
RÉSEAU ET PROTOCOLE NETWORK ADDRESS TRANSLATION

Problème d'IP

- Les adresses IP publiques sont rares
 - Une classe C pour utiliser uniquement 10 adresses...
 - trop coûteux
 - Difficile d'obtenir une classe
 - Solution :
 - utiliser des adresses privées en interne
 - L'IETF à réservé trois plages d'adresse à cet égard:
 - 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
 - utiliser des adresses publiques en externe
 - cacher les X postes avec une seule adresse IP

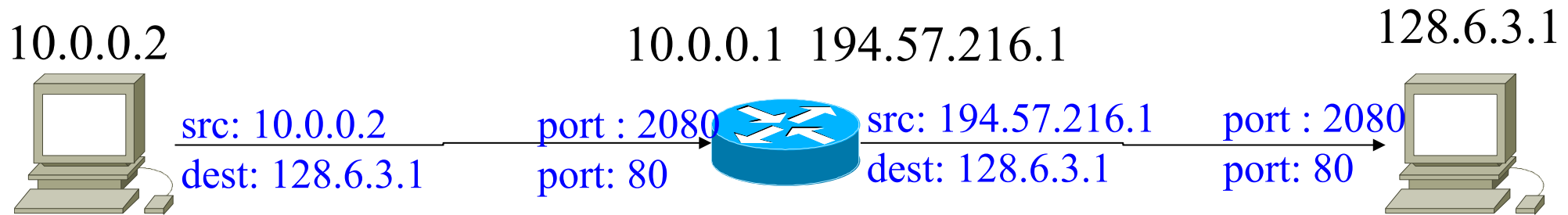
Fonctionnement

- Utiliser des adresses privées dans le réseau interne
- Utiliser une/des adresses publiques pour communiquer avec Internet
- Quand un paquet sort du réseau privé:
 - remplacer son adresse source par une adresse publique
- Quand un paquet arrive d'Internet
 - remplacer la destination publique par une adresse privée
- utilisation d'une table de translation
 - adresse publique / adresse privée

NAT Dynamique

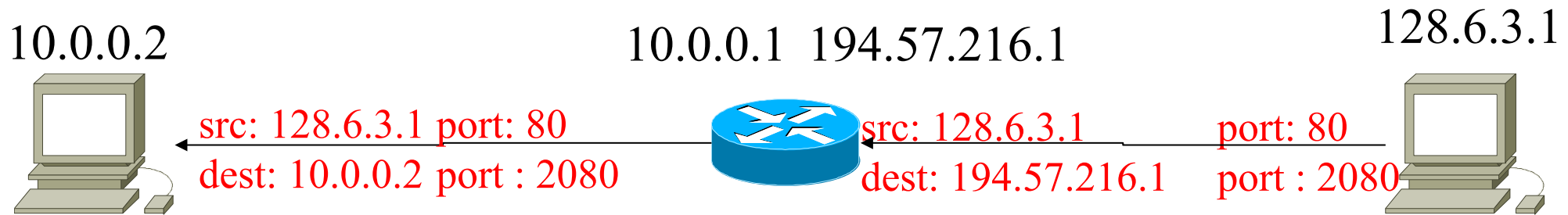
- Initialement
 - Quand un paquet sort,
 - remplacer l'adresse source par une adresse publique
 - noter les adresses et ports source et destination internes et externes
 - Quand une réponse à un paquet arrive depuis Internet
 - chercher la source externe qui correspond à la destination du paquet
 - remplacer la destination par la source interne

NAT Dynamique



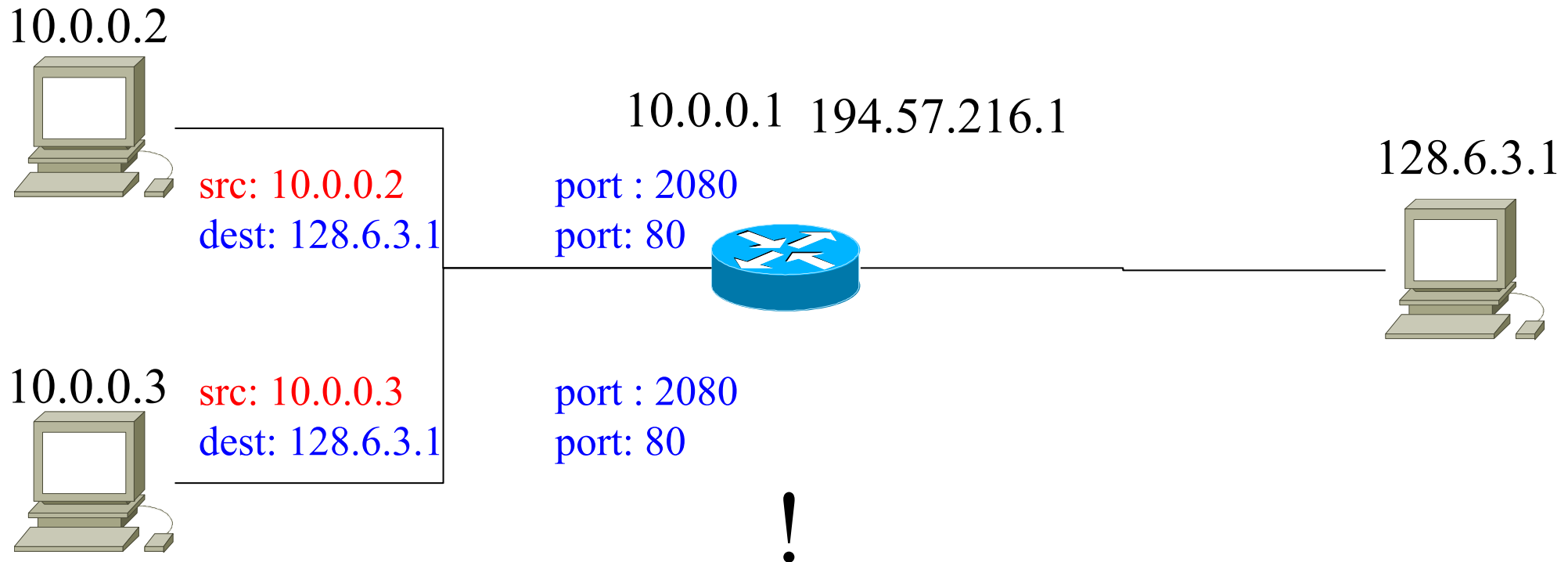
Interne				Externe			
Source		Destination		Source		Destination	
@	Port	@	Port	@	Port	@	Port
10.0.0.2	2080	128.6.3.1	80	194.57.216.1	2080	128.6.3.1	80

