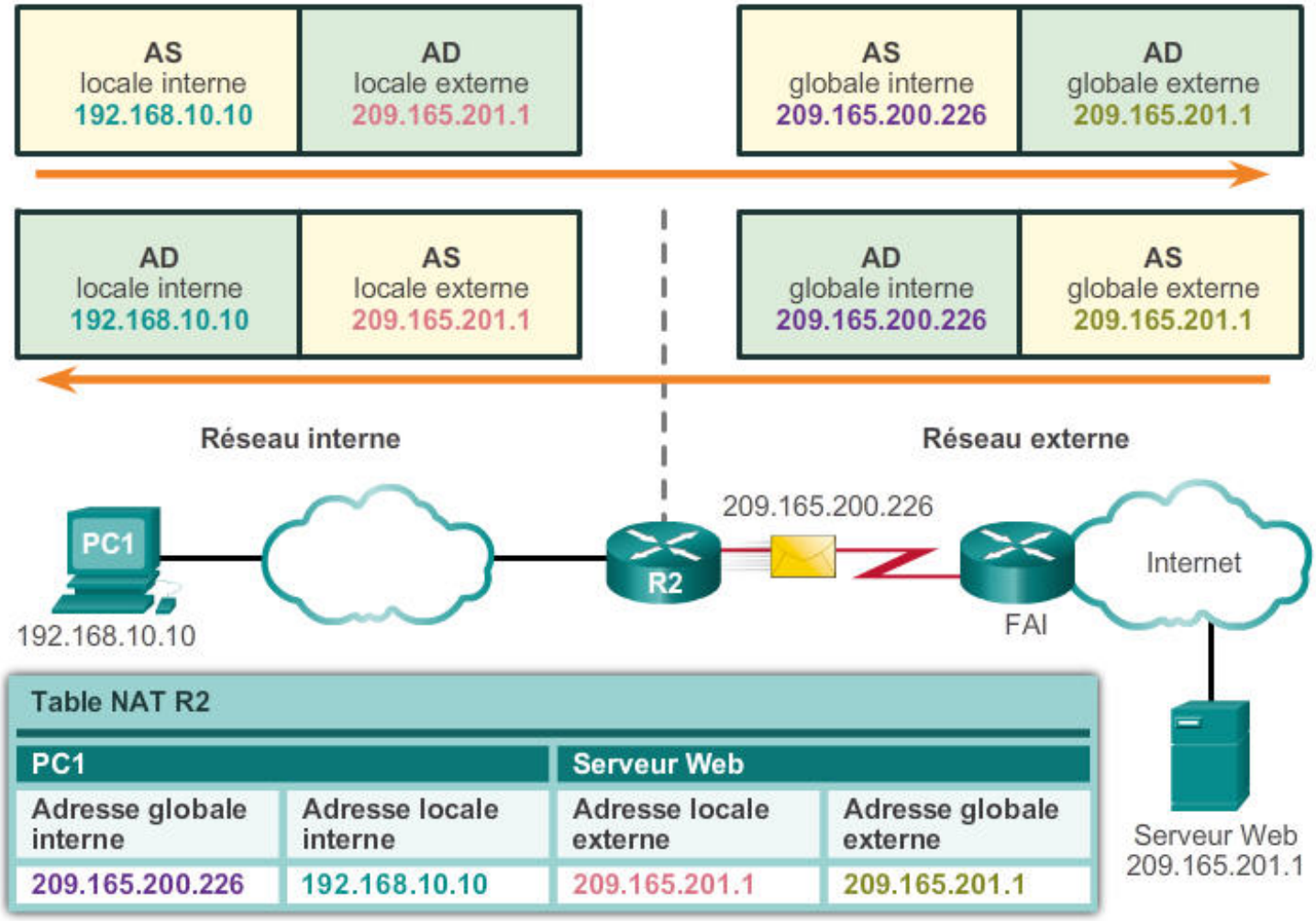


Table NAT R2

PC1		Serveur Web	
Adresse globale interne	Adresse locale interne	Adresse locale externe	Adresse globale externe
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

NAT statique

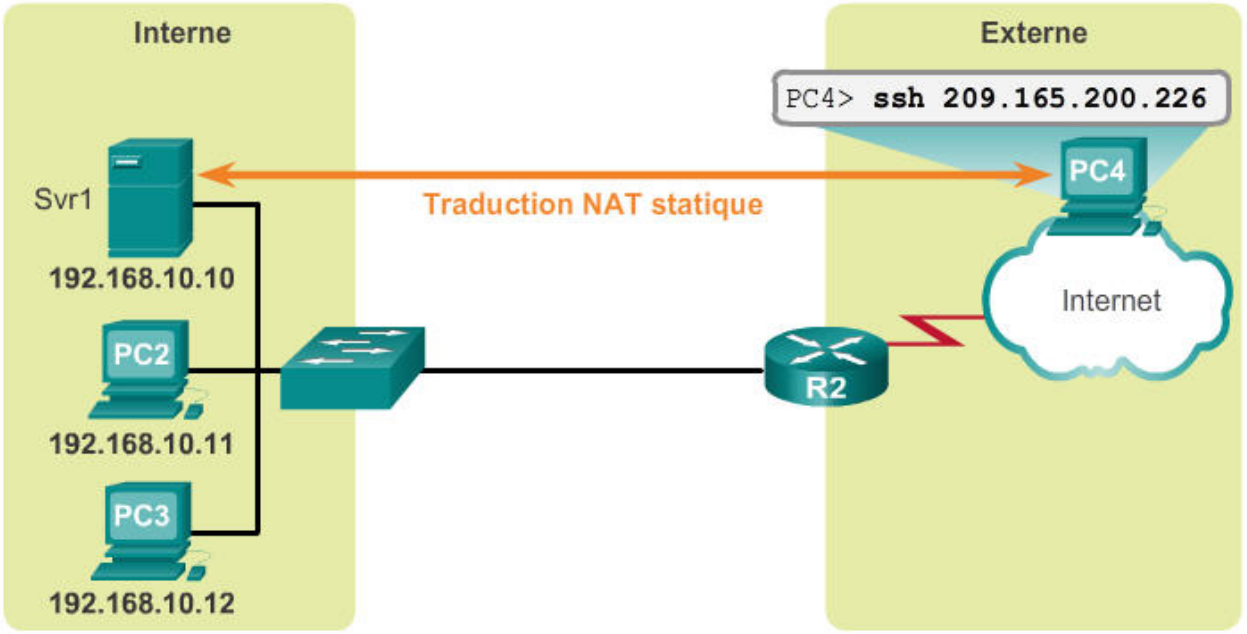
- La fonction NAT statique utilise un mappage « un à un » entre les adresses locales et globales.
- Ces mappages sont configurés par l'administrateur réseau et ne changent pas.
- La fonction NAT statique est particulièrement utile lorsque les serveurs hébergés dans le réseau interne doivent être accessibles depuis le réseau externe.
- L'administrateur réseau peut établir une connexion SSH vers un serveur du réseau interne en faisant pointer son client SSH sur l'adresse globale interne appropriée.

