Master d'Informatique – 1ère année

Réseaux et protocoles

Adresses privées et NAPT - NAT

Bureau S3-354
mailto://Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M1/rezo

Adresses privées (1)

Les techniques IP peuvent s'utiliser dans un réseau privé. Seul problème : quelles adresses choisir ? (pas d'autorité pour les attribuer).
Si le réseau reste privé, toutes adresses conviennent, mais :
Si le réseau se raccorde, soit à Internet, soit à d'autres réseaux privés (fusion d'entreprises) il y a risque de conflit d'adresses.

Adresses privées (2)

L'IETF a défini des plages d'adresses privées (donc distribuées à aucun organisme, mais pouvant être utilisés par tous en interne).
Résout le pb de raccordement ultérieur à Internet, en ajoutant des adresses publiques là ou c'est nécessaire.
Autorise des réseaux mixtes privés : publics.
Économise les adresses IP

Adresses privées (3)

Plages d'adresses privées :
10.0.0.0 /8 (1 classe A)
172.16.0.0 /12 (16 classes B)
192.168.0.0 /16 (256 classes C)

Ces adresses sont bloquées par tous les routeurs "publics" (i.e. fournisseurs d'accès Internet).
Au pire, un dg avec une telle ad source pourrait arriver à destination, mais jamais la réponse.

Traduction d'adresse (1)

À cause du manque d'adresses v4, les adresses privées sont utilisées aussi sur des postes devant avoir un accès à l'Internet.
=> nécessité de traduire l'adresse (privée) en une adresse publique (en général, la même pour toutes les machines de l'entreprise).
Problème : la réponse parvenant à cette adresse publique, comment la transmettre à la machine d'origine de la requête ?

Traduction d'adresse (2)

Une requête (en général UDP ou TCP) provient de la machine d'ad privée A, port utilisateur P.
La machine traductrice remplace A par son adresse publique, mais peut-elle utiliser le même numéro de port ?
Oui s'il est libre sur la machine traductrice, mais non en général.
= > nécessité de traduction d'adresse et de port.

Traduction d'adresse (3)

La machine traductrice mémorise la correspondance entre adresse privée du demandeur et no de port alloué par elle à cette demande.
=> la réponse parvenant à ce no de port sera redirigée vers la machine initiale (et sur le no de port choisi par cette dernière).
OK pour applis clientes, mais serveurs ?

Traduction d'adresse (4)

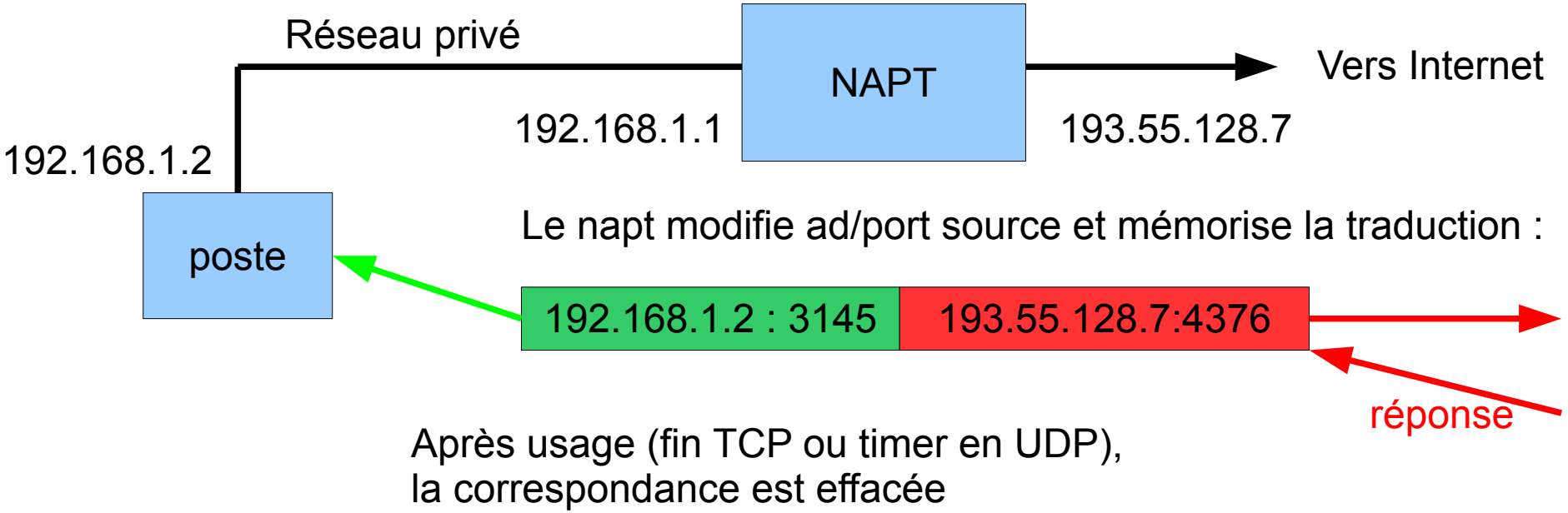
Pour les serveurs situés dans un espace d'adresses privé, mais susceptibles d'avoir un accès public :
Le port "bien connu" (ex 80) de la machine traductrice est ré-aiguillé de manière permanente vers le même port du serveur interne, d'adresse privée.
=> un seul serveur de ce type dans le réseau privé.