NAT Dynamique



Interne				Externe			
Source		Destination		Source		Destination	
@	Port	@	Port	@	Port	@	Port
10.0.0.2	2080	128.6.3.1	80	194.57.216.1	2080	128.6.3.1	80

NAT Dynamique



Interne				Externe			
Source		Destination		Source		Destination	
@	Port	@	Port	@	Port	@	Port
10.0.0.2	2080	128.6.3.1	80	194.57.216.1	4000	128.6.3.1	80
10.0.0.3	2080	128.6.3.1	80	194.57.216.1	5000	128.6.3.1	80

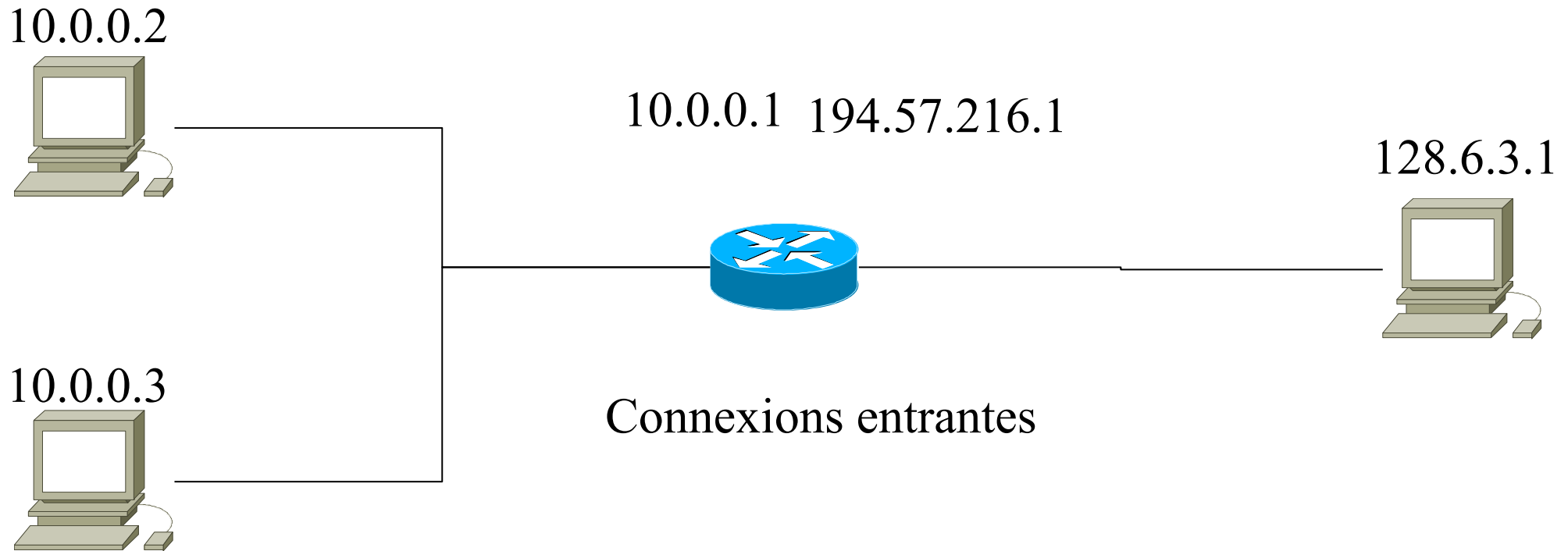
NAT Dynamique

- 2 connexions sont différentes par @/port
 - → collision
 - Solution :
 - utiliser un pool d'adresses publiques
 - changer le port source (Port and Adresse Translation PAT)
- NAT dynamique
 - Pas l'établissement de connexions entrantes
 - bonne protection par défaut
 - Traduire des adresses internes en adresses externes
 - Table construite dynamiquement

NAT Statique

- Permettre des connexions entrantes
 - Définir des entrées statiques dans la table de translation
 - Une entrée par protocole (SMTP, HTTP, ...)
 - Les différents ports d'une même adresse externe peuvent aboutir sur différentes adresses internes

NAT Statique



Interne				Externe			
Source		Destination		Source		Destination	
@	Port	@	Port	@	Port	@	Port
		10.0.0.2	8080			194.57.216.1	80
		10.0.0.3	25			194.57.216.1	25

Inconvénients/Avantages

- Inconvénients

- protocoles échangeant les IP/port dans les data
 - besoin de
 - modifier les données (changer l'adresse/port dans les données)
 - connaître le protocole
 - Exemples : FTP, RealAudio, Quake3, X windows
 - protocoles ne supportant pas de modifications des paquets : IPSec

- Avantages

- Moins d'adresses publiques, coûts limités
 - Facilité pour changer de fournisseur d'accès
 - Facilité pour organiser le réseau interne
- Effet automatique de protection (cf NAT statique)
- Dissimule la structure interne du réseau