Types de NAT

NAT statique

NAT statique

Table NAT statique	
Adresse locale interne	**Adresse globale interne - adresses accessibles via R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



NAT dynamique

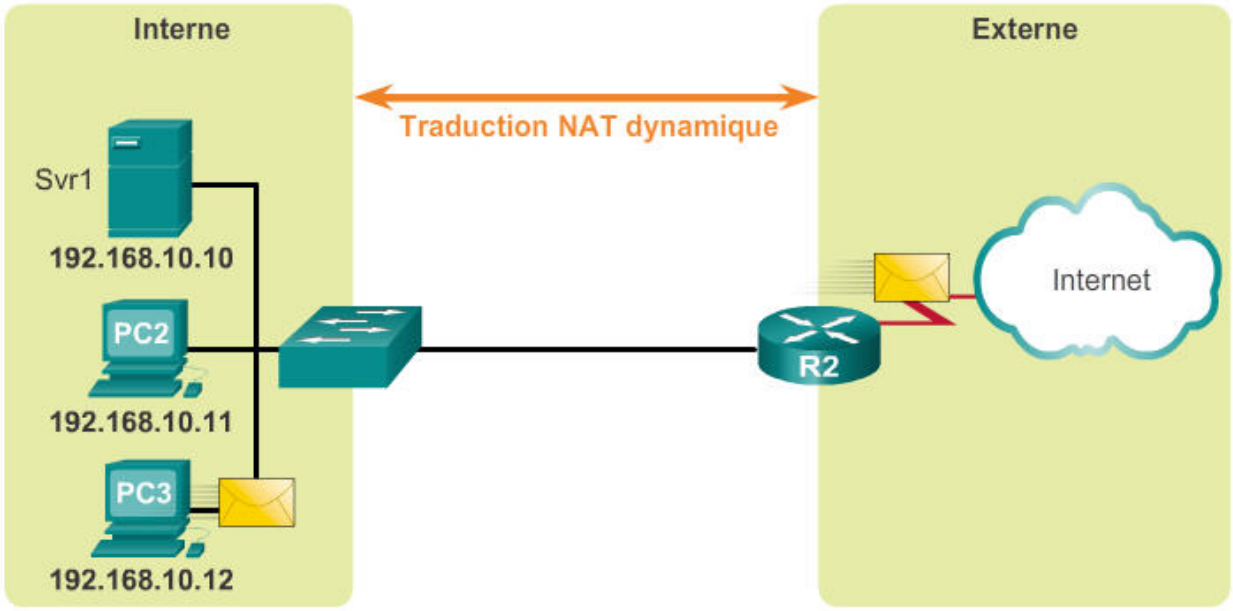
- La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi.
- Lorsqu'un périphérique interne demande l'accès à un réseau externe, la NAT dynamique attribue une adresse IPv4 publique disponible du pool.
- Il doit y avoir suffisamment d'adresses publiques disponibles pour le nombre total de sessions utilisateur simultanées.

Types de NAT

NAT dynamique

NAT dynamique

Pool NAT IPv4	
Adresse locale interne	**Pool d'adresses globales internes - adresses accessibles via R2**
192.168.10.12	209.165.200.226
Disponible	209.165.200.227
Disponible	209.165.200.228
Disponible	209.165.200.229
Disponible	209.165.200.230



Traduction d'adresses de port (PAT)

- La fonction PAT mappe les adresses IPv4 privées à des adresses IP publiques uniques ou à quelques adresses.
- Elle utilise la paire port source/adresse IP source pour garder une trace du trafic de chaque client interne.
- La PAT est également appelée surcharge NAT.
- Comme elle utilise également le numéro de port, elle peut transférer les paquets de réponse au périphérique interne approprié.
- Elle vérifie aussi que les paquets entrants étaient demandés, ce qui ajoute un niveau de sécurité à la session.

Comparaison entre NAT et PAT

- La fonction NAT traduit les adresses IPv4 selon un mappage « un à un » entre les adresses privées et les adresses publiques.
- La fonction PAT modifie à la fois l'adresse et le numéro de port.
- La NAT achemine les paquets entrants vers leur destination interne en faisant référence à l'adresse IPv4 source entrante donnée par l'hôte sur le réseau public.
- Avec la PAT, il n'y a généralement qu'une adresse IPv4 exposée publiquement, ou très peu.
- La PAT peut également traduire les protocoles qui n'utilisent pas les numéros de port tels qu'ICMP. Chacun de ces protocoles est pris en charge différemment par la PAT.

Avantages de la NAT

Avantages de la fonction NAT

- Elle conserve le schéma d'adressage officiellement inscrit
- Elle augmente la souplesse des connexions au réseau public
- Elle assure la cohérence des schémas d'adressage du réseau interne
- Elle garantit la sécurité du réseau

Inconvénients de la NAT

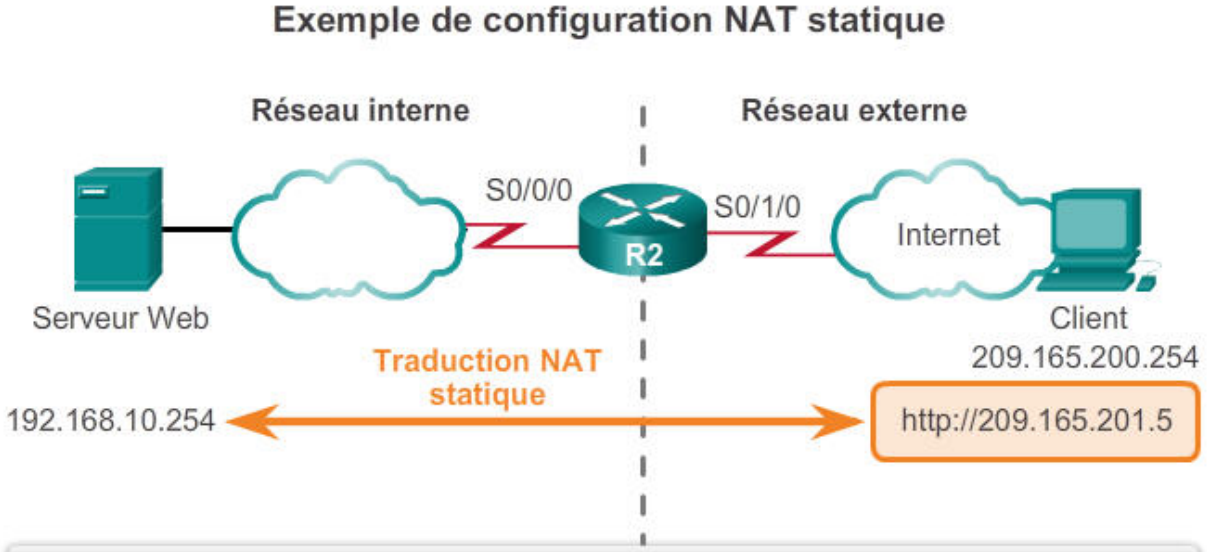
Inconvénients de la fonction NAT

- Dégradation des performances
- Dégradation de la fonctionnalité de bout en bout
- Perte de la traçabilité IP de bout en bout
- Complexification de la transmission tunnel
- Perturbations éventuelles de l'établissement des connexions TCP

