Administration système et réseau avancée 2005-2006

- rappel sur le routage
- traduction d'adresse
- Firewall
- Les pares-feus libres :
  - Netfilter/iptables
  - IP Filter
  - packet Filter

Rappel réseau: routage

- Une machine sait transmettre les datagrammes sur les sous-réseaux de ses interfaces (réseaux locaux)
- Les autres datagrammes sont envoyés à un routeur directement joignable (situé sur un réseau local)
- Une machine qui sait transmettre un datagramme reçu sur l'une de ses interface sur une autre de ses interface est appelée routeur (ou, par abus de langage, passerelle).

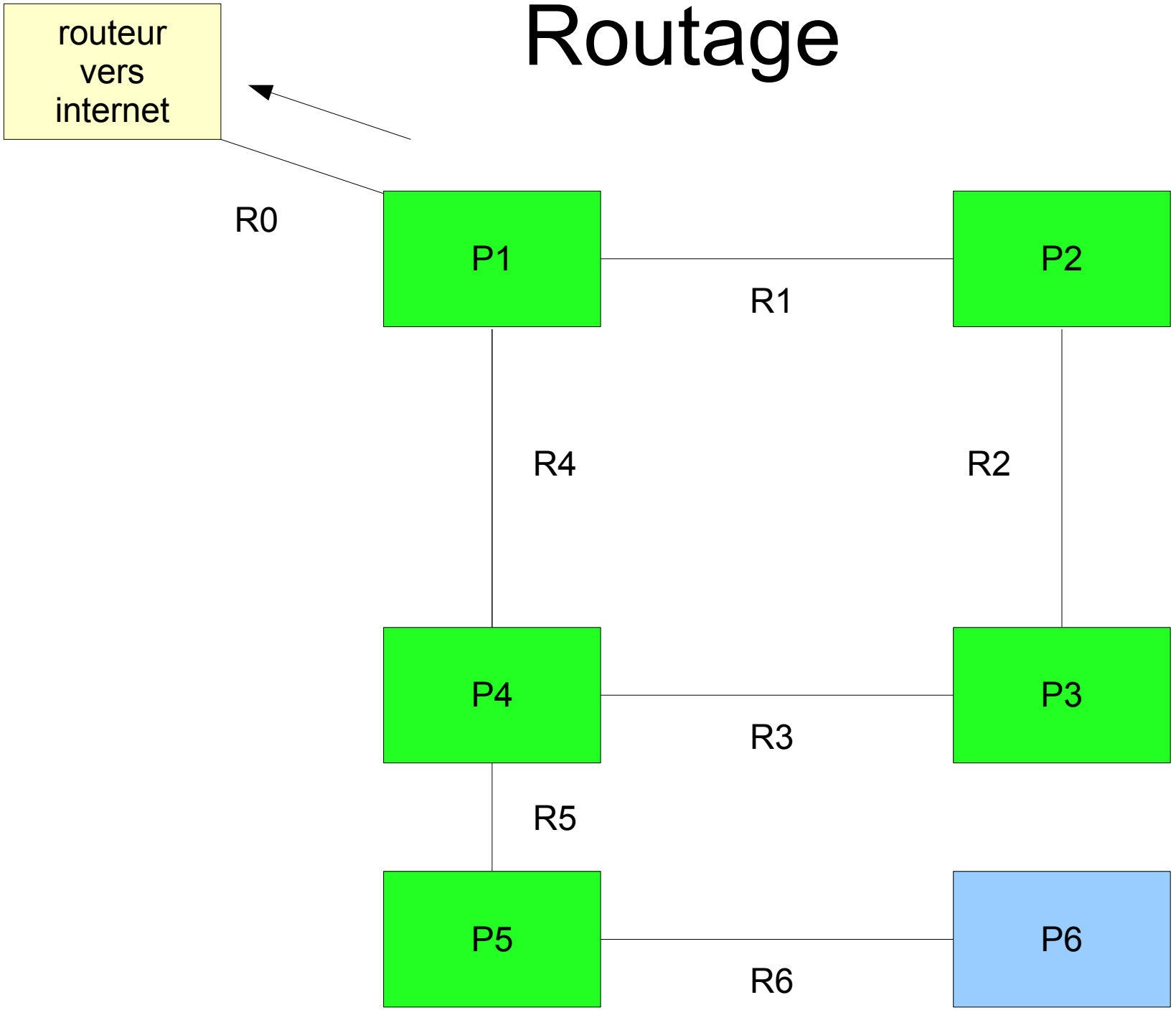
routage (2)

- Table de routage (netstat -nr)
- Routage dynamique : un programme externe modifie la table de routage

Algorithme de routage

- quand une machine M a un paquet à transmettre, elle applique l'algorithme suivant :
  - si le paquet est pour une machine située sur l'un des sous-réseaux d'une de ses cartes réseau, il est envoyé directement à la destination
  - si le paquet est pour un hôte pour lelque M a une route définie, il est envoyé au routeur défini dans la route
  - si le paquet est pour un réseau pour lelque M a une route définie, il est envoyé au routeur défini dans la route
  - sinon, le paquet est envoyé à la passerelle par défaut de M

