Traduction d'adresses réseau NAT

(Network Address Translation)

- @IP privées
- Les services
- NAT statique
- NAT dynamique
- NAT surchargé (PAT) /traduction de port
- Réacheminement de port (Port Forwarding)

Pr. Ibrahimi, FSK

Les adresses IP privées

- Adresse IP ? @IPv4 en 32 bits. Le nombre d'dresses IP possibles est 2^{32} = 4 milliards valeurs.
- Aujourd'hui cette valeurs est insuffisante. On parle l'épuisement de cet espace d'adressage. Un nouveau protocole d'adresse IP pour le futur (IPv6)
- Certains valeurs /@IP ne seront pas visibles sur Internet (non routable, le routeur détruit le paquet). Elles s'appellent des adresses IP privées.
- Les adresses IP visibles sur Internet (routable, le routeur le réachemine vers un autre routeur) s'appellent des adresses IP publiques.
- Les @IP privées de chaque classe:
  - Classe A: 10.0.0.0/8 (10.0.0.0 à 10.255.255.255)
  - Classe B: 172.16.0.0/12 (172.16.0.0 à 172.31.255. 255)
  - Classe C: 192.168.0.0/16 (192.168.0.0 à 192.168.255.255)
- Les adresses IP privées seront utilisées en privé au sein d'un réseau local (LAN/WLAN).
- Problème: Les équipements du LAN ne peuvent pas se connecter à l'Internet.
- Solution: Traduction des @IP privées par d'autres @IP publiques.
- Type de traduction: statique, dynamique.

Les adresses IP privées

- NAT statique: traduire une adresse IP privée par une adresse IP publique de manière fixe.
- Besoin d'une plage d'adresses IP publiques (p). Dans ce cas, on peut associer uniquement p @Ip privées.

- Dans le LAN, si vous avez n machines, alors si n = p ou n<p, pas de problèmes. Si n>p, certains machines p+1, ⋯, n ne seront pas capable de sortir vers l'internet (problème).

- Solution: l'utilisation de la traduction dynamique.

- NAT dynamique: partage du même pool d'adresses p entre toutes les @IP privées en fonction de la demande des équipements qui souhaitent accéder à l'Internet. Supposons que n>p machines demandent l'accès à l'Internet, on a pas d'adresses libres (problème- surcharge (overload)).
- Solution: utilisation de traduction de ports (PAT port address translation).

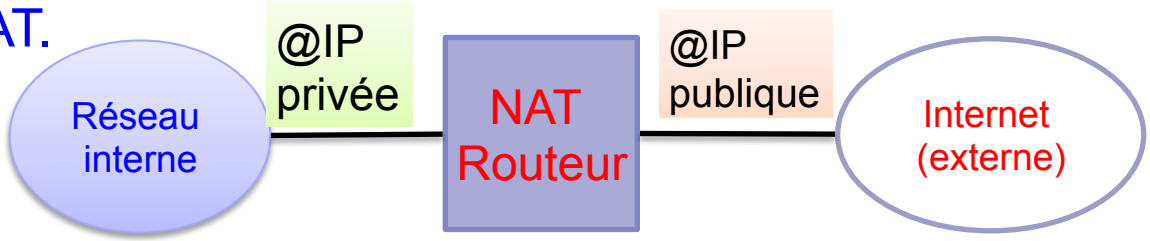
NAT

- NAT à l'envoi:
  - NAT reçoit un paquet d'une machine avec une @IP privée.
  - Il consulte sa table et trouve une @IP publique libre.
  - Il modifie le paquet reçu en modifiant @IP privée par @IP publique libre.
  - Ensuite, il envoie le paquet vers le serveur externe.

- NAT à la réception du réponse du serveur:
  - NAT reçoit un paquet du serveur.
  - Il consulte sa table et trouve une @IP publique associée.
  - Il modifie le paquet reçu en modifiant @IP publique par @IP privée de la machine concernée.
  - Ensuite, il envoie le paquet vers la machine.

NAT statique: exemple

- NAT statique: traduire une adresse IP privée par une adresse IP publique de manière fixe.
- @IP publique: 20.20.20.1, 20.20.20.2
- @IP privées : 10.0.0.1, 10.0.0.2, 10.0.0.3
- Serveur Web distant: 212.212.100.1
- Table NAT.