Configuration de la NAT statique

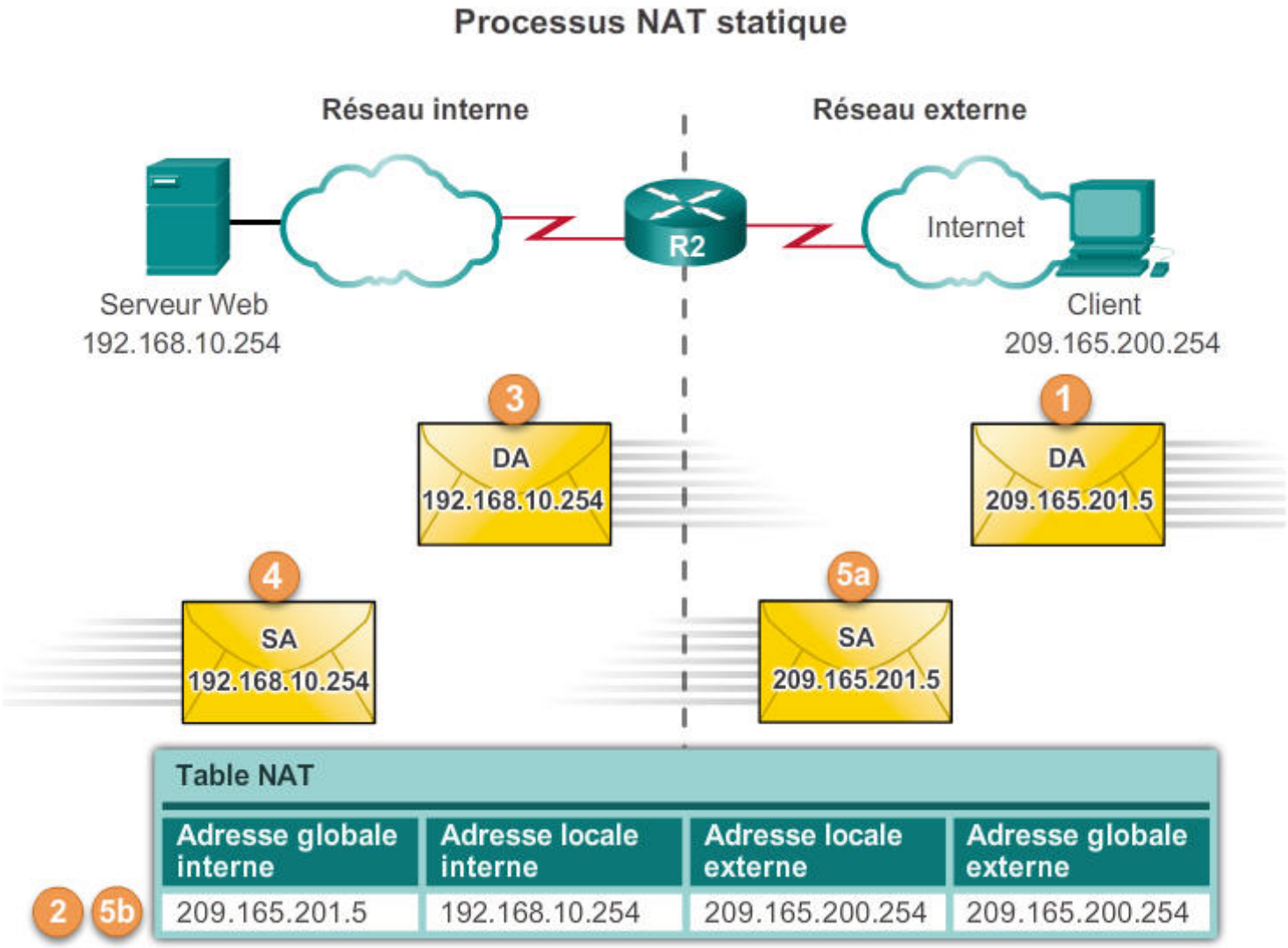
- La configuration de la traduction des adresses réseau statiques implique deux tâches de base :
  - Créer le mappage entre les adresses locales internes et les adresses locales externes
  - Définir quelle interface appartient au réseau interne et laquelle appartient au réseau externe

Configuration de la NAT statique




```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Analyse de la NAT statique



Configuration de la NAT statique

Vérification de la NAT statique

La traduction statique est toujours présente dans la table NAT.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

La traduction statique pendant une session active.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

Configuration de la NAT statique

Vérification de la NAT statique

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<output omitted>
```

