

# Réseaux fixes

## I.2 Segmentation

### **NAT :** Network Address Translation

Luc Deneire Chapitre tiré de Kwiatkowski  
EII-5, Option Réseaux et Objets Connectés (ROC)

# Traduction d'adresse (Network Address Translation)

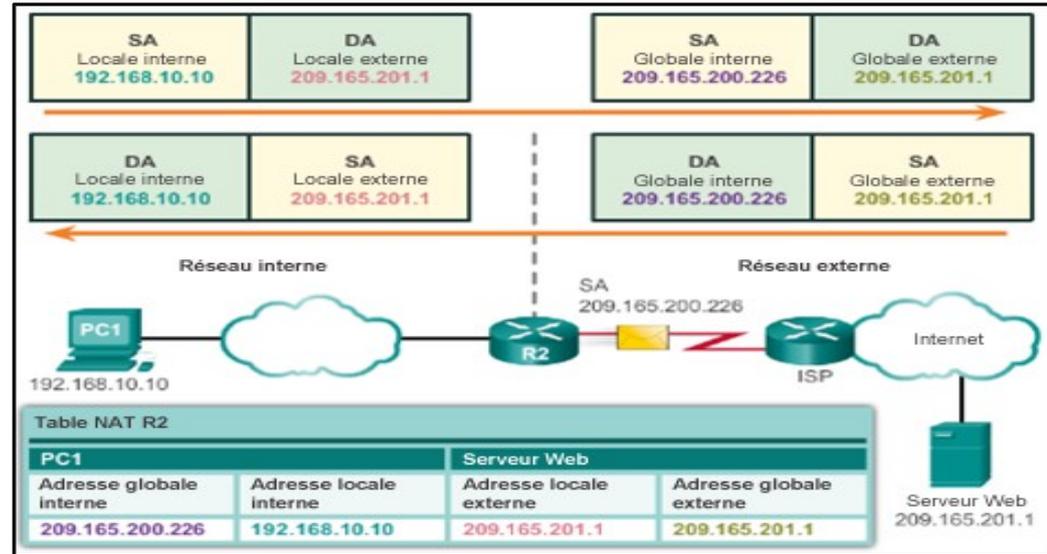
- Traduction d'adresses IP et ports (TCP/UDP) LAN ↔ WAN
- Pallie la pénurie d'adresses IPv4
- Permet l'utilisation d'adresses privées dans le LAN de/vers les adresses publiques
- Implémenté dans les routeurs et firewall

# Les caractéristiques de la NAT

- Espace d'adressage privé IPv4
  - 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16

