Administration réseau
Réseaux privés

A. Guermouche

Plan

Plan

Pourquoi avoir des adresses privées?

- ⋆ Gérer la pénurie d'adresses au sein d'un réseau
- ⋆ Masquer l'intérieur du réseau par rapport à l'extérieur (le réseau peut être vu comme une seule et même machine)
- ⋆ Améliorer la sécurité pour le réseau interne
- ⋆ Assouplir la gestion des adresses du réseau interne
- ⋆ Faciliter la modification de l'architecture du réseau interne

$\longrightarrow$ Mécanisme de translation d'adresses (NAT - Network Address Translation)
Deux types de NAT :

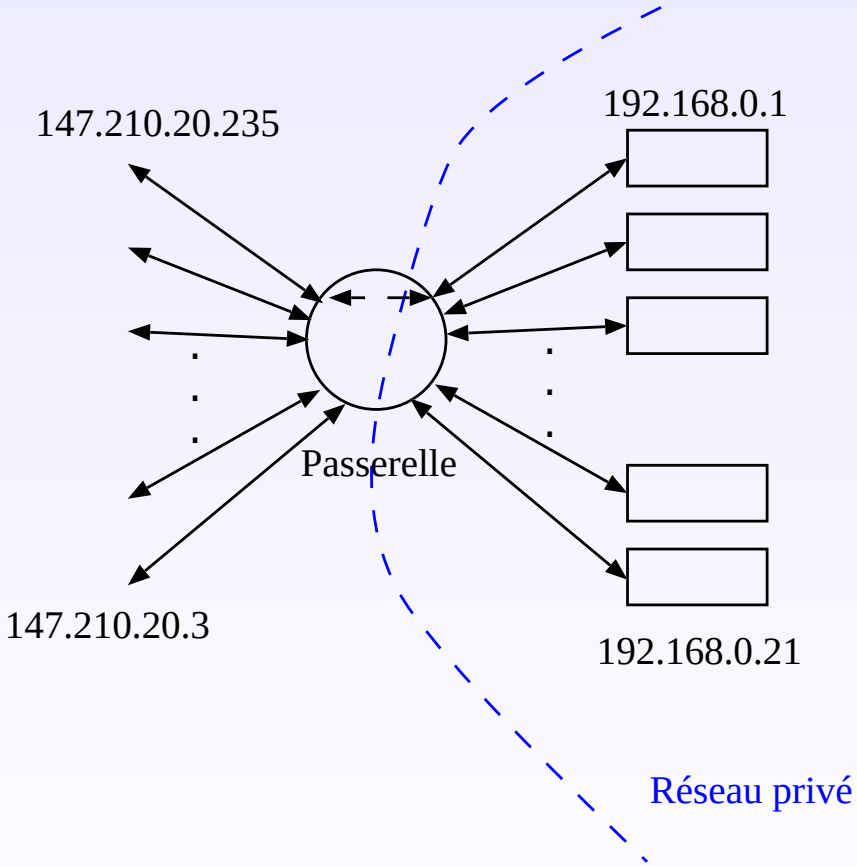
statique. association entre *n* adresses publiques et *n* adresses privées.

dynamique. association entre 1 adresse publique et *n* adresses privées.

Plan

NAT statique

Association entre une adresse publique et une adresse privée.



NAT statique

Association entre une adresse publique et une adresse privée.

Intérêt :

