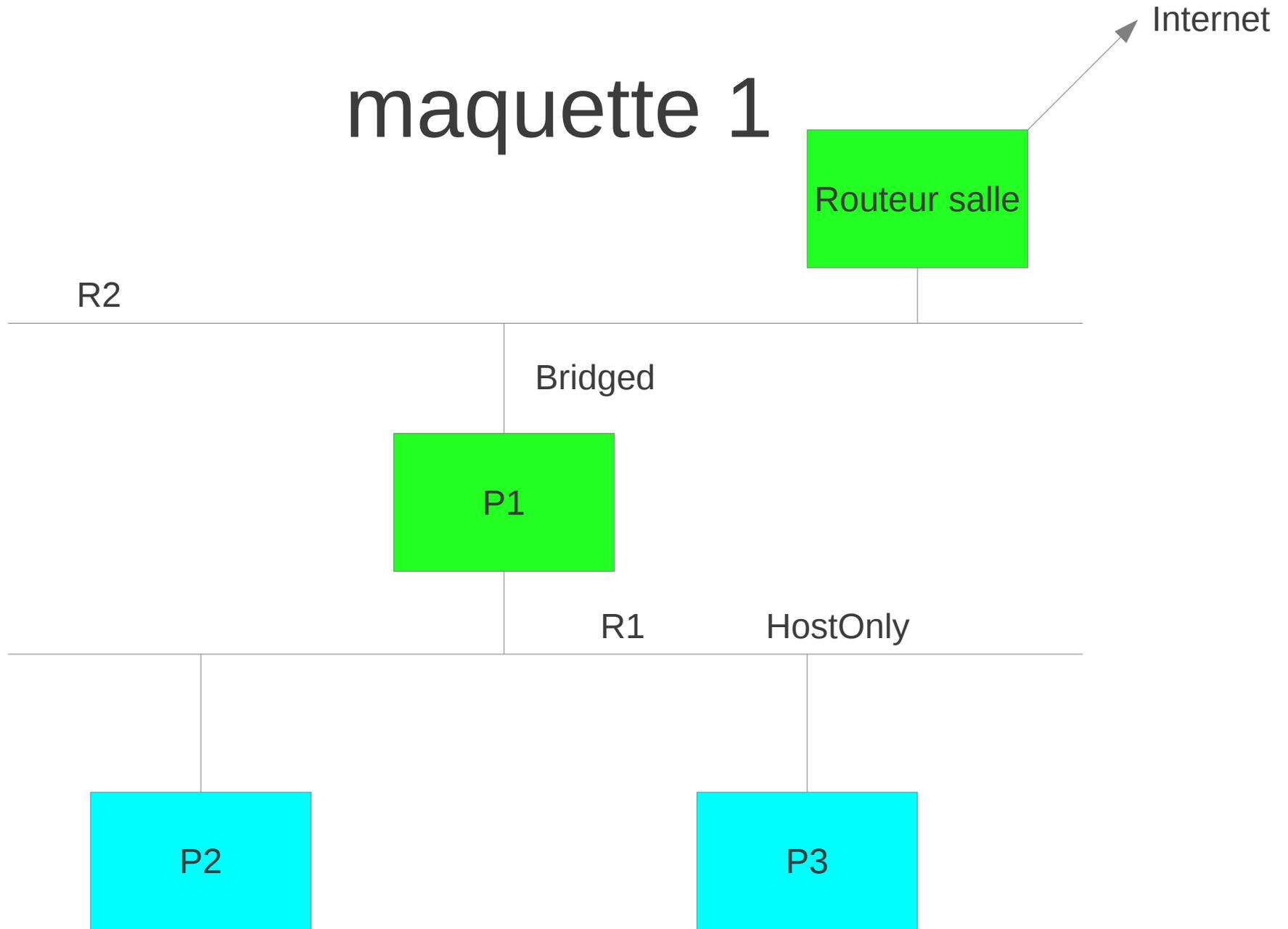


Traduction d'adresses

- problématique
- divers types de traduction d'adresses
- de l'obligation de pouvoir modifier les identifiants de transport
- configuration sous Linux et sous Windows
- limitation de la traduction d'adresses: ftp et ALG (helpers)
- traduction d'adresse et sécurité
- Bibliographie

maquette 1



Couleurs:

- vert: routage activé
- - bleu: hôtes non routeur

R1: 192.168.10/24

R2: 192.168.195/24

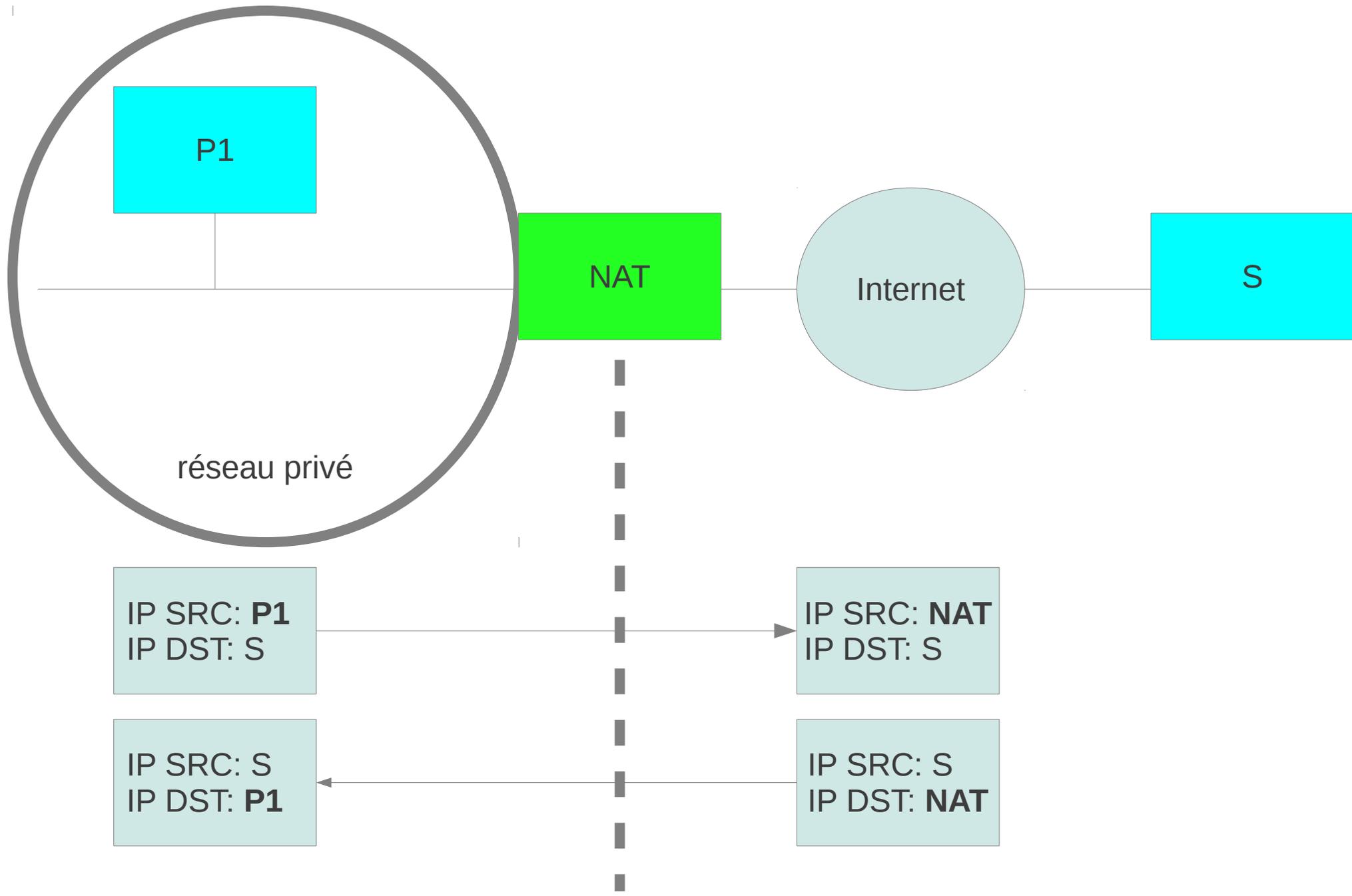
Maquette 1

- la machine P1 a une interface réseau en mode bridged sur R2 et une interface réseau en mode « host only » sur R1.
- les autres ordinateurs ont une seule interface réseau en mode « host only » sur R1.
- Le routeur de la salle n'est pas administré par vous. Sa configuration ne tient pas compte de votre sous-réseau.
- Quid de la connectivité IP entre P2 et P3, P2 et P1, P1 et le routeur de la salle (192.168.195.2), P2 et le routeur de la salle ?

traduction d'adresse

- motivations d'origine:
 - palier la pénurie d'adresses IP
 - permettre un accès à internet depuis des adresses privées (RFC 1918)
- Principe:
 - un routeur remplace les adresses IP sources ou destinations des paquets qu'il route de façon à ce que seules des adresses ip publiques apparaissent
 - les ports tcp/udp peuvent aussi être modifiés (selon le type de NAT)
 - la charge utile du paquet peut parfois être modifiée

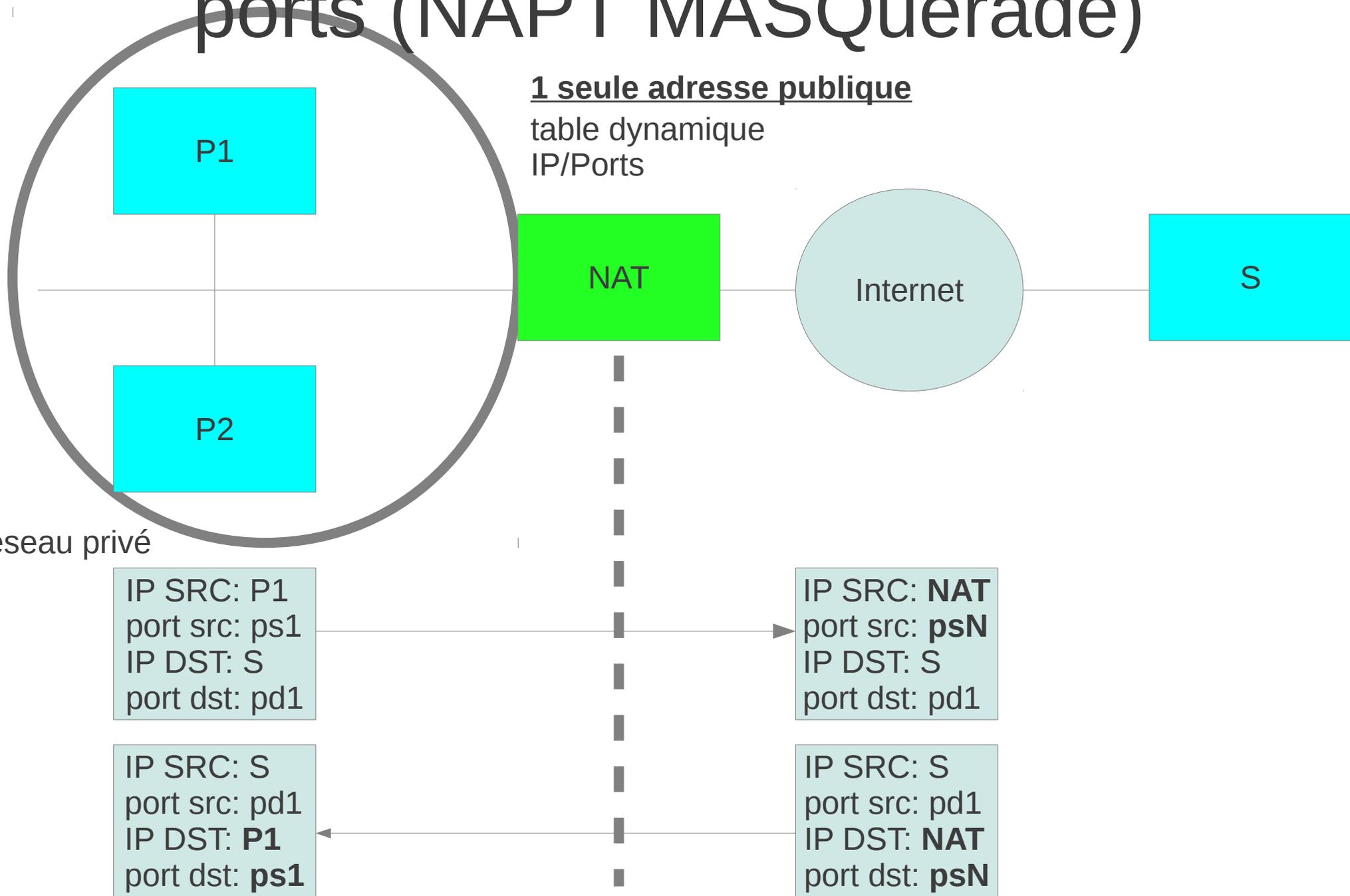
traduction d'adresse



type de NAT:

- nat de base
- nat dynamique
- NAT: traduction d'adresses et de ports (NAPT MASQUerade)
- NAT bi-directionnel
- NAT double (twice NAT)
- NAT avec redirection de port (port forwarding)

