La translation d'adresses (NAT/PAT)

Objectifs :

- **Comprendre le fonctionnement du NAT (Network Address Translation) ;**
- **Configurer le NAT sur des routeurs Cisco ;**
- **Diagnostiquer le service NAT.**

1. Rappel :

➢ Rappeler les particularités des adresses IP privées :
- Adresses réservées aux réseaux locaux privés
- Plages :
  - Classe A : 10.0.0.0/8 à 10.255.255.255/8
  - Classe B : 172.16.0.0/12 à 172.31.255.255/12
  - Classe C : 192.168.0.0/16 à 192.168.255.255/16
- Adresses non routables sur le réseau public Internet

➢ Rappeler les particularités des adresses IP publiques :
- Adresses routable sur internet
- Unique
- Gérées par l'IANA, les RIR, registre nationaux, FAI

2. Problématique :

Comment faire communiquer les postes d'un réseau privé avec Internet ?

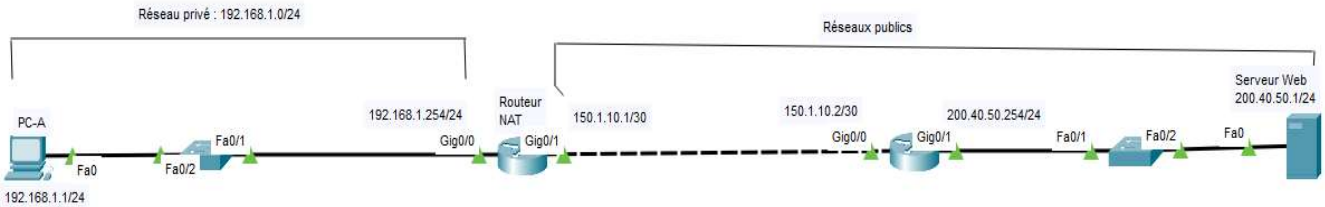
3. Solution :

La technique de **translation d'adresses (NAT)** est apparue à l'origine pour pallier le manque croissant d'adresses IPV4. Elle consiste à utiliser **une ou quelques adresses IP publiques** pour permettre à tous les postes d'un réseau local (LAN) de communiquer avec l'extérieur (Internet et/ou autres réseaux).
- La translation (NAT) se fait au niveau des **routeurs** (passerelles) qui font le lien entre le réseau local (LAN) et Internet.
- La translation est effectuée pour les **paquets sortants** et **rentrants**.
- La translation permet la **modification** de **l'adresse IP source** (en mettant l'adresse IP publique à la place de l'adresse IP privée pour les paquets sortants).

Remarque : Toutes les Box Internet gèrent la fonction du NAT.

4. Illustration :

Sur cette maquette, le réseau privé (LAN) est à gauche. Il a l'adresse IP privée 192.168.1.0/24.
Internet (le réseau public) est à droite du routeur NAT.



IP source : 192.168.1.1	IP destination : 200.40.50.1	➔➔	IP source : 150.1.10.1	IP destination : 200.40.50.1

Explications :

- Paquets **sortants** (du LAN vers Internet) : Le routeur NAT modifie **l'adresse IP source privée** en mettant l'adresse **publique** de son interface externe.
- Paquets entrants (d'Internet vers le LAN) : Le routeur NAT **modifie** l'adresse IP destination en mettant **l'adresse privée** du poste émetteur.

5. Différents types du NAT :

a. **Le NAT statique** (à une IP privée correspond une IP publique). Pour un accès permanent à une ressource sur un réseau privé depuis Internet. Utilisé pour un serveur web s'il est contraint d'être placé sur un réseau privé. Annule le bénéfice des IP privées car ne diminue pas le besoin en IP publiques.
b. **Le NAT dynamique avec pool d'adresses** (à N IP privées correspondent X IP publiques avec X ≤ N).
c. **Le NAT dynamique avec surcharge** = NAT overload = PAT (à N IP privées correspond une seule IP publique). C'est celui utilisé par les Box Internet grand public.

6. La table NAT :

Les routeurs NAT gèrent **une table NAT** pour mémoriser les adresses translatées.

IP source	IP modifiée
192.168.1.1	150.1.10.1
192.168.1.2	150.1.10.1
192.168.1.1	150.1.10.1

Problématique, la table NAT ci-dessus n'est pas suffisante pour assurer l'unicité des couples adresses privée/publique.

