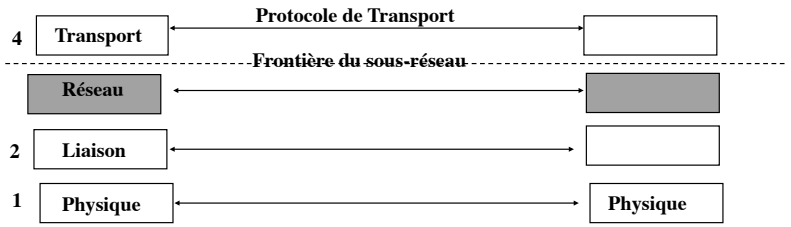
Administration Réseau
Niveau routage

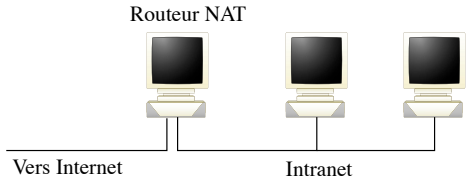


Intérêt du NAT
(Network Address Translation)

- Possibilité d'utilisation d'adresses privées dans l'Intranet
- Tout en rendant possible l'accès à l'extérieur depuis et vers ces machines
- Au départ pour conçu pour économiser des adresses
- Vue de l'extérieur: Plage d'adresse publique
- Sécurité: Rend invisible la configuration d'un Intranet
- Va disparaître avec la généralisation de IPV6

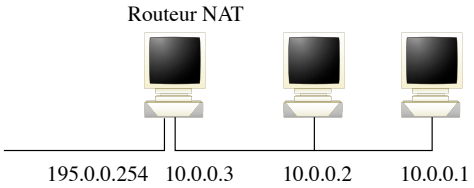
Principe NAT

- On doit administrer un Intranet
- On possède une liste d'adresse publique qui nous a été attribué
- Par exemple: 195.0.0.129/25 à 195.0.0.255/25 (réseau 195.0.0.128/25)
- Il existe sur notre Intranet un routeur de sortie vers l'Internet qui va implémenter la translation d'adresse



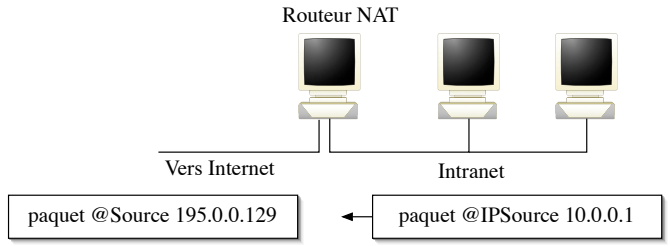
Exemple d'Intranet

- **On donne une adresse privée à chaque machine de l'Intranet**
- Liste des adresses privées
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
    172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
    192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- **Une des adresses publiques à l'interface de sortie du routeur**



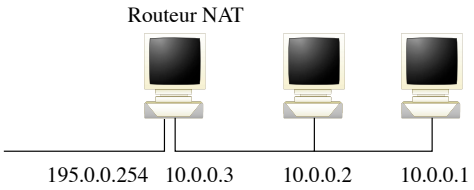
NAT: principe

- Le routeur de sortie va modifier l'entête IP de tout paquet provenant d'une machine interne en remplaçant l'adresse source IP privée par une adresse publique
- Vue de l'extérieur, le routeur se fait passer pour la machine source
- **Deux types de NAT : statique et dynamique**
  - **Statique la correspondance @ Privée / @ publique est fixe**
  - **Dynamique : elle peut changer dans le temps**



NAT STATIQUE: principe

- **Une adresse publique associée à chaque adresse privée**
- **Plage d'adresse publique 195.0.0.248/29**
- **Exemple d'associations Nat:**
  - **10.0.0.1 195.0.0.249**
  - **10.0.0.2 195.0.0.250**



NAT STATIQUE: principe

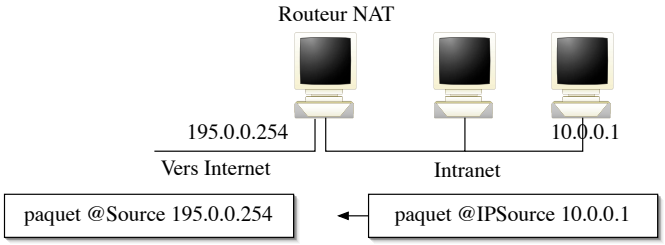
- **Problèmes et configuration du routage**
  - Il faut que le routeur se fasse passer pour l'ensemble des machines d'adresses publiques au niveau des requêtes ARP du premier routeur extérieur
  - Proxy ARP: le routeur NAT met dans sa table ARP son adresse Ethernet pour toutes les adresses publiques
  - Au retour d'un paquet dans le routeur NAT , il faut qu'il redirige le paquet vers la bonne machine de l'Intranet
  - Il doit donc avoir dans sa table de routage
    - » 195.0.0.249 10.0.0.1 (netmask 255.255.255.255)
    - » Pour l'adresse 195.0.0.249 envoyer à 10.0.0.1