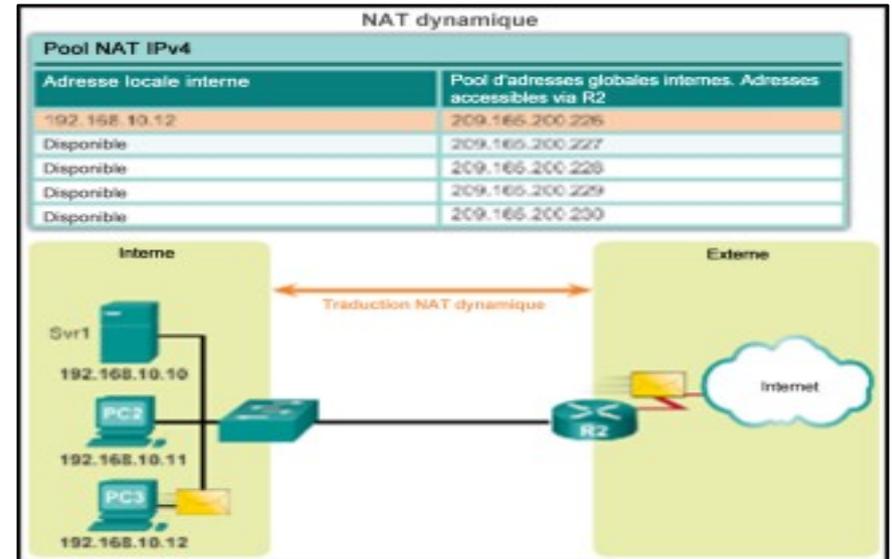
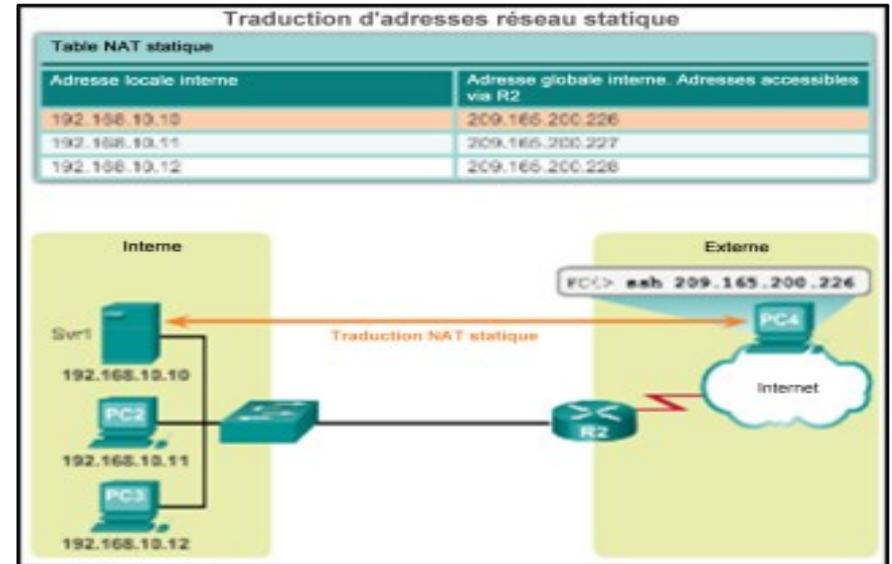
- Terminologie NAT

- Adresse interne
- Adresse locale interne
- Adresse globale interne
- Adresse externe
- Adresse locale externe
- Adresse globale externe



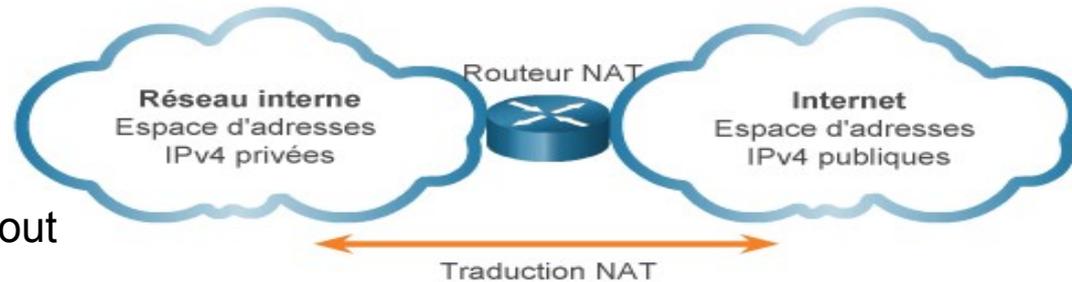
# Les types de NAT

- Traduction d'adresses réseau statique
  - Une adresse locale ↔ Une adresse globale
  - configuré par l'administrateur réseau et constant
- NAT dynamique
  - pool d'adresses publiques « 1<sup>er</sup> arrivé 1<sup>er</sup> servi »
  - Il doit exister suffisamment d'adresses publiques
- Port Address Translation (PAT)
  - Multiples IPv4 privées ↔ Un (ou quelques) IPv4 publiques
  - Appelée également surcharge de NAT
  - Confirme que les paquets entrants ont été demandés
  - Utilise les numéros de port pour transmettre les paquets de réponses au bon appareil interne