Client PC establishes a session with the web server

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<output omitted>
```

Fonctionnement de la NAT dynamique

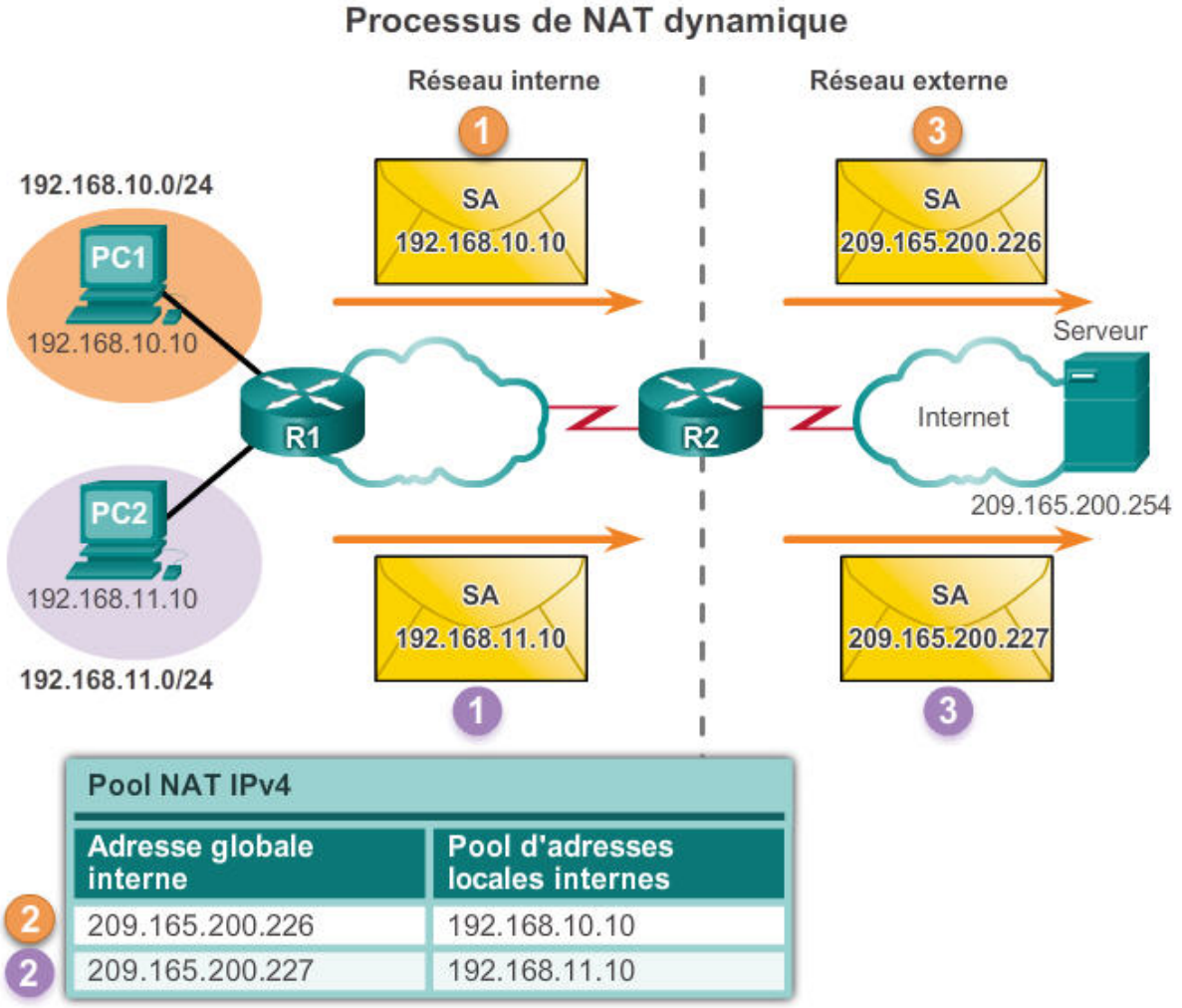
- Le pool d'adresses publiques IPv4 (pool d'adresses globales internes) est disponible pour n'importe quel périphérique du réseau interne selon le principe du premier arrivé, premier servi.
- Avec la NAT dynamique, une seule adresse interne est traduite en une seule adresse externe.
- Le pool doit être suffisamment vaste pour accommoder tous les périphériques internes.
- Un périphérique ne pourra pas communiquer avec les réseaux externes si aucune adresse n'est disponible dans le pool.

Configuration de la NAT dynamique

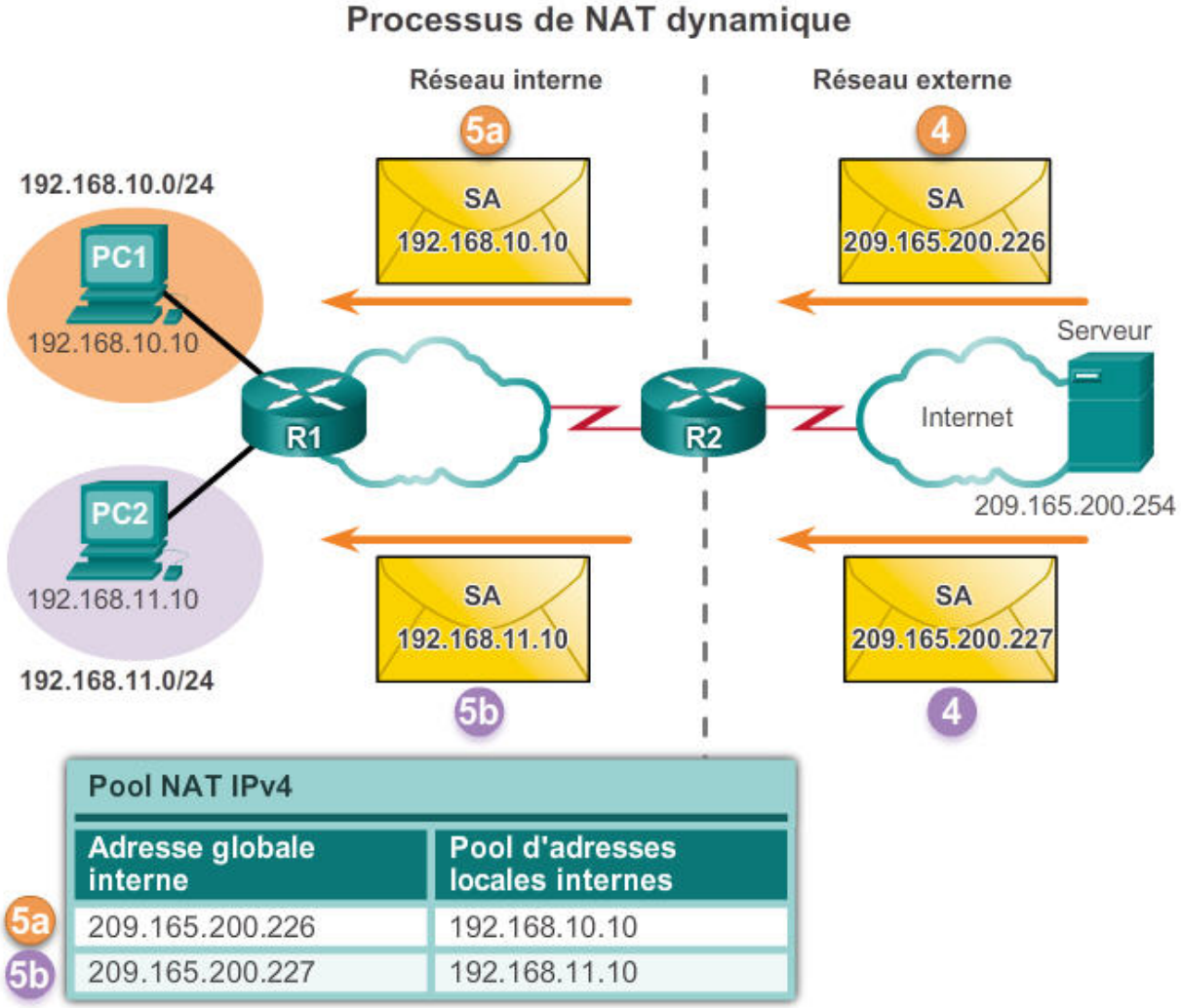
Étapes de configuration de la NAT dynamique

Étapes de configuration de la NAT dynamique	
Étape1	Définissez un pool d'adresses globales à utiliser pour la traduction. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
