Institut Supérieur des Sciences Appliquées et de Technologie de Sousse

Internet ET Protocoles

DNI-A1

Semestre 2

Enseignante: **INSAF SAGAAMA**

Année universitaire: 2024 - 2025

Ce document doit être complété par les notes de cours !

Chapitre 5: Traduction d'adresse réseau pour IPv4

1. Mécanisme de translation d’adresse
2. NAT Statique
3. NAT Dynamique

Network Address Translation (NAT)

Adressage IP

- Chaque station connectée à un réseau IP est identifiée par une adresse IP

- L'adresse IP **DOIT** être unique pour permettre d'identifier la station sur tout réseau Internet

- En tant qu'adresse logique, l'adresse IP premet :
  - d'identifier le réseau auquel appartient la station
  - d'identifier la station dans ce réseau.

Adresses IP privées

- Le protocole IP défini un ensemble d'adresses dites **privées**
  - Ces adresses ne sont pas reconnues dans Internet
  - Elles sont destinées à être utilisées à l'intérieur de réseaux privés

- Ces adresses ne sont pas reconnues par les routeurs dans Internet
  - On ne peut pas envoyer un paquet qui a comme adresse destination une adresse privée
  - Un paquet IP ne peut pas avoir une adresse privée comme adresse source dans Internet

- Trois intervalles d'adresse privées:
  - [10.0.0.0 , 10.255.255.255]
  - [172.16.0.0 , 172.31.255.255]
  - [192.168.0.0, 192.168.255.255]

Penurie des adresses IP publiques

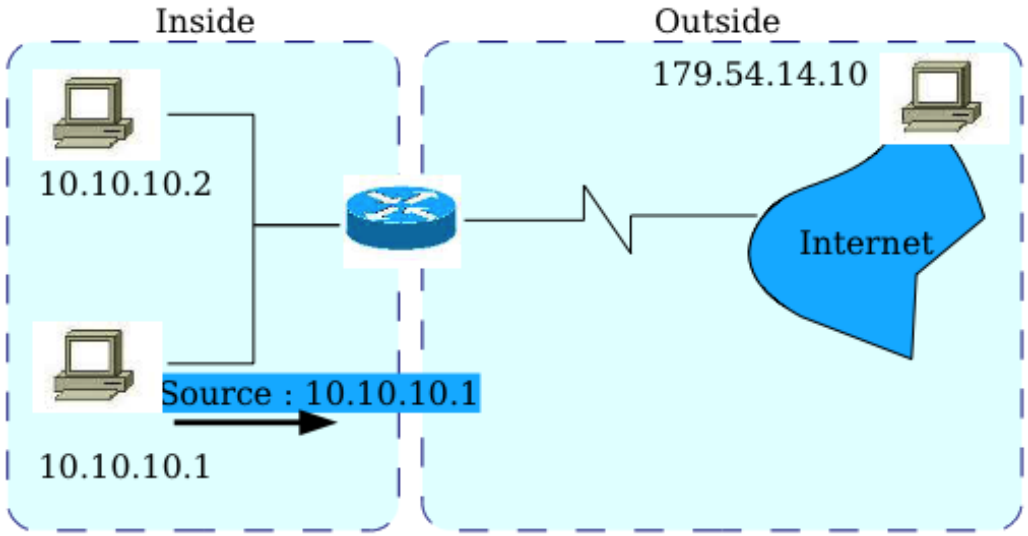
- L'augmentation exponentielle du nombre d'ordinateurs connectés à Internet a rapidement saturé l'espace d'adressage IP
  - Il n'est plus possible d'attribuer une adresse IP à chaque station connectée à Internet
- Le CIDR a permis de régler en partie le problème, l'espace d'adressage IPv4 demeure insuffisant !
- Dans les faits
  - Une organisation (entreprise/particulier) qui possède un nombre B de stations ayant besoin d'un accès Internet n'obtient généralement qu'un petit nombre **n** d'adresses IP dites publiques
    - **n est beaucoup plus petit que B (et en général n=1 !)**