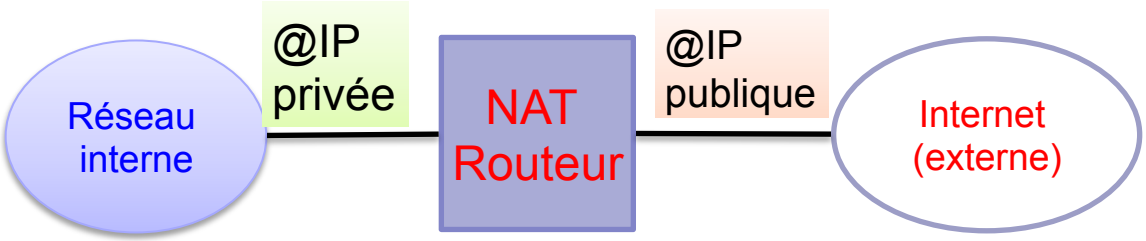


Interne		Externe	
@IP source	@IP destination	@IP source	@IP destination
10.0.0.1	212.212.100.1	20.20.20.1 (fixe)	212.212.100.1
10.0.0.2	212.212.100.1	20.20.20.2 (fixe)	212.212.100.1
10.0.0.3	212.212.100.1	Pas d'adresse	

NAT dynamique: exemple

NAT routeur possède un pool d'adresses publiques (p =2)

- @IP publique: 20.20.20.1, 20.20.20.2
- @IP privées : 10.0.0.1, 10.0.0.2, 10.0.0.3
- Serveur Web distant: 212.212.100.1
- Table NAT.

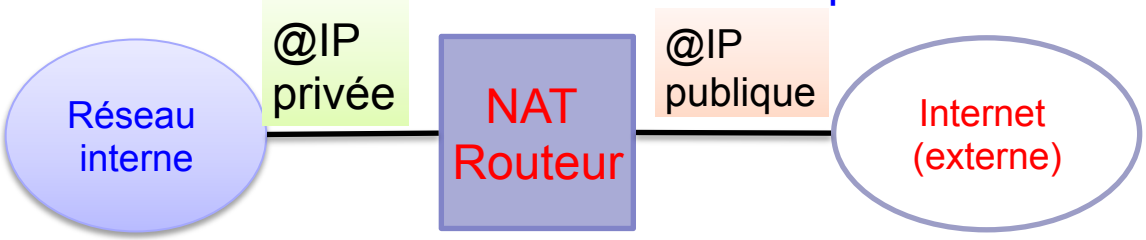


Interne		Externe	
@IP source	@IP destination	@IP source	@IP destination
10.0.0.1	212.212.100.1	20.20.20.2 (dynamique)	212.212.100.1
10.0.0.2	212.212.100.1	20.20.20.1 (dynamique)	212.212.100.1
10.0.0.3	212.212.100.1	Pas d'adresse (attend la libération des adresses)	

NAT dynamique (PAT): exemple

NAT routeur possède un pool d'adresses publiques (p =2)

- @IP publique: 20.20.20.1, 20.20.20.2
- @IP privées : 10.0.0.1, 10.0.0.2, 10.0.0.3 et des numéros de ports aléatoires > 1024.
- Serveur Web distant: 212.212.100.1
- Table NAT va être modifier aves les numéros de ports.

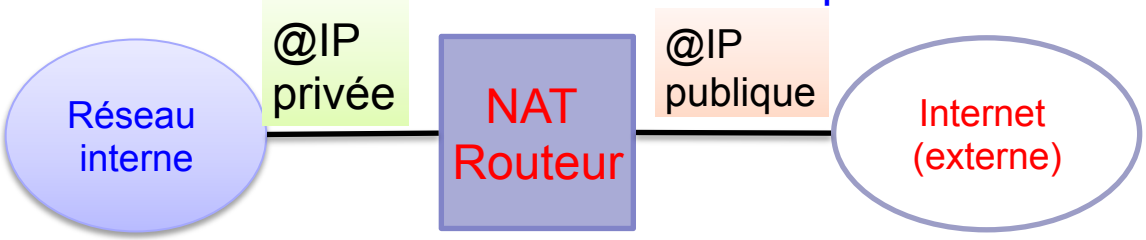


Interne				**Externe**			
@IP source	N° Port SRC	@IP destination	N° Port Des	@IP source	N°Port SRC	@IP destination	N°Port Des
10.0.0.1	1025	212.212.100.1	80	20.20.20.2	1025	212.212.100.1	80
10.0.0.2	1026	212.212.100.1	80	20.20.20.1	1026	212.212.100.1	80
10.0.0.3	1027	212.212.100.1	80	20.20.20.1	1027	212.212.100.1	80

NAT dynamique (PAT): exemple

NAT routeur possède un pool d'adresses publiques (p =2)

- @IP publique: 20.20.20.1, 20.20.20.2
- @IP privées : 10.0.0.1, 10.0.0.2, 10.0.0.3 et des numéros de ports aléatoires > 1024 identiques 1025.
- Serveur Web distant: 212.212.100.1
- Table PAT va être modifier aves les numéros de ports.