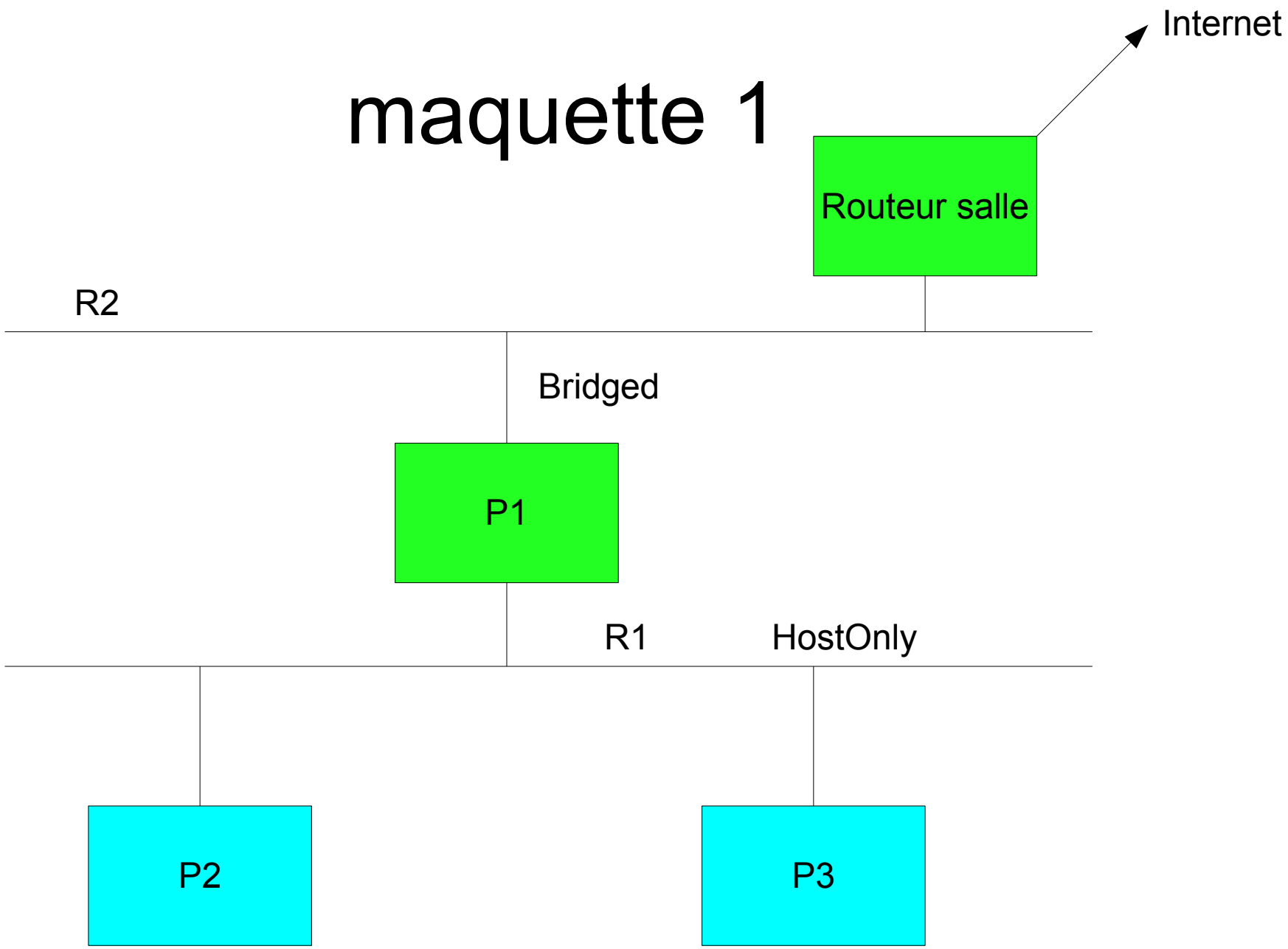
Routage



Traduction d'adresses

- problèmatique
- 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

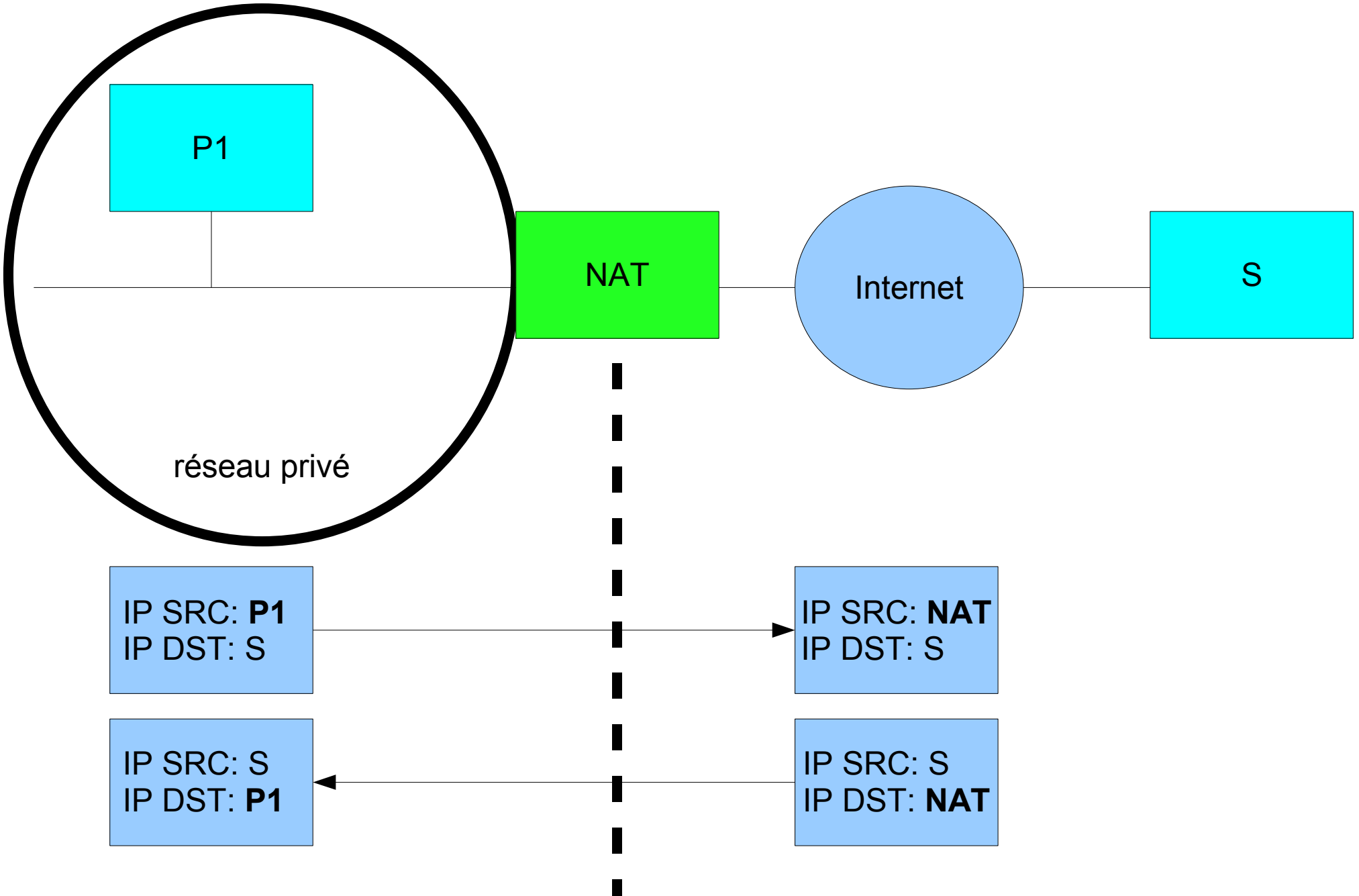
Maquette 1

- 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

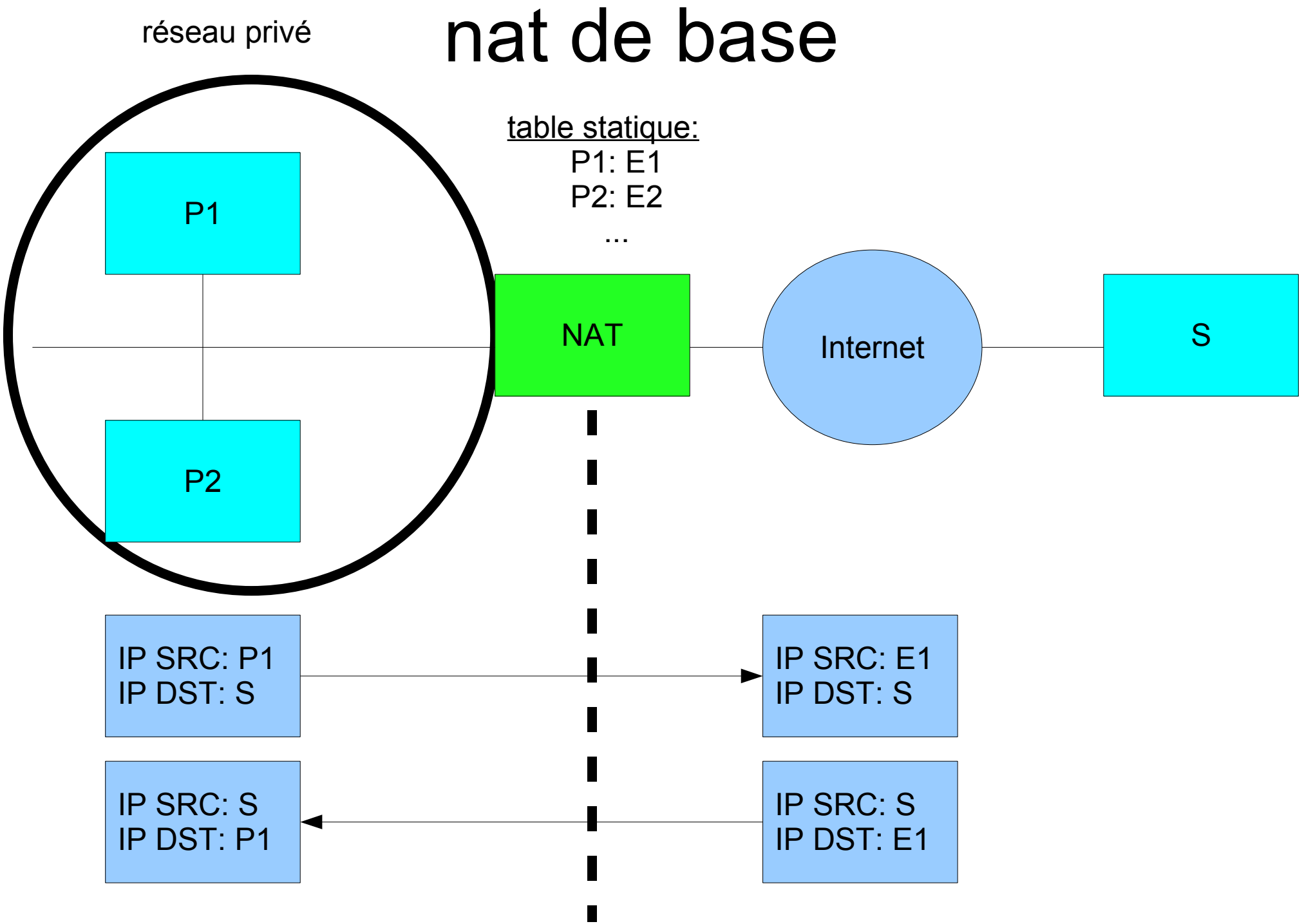