# Les bénéfices 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 fonction NAT
  - Dégradation des performances
  - Dégradation de la fonctionnalité de bout en bout
  - Perte de la traçabilité IP de bout en bout
  - Tunneling plus complexe
  - Perturbations éventuelles de l'établissement des connexions TCP



# Configuration de la NAT statique

- Configuration de la fonction NAT statique
  - Créez le mappage entre les adresses locales internes et les adresses locales externes

```
ip nat inside source static local-ip global-ip
```

- Définissez quelles interfaces appartiennent au réseau interne et lesquelles appartiennent au réseau externe

```
ip nat inside
```

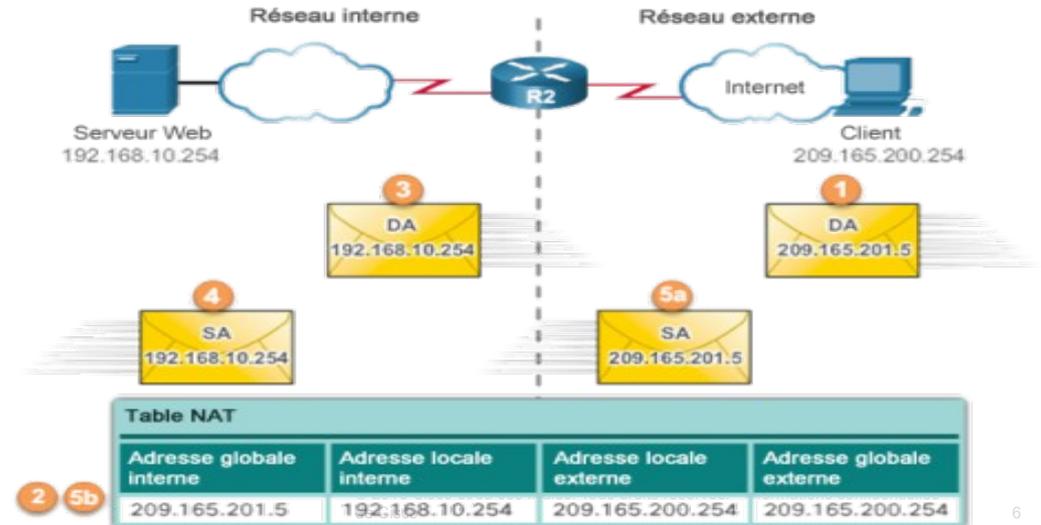
```
ip nat outside
```

- Analyse de la NAT statique
- Vérification de la NAT statique

```
show ip nat translations
```

```
show ip nat statistics
```

```
clear ip nat statistics
```



# Configuration de la NAT dynamique

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

# Configuration de la NAT dynamique (suite)

- Configuration de la NAT dynamique

- Créez le mappage entre les adresses locales internes et les adresses locales externes

```
ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
```

- Créez une liste de contrôle d'accès standard pour permettre la traduction de ces adresses

```
access-list access-list-number permit source [source-wildcard]
```

- Reliez la liste de contrôle d'accès au pool

```
ip nat inside source list access-list-number pool name
```

- Identifiez les interfaces interne et externe

```
ip nat inside
```

```
ip nat outside
```