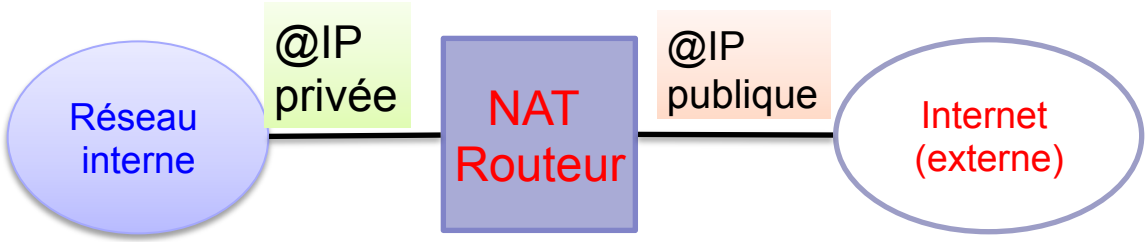


Interne				Externe			
@IP source	N° Port SRC	@IP destination	N° Port Des	@IP source	N°Port SRC	@IP destination	N°Port Des
10.0.0.1	1025	212.212.100.1	80	20.20.20.2	1025	212.212.100.1	80
10.0.0.2	1025	212.212.100.1	80	20.20.20.1	1025	212.212.100.1	80
10.0.0.3	1025	212.212.100.1	80	20.20.20.1	1025	212.212.100.1	80

Des paquets vont quitter le routeur avec même adresse et même port. À la réception d'une réponse, on ne peut pas différencier les machines.

NAT dynamique (PAT): exemple

NAT routeur traduire également les numéros de ports associés aux adresses privées par d'autres valeurs. On évite les mêmes numéros de ports.



Interne				**Externe**			
@IP source	N° Port SRC	@IP destination	N° Port Des	@IP source	N°Port SRC	@IP destination	N°Port Des
10.0.0.1	1025	212.212.100.1	80	20.20.20.2	1225	212.212.100.1	80
10.0.0.2	1025	212.212.100.1	80	20.20.20.1	1226	212.212.100.1	80
10.0.0.3	1025	212.212.100.1	80	20.20.20.1	1227	212.212.100.1	80

Tout le monde peut sortir à l'Internet en même temps.

Accès aux ressources du LAN

La connexion vient la première fois de l'externe vers le serveur web du LAN.
Serveur web 10.0.0.2 (80).
NAT utilise la réacheminement des ports.

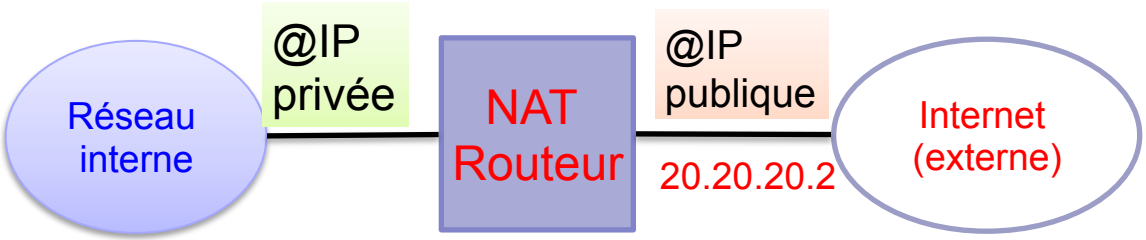


Table port forwarding:

Externe		Interne	
@IP source	N° Port SRC	@IP destination	N° Port Des
20.20.20.2	80	10.0.0.1	80
20.20.20.2	21	10.0.0.1	21

Les services du LAN:
FTP (21), Telnet (23), SMTP (25), POP3 (110), HTTP (80).