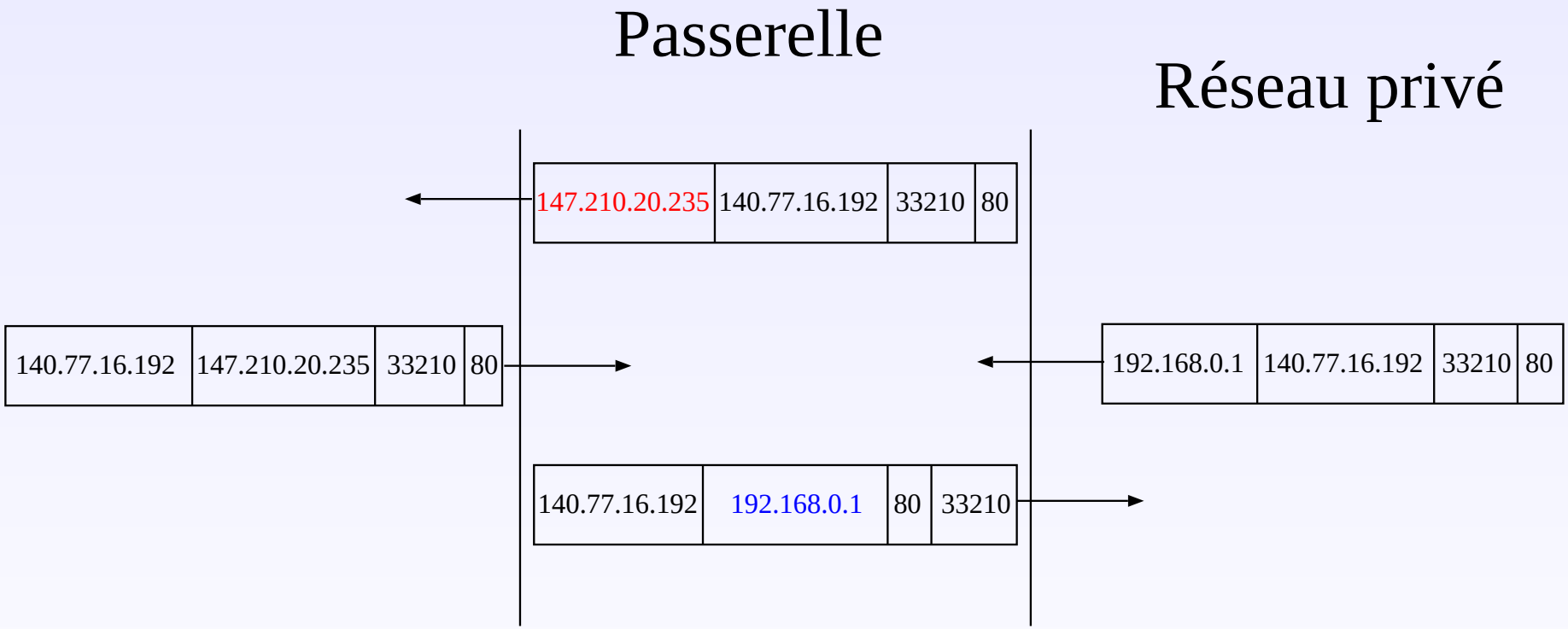
- Uniformité de l'adressage dans la partie privée du réseau (modification de la correspondance @publique/@privée facile)
- Sécurité accrue (tous les flux passent par la passerelle NAT)

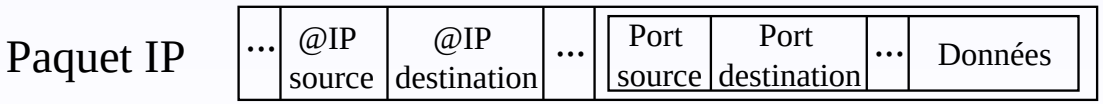
Inconvénient :

- Problème de pénurie d'adresses IP publiques non-résolu

NAT statique : Principe

Pour chaque paquet sortant (resp. entrant), la passerelle modifie l'adresse source (resp. destination).