LANs et Adresses privées

- Il y a plusieurs autres raisons qui poussent un administrateur réseau d'utiliser des adresses privées dans son LAN?
  - **Gérer le nombre limité d'adresses publiques disponibles**
  - 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
    - L'échange avec l'extérieur se fait forcement via un intermédiaire
  - Assouplir la gestion des adresses du réseau interne
    - L'adressage interne n'est pas visible de l'extérieur → l'affectation des adresses peut être gérer selon les besoins internes sans impact sur l'échange avec l'exterieur
  - Faciliter la modification de l'architecture du réseau interne

Mécanisme de translation d'adresse

- Pour permettre à un réseau local qui utilise des adresses privées de communiquer avec l'exterieur, il faut un **mécanisme de translation d'adresse**
  - **NAT - Network Address Translation**
- Principe de la translation d'adresse
  - **Une passerelle** (qui est un routeur qui implémente le NAT) est placée entre le réseau local et Intenet
  - **La passerelle** est le seul point de passage entre le Site NAT LAN et le réseau externe
  - **La passerelle** possède et gère les n adresses publiques



Mécanisme de translation d'adresse (suite)

- les stations LAN n'ont pas connaissance des adresses publiques de la passerelle et ne les utilisent pas
- Ces stations ont des adresses privées dans les plages définies à cet effet
- Pour les stations du réseau Internet, seules les n adresses de la passerelle existent et le LAN avec ses adresses privées est invisible
- à l'interieur du LAN, les stations communiquent entre elles en utilisant leurs adresses privées
- sans le mécanisme NAT dans la passerelle, un message envoyé à l'extérieur ne peut pas avoir une réponse car les adresses privées ne sont pas reconnues dans Internet
    - La passerelle (via le mécanisme NAT) doit traduire (remplacer) dans un message destiné à l'extérieure, l'adresse privée par une adresse publique, et inversement pour la réponse