# Configuration de la NAT dynamique (suite)

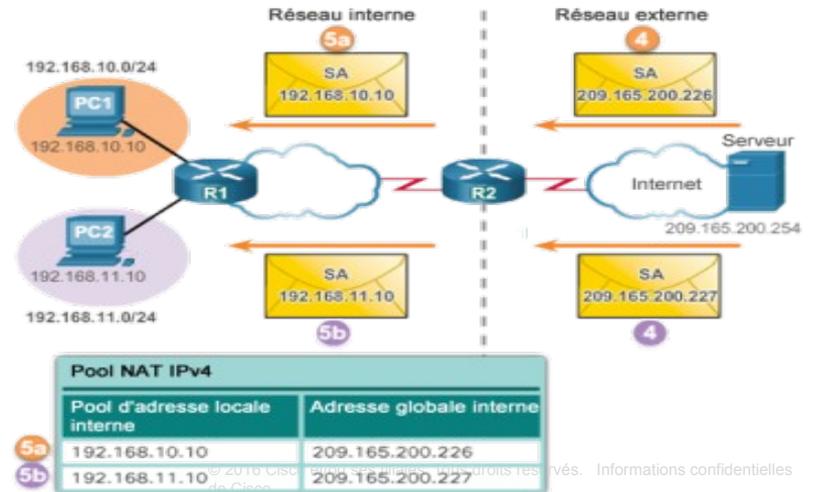
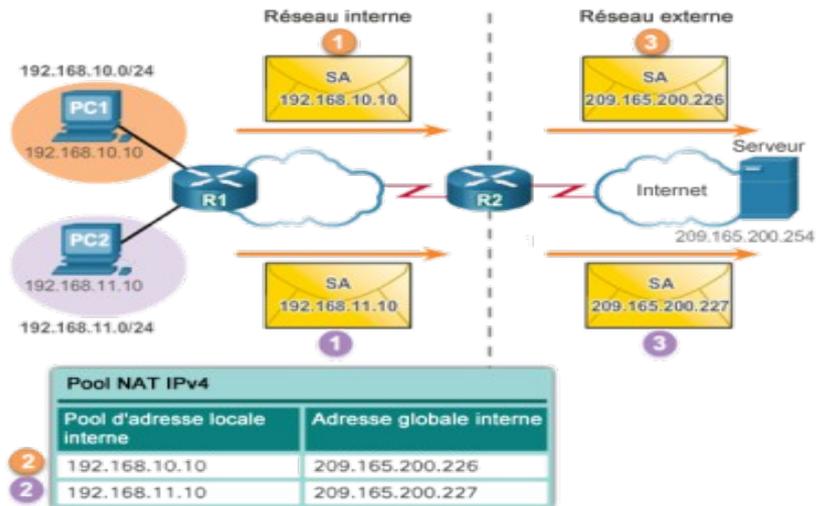
- Analyse de la NAT dynamique
- Vérification de la NAT dynamique

```
show ip nat translations
```

```
show ip nat translations verbose
```

```
clear ip nat statistics
```

```
clear ip nat translations *
```



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

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

### ▪ Configuration de la PAT : pool d'adresses

- Créez le mappage entre les adresses locales internes et les adresses locales externes

```
ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
```

- Créez une liste de contrôle d'accès standard pour permettre la traduction de ces adresses

```
access-list access-list-number permit source [source-wildcard]
```

- Reliez la liste de contrôle d'accès au pool

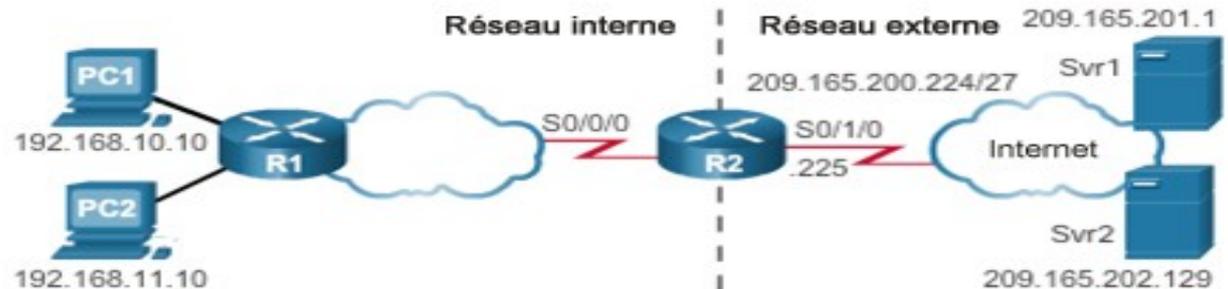
```
ip nat inside source list access-list-number pool name
```