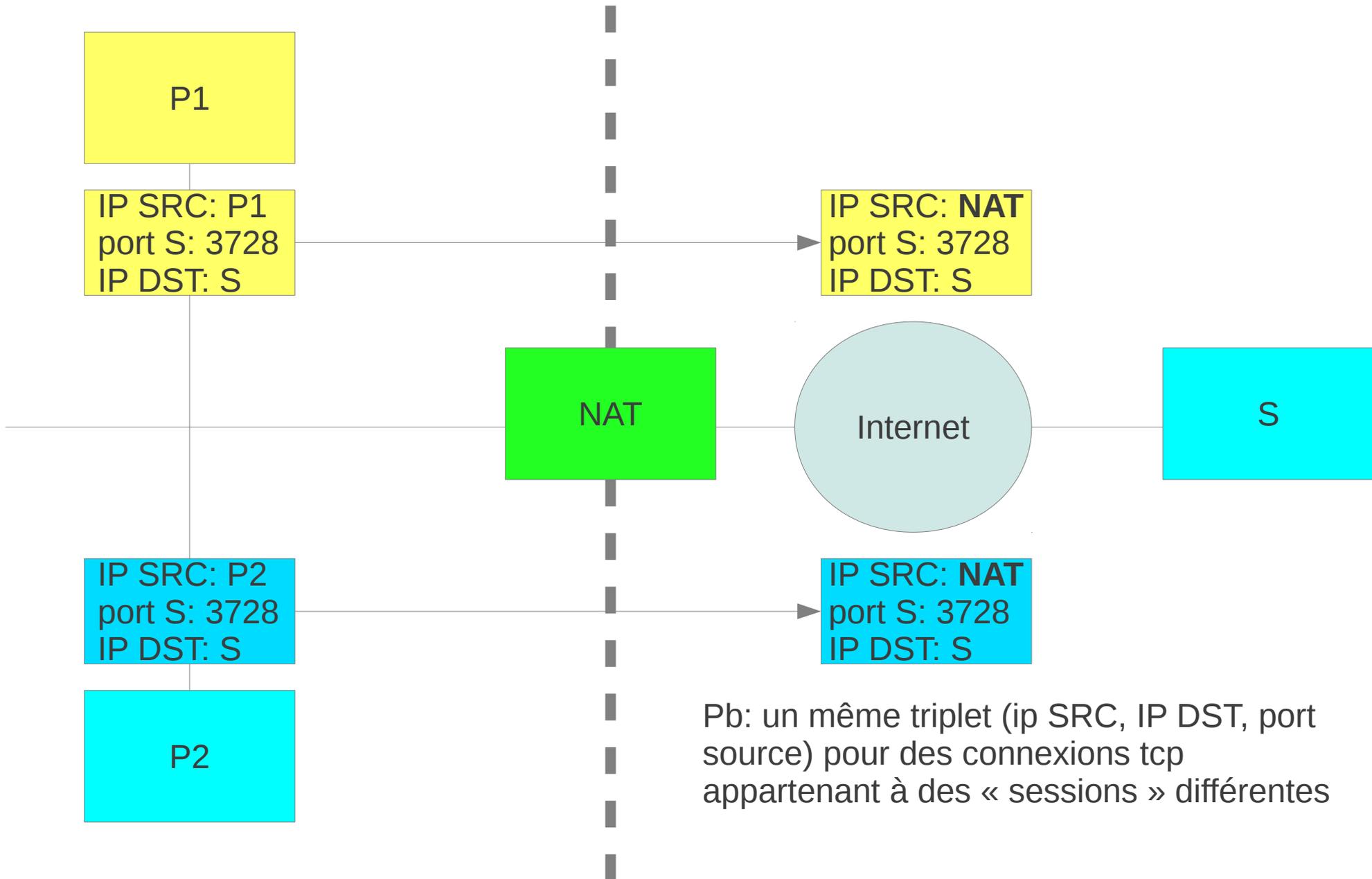
NAPT: traduction d'adresses et de ports (NAPT MASQUERADE)



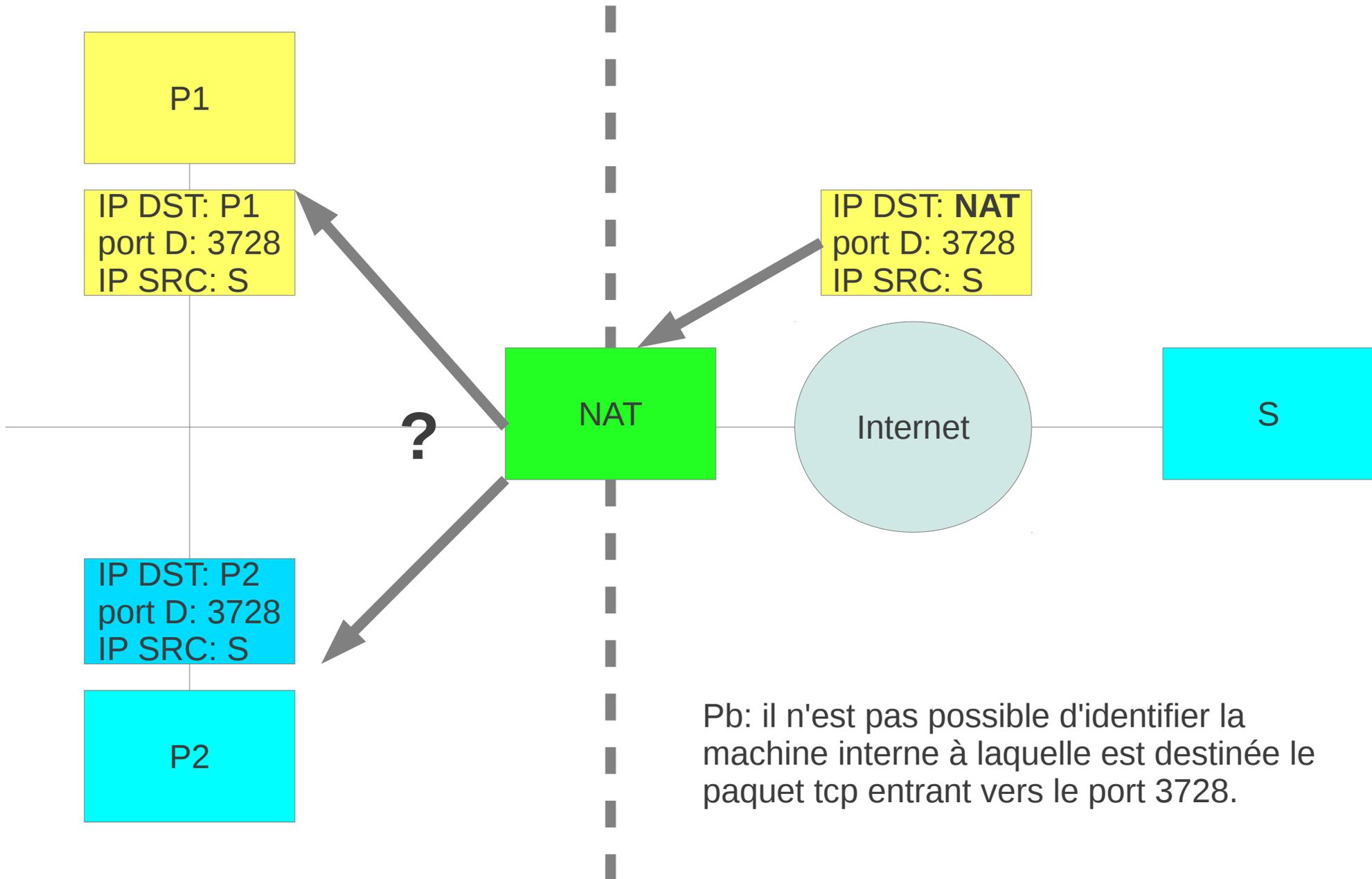
identifier des « connexions » venant de la même source