Intêret NAT STATIQUE: principe

- Intranet invisible depuis l'extérieur
- Administration en cas de changement de l'Intranet seulement sur routeur
- Economise des adresses en cas de découpage de l'Intranet en sous-réseaux (adresses perdues à cause du découpage)
- Mais on n'économise pas d'adresses publiques
- Pour cela il faut alors faire de la NAT dynamique

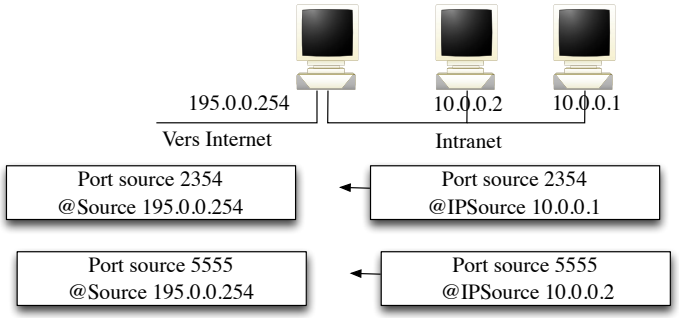
NAT dynamique ou IP masquerading : principe

- Permet d'attribuer dynamiquement lors des connexions des adresses IP publiques aux adresses privées
- L'adresse source des paquets devient l'adresse externe du routeur
- Problème : En cas de plusieurs connexions en parallèle comment le routeur peut il diriger les paquets vers la bonne machine ?



L'association connexion/@privée

- Se fait au moment du premier paquet qui sort en se rappelant le numéro de port source (mémorisation dans une table)

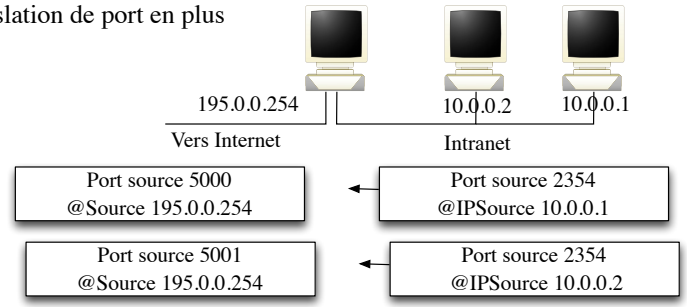


Mémorisation dans la table NAT:

2354 10.0.0.1
5555 10.0.0.2

L'association connexion/@privée

- Problème : si plusieurs connexions avec le même port source en même temps ?
- Attribution d'un port source virtuel unique à chaque connexion
- Translation de port en plus



Mémorisation dans la table NAT:

2354 10.0.0.1 5000
2354 10.0.0.2 5001

Nat Dynamique

- Une seule adresse publique suffit pour un nombre quelconque de machines dans l'Intranet
- On ne peut pas initier une connexion depuis l'extérieur
- Comment avoir un serveur WEB par exemple dans l'Intranet ?

Le *port forwarding*

- **Utiliser dans la NAT dynamique pour rendre une machine accessible depuis l'extérieur**
- **On mets en dur dans la table NAT du routeur**
  - port fixe: port privée/ adresse privée
  - Par exemple **21: 21/10.0.0.1** (port d'un serveur FTP)
  - Les paquets arrivant de l'extérieur vers (**195.0.0.254, 21**) seront redirigés vers (**10.0.0.1, 21**)
  - Problème si deux serveurs FTP sur 2 machines différentes ?
- **Le "*port mapping*" consiste à changer de port sur la machine interne**
  - Par exemple : **80: 8080/10.0.0.1**
  - Un serveur http est lancé sur 10.0.0.1 sur le port 8080

Problèmes NAT Dynamique

- **Applications n'utilisant pas UDP/TCP**
  - Exemple ICMP
  - Il faut faire une configuration spéciale du routeur pour lui dire de se référer à autre chose que le port
  - Le numéro d'identifiant du paquet ICMP par exemple
- **L'application FTP**
  - Rappel en mode actif:
    - » En cas d'une connexion sur un serveur extérieur
    - » La connexion pour les données est initiée depuis le serveur
  - Il ne peut être utilisé qu'en mode passif dans lequel toutes les connexions sont initiées depuis le client
  - Les données de FTP contiennent des informations se rapportant aux adresses IP
  - Plus de problème avec SFTP (une seule connexion initiée par le client)