- Identifiez les interfaces interne et externe

```
ip nat inside
```

```
ip nat outside
```

Exemple de PAT avec un pool d'adresses



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

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

### Configuration de la PAT : adresse unique

- Définissez une liste de contrôle d'accès standard pour permettre la traduction de ces adresses

```
access-list access-list-number permit source [source-wildcard]
```

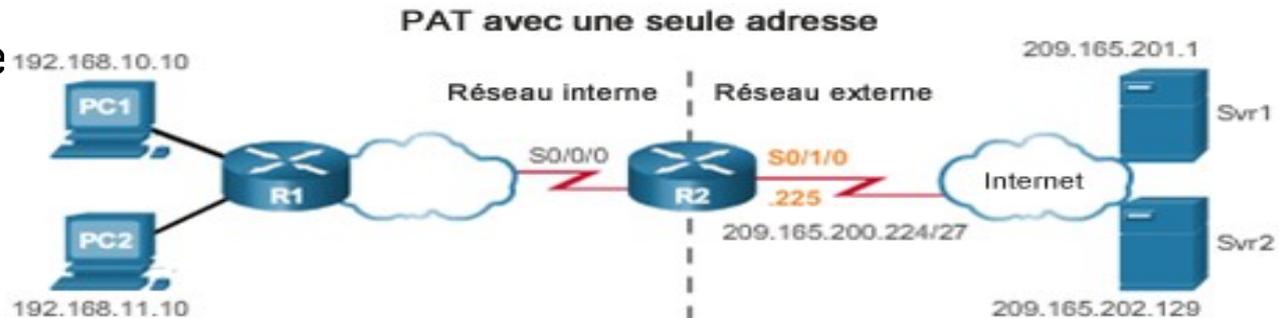
- Établissez une traduction dynamique de la source, en spécifiant la liste de contrôle d'accès, l'interface de sortie et l'option de surcharge

```
ip nat inside source list access-list-number interface type name overload
```

- Identifiez les interfaces interne

```
ip nat inside
```

```
ip nat outside
```



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

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

### Analyse de la PAT

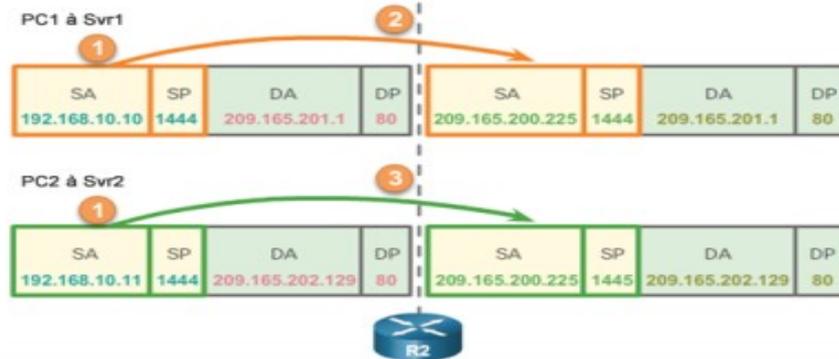
- Vérification de la PAT

```
show ip nat translations
```

```
show ip nat statistics
```

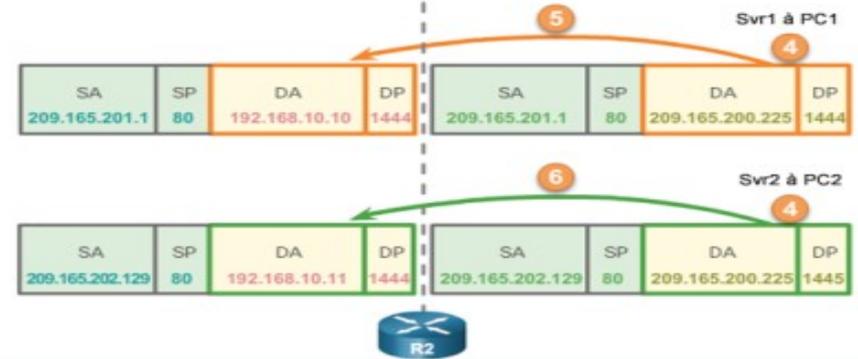
```
clear ip nat statistics
```

Analyse de la PAT des ordinateurs aux serveurs



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 des serveurs aux ordinateurs



