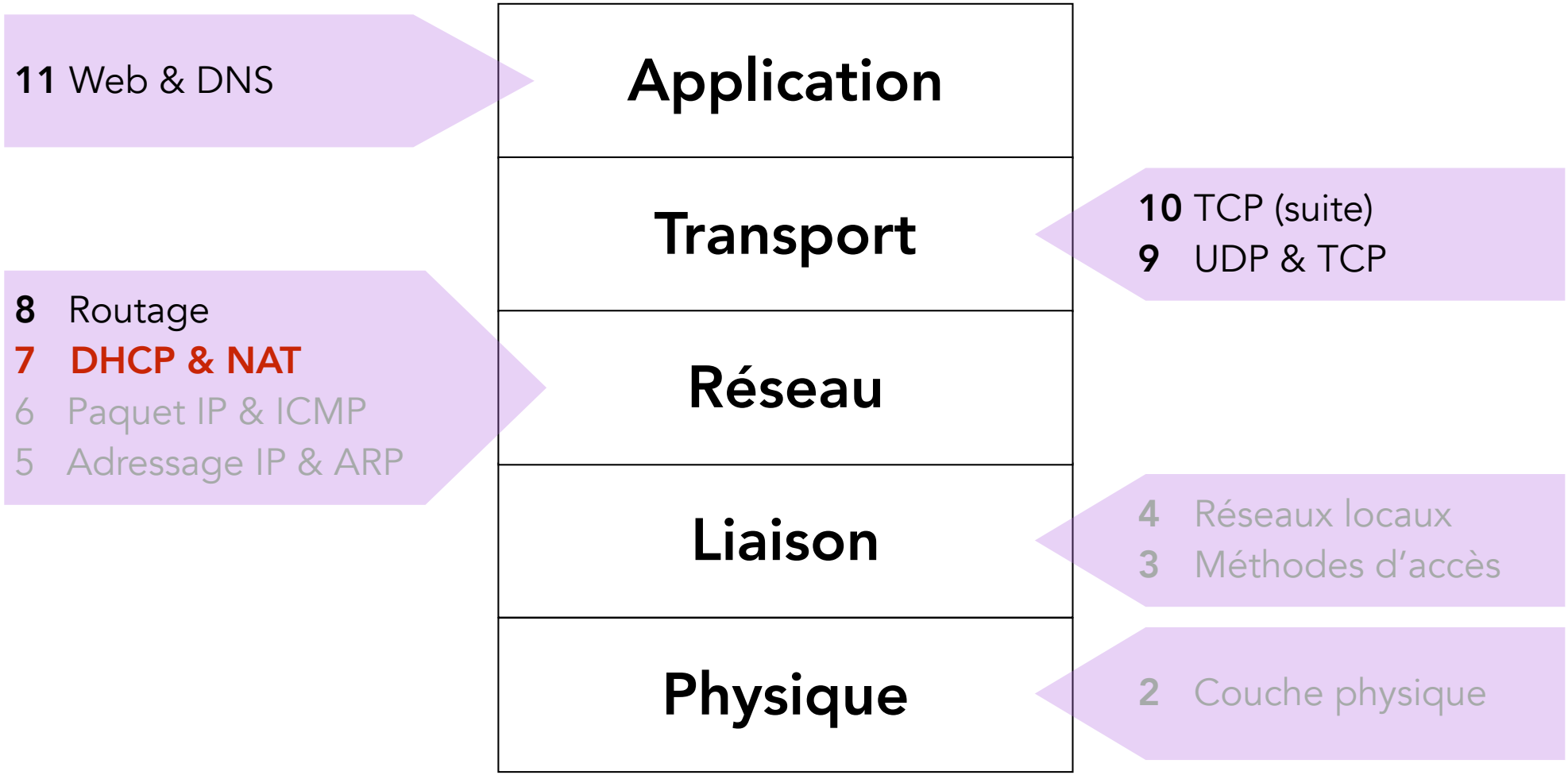
Couche Réseau
DHCP & NAT

UE LU3IN033 Réseaux
2023-2024

Bruno Baynat
Bruno.Baynat@sorbonne-universite.fr

Programme de l'UE LU3IN033



Plan du cours

- Découverte et configuration des paramètres réseau
  - Statique (manuelle)
  - Dynamique (à la demande) : DHCP
- DHCP (*Dynamic Host Configuration Protocol*)
  - Obtention des paramètres réseau
  - Renouvellement de bail
  - Libération de bail
  - Relais DHCP
- NAT (*Network Address Translation*)
  - Adresse IP privées vs adresse IP publique
  - Dissimulation des adresses privées au moyen de boîtiers NAT

L'Internet en pratique

- Les machines hôtes sont mobiles
  - leur adresse IP change selon leur position (DHCP et NAT)
- Les adresses IPv4 disponibles sont épuisées
  - attribution des adresses IP à la demande (DHCP)
  - utilisation d'adresses IP privées (NAT)
- Les attaques sont nombreuses
  - surveiller le traffic entrant dans un réseau (IDS)
  - bloquer les paquets malveillants ou indésirables (*firewall* et NAT)
- Les performances doivent être assurées
  - contrôler l'utilisation de la bande passante (régulateur de trafic)
  - mettre en mémoire les contenus populaires à proximité des clients (*proxy*)
- Les box internet assurent toutes ces fonctions (DHCP, NAT, firewall, proxy, …)