NAT

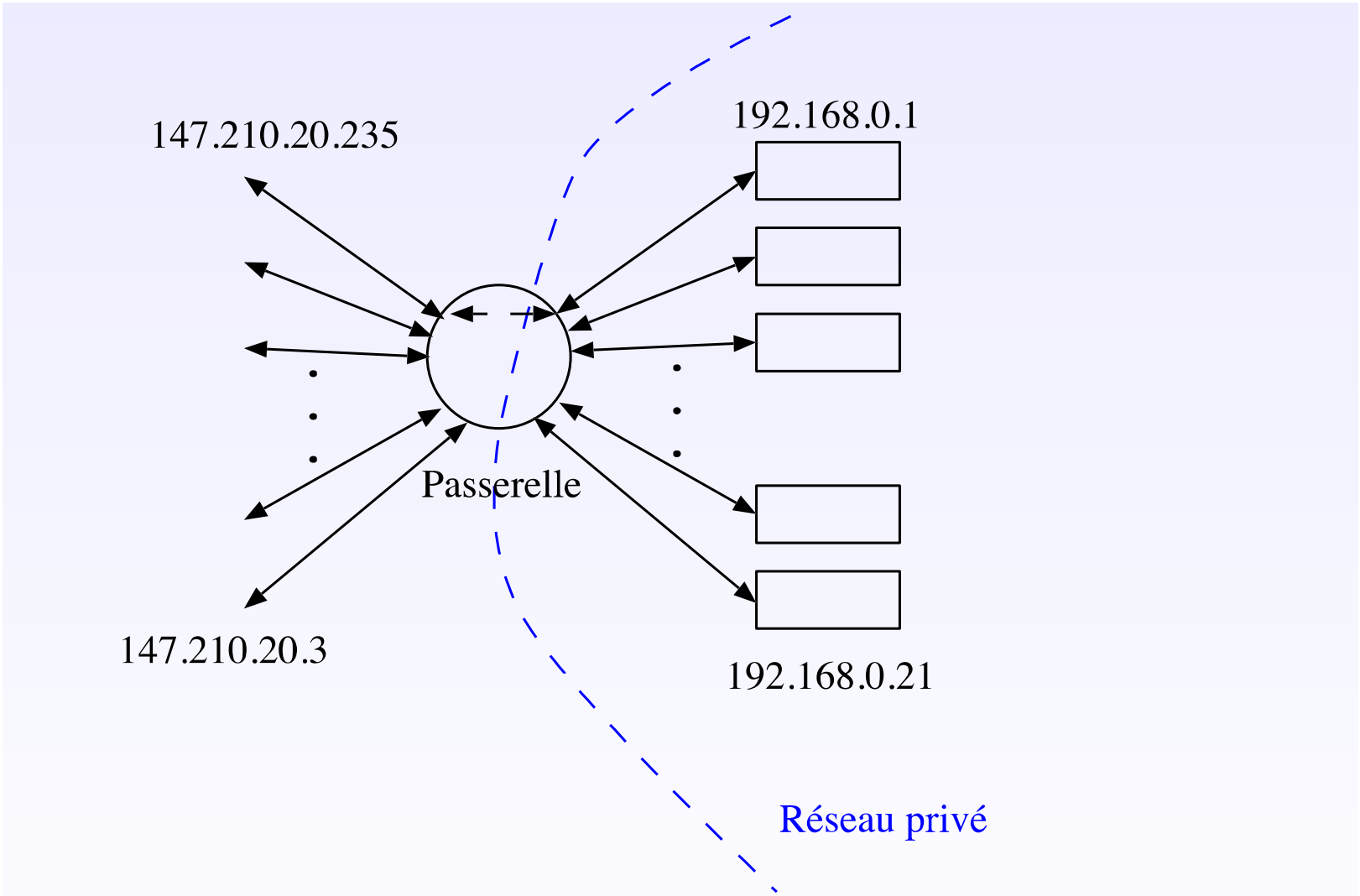
- Il existe deux types de NAT :
  - **NAT statique:** association entre *n* adresses publiques et *n* adresses privées.
  - **NAT dynamique :** association entre 1 adresse publique et *n* adresses privées.

NAT statique

- Association entre une adresse publique et une adresse privée
  - À une adresse privée dans le réseau LAN, on associe une adresse publique au niveau de la passerelle
- Intérêt :
  - Uniformité de l'adressage dans la partie privée du réseau (modification de la correspondance @publique/@privée facile)
  - Augmenter la sécurité dans le LAN
    - tous les échanges de données avec l'exterieur passent par la passerelle NAT
- Inconvénient :
  - Problème de pénurie d'adresses IP publiques!!!