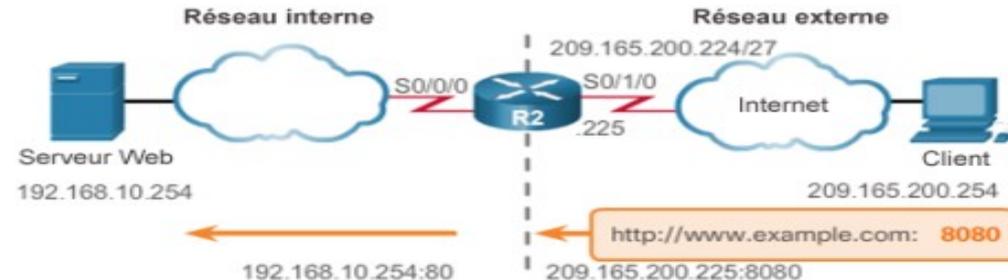
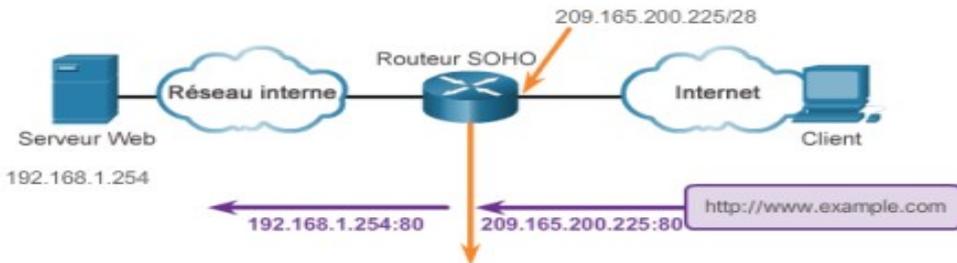
Adresse locale interne	Adresse globale interne	Adresse globale externe	Adresse locale externe
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

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

# Le transfert de port

- Transfert de port
  - Le transfert de port consiste à transférer un port réseau d'un nœud réseau à un 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.
  - Cette procédure est utile lorsque les serveurs ont des adresses privées, lesquelles ne sont pas accessibles depuis des réseaux externes.
- Exemple de routeur sans fil
- Configuration du transfert de port avec IOS

```
ip nat inside source [static {tcp | udp local-ip local-port global-ip  
global-port} [extendable]
```