Étape2	Configurez une liste d'accès standard autorisant les adresses qui doivent être traduites. **access-list** *access-list-number* **permit** *source*[*source-wildcard*]
Étape3	Établissez une traduction dynamique de la source, en spécifiant la liste d'accès et le pool définis lors des étapes précédentes. **ip nat inside source list** *access-list-number* **pool** *name*
Étape4	Identifiez l'interface interne. **interface** *type number* **ip nat inside**
Étape5	Identifiez l'interface externe. **interface** *type number* **ip nat outside**

Analyse de la NAT dynamique



Analyse de la NAT dynamique



Vérification de la NAT dynamique

Vérification de la fonction NAT dynamique à l'aide de `show ip nat translations`

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
--- 209.165.200.227   192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---     ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

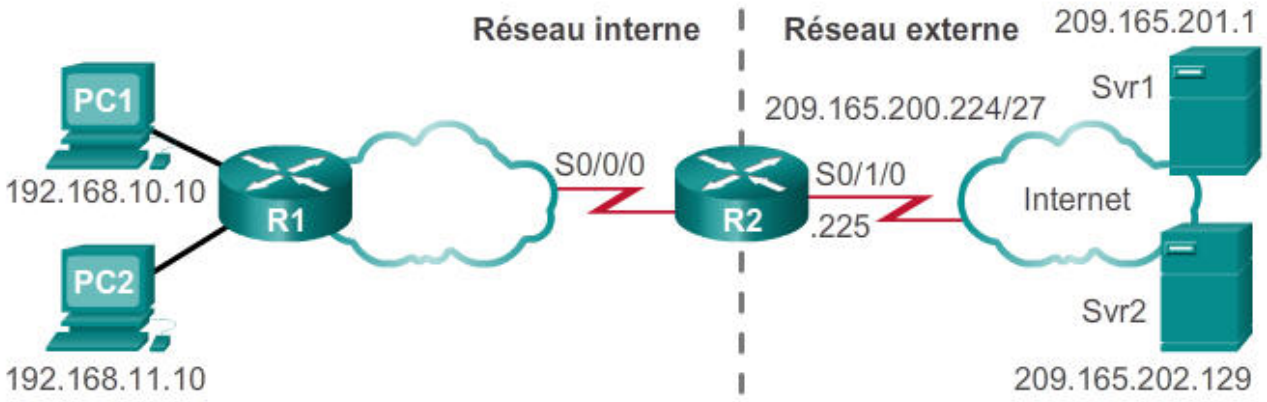
Vérification de la NAT dynamique

Vérification de la NAT dynamique à l'aide de show ip nat statistics