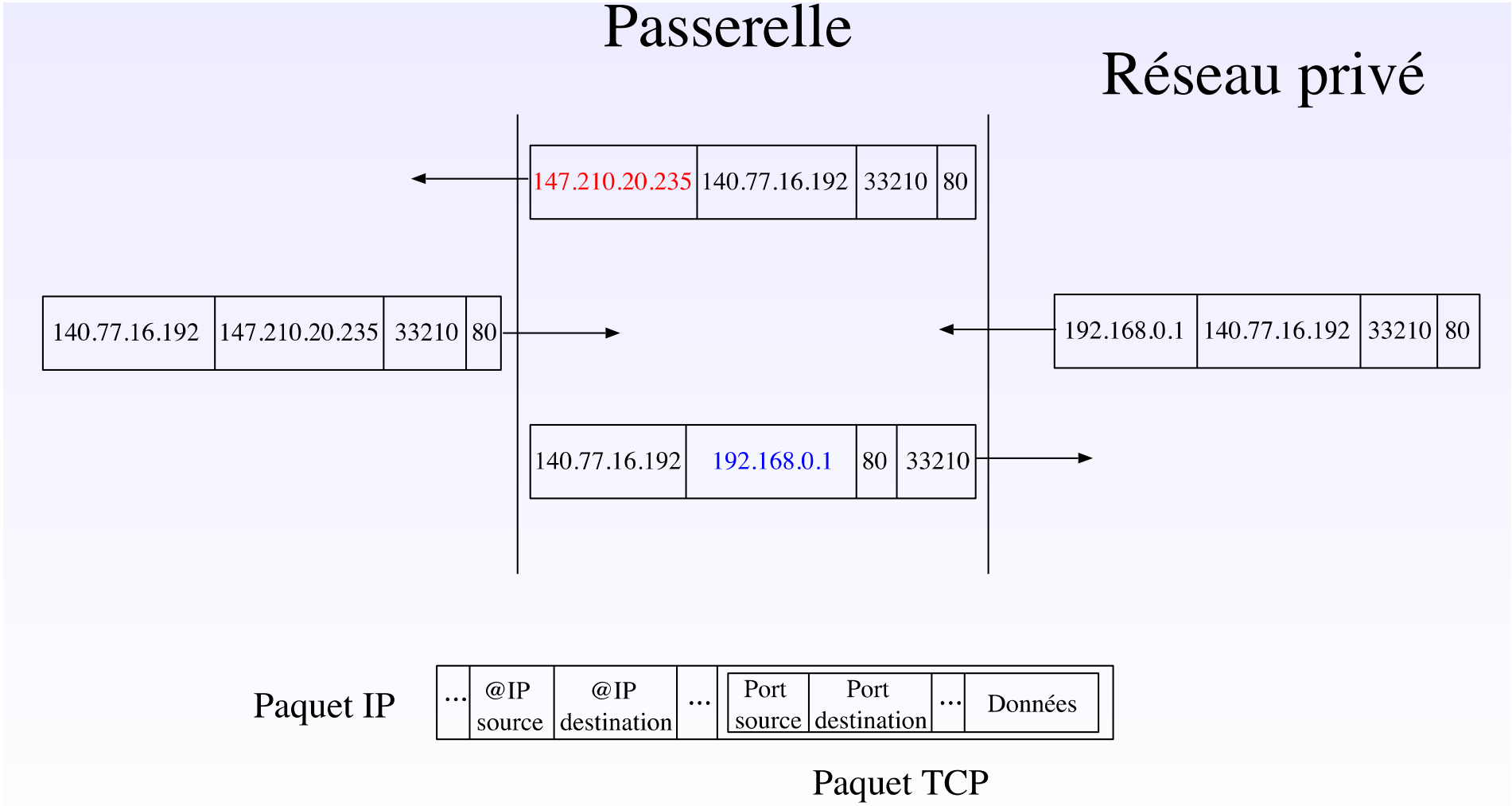
NAT statique (suite)

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



NAT statique (suite)