traduction d'adresse



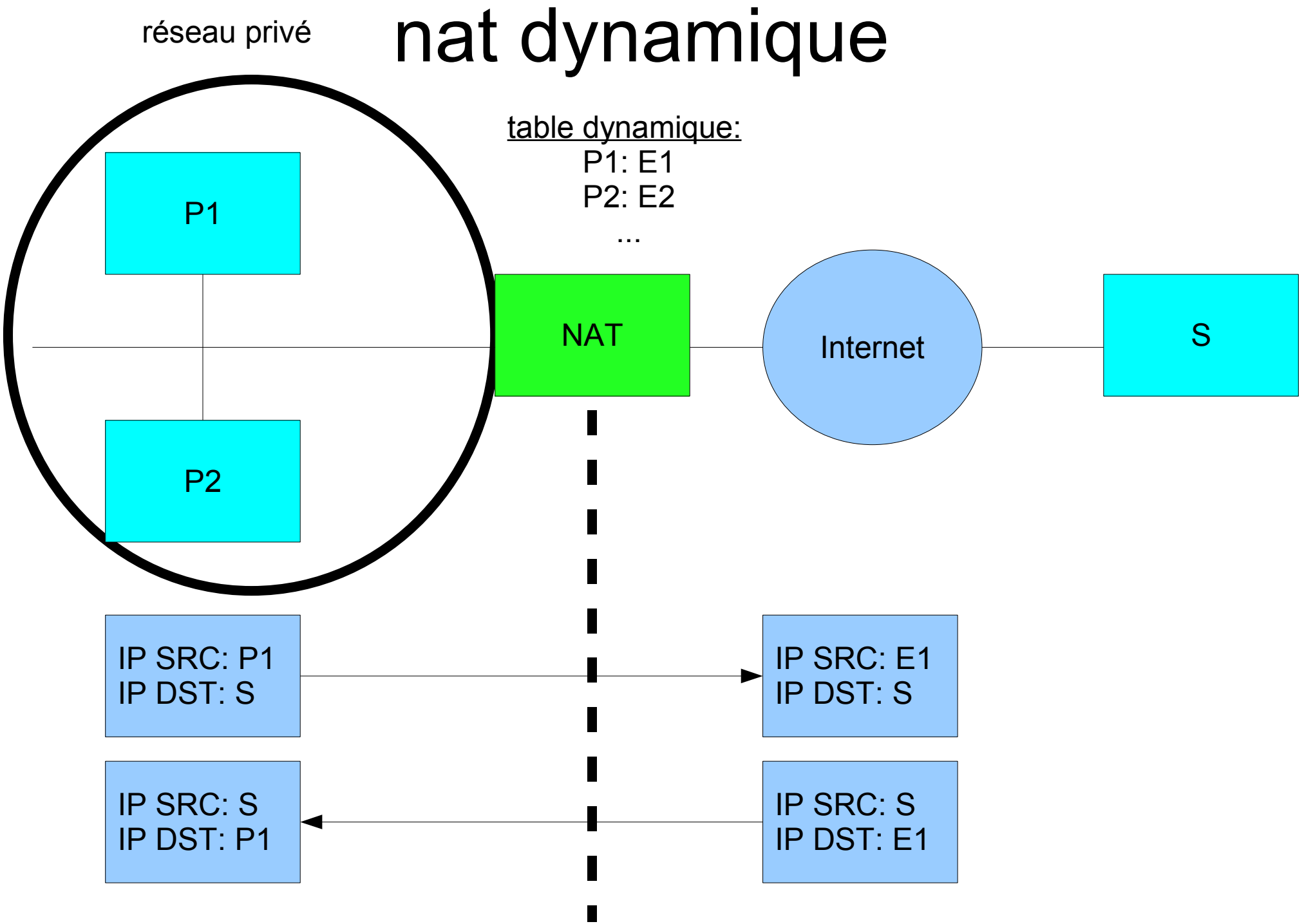
type de NAT:

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

nat de base


réseau privé
table statique:
P1: E1
P2: E2
...
P1
P2
NAT
Internet
S
IP SRC: P1
IP DST: S
IP SRC: E1
IP DST: S
IP SRC: S
IP DST: P1
IP SRC: S
IP DST: E1