```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Configuration de la PAT : pool d'adresses

Exemple de PAT avec un pool d'adresses



Définissez un pool d'adresses publiques IPv4 sous le nom de NAT-POOL2.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Définissez les adresses pouvant être traduites.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Reliez NAT-POOL2 à l'ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL2
overload
```

Identifiez l'interface série 0/0/0 comme étant une interface NAT interne.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifiez l'interface série 0/1/0 comme étant l'interface NAT externe.

Configuration de la PAT : adresse unique

Étape 1	Définissez une liste d'accès standard autorisant les adresses qui doivent être traduites. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
Étape 2	Établissez une traduction dynamique de la source, en spécifiant l'ACL, l'interface de sortie et les options de surcharge. **ip nat inside source list** *access-list-number* **interface** *type number* **overload**
Étape 3	Identifiez l'interface interne. **interface** *type number* **ip nat inside**
Étape 4	Identifiez l'interface interne. **interface** *type number* **ip nat outside**

Configuration de la traduction d'adresses de port (PAT)

Analyse de la PAT

Analyse de la PAT des ordinateurs aux serveurs

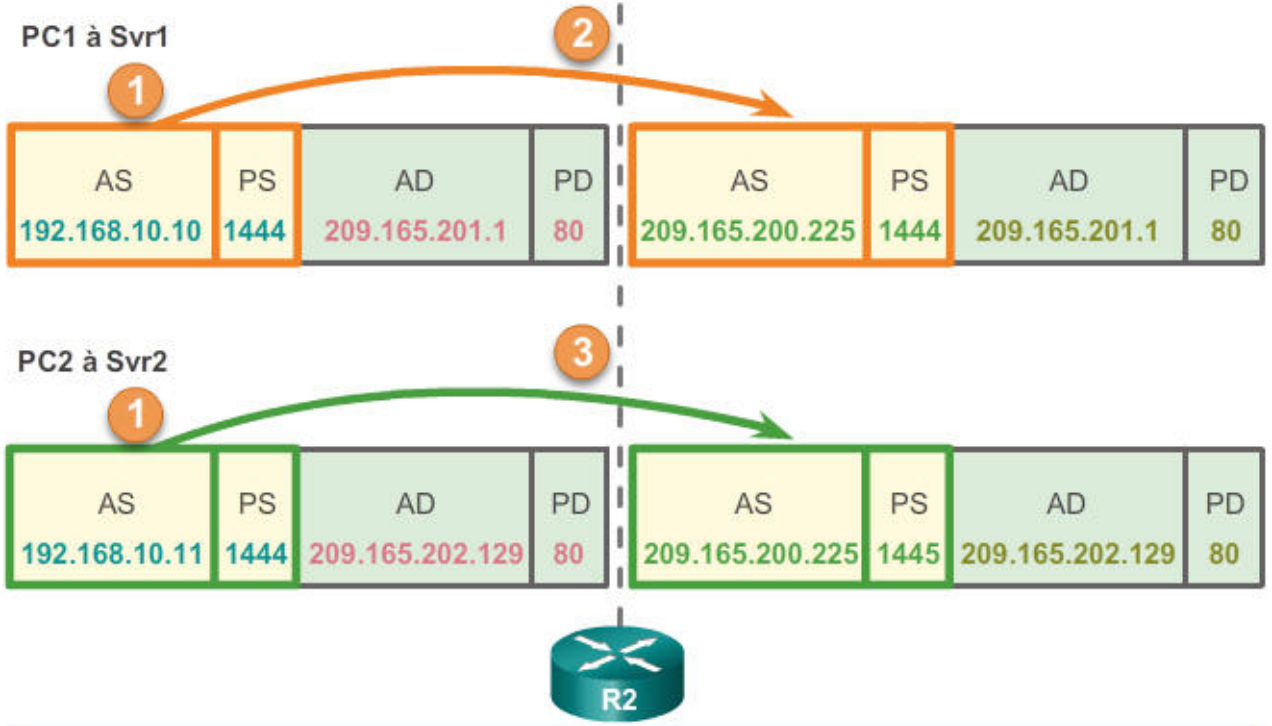


Table NAT

Adresse locale interne	Adresse globale interne	Adresse globale externe	Adresse locale externe