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

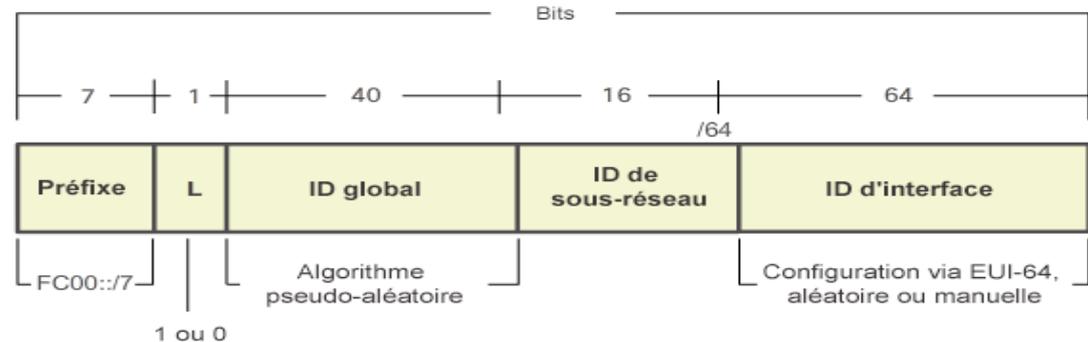
# Configuration de la NAT et d'IPv6

### ■ NAT pour IPv6 ?

- IPv6 fournit 340 sextillions d'adresses à partir d'une adresse 128 bits.
- L'espace d'adressage n'est pas un problème pour IPv6.
- De par sa conception, IPv6 n'a pas besoin de recourir à la NAT publique-privée IPv4. Toutefois, IPv6 implémente une forme d'adresses privées qui sont mises en œuvre différemment par rapport à IPv4.

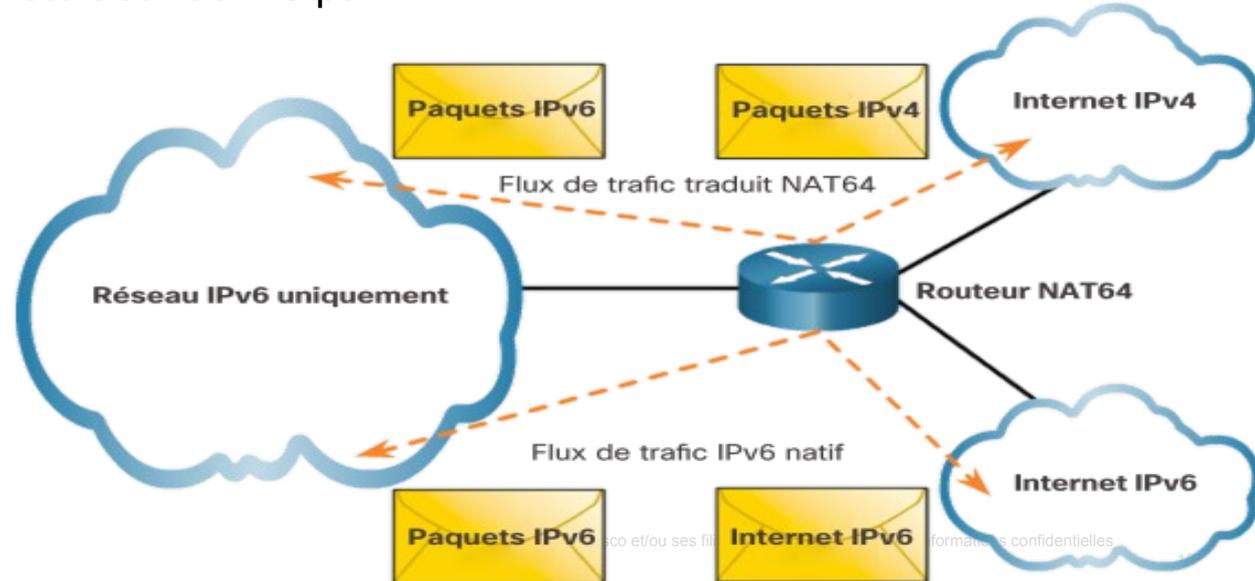
### ■ Adresse locale unique IPv6

- 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.
- On les appelle également adresses IPv6 locales (à ne pas confondre avec les adresses de liaison locale IPv6).



# Configuration de la NAT et d'IPv6 (suite)

- 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 une solution permanente, mais plutôt un mécanisme de transition.
  - La traduction d'adresses réseau/de protocoles (NAT-PT) était un autre mécanisme de transition vers IPv6 basé sur la NAT, mais celui-ci a été abandonné par l'IETF.
  - NAT64 est désormais recommandé.



# Dépannage des configurations de la NAT

- Dépannage de la NAT : commandes show

```
clear ip nat statistics
```

```
clear ip nat translations *
```

```
show ip nat statistics
```

```
Show ip nat translations
```

- Dépannage de la NAT : commandes debug

```
debug ip nat
```