nat dynamique



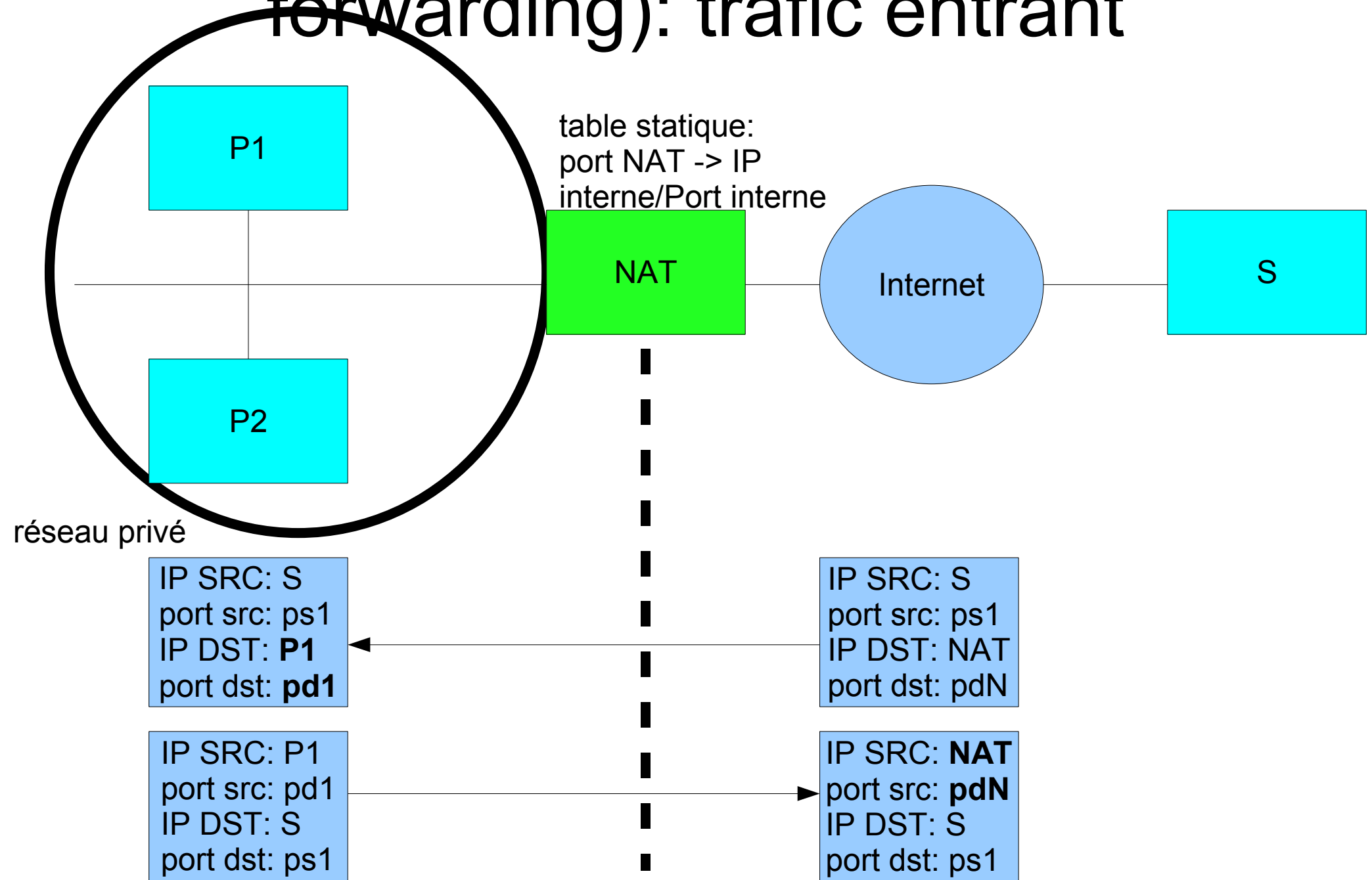
NAT bi-directionnel

- dans une version ultérieure de ce support
- pour permettre à des machines distantes d'accèder directement à des machines internes
- s'appuie sur le dns:
  - le serveur dns (en général la passerelle NAT) permet à la passerelle NAT de noter les association requete dns, ip distante
  - quid en cas de plusieurs requetes depuis la même ip distante ?

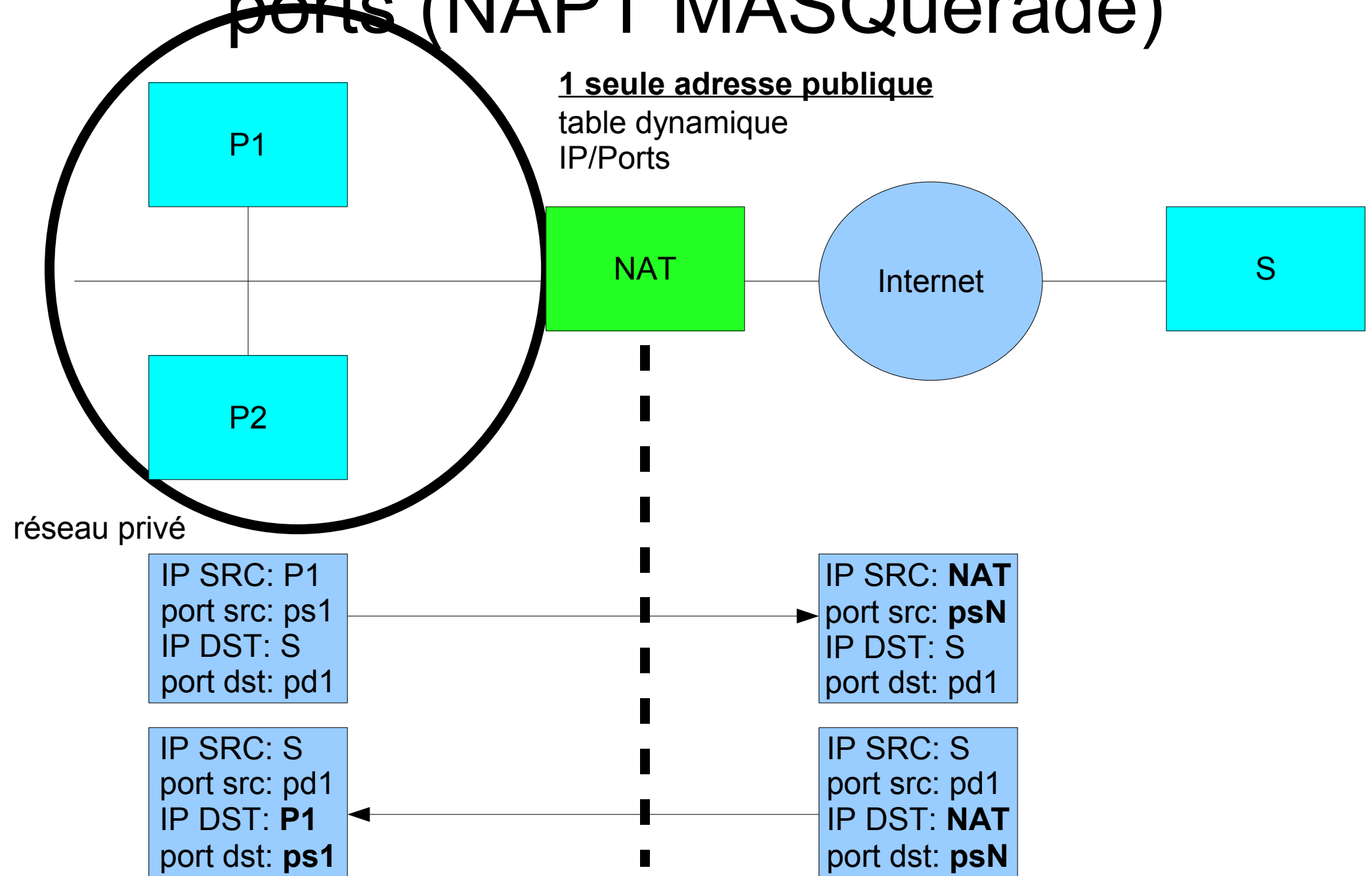
NAT double (twice NAT)

- on change adresses sources et destination.
- utilisé pour cacher les adresses sources aux destinations et lycée de Versailles.
- utile en cas de collision d'adresses entre sources et destination. Exemple: une entreprise qui a utilisé deux sous-réseaux privés identiques.