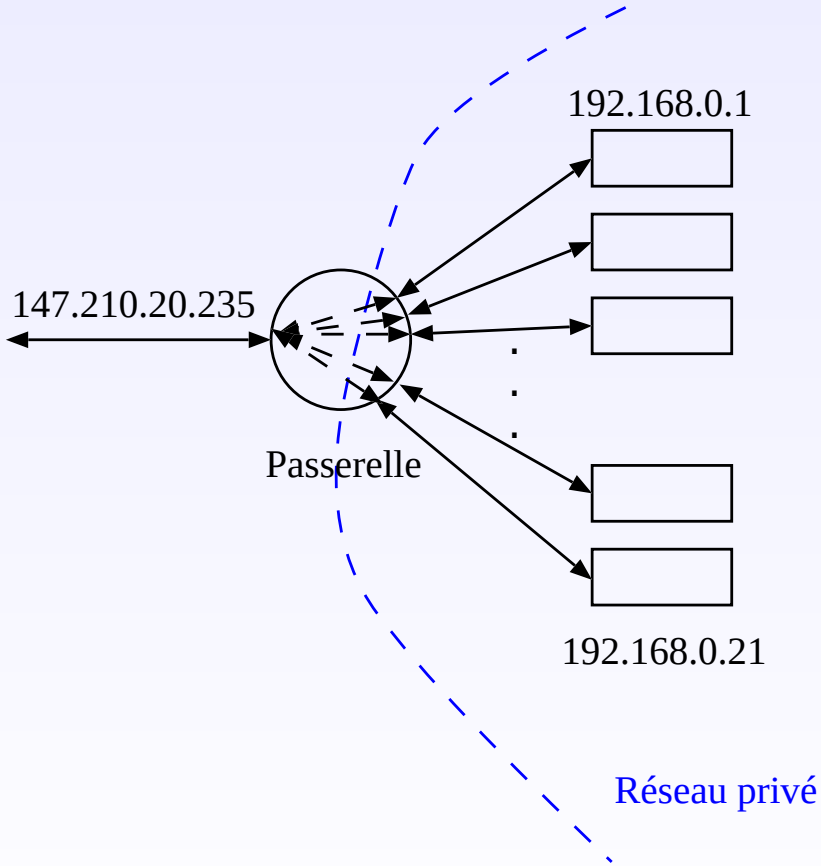




Plan

NAT dynamique : Masquerading

Association entre m adresses publiques et n adresses privées ($m < n$).



NAT dynamique : Masquerading

Association entre m adresses publiques et n adresses privées ($m < n$).

Intérêt :

- Plusieurs machines utilisent la même adresse IP publique pour sortir du réseau privé
- Sécurité accrue (tous les flux passent par la passerelle NAT)

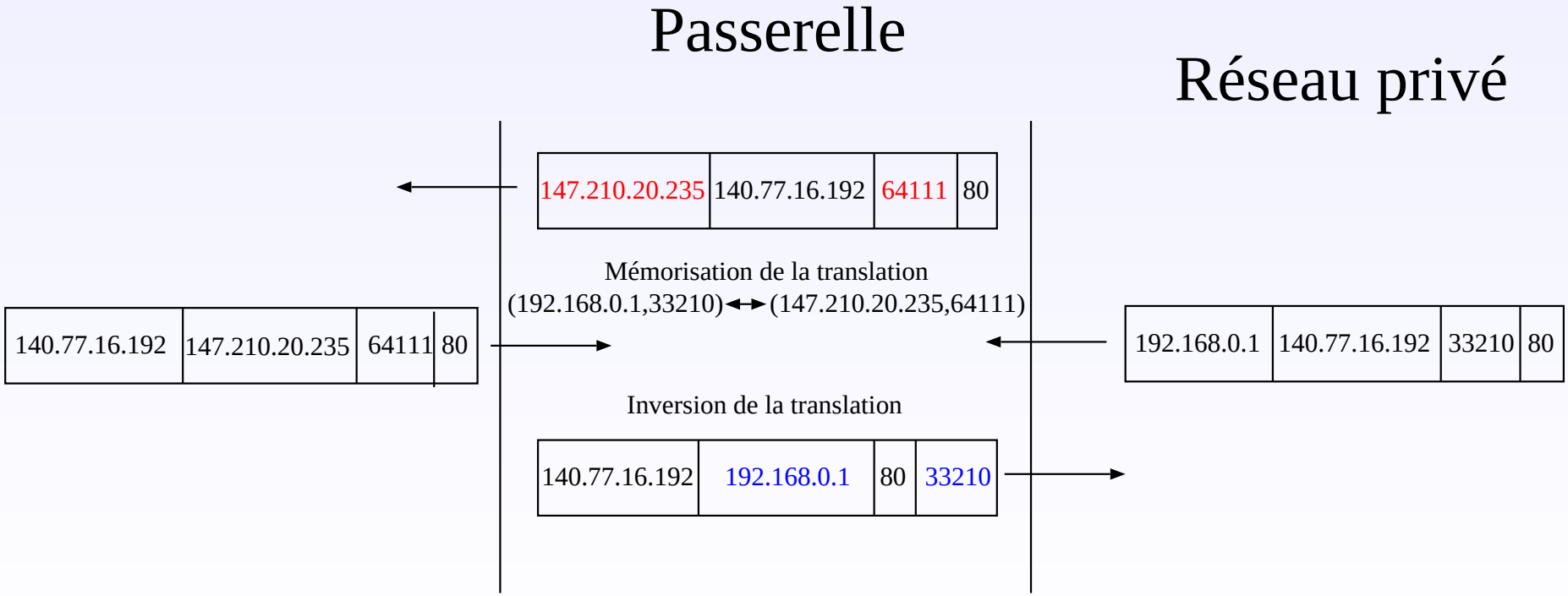
Inconvénient :