7. La translation de port (PAT)

Le NAT dynamique utilise la translation de port (Port Address Translation : PAT) ;
Le PAT consiste à affecter un **port source différent** à chaque requête. Cela permet de maintenir une correspondance entre les requêtes sortantes et les réponses provenant de l'extérieur.

8. La table NAT/PAT :

Les routeurs NAT gèrent **une table NAT/PAT** pour mémoriser les adresses et les ports translatées.

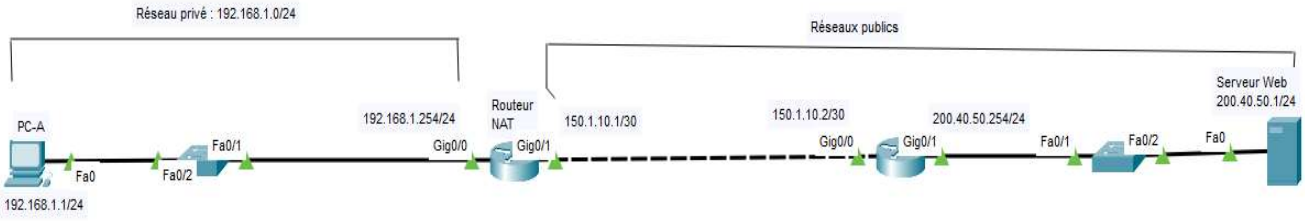
IP : port source	IP : port modifiés
192.168.1.1 :24000	150.1.10.1 :15000
192.168.1.2 :24600	150.1.10.1 :15001
192.168.1.1 :22000	150.1.10.1 :15002

9. Avantages du NAT :

- Economie des adresses IP publiques ;
- **Sécurité** : le NAT masque les adresses IP privées. L'adressage privé est **masqué** (caché) par le routeur NAT.

10. Mise en place du NAT dynamique sur un routeur Cisco :

a. Réaliser la maquette suivante :



b. Configurer les postes et les interfaces des routeurs.
c. Configurer le routage statique sur les routeurs.
d. Définir les interfaces pour le NAT entrant et sortant.

Router(config)#`interface` *`nom_interface`*	*#interface interne (côté LAN)*
Router(config-if)#`ip nat inside`	
Router(config)# **`interface nom_interface`**	*#interface externe (côté WAN)*
Router(config-if)#`ip nat outside`	

e. Configuration de la liste d'accès (ACL)

Une liste d'accès ou Access Control List (ACL) **permet de filtrer les paquets IP au niveau 3** du modèle OSI.
Ainsi, une ACL va indiquer au routeur les paquets qu'il doit accepter et ceux qu'il doit refuser, notamment en fonction de **leur adresse IP de provenance, leur IP destination et les ports source et destination**.

Le masque générique : les ACL utilisent des masques appelés « masques génériques ».

Un masque générique est l'inverse du masque classique.

Exemple : calculer le masque générique correspondant au masque normal 255.0.0.0

Exemple : création de la liste d'accès n° 10 autorisant les paquets du réseau 10.0.0.0/8 à traverser le routeur

Router(config)#access-list n°liste permit @réseau ***masque_générique***

Remarque : Le masque générique est l'inverse du masque classique.

✓ **Calculer le masque générique correspondant au masque 255.255.255.0**

0.0.0.255

✓ **Crée la liste d'accès (ACL) adaptée à votre contexte**

Router(config)#

f. Configuration du NAT dynamique

Router(config)#**ip nat** inside source list n°liste interface *nom-interface-externe* **overload**

✓ **Adapter la commande ci-dessus à votre contexte.**

g. Vérifier le bon fonctionnement de NAT

Réaliser plusieurs ping entre PC-A et le serveur Web puis, taper la commande suivante :

#show ip nat translation

Réaliser une copie d'écran et commenter le résultat :

Activer le mode « debug » et réaliser un ping entre PC-A et le serveur Web :

#debug ip nat

Réaliser une copie d'écran et commenter le résultat :

h. Analyser le contenu des trames en réalisant des copies d'écrans et les commentant

La requête du PC-A vers le serveur Web :

- Au niveau du PC-A :
- A l'arrivée sur le routeur NAT :
- En sortie du routeur NAT :
- A l'arrivée sur le serveur Web :

La réponse du serveur Web :

- Au niveau du serveur Web :
- A l'arrivée sur le routeur NAT :
- En sortie du routeur NAT :
- A l'arrivée sur le PC-A :