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



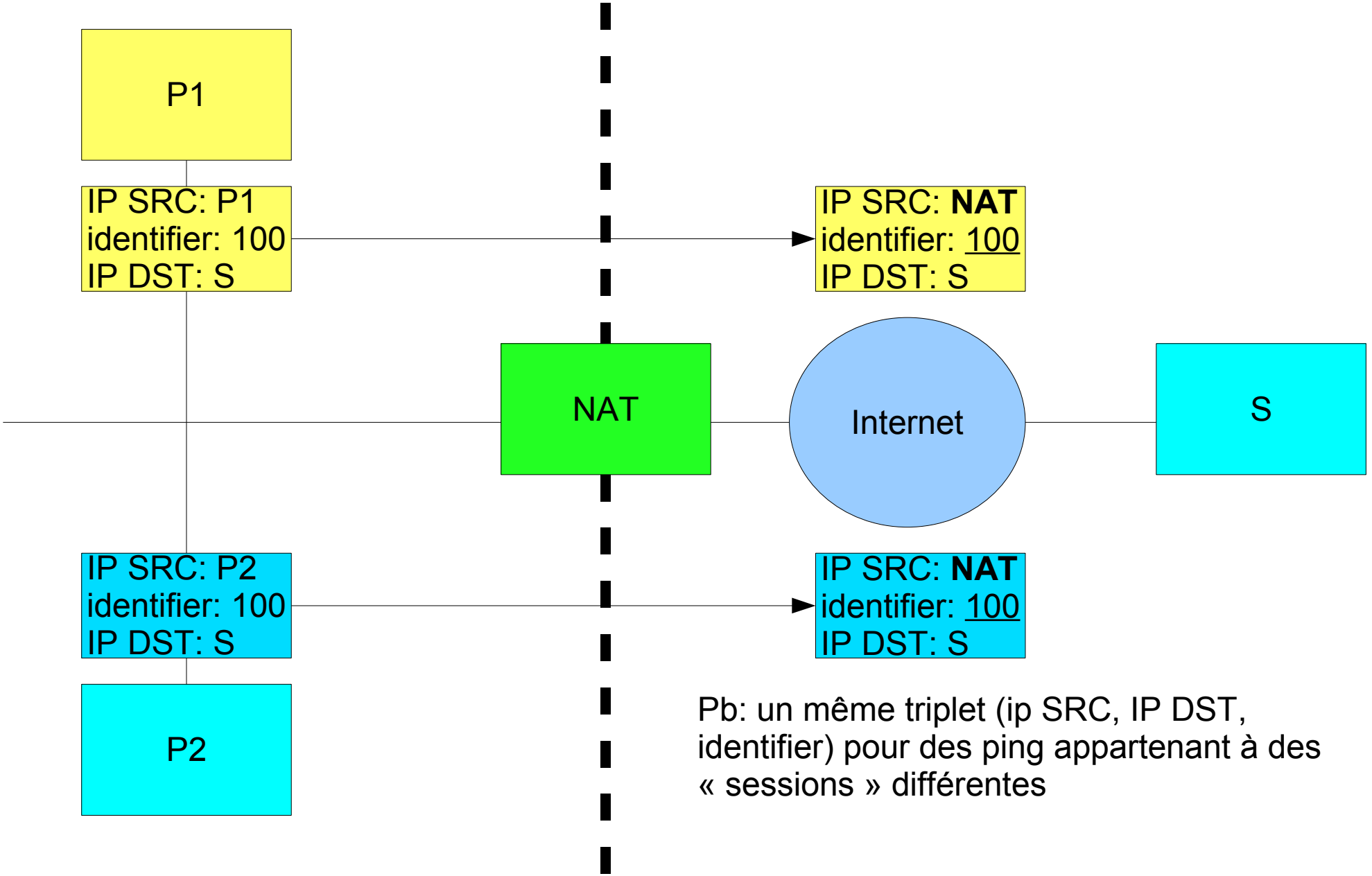
NAPT: traduction d'adresses et de ports (NAPT MASQuerade)



identifier des « connexions »venant de la même source

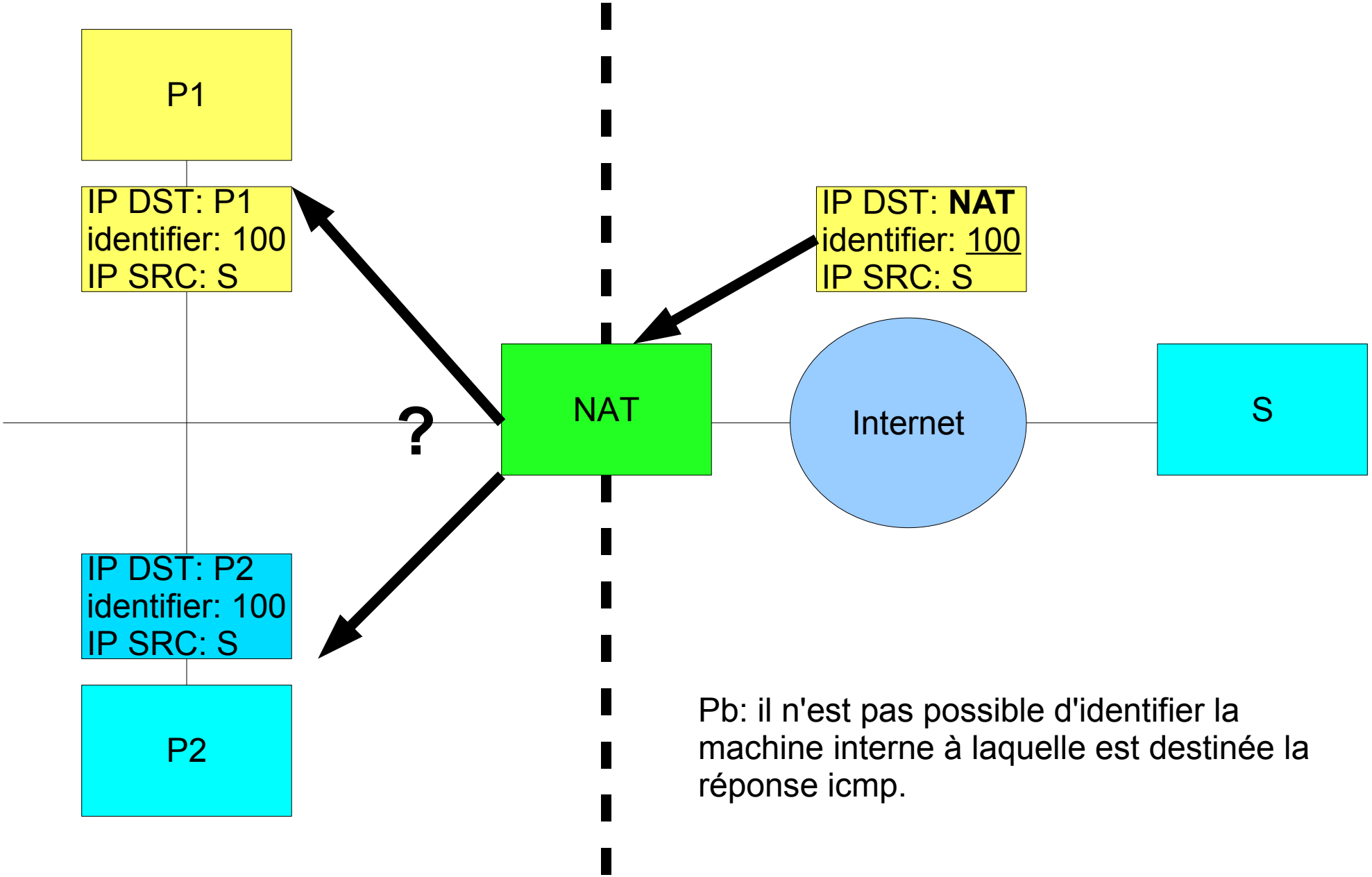
- problème classique sans NAT: gestion des « connexion » venant du même hôte
- Exemples:
  - TCP: 2 connexions ssh ayant même IP SRC et DST.
  - UDP: deux requêtes dns ayant même IP SRC et DST.
    - solution: le port source de chaque connexion est différent
  - deux ping (icmp echo) ayant même IP SRC et DST
    - solution: chaque série de ping a un champ « identifier » qui permet de l'idenfier 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 « identifiers » différents.