Traduction d'adresse (5)

La traduction d'adresses (NAT ou NAPT) pose des problèmes :

- applis nécessitant un port déterminé côté client
- (applis "peer-to-peer" notamment)
- ne résout pas complètement le manque d'adresses (1 seul serveur public de port donné dans le réseau privé)
- entraîne souvent une confusion entre NAT/NAPT et firewall

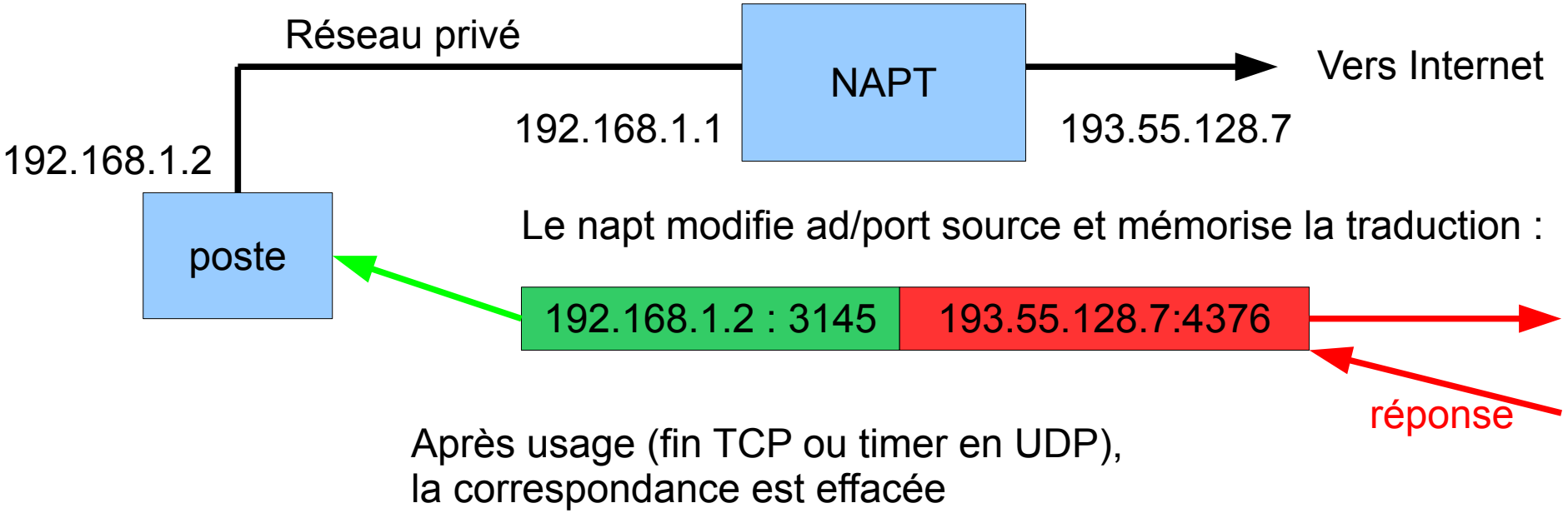
Mécanisme de traduction (1)