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



NAT dynamique

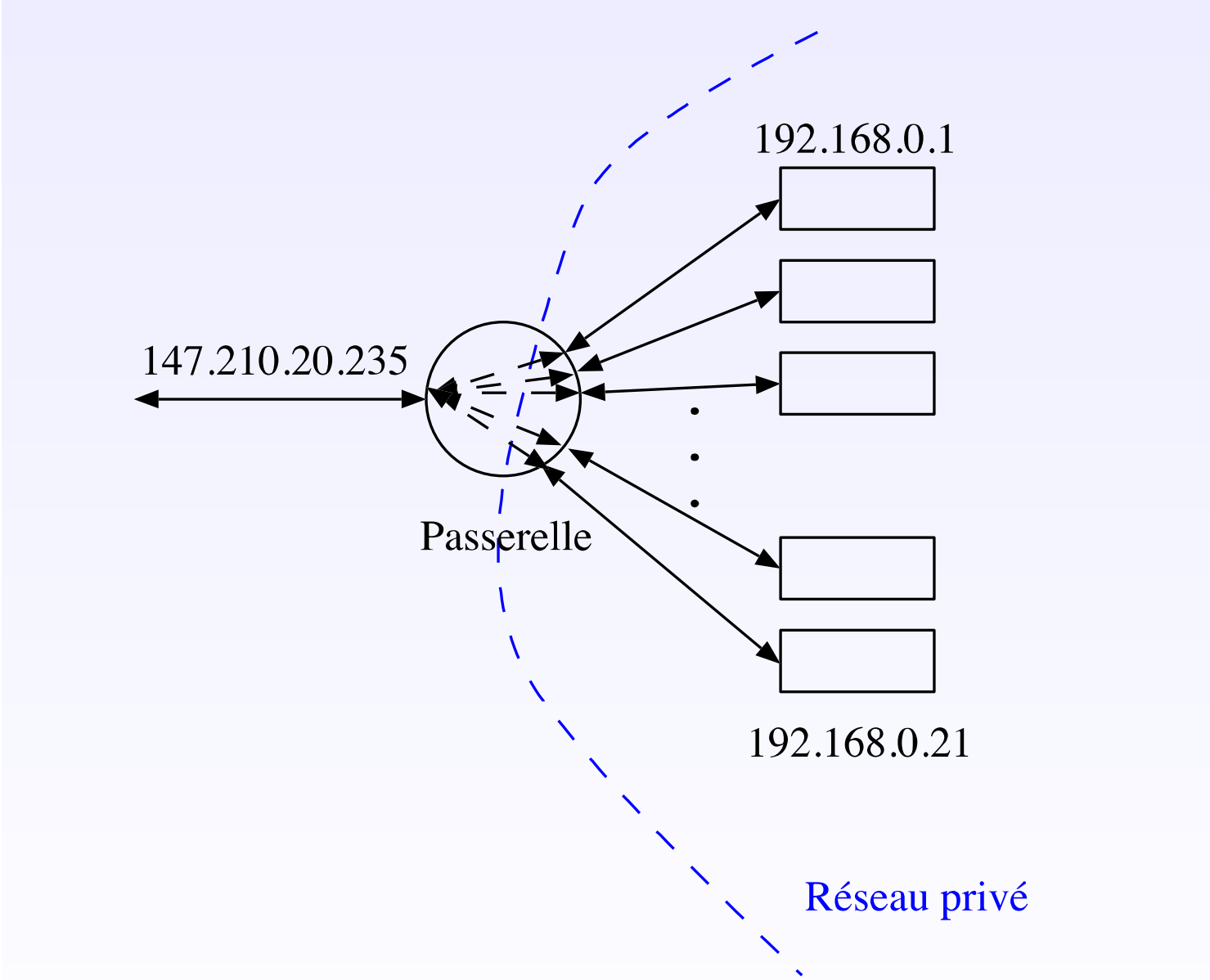
- Appelé aussi **Masquerading**

- 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
  - Augmente la sécurité
    - tous les échanges avec l'extérieur passent par la passerelle NAT

