



Service NAT Network Address Translation

BTS – SN 2

1h

Comment un ordinateur local (adresse privée) peut-il communiquer avec un serveur (adresse publique) sur Internet ?

1 – Historique

Pour économiser quelques adresses IPv4, on a créé les adresses privées utilisables sur les réseaux privés d'entreprises. Cela a permis d'économiser un grand nombre d'adresses publiques.

Préfixe (adresses privées) :

- 10.0.0.0 / 8
- 172.16.0.0 / 12
- 192.168.0.0 / 16

Si toutes les entreprises utilisent des adresses privées → Il y a forcément plusieurs ordinateurs d'entreprises différentes qui ont la même adresse.

→ Ils ne peuvent pas communiquer directement entre-eux puisqu'ils ont la même adresse.

Solution : il faut "filtrer et modifier" les adresses IP privées

- ⇒ On remplace l'adresse privée par une adresse publique
- ⇒ Cette opération se nomme "Translation NAT". Elle est effectuée par le service NAT au niveau du routeur

2 – Types de services NAT

- Service NAT Statique

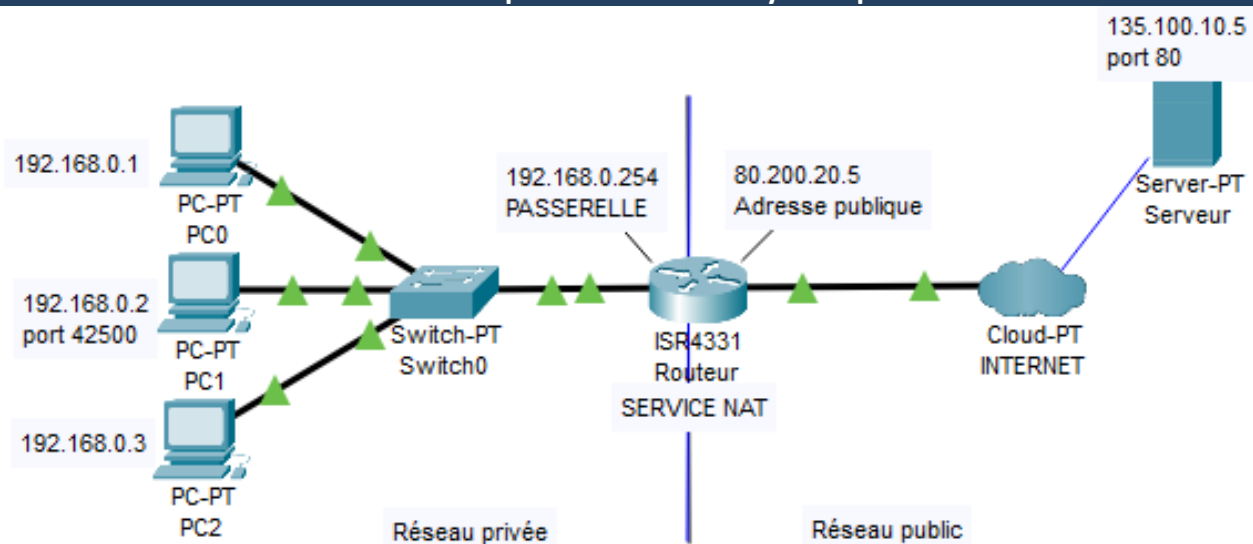
Le service NAT assure la translation d'adresse privée → publique. On dispose du même nombre d'adresses privées que d'adresses publiques.

== > Très peu utilisé

- Service NAT Dynamique

On dispose de beaucoup moins d'adresses publiques que d'adresses privées. Une adresse publique est utilisée pour gérer plusieurs adresses privées. Pour différencier les machines on utilise les ports et on tient à jour une table NAT au niveau du serveur NAT.