- problème classique sans NAT: gestion des « connexion » venant du même hôte
- Exemples:
 - TCP: 2 connexions ssh ayant même IP SRC et DST.
 - UDP: deux requêtes dns ayant même IP SRC et DST.
 - solution: le port source de chaque connexion est différent
 - deux ping (icmp echo) ayant même IP SRC et DST
 - solution: chaque série de ping a un champ « identifier » qui permet de l'identifier et de faire correspondre chaque « réponse echo » à la bonne « requête echo ». Il est garanti que deux sessions ping originaire du même hôte aient des « identifiants » différents.

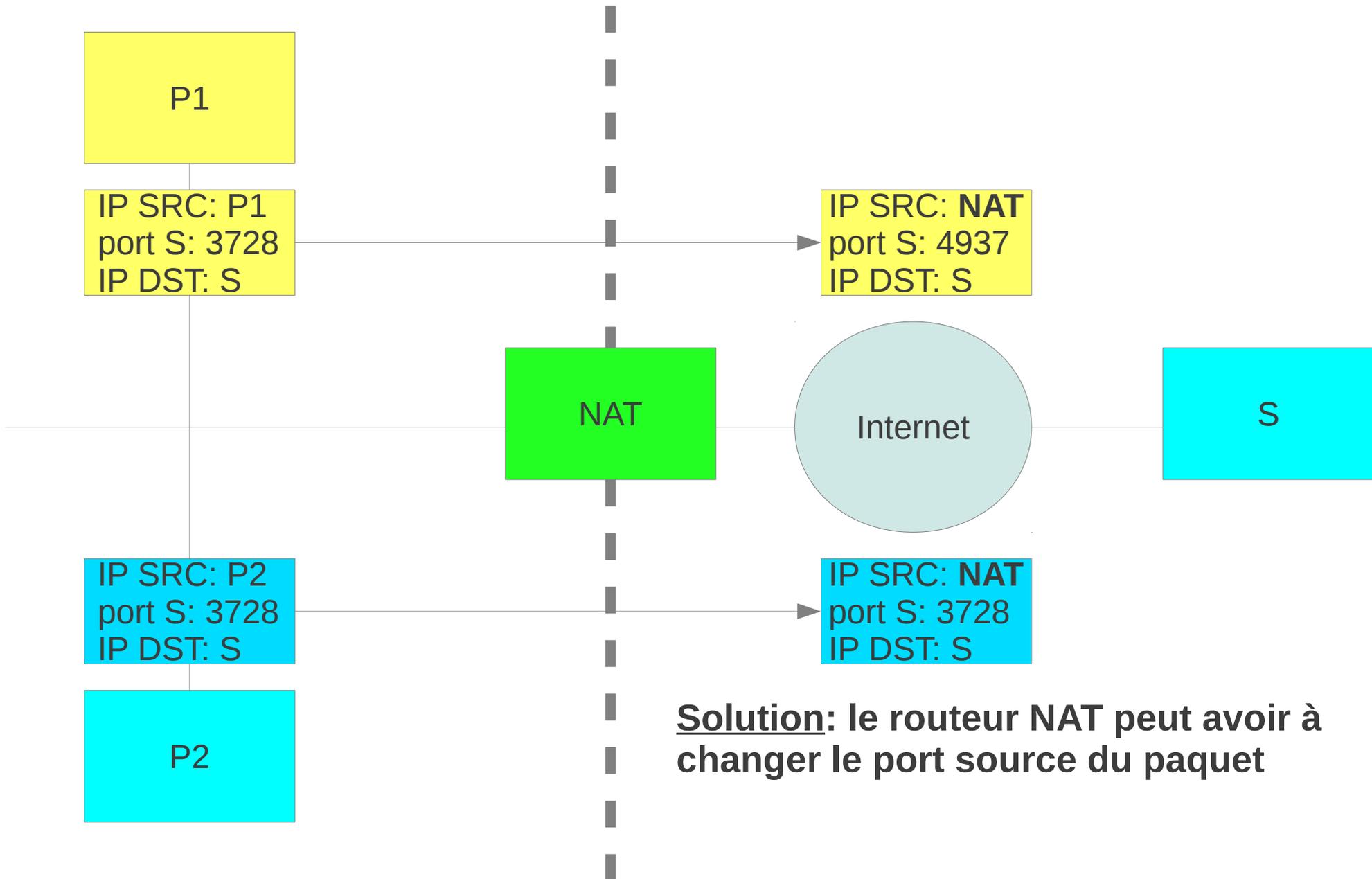
NAPT et tcp/udp: problème