Paramètres réseau

Paramètres réseau qu'une machine doit connaitre pour communiquer sur Internet

Informations la concernant

- son adresse IP (adresse source de ses paquets)
- le masque de son sous-réseau (pour déterminer si une destination est située sur le même réseau)
- l'adresse IP de la *gateway* (pour joindre une destination située sur un réseau distant)
- l'adresse IP du serveur DNS local (pour connaitre l'adresse IP de la destination à partir de son nom)
- son adresse MAC (adresse source de ses trames)
- Tous ces paramètres à l'exception de son adresse MAC peuvent être configurés
  - manuellement
  - dynamiquement : protocole DHCP

Informations sur la destination

- Destination locale
  - l'adresse IP de la destination (DNS)
  - l'adresse MAC de la destination (ARP)
- Destination distante
  - l'adresse IP de la destination (DNS)
  - l'adresse IP de la *gateway* (configuration manuelle ou DHCP)
  - l'adresse MAC de la *gateway* (ARP)

Mécanismes de résolution d'adresses

- *Dynamic Host Configuration Protocol* (DHCP)
  - Découvrir son adresse IP
    - l'adresse source de mes paquets
  - … et d'autres paramètres sur le réseau local
    - masque du sous-réseau, adresse de la passerelle par défaut, adresses du serveur DNS local

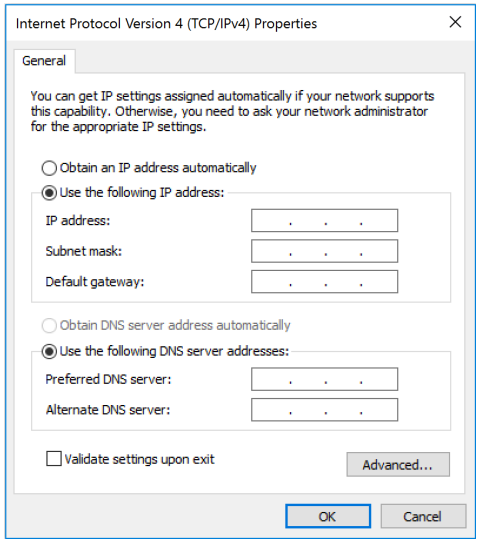
- *Domain Name System* (DNS)
  - Découvrir l'adresse IP d'une destination connaissant son nom

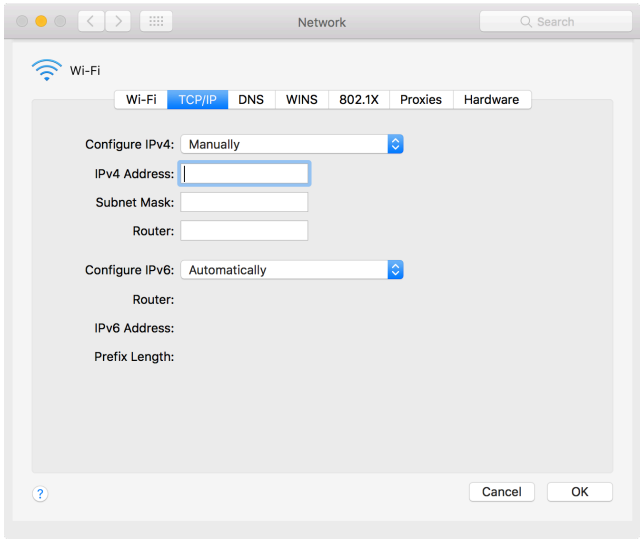
- *Address Resolution Protocol* (ARP)
  - Découvrir l'adresse MAC d'une destination locale connaissant son adresse IP

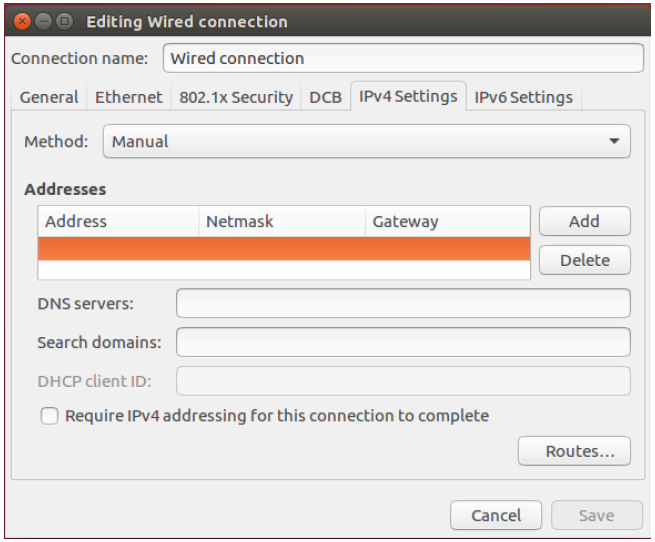
DHCP
Configuration dynamique des machines hôtes

Configuration manuelle des paramètres réseau

- Paramètres spécifiés par l'administrateur réseau
  - configurés manuellement
  - dans un fichier système lu au