3 – Principe du service NAT dynamique



On désire établir une connexion entre PC1 et le site web 135.100.10.5

Cette communication s'effectuera en deux étapes : communication entre PC1 et le routeur (Service) NAT puis entre le routeur et le serveur.

Etape 1 : Communication entre PC1 et le routeur

@MAC Dest Passerelle	@MAC Source PC1	@IP source 192.168.0.2	@IP destination 135.100.10.5	Port Source 42500	Port Destination 80
--------------------------------	---------------------------	----------------------------------	--	-----------------------------	-------------------------------

Etape 2 : Communication entre le routeur et le serveur

@MAC Dest MAC du prochain routeur	@MAC Source MAC routeur coté public	@IP source 80.200.20.5	@IP destination 135.100.10.5	Port Source 42500	Port Destination 80
---	---	----------------------------------	--	-----------------------------	-------------------------------

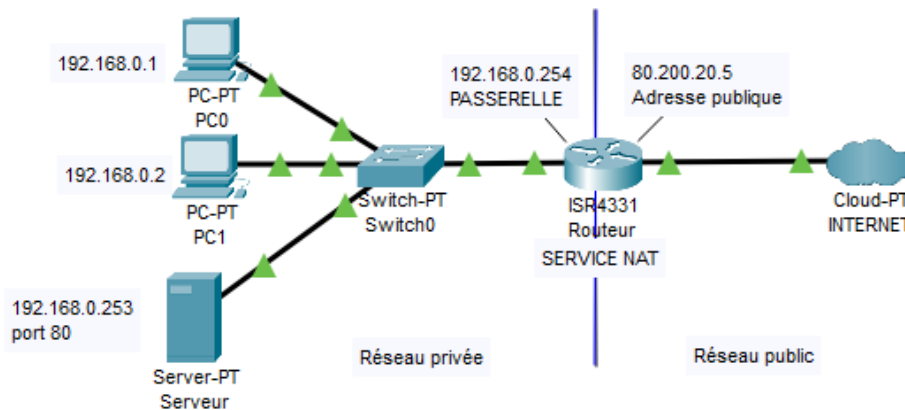
Comment le routeur fait-il pour rediriger la réponse du serveur vers le bon poste (PC1) ?
 ⇒ Il utilise une table NAT pour mémoriser les adresses IP et les ports utilisés.

Table NAT	
Infos réseau local	Info réseau public
@IP Source / @IP Dest Port Source / Port Dest	@IP Source / @IP Dest Port Source / Port Dest
192.168.0.2 / 135.100.10.5 42500 / 80	80.200.20.5 / 135.100.10.5 42500 / 80

4 – Le port Forwarding (ou PAT)

Le routeur NAT permet à un élément du réseau privé de communiquer avec le réseau public **ET** bloque toutes demandes de l'extérieur (du réseau public vers le réseau privé).

- ⇒ C'est un avantage d'un point de vue sécurité ... sauf si on héberge un serveur sur notre réseau interne.
- ⇒ Il n'est pas accessible depuis le réseau public.
- ⇒ **Solution : le port FORWARDING.**



Exemple de table FORWARDING

@ IP externe routeur (@IP publique)	Port externe routeur	@IP interne (@IP serveur)	Port interne (Serveur)
80.200.20.5	80	192.168.0.253	80

5 – TD

En tant qu'administrateur réseau, vous devez mettre en place le réseau de votre entreprise. Proposez une solution de routage NAT avec Port Forwarding.

Votre réseau : @IP 10.0.0.0 / 23

5 serveurs SSH (port TCP 22)	@IP 10.0.1.1 → 10.0.1.5
4 serveurs Web (port TCP 80)	@IP 10.0.1.6 → 10.0.1.9
2 serveurs DNS (port UDP 53)	@IP 10.0.1.11 → 10.0.1.12
Il y a 200 salariés environ	@IP 10.0.1.20 → 10.0.1.250

Vous avez acheté une plage d'adresse sur internet : 194.34.56.0 / 29.