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Analyse de la PAT

Analyse de la PAT des serveurs aux ordinateurs

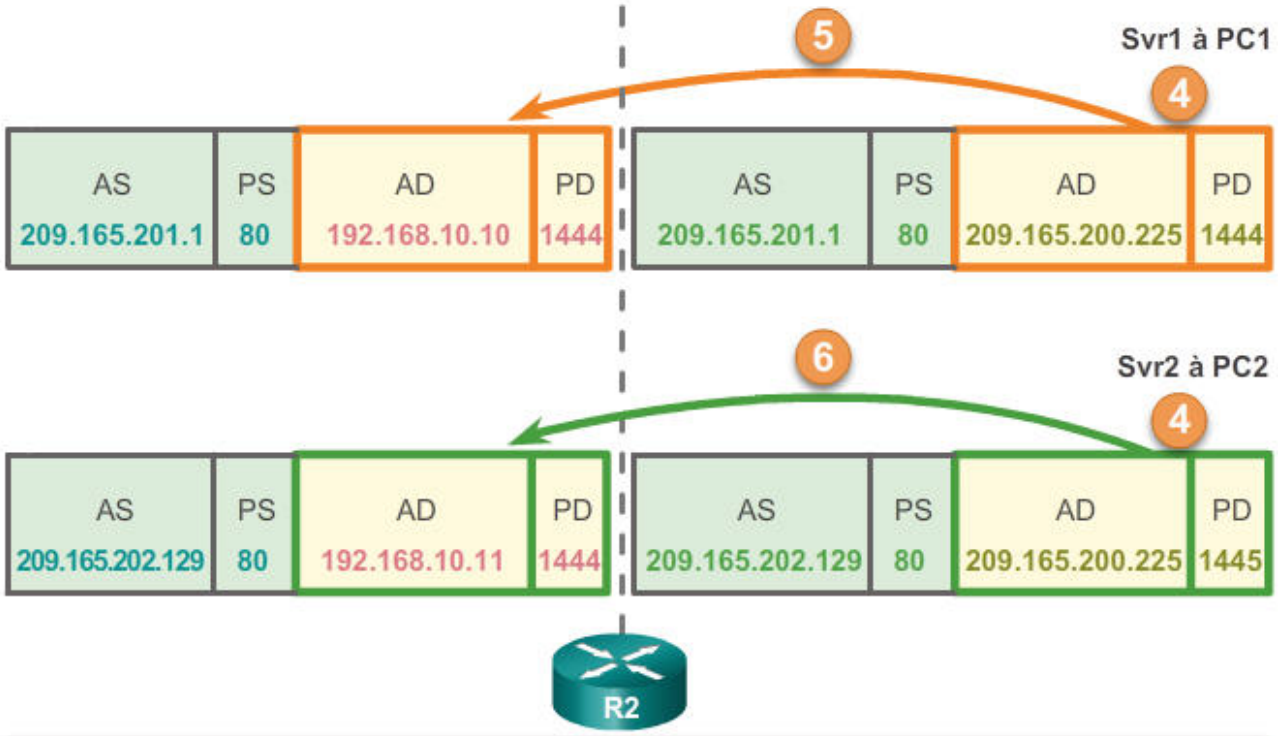


Table NAT

Adresse locale interne	Adresse globale interne	Adresse globale externe	Adresse locale externe
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

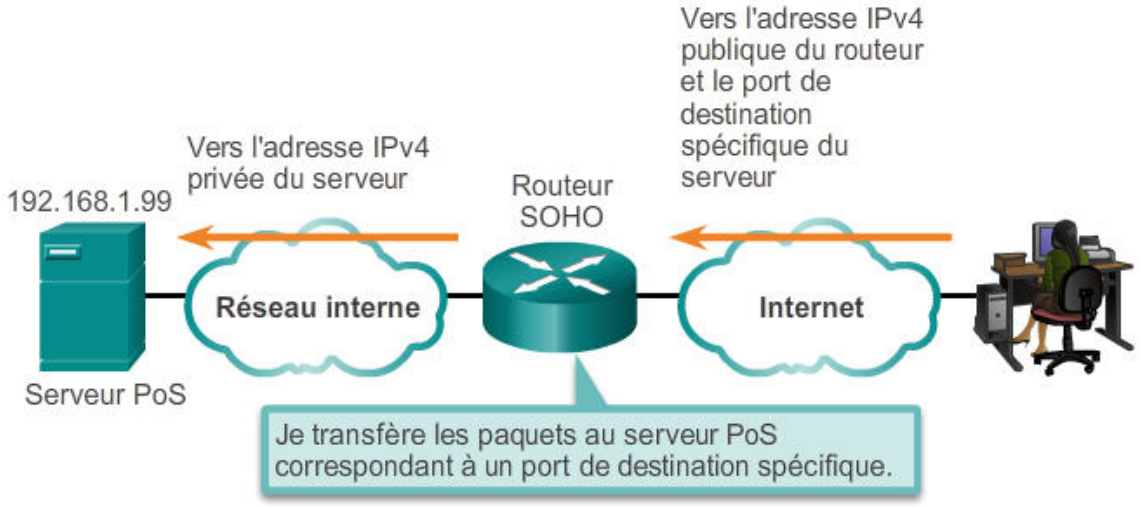
Vérification de la PAT

Vérification des traductions PAT

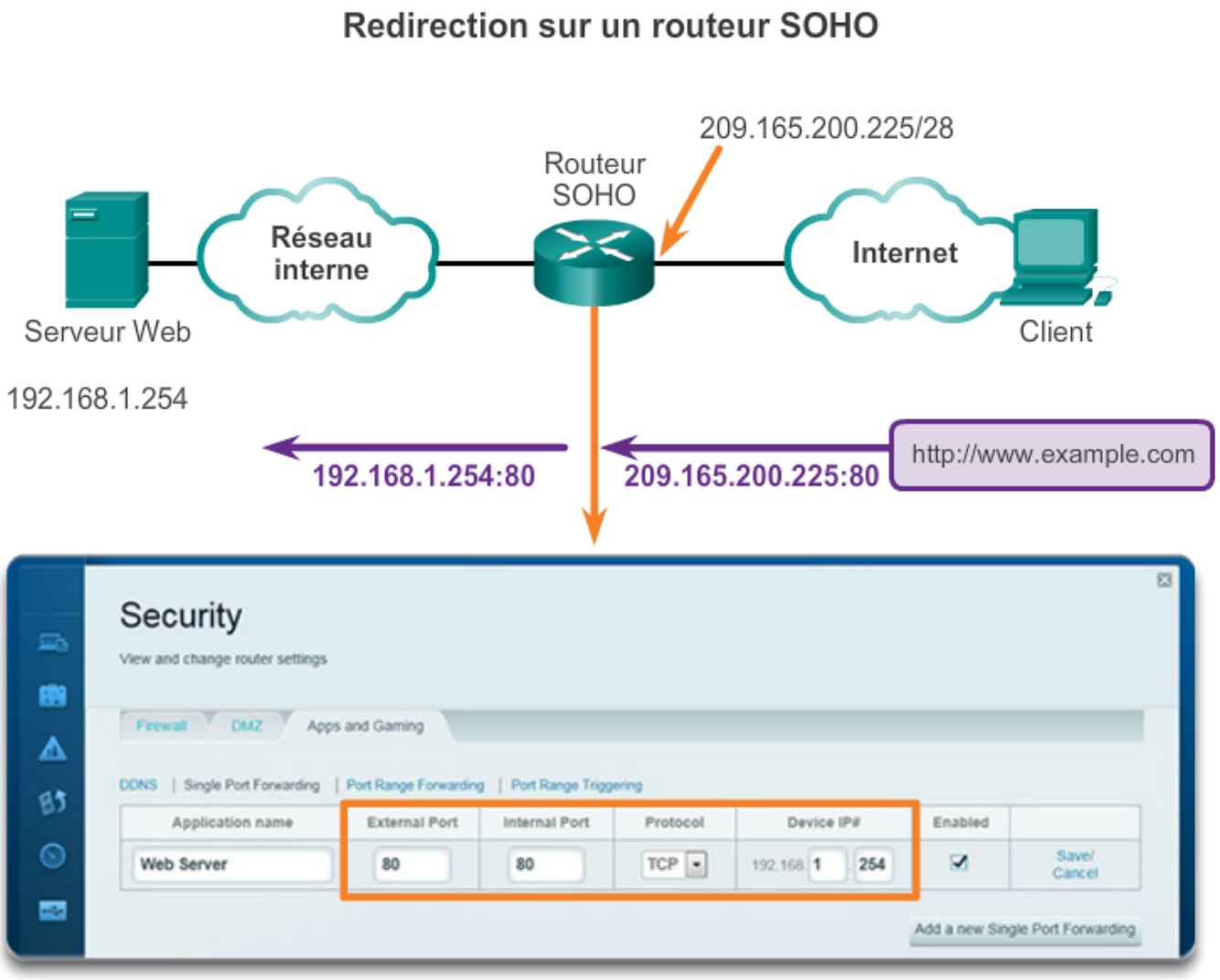
```
R2# show ip nat translations
Pro  Inside global          Inside local         Outside local
tcp  209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:8
tcp  209.165.200.226:42558  192.168.11.10:42558  209.165.202.129
R2#
```

Redirection

- La redirection consiste à transférer un port réseau d'un nœud à l'autre.
- Un paquet envoyé à l'adresse IP publique et au port d'un routeur peut être transféré à une adresse IP privée et à un port d'un réseau interne.
- Cela est utile lorsque les serveurs ont des adresses privées, lesquelles ne sont pas accessibles depuis des réseaux externes.

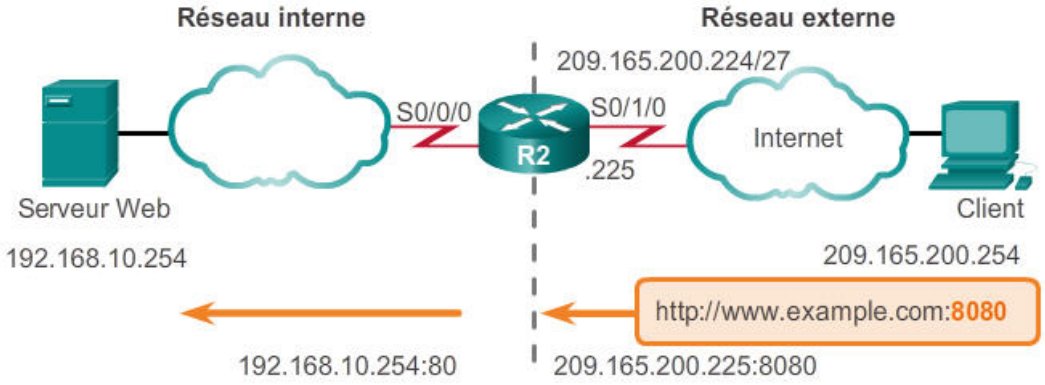


Exemple de SOHO



Configuration de la redirection avec IOS

- Dans IOS, la redirection est en fait une traduction NAT statique avec un numéro de port TCP ou UDP spécifique.



La commande établit la traduction statique entre une adresse locale interne et un port local, et entre une adresse globale interne et un port global.