Problèmes NAT Dynamique

- **Authentification et cryptage:**
  - Pas de mécanisme d'authentification de bout en bout puisque le paquet est modifié
  - Encryptage de l'entête IP à la source et vérification à l'arrivée
  - Possibilité de tunneling (mise en place de Tunnel IPSEC vers l'extérieur)
- **Le routeur a du travail supplémentaire**
  - re calcul des checksums IP TCP et UDP
  - modification des données FTP... (fait par proxy)
  - limitation de la bande passante si le routeur n'est pas assez puissant
- **Argument des opposants au NAT: non indépendance des couches**

Combinaison NAT Statique et Dynamique

- **Statique:**
  - Intéressant si certaines machines de l'Intranet doivent être visibles depuis l'extérieur (serveur WEB ...)
- **Dynamique:**
  - Economie d'adresse
  - Sécurité

Exercice sur NAT (Network Address Translation)

NAT STATIQUE:

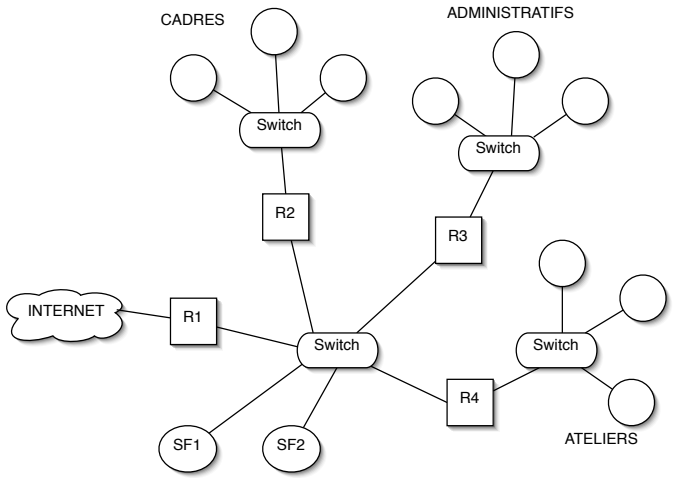
- Donnez un plan d'adressage pour l'Intranet donné dans le transparent suivant avec des adresses privées
- Donnez les tables de routage des routeurs et des machines pour que l'ensemble des machines de l'Intranet puissent communiquer avec l'extérieur (Internet)
- Donnez la table ARP du routeur de sortie

Exercice sur NAT

NAT STATIQUE/DYNAMIQUE:

- On utilise de la NAT dynamique pour l'ensemble des machines de l'Intranet
- On veut mettre sur la machine servant de serveur de fichier SF1 un serveur WEB et un serveur SFTP accessibles depuis l'extérieur
- Combien d'adresse publique est il nécessaire de posséder ?
- Donnez les tables de routage des routeurs et des machines pour que l'ensemble des machines de l'Intranet puissent communiquer avec l'extérieur (Internet)

INTRANET



Exercice sur NAT

NAT STATIQUE/DYNAMIQUE:

- On ne veut pas utiliser de NAT statique
- Comment configurer le routeur de sortie (table NAT) pour que les serveurs WEB et Sftp sur SF1 soient accessibles depuis l'extérieur ?

Exercice sur NAT STATIQUE/DYNAMIQUE

- On utilise de la NAT dynamique pour l'ensemble des machines de Atelier et Administratif
- On veut utiliser de la NAT statique pour les machines "cadres"
- On veut mettre sur la machine servant de serveur de fichier SF1 un serveur WEB et un serveur SFTP accessibles depuis l'extérieur
- Combien d'adresse publique est il nécessaire de posséder ?
- Donnez les tables de routage des routeurs et des machines pour que l'ensemble des machines "cadres" puissent communiquer avec l'extérieur (Internet)
- Peux t-on accéder aux machines administratif et atelier depuis Internet ?
  - Et dans l'autre sens ?

Exercice sur NAT (Network Address Translation)

- NAT STATIQUE/DYNAMIQUE:
- Mettre dans le cas de la configuration précédente les filtres nécessaires sur le routeur de sortie pour que les ateliers et administratif ne puissent pas accéder à l'Internet
- Même question si l'on veut "bloquer" toute communication des cadres avec Internet sauf serveur WEB et serveur ssh ?