NAPT et ping: problème



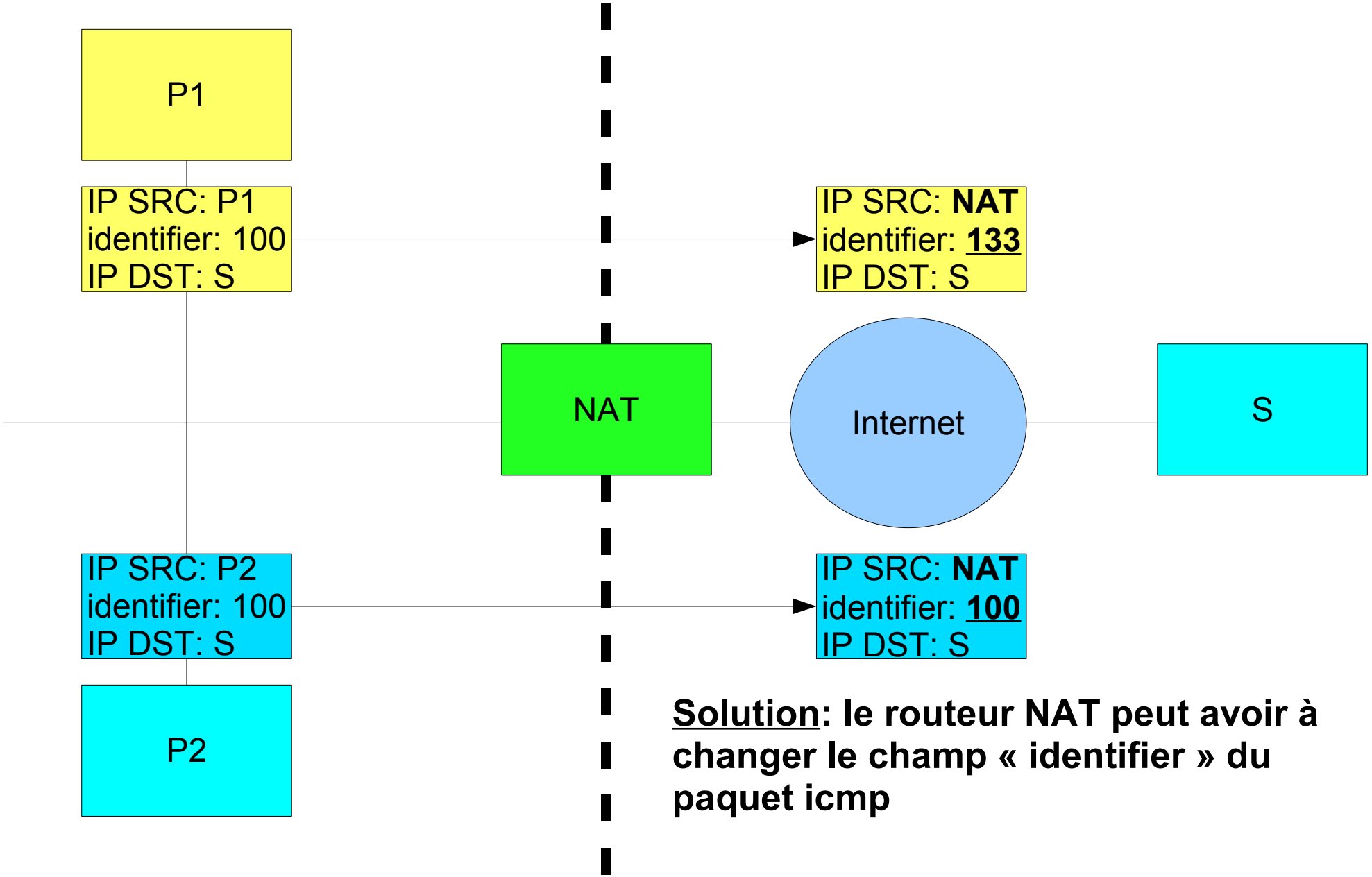
Pb: un même triplet (ip SRC, IP DST, identifier) pour des ping appartenant à des « sessions » différentes

NAPT et ping: problème



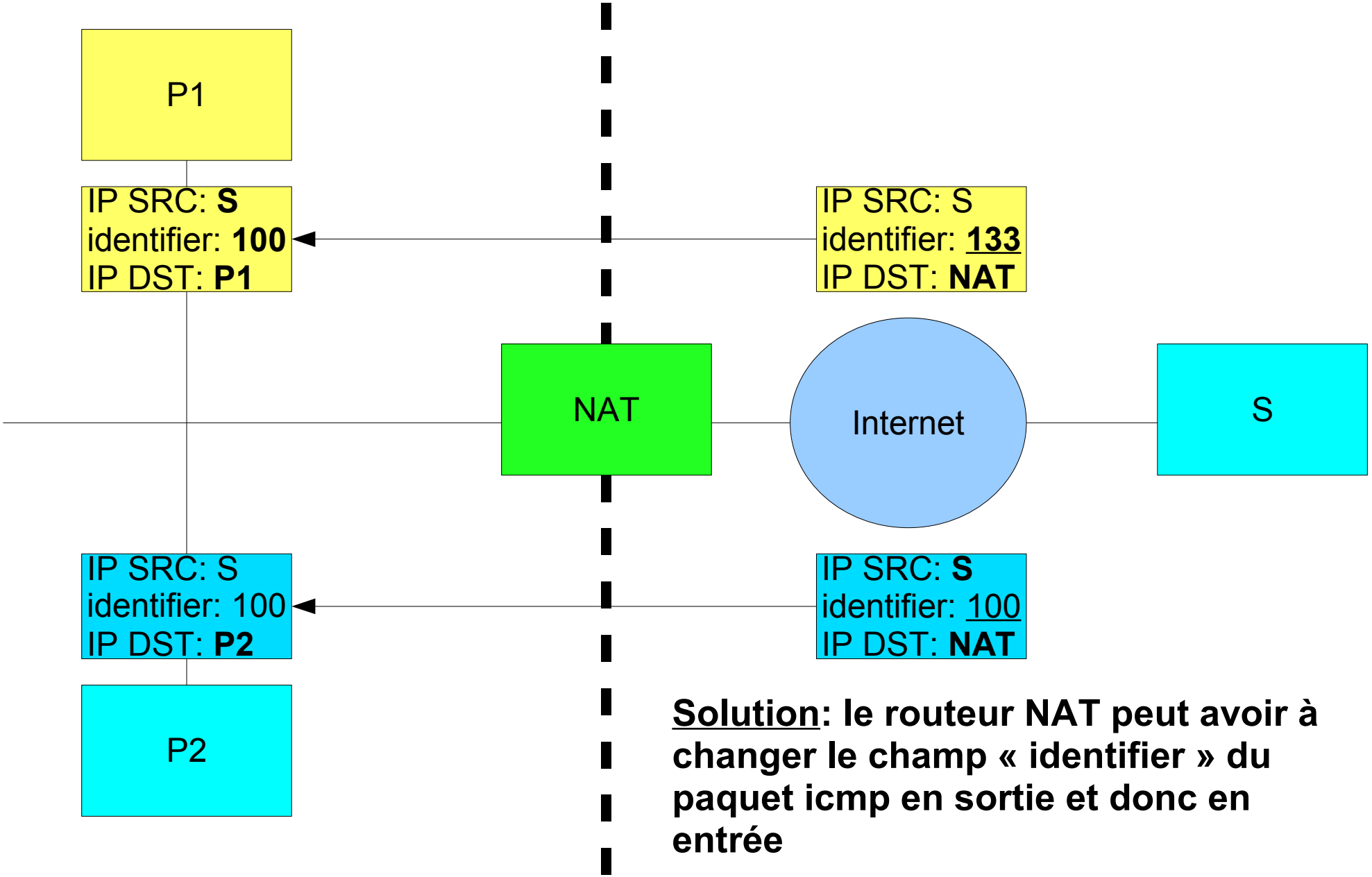
Pb: il n'est pas possible d'identifier la machine interne à laquelle est destinée la réponse icmp.