Configuration NAT

- Routeur a deux interface :
  - Interface interne: Fa0/0

    R(config-if)# ip nat inside
  - Interface externe: Serial2/0

    R(config-if)# ip nat outside
- NAT statique:
  - R(config)#ip nat inside source static 10.0.0.1 20.20.20.1
  - R(config)#ip nat inside source static 10.0.0.2 20.20.20.2
  - Vérification:
  - R#show ip nat translations/ip debug paquet
- NAT dynamique: (créer un pool nommé LAN10)
  - R(config)#ip nat pool LAN10 20.20.20.1 20.20.20.4 netmask 255.0.0.0
  - Quelles sont les machines du LAN10 qui vont translater?
  - On doit définir une manière de filtrer les machines du LAN, ACL.
  - R(config)#access-list 1 deny 10.0.0.3 (client) (règle 1)
  - R(config)#access-list 1 10.0.0.3 permit 10.0.0.0 0.255.255.255 (les autres) (règle 2)
  - R(config)#ip nat inside source list 1 pool LAN10

Configuration NAT

- PAT dynamique: R(config)#ip nat inside source list 1 pool LAN10 overload

- Pour supprimer le NAT statique:

R(config)#no ip nat inside source static 10.0.0.1 20.20.20.1

- Pour supprimer le pool:

R(config)#no ip nat pool LAN10

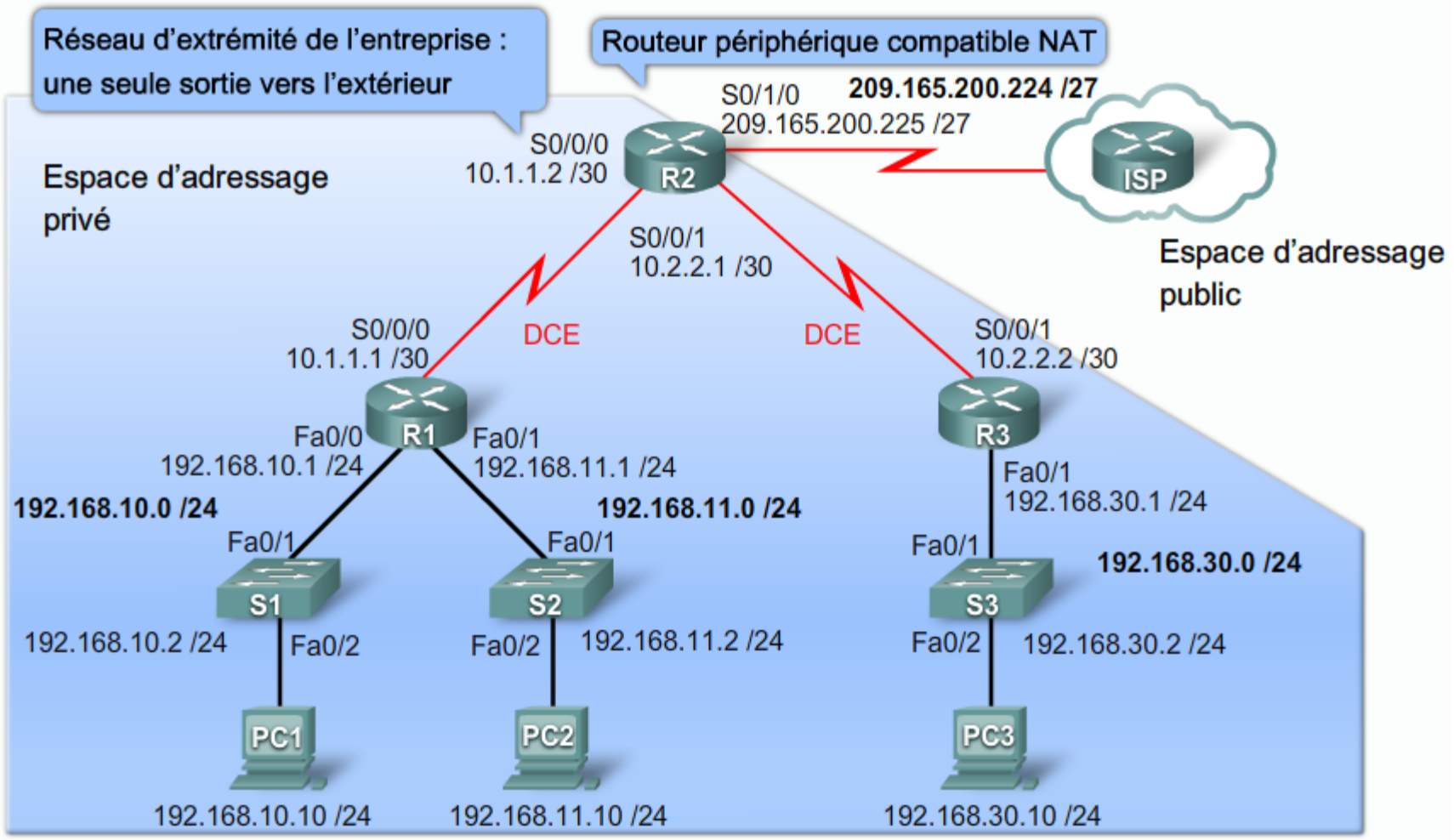
- Pour supprimer la liste:

R(config)#no access-list 1

- Pour supprimer la source dynamique:

R(config)#no ip nat inside source

La fonction NAT traduit les adresses privées en adresses publiques



Surcharge NAT

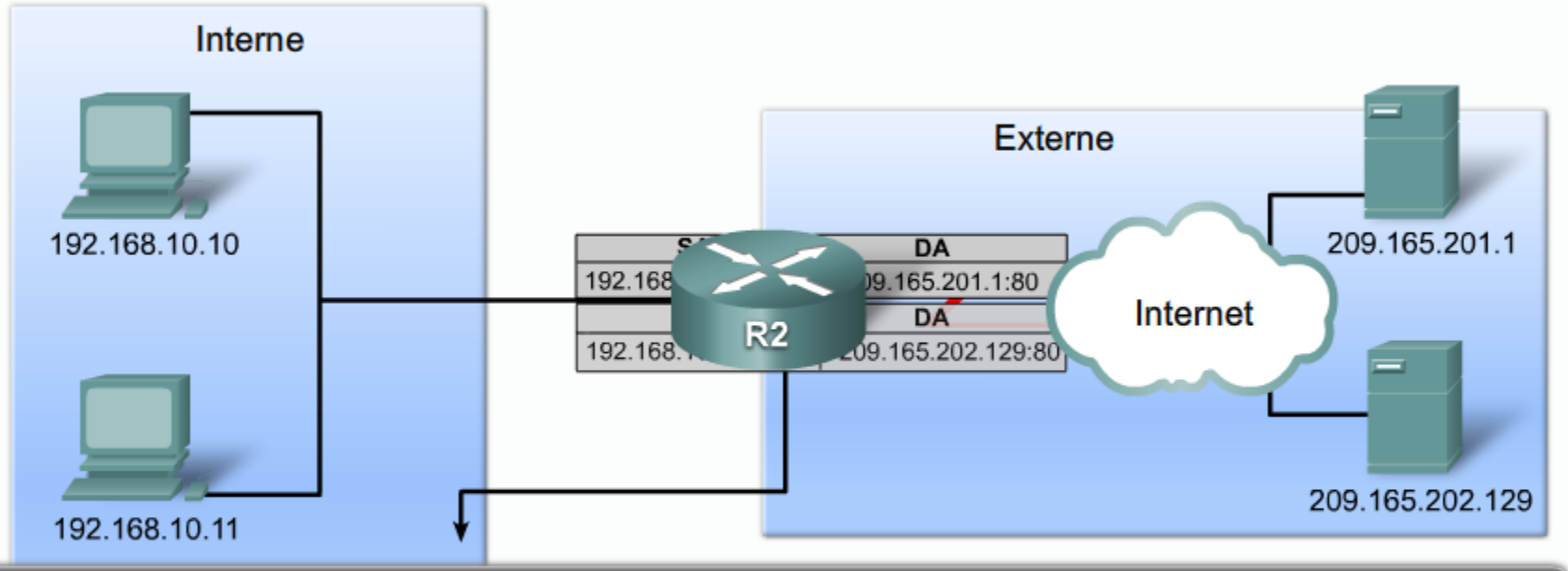


Table NAT avec surcharge			
Adresse IP locale interne	Adresse IP globale interne	Adresse IP globale externe	Adresse IP locale externe
192.168.10.10:1555 192.168.10.11:1331	209.165.200.226:1555 209.165.200.226:1331	209.165.201.1:80 209.165.202.129:80	209.165.201.1:80 209.165.202.129:80

La surcharge NAT (parfois appelée traduction d'adresses de port ou PAT) mappe plusieurs adresses IP privées à une seule adresse IP publique ou à quelques adresses. C'est ce que font la plupart des routeurs personnels. Votre FAI attribue une adresse à votre routeur et pourtant, plusieurs membres de votre famille peuvent surfer simultanément sur Internet.