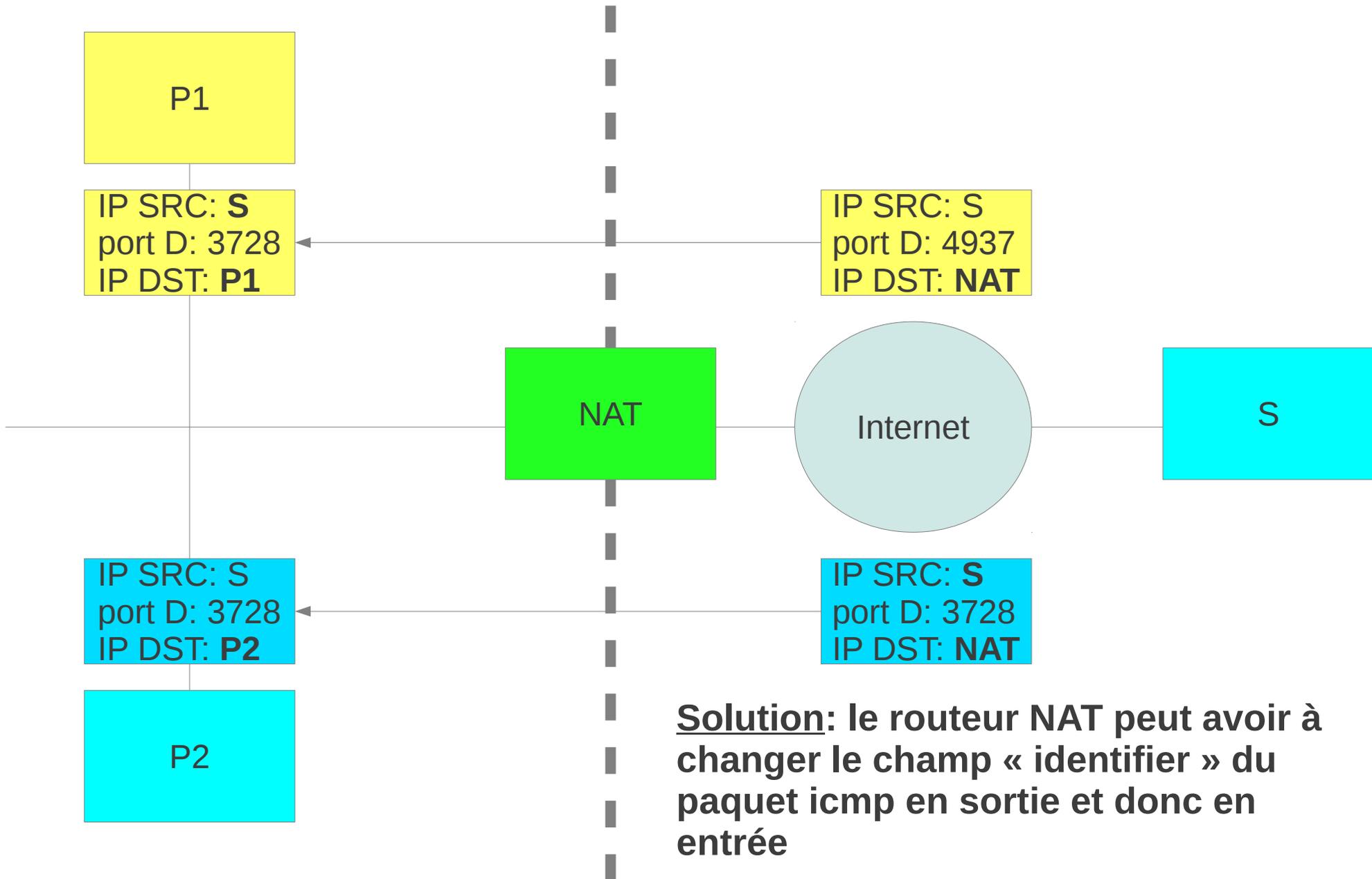
NAPT et tcp/udp: problème



NAPT et tcp/udp: solution

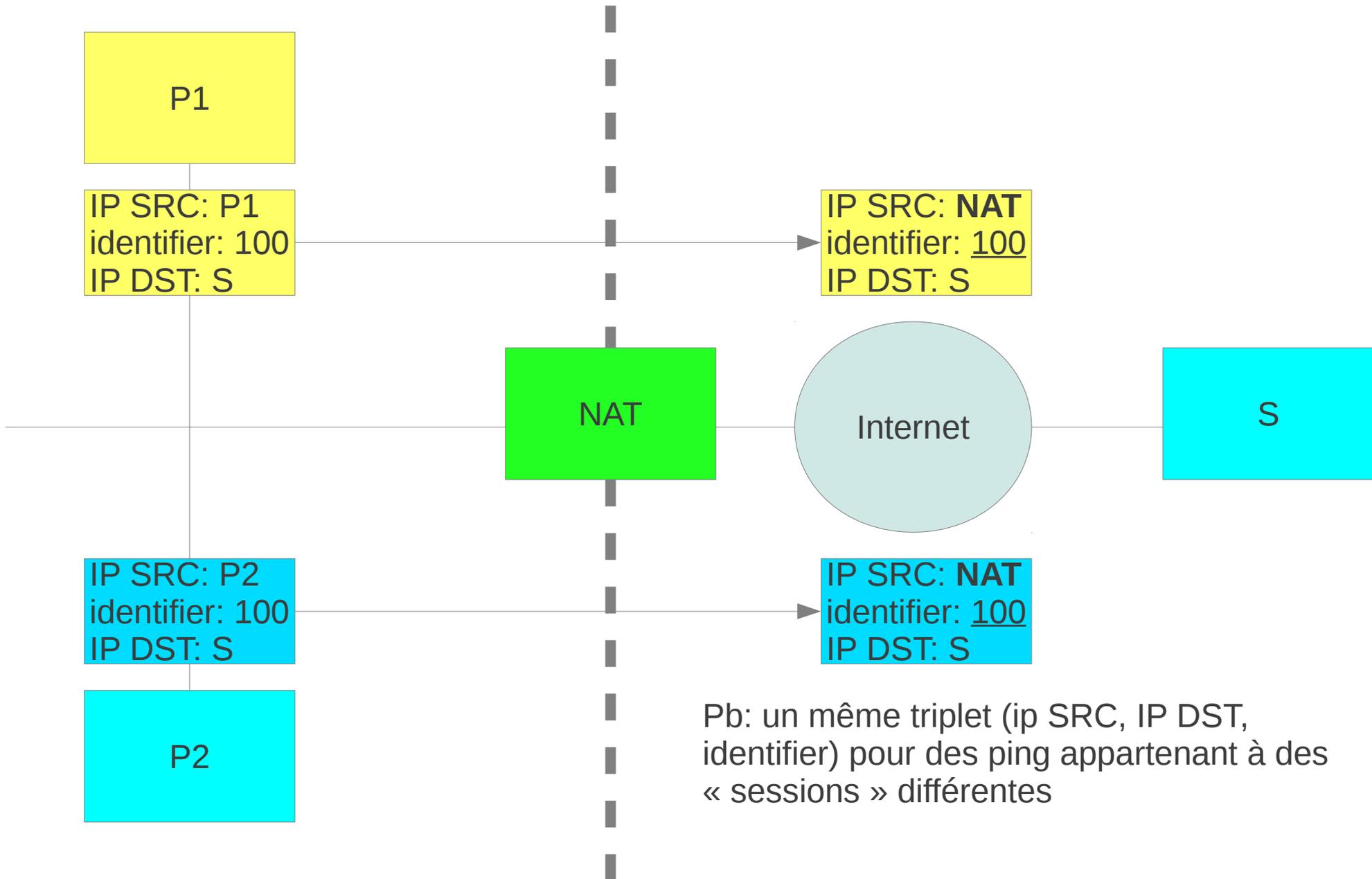


NAPT et tcp/udp: solution

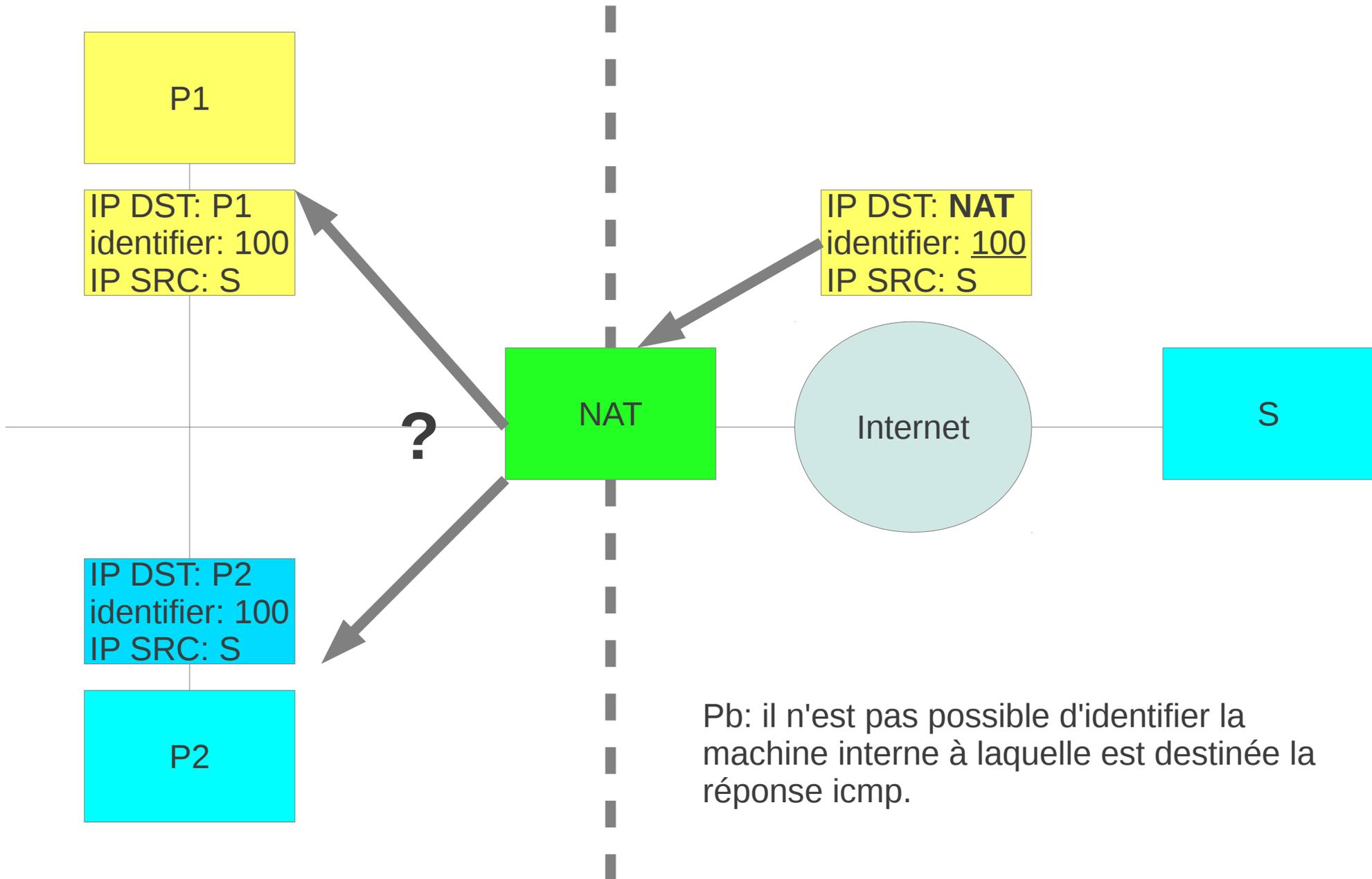


Solution: le routeur NAT peut avoir à changer le champ « identifier » du paquet icmp en sortie et donc en entrée