NAPT et ping: solution



Solution: le routeur NAT peut avoir à changer le champ « identifier » du paquet icmp

NAPT et ping: solution



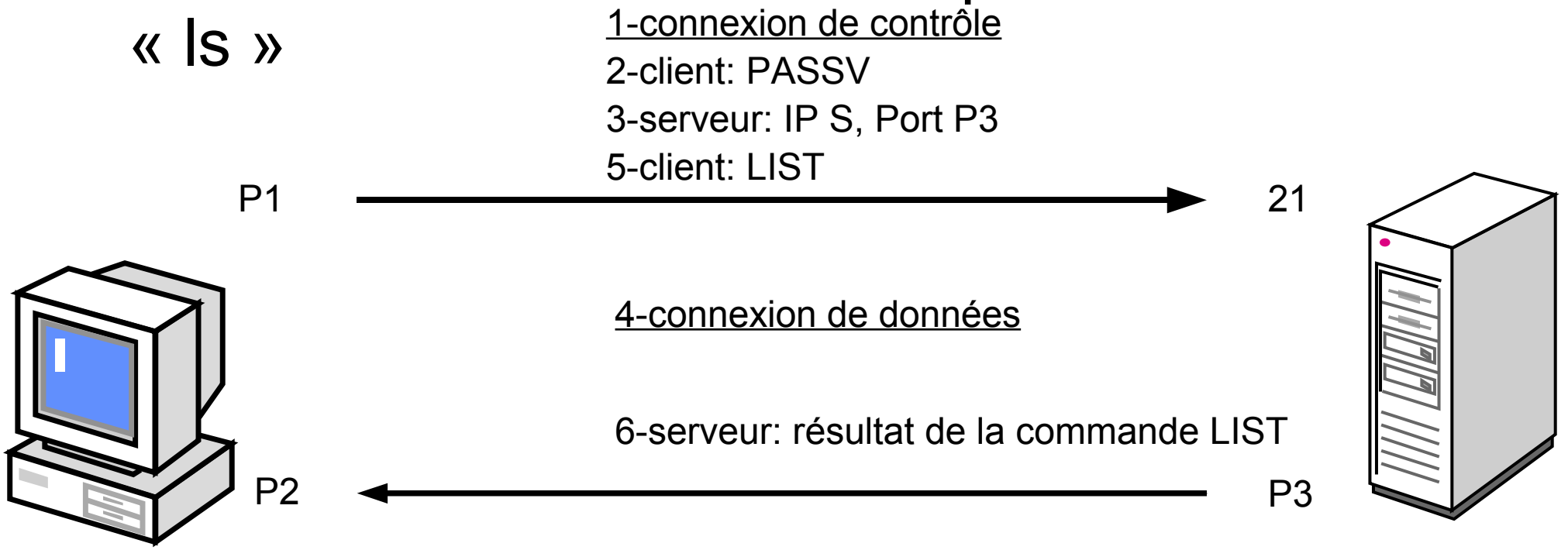
Solution: le routeur NAT peut avoir à changer le champ « identifier » du paquet icmp en sortie et donc en entrée

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.

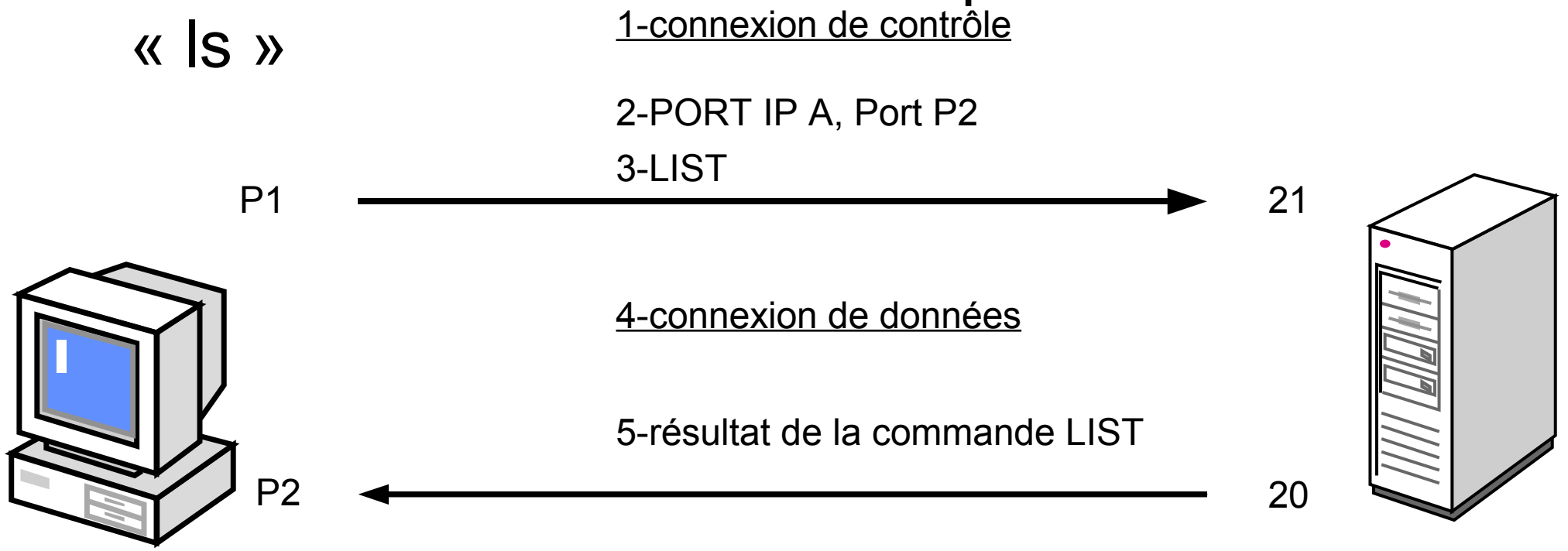
ftp : mode passif

- l'utilisateur se connecte et tape la commande « ls »



ftp : mode actif

- l'utilisateur se connecte et tape la commande « ls »



NAT/ftp: gestion mode actif d'un client

- Problèmes:
  - ne pas avoir d'IP interne mentionnée à une machine externe avec la commande PORT
  - prévoir le port où va arriver la connexion donnée pour l'associer à la bonne machine interne
  - (classique) : que la connexion de donnée entrante arrive sur un port inutilisé
- Solutions:
  - 1) lire/modifier le niveau application (commande PORT): passerelle de niveau application (ALG (rfc) ou helper (netfilter)
  - 2) utiliser un mandataire (proxy) ftp avec une adresse publique.

paquets/connexions/sessions

- paquets
- connexions
- sessions
- traitement à état (« statefull »)
- passerelles de niveau application (ALG: Application Layer Gateway, helper dans la terminologie Netfilter)

Configuration d'un routeur NAPT 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 (ràf: 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

Coupes-feux

- Coupe Feu: généralités, problèmatique
- Filtre de paquet: exemples d'utilisation, limitations
- coupefeu à états: notion d'état, exemples
- Limitation des pares-feux
- limitation des pares feux à état
- bibliographie

Coupe Feu: généralités

- termes équivalents : parefeu, coupefeu, garde barrière (US: firewall)
- élément d'une politique de sécurité :
  - Buts possibles:
    - protéger les postes internes des attaques
    - interdire la fuite des données de l'entreprise (cas d'un espion en interne)
    - contrôler les accès réseau des programmes présents sur un poste de travail
  - Moyens:
    - filtrer/interdire le trafic non autorisé/dangereux,
    - laisser passer le trafic légitime
    - modifier les paquets (NAT, REDIRECT, mandataire transparent, ...)