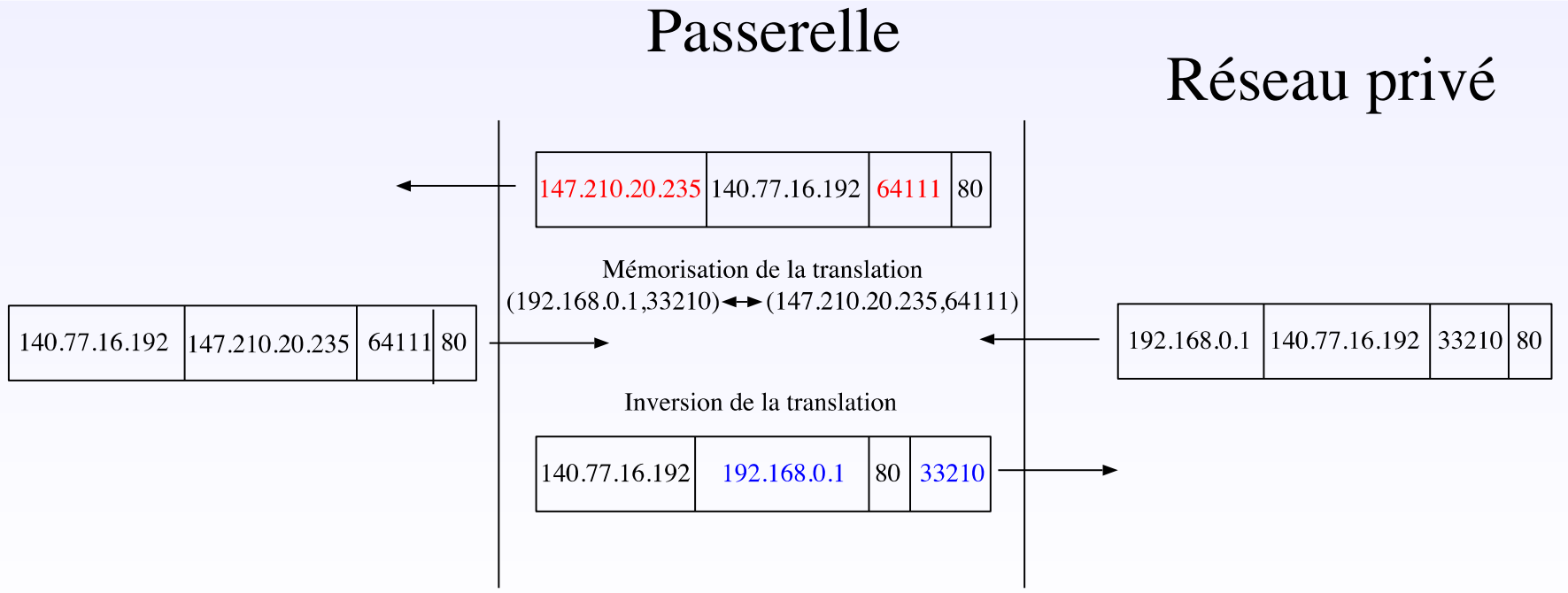
- Inconvénient :
  - Les machines du réseau interne ne sont pas accessibles de l'extérieur (impossibilité d'initier une connexion de l'extérieur)

NAT dynamique (suite)



NAT dynamique (suite)

- 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



- Comment est ce que **la passerelle NAT** fait la différence les paquets qui lui sont destinés et ceux qu'elle doit relayer vers les stations du LAN?

NAT dynamique : principe

- **À chaque nouvelle connexion :**
  - Modifier l'adresse source et le port source : (@source_privée,port_source)!(@publique,port_source_intermediaire)
  - Sauvegarder l'association dans la table NAT
- **Pour chaque paquet entrant :**
  - Chercher une association correspondant au couple (@destination, port_destination)
  - **Si** une association est trouvée dans la table NAT **Alors**
    - Modifier l'adresse de destination et le port de destination
    - Relayer le paquet
  - **Sinon**

    /* Erreur de routage */
  - **Fin du Si**

NAT dynamique : problémes

- Comment faire de la translation d'adresse sur des protocoles applicatifs qui ne sont pas basés sur TCP ou UDP (pas de numéro de port)?
  - Nécessité d'implémenter une méthode spécifique au protocole
  - Dans le cas des protocoles applicatifs dont les données contiennent des données relatives aux adresses IP, il est nécessaire de mettre en place des "proxy" (FTP par exemple).

- Comment rendre joignables des machines du LAN à partir de Internet? (serveur Web par exemple)
  - Nécessité de faire de la redirection de port (port forwarding/mapping).
  - Principe: Toutes les connexions entrantes sur un port donné sont redirigées vers une machine du réseau privé sur un port.

Proxy ou mandataire

- Un proxy est un intermédiaire dans une connexion entre le client et le serveur d'une application
- Un client s'adresse toujours au proxy
  pour contacter le serveur
- Un proxy est spécifique à un type d'application donné (HTTP, FTP, ...)
- Le Proxy peut modifier des informations échangées entre le client et le serveur.