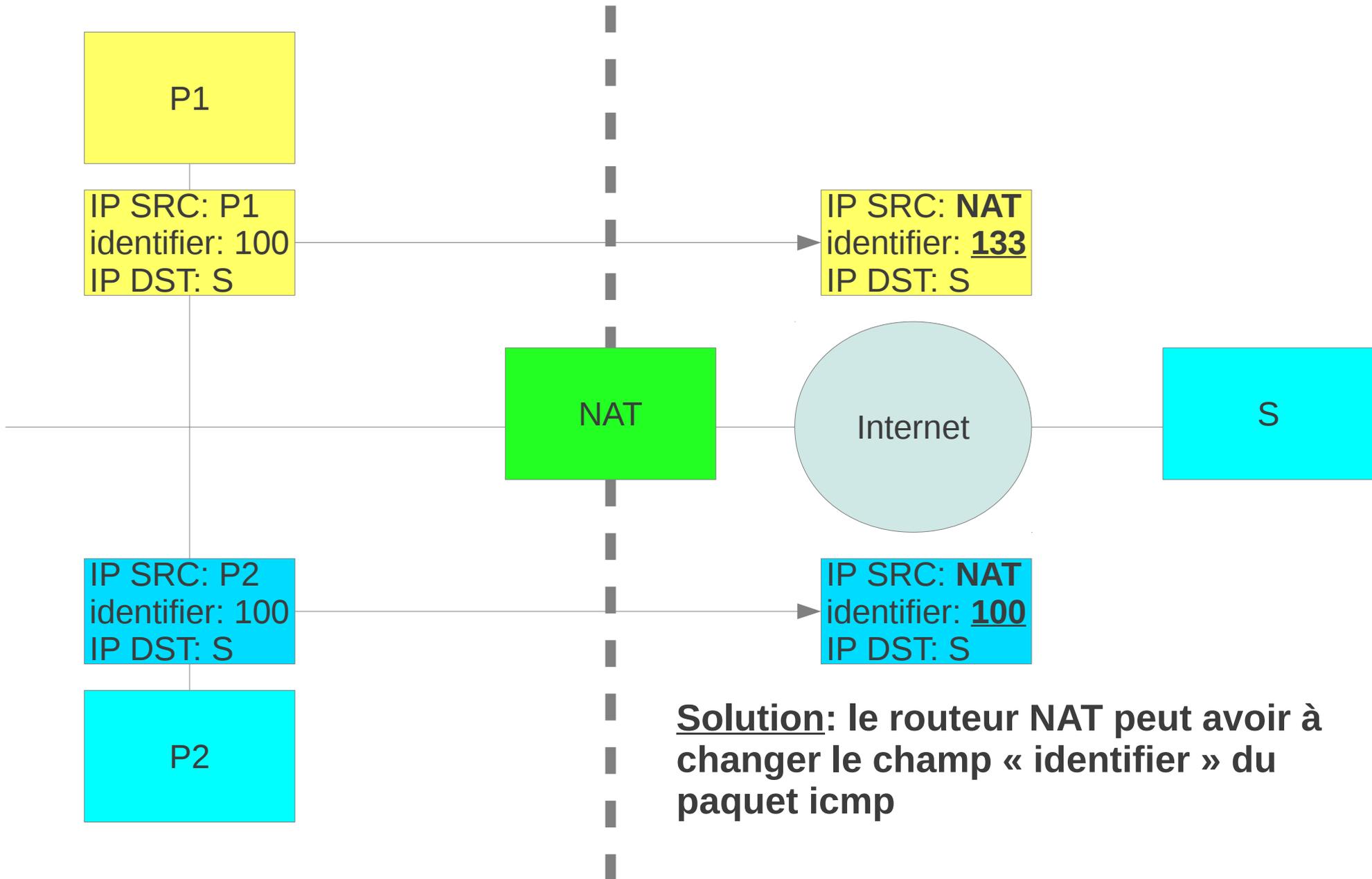
NAPT et ping: problème



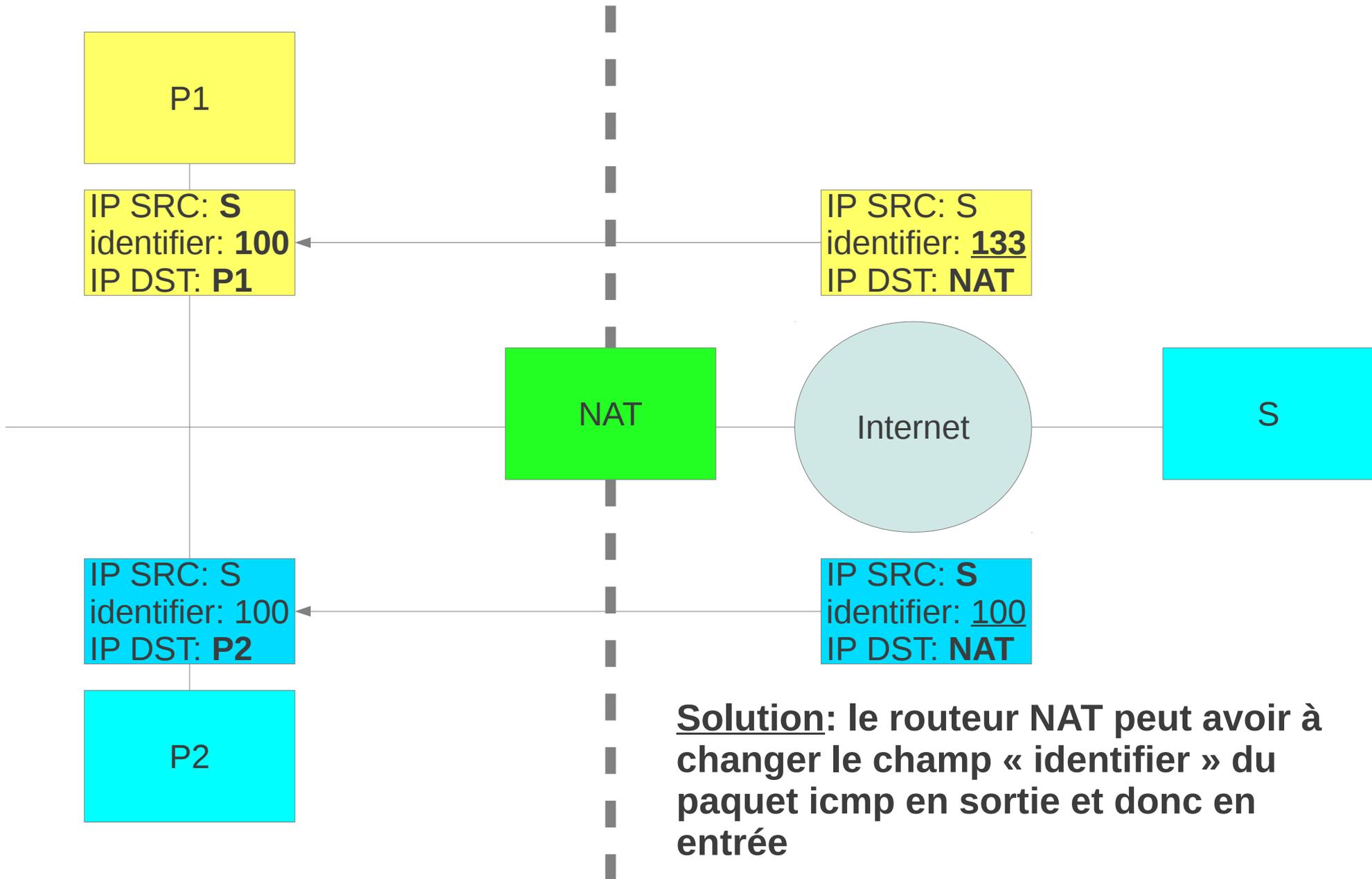
NAPT et ping: problème



NAPT et ping: solution



NAPT et ping: solution



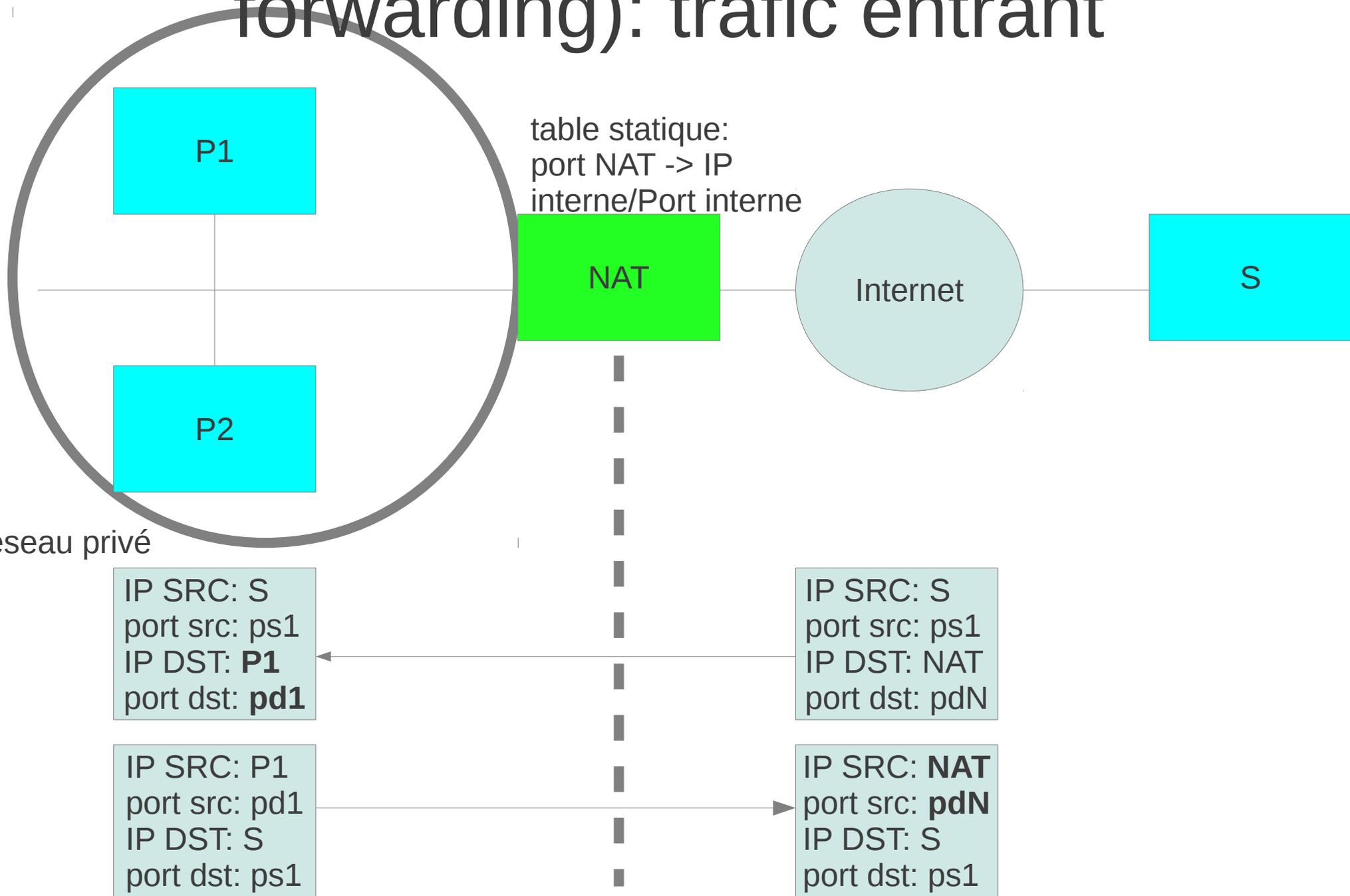
NAPT: identifier les paquets entrant

- Vu de l'extérieur, tous les paquets semblent venir du routeur NAT
- On ne peut plus forcément garantir l'unicité des informations d'identification des paquets des connexions sortantes:
 - TCP/UDP: (IP SRC, port SRC, IP DST, PORT DST) si seule l'IP SRC est remplacé par celle du routeur
 - ICMP: (IP SRC, IP DST, « identifier », No de séquence)
- solution:
 - le routeur NAT modifie aussi l'identifiant de transport source: port tcp/udp, identifiant icmp.
 - la correspondance est stockée dans une table

NAPT avec redirection de port (port forwarding): trafic entrant

- Problème :
 - comment permettre à une machine internet d'être joignable depuis l'extérieur ?
 - on suppose qu'elle héberge un service sur un port tcp ou udp donné
- solution :
 - mettre en place une correspondance statique
 - entre un port/protocole du routeur NAT (ex. : 80/tcp)
 - et un port d'une machine interne
- mécanisme classique sur les routeurs/box ADSL
- notion de dmz :
 - tout le trafic entrant est redirigé vers une machine interne donnée

NAPT avec redirection de port (port forwarding): trafic entrant



freebox port forwarding

Redirections de ports:

Port	Protocole	Destination	Port	
47624	tcp	192.168.0	10	47624 X
47624	udp	192.168.0	10	47624 X
	udp	192.168.0		Ajouter

Redirections de plages de ports:

Début	Fin	Protocole	Destination	Port	
2300	2400	tcp	192.168.0	10	X
2300	2400	udp	192.168.0	10	X
28800	29100	tcp	192.168.0	10	X
28800	29100	udp	192.168.0	10	X
		tcp	192.168.0		Ajouter

source de l'image : <http://www.archangelcastle.com/acforum/viewtopic.php?t=105>

Configuration d'un routeur NATP sous Linux

- `iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source adresseIPPublique` avec eth0: interface pour l'accès à internet (à adapter)
- pour effacer les règles correspondantes :
 - `iptables -t nat -F`
- pour les lister :
 - `iptables -t nat -L`

Configuration d'un routeur NATP sous windows

- mmc « routage et accès distant »
- puis « nom de votre serveur »/routage IP/general
- clic droit ou Action/nouveau protocole de routage
- « traduction d'adresse réseau (NAT) »
- « nom de votre serveur »/routage IP/NAT puis clic droit/nouvelle interface. Préciser pour chaque interface
 - si elle est du côté public ou privé
 - s'il faut activer la traduction de ports (cocher « traduire les entêtes tcp/udp »)

limitations de la traduction d'adresses

- la traduction d'adresse casse le fait que tcp/ip part du principe qu'on a une liaison point à point entre source et destination (râf: mal dit)
 - applications transportant les adresses IP/ports dans la charge utile TCP/IP
 - applications avec des sessions multiples interdépendantes, négociées dynamiquement
 - débogage et flicage
- fragmentation: défragmenter pour travailler sur la charge utile des paquets
- gestion des états : 15 à 20% de charge pour les routeurs/fw

traduction d'adresse et sécurité

- du point de vue des machines internes :
 - le réseau interne n'est pas directement joignable
 - si les adresses internes sont affectées par dhcp: augmentation de la difficulté pour un intrus de désigner précisément un hôte
 - le routeur NAT est un point central critique en cas de piratage :
 - syndrome du « renard dans le poulailler »
 - MiM sur tout le trafic sortant
- du point de vue des machines externes:
 - tout est vu comme venant du routeur NAT ce qui ne facilite pas l'identification de la source d'une attaque

Bibliographie : traduction d'adresses

:

- résumé en français : <http://www.securiteinfo.com/conseils/nat.shtml>
- rfc 3022: Traditional IP Network Address Translator (Traditional NAT)
- rfc 2663: IP Network Address Translator (NAT) Terminology and Considerations
- rfc 2993: Architectural Implications of NAT (bonne synthèse, clair)
- TCP/IP: « TCP/IP illustré: les protocoles »: W. R. Stevens