- Les machines du réseau interne ne sont pas accessibles de l'extérieur (impossibilité d'initier une connexion de l'extérieur)

NAT dynamique : Principe (1/2)

L'association de *n* adresses privées à 1 adresse publique nécessite, au niveau de la passerelle, de :

- ★ modifier l'adresse source (resp. destination) des paquets sortant (resp. entrants)
- ★ changer le numéro de port source pour les flux sortant



NAT dynamique : Principe (2/2)

Comment est ce que le routeur différencie les paquets qui lui sont destinés de ceux qu'il doit relayer?

À chaque nouvelle connexion :

1: Modifier l'adresse source et le port source : (@source_privée,port_source)→(@publique,port_source')
2: Sauvegarder l'association dans la table `NAT`

Pour chaque paquet entrant :

3: Chercher une association correspondant au couple (@destination, port_destination)
4: **Si** ∃ une association dans la table `NAT` **Alors**
5: Modifier l'adresse de destination et le port de destination
6: Relayer le paquet
7: **Sinon**
8: /* Erreur de routage */
9: **Fin du Si**

NAT dynamique : Principe (2/2)

Comment est ce que le routeur différencie les paquets qui lui sont destinés de ceux qu'il doit relayer?

À chaque nouvelle connexion :

1: Modifier l'adresse source et le port source : (@source_privée,port_source)→(@publique,port_source')
2: Sauvegarder l'association dans la table `NAT`

Pour chaque paquet entrant :

3: Chercher une association correspondant au couple (@destination, port_destination)
4: **Si** ∃ une association dans la table `NAT` **Alors**
5: Modifier l'adresse de destination et le port de destination
6: Relayer le paquet
7: **Sinon**
8: /* Erreur de routage */
9: **Fin du Si**

Le routeur gère toutes les associations

⇒ Unicité de l'association (donc du port source après translation)

Problèmes liés à NAT dynamique

Comment faire de la translation d'adresse sur des protocoles qui ne sont pas basés sur TCP ou UDP (pas de numéro de port)?

- Nécessité d'implémenter une méthode spécifique au protocole (identifiant ICMP pour ICMP par exemple).
- Dans le cas des protocoles dont les paquets contiennent des données relatives aux adresses IP, il est nécessaire de mettre en place des "proxy" (`FTP` en mode actif par exemple).

Comment rendre joignables des machines du réseau local?

- Nécessité de faire de la redirection de port (port forwarding/mapping).

  Principe. Toutes les connexions entrantes sur un port donné sont redirigée vers une machine du réseau privé sur un port (qui peut être le même ou non).

Plan

Proxy ou mandataire

Définition :

- ★ Un proxy est un intermédiaire dans une connexion entre le client et le serveur
- ★ Le client s'adresse toujours au proxy
- ★ Le proxy est spécifique à une application donnée (`HTTP`, `FTP`, ...)

→ Possibilité de modification des informations échangées entre le client et le serveur.

Proxy ou mandataire

Définition :

- Un proxy est un intermédiaire dans une connexion entre le client et le serveur
- Le client s'adresse toujours au proxy
- Le proxy est spécifique à une application donnée (`HTTP`, `FTP`, ...)