```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

La commande identifie l'interface série 0/0/0 comme étant une interface NAT interne.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

La commande identifie l'interface série 0/1/0 comme étant l'interface NAT externe.

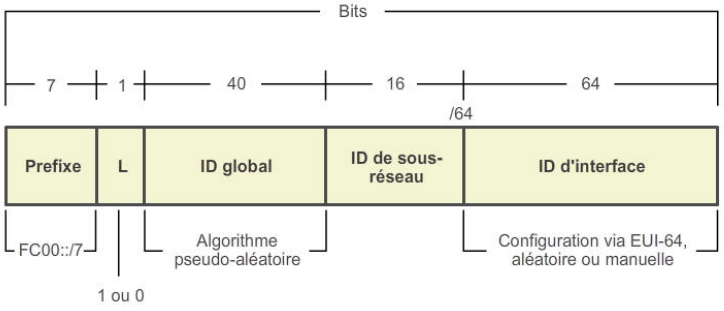
```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

NAT pour IPv6 ?

- La NAT est une solution à la pénurie d'adresses IPv4.
- Avec une adresse 128 bits, IPv6 fournit 340 undécillions d'adresses.
- L'espace d'adressage n'est pas un problème pour IPv6.
- Du fait de sa conception, IPv6 rend inutile la traduction d'adresses IPv4 publiques/privées.
- Toutefois, IPv6 implémente une forme d'adresses privées qui sont mises en œuvre différemment par rapport à IPv4.

Adresses locales uniques IPv6

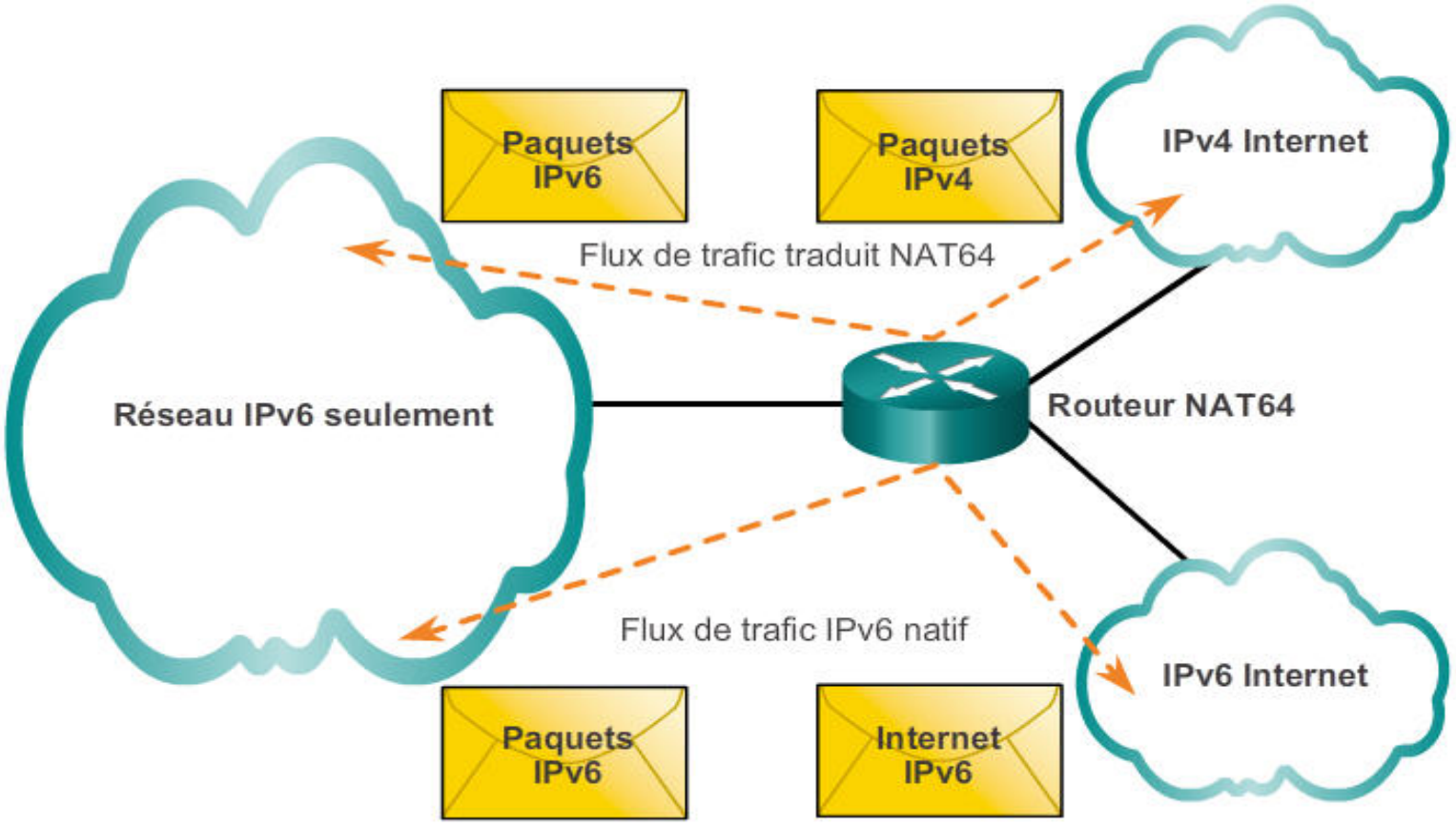
- Les adresses locales uniques (ULA, Unique Local Address) IPv6 sont conçues pour permettre les communications IPv6 à l'intérieur d'un site local.
- Ces adresses n'ont pas vocation à fournir un espace d'adressage IPv6 supplémentaire.
- Elles ont le préfixe FC00::/7, ce qui aboutit à une première plage d'hextets de FC00 à FDFF.
- Elles sont définies dans la RFC 4193.
- On les appelle également adresses IPv6 locales (à ne pas confondre avec les adresses link-local IPv6).



NAT pour IPv6

- IPv6 utilise également la NAT, mais dans un contexte très différent.
- Dans IPv6, la NAT est utilisée pour établir une communication transparente entre IPv6 et IPv4.
- NAT64 n'est pas prévu pour être une solution permanente. Il s'agit d'un mécanisme de transition.
- La traduction adresse réseau/protocole (NAT-PT) était un autre mécanisme de transition vers IPv6 basé sur la NAT, mais celui-ci a été abandonné par l'IETF
- au profit de NAT64.

NAT pour IPv6



Dépannage de la NAT : commandes show

```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
```

Host 192.168.10.10 telnets to server at 209.165.201.1

```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:09 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 31  Misses: 0
CEF Translated packets: 31, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
```

<output omitted>

```
R2# show ip nat translations
Pro Inside global         Inside local         Outside local      Outside global
tcp 209.165.200.226:19005 192.168.10.10:19005  209.165.201.1:23   209.165.201.1:23
R2#
```

Dépannage de la NAT : commande debug

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2817]
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4180]
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2818]
*Feb 15 20:01:311.702: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2819]
*Feb 15 20:01:311.710: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2820]
*Feb 15 20:01:311.710: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4181]
*Feb 15 20:01:311.722: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4182]
*Feb 15 20:01:311.726: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2821]
*Feb 15 20:01:311.730: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4183]
*Feb 15 20:01:311.734: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2822]
*Feb 15 20:01:311.734: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4184]
output omitted
```

Chapitre 11 : résumé

- Ce chapitre a décrit la manière dont la NAT est utilisée pour éviter la pénurie d'espace d'adressage IPv4.
- La NAT permet de ménager l'espace d'adressage public et représente une économie considérable en termes de coûts d'administration liés à la gestion des ajouts, des déplacements et des modifications.
- Ce chapitre a abordé la NAT pour IPv4, notamment :
- Caractéristiques de la NAT, terminologie et fonctionnement général
- Les différents types de NAT sont les suivants : NAT statique, NAT dynamique et NAT avec surcharge
- Les avantages et les inconvénients de la NAT

Chapitre 11 : résumé (suite)

- La configuration, la vérification et l'analyse de la NAT statique, de la NAT dynamique et de la NAT avec surcharge
- La manière dont la redirection peut être utilisée pour accéder aux périphériques internes à partir d'Internet
- Le dépannage de la NAT à l'aide des commandes **show** et **debug**
- La manière dont la NAT pour IPv6 est utilisée pour la conversion entre les adresses IPv6 et les adresses IPv4

Cisco | Networking Academy®

Mind Wide Open™