Transmission au routeur par défaut : 192.168.1.1

Requête du poste : ad source 192.168.1.2, port source 3145

Mécanisme de traduction (1)

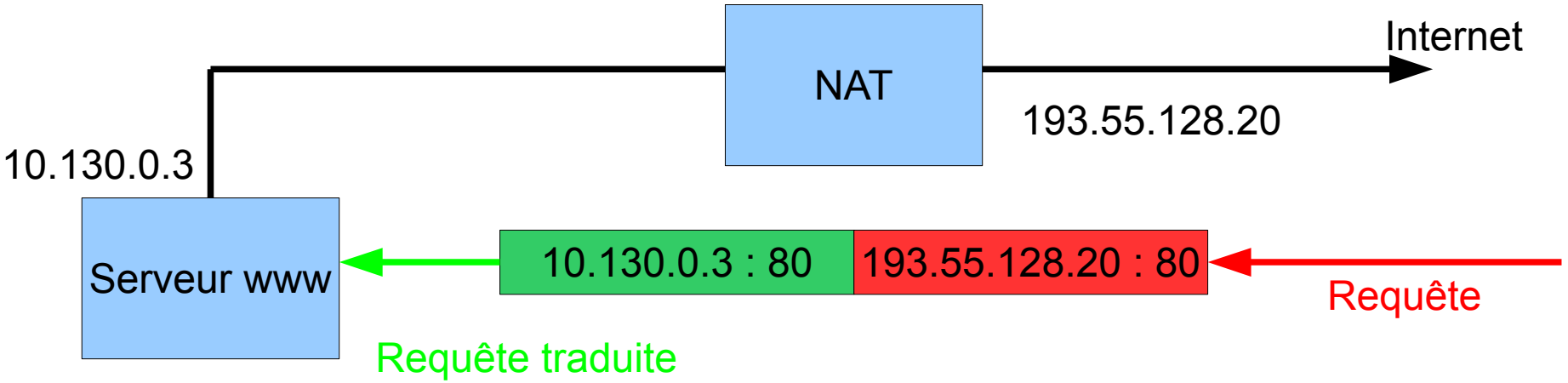


Transmission au routeur par défaut : 192.168.1.1

Requête du poste : ad source 192.168.1.2, port source 3145

Mécanisme de traduction (2)

Traduction fixe pour un serveur dans le réseau privé (exemple)



Adresses privées v6 ?

Translation d'adresses inutiles en v6
(assez d'adresses globales pour tous).
On peut toutefois souhaiter un adressage privé, sans accès Internet pour certaines machines.

Pour interdire certains accès seulement, on utilisera des règles de filtrage.

Adresses lien-local v6

Adresses lien-local
Uniquement sur réseau physique
préfixe fe80::0/64, partie machine auto-calculée (ou choisie aléatoirement, ...).
Utile pour premier accès réseau, avant config.
Complète, ou bien pour créer un réseau local.
Ne passe pas les routeurs.

Adresses site-local v6

Adresses site-local
Interne à l'entreprise
préfixe fec0::0/48, et 16 bits pour sous-adressage.
Possibilités de routage interne à l'entreprise
(plus exactement à 1 site)
Mais ...pb de définition du "site"
=> "deprecated" en 2004

Adresses unique-local v6

En remplacement de site-local
préfixe fc00::/7, la moitié pour gestion globale, l'autre pour dériver des /48 en ajoutant 40 bits aléatoires.
Risque d'adresses dupliquées, faible
Possibilité de gérer ces adresses au niveau mondial.