Divers types de coupes-feux

- terme recouvrant des réalités variées :
  - filtre de paquet
  - coupe feu à état
  - mandataire (proxy applicatif)
  - coupe feu personnel
- agissant à des niveaux variés:
  - couche liaison
  - couche réseau/transport
  - couche application

objet du thème: coupe feu pour sécurité périmétrique

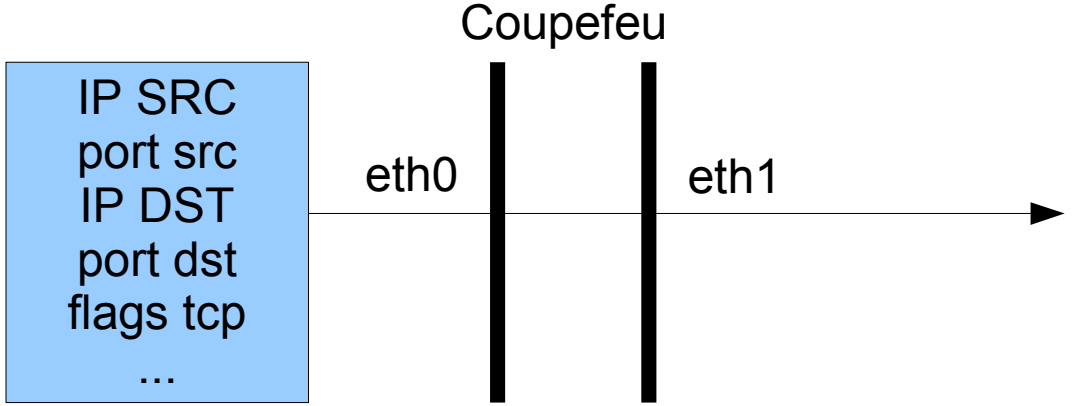
- sécurité périmétrique
- indispensable mais insuffisante contre les ennemis de l'intérieur:
    - WeB, mail,portable ramenés à la maison puis dans l'entreprise, vpn, ...
  - ces accès directs aux postes clients nécessitent des mesures spécifiques pas forcément compatibles avec les demandes des utilisateurs:
    - mandataire WeB avec antivirus & Co
    - relais smtp entrant avec antivirus
    - politique de sécurité stricte sur les portables, sous-réseau dédié en interne, ...

Architecture classique:

- dmz
- mandataires
- But :
  - limiter/interdire l'accès direct de/vers l'extérieur aux postes/serveurs internes
  - réserver l'accès de/vers l'extérieur à des machines ciblées, surveillées et configurées en conséquence
- ces architectures avec protection périmétrique ont quand même quasiment fait disparaître les attaques directes.

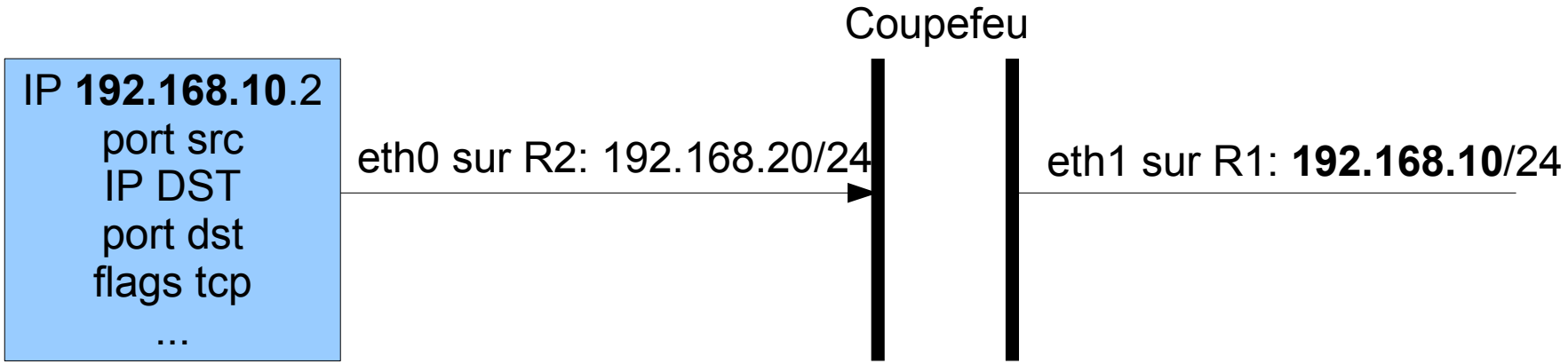
Filtre de paquet

- analyse les paquets indépendamment les uns des autres
- critères de filtrage:
  - paquet IP: IP src, IP destination, ports sources et destination
  - interface réseau sur laquelle se présente le paquet



Filtre de paquet: exemples typiques (1)

- filtrage de paquet avec une source sur un sous-réseau incorrect:
  - le coupe feu ne doit pas accepter sur eth0 des paquets ayant une IP source sur R1 (eth1)



Filtre de paquet: exemples typiques (2)

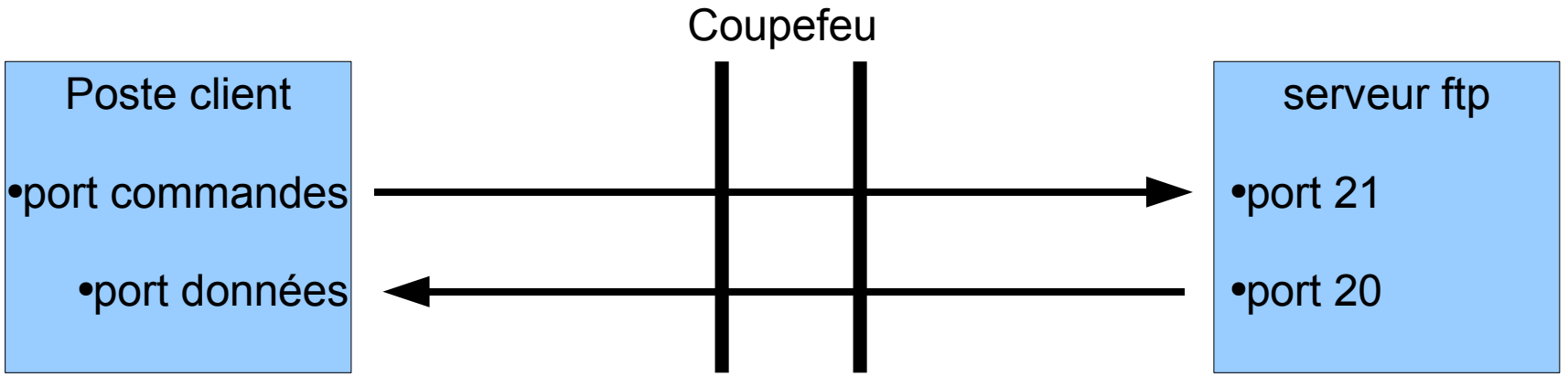
- autorisation des accès au WeB (http: tcp/80, https: tcp/443)
- en sortie: paquet vers le port 80 de toute machine externe
- paquet retour: paquet depuis le port 80 de toute machine externe
- Problème: tout paquet venant de l'extérieur et ayant le port 80 comme port source sera autorisé.
- dans la vraie vie, on utilise un mandataire WeB (proxy WeB) qui est la seule machine visible de l'extérieur

Filtre de paquet: exemples typiques (3)

- connexion tcp: l'ouverture de session est déterminée par les flags des segments
- exemple: autoriser uniquement les connexions tcp sortantes:
  - paquets tcp sortant avec flag SYN: OK
  - paquet tcp entrant avec flags Syn+Ack: OK
  - paquets tcp entrant ou sortant sans flag SYN: OK
- Questions :
  - comment réagit une machine qui reçoit un paquet syn/ack comme premier paquet d'une connexion tcp ?
  - est-il pertinent de faire confiance aux drapeaux des segments ?

Filtre de paquet: exemples typiques (4): ftp

- le port «données» est négocié dans la session
- on peut juste le supposer >= 1024



Filtre de paquets: bilan

- analyse paquet par paquet
- simple à implémenter
- syntaxe simple s'appuyant sur les propriétés du paquet (interface réseau entrante comprise)
- pas de suivi de l'historique des paquets
  - => manque de souplesse pour les autorisation
  - choix entre trop fermer (ne pas rendre le service) ou trop ouvrir (ne plus protéger)
  - cf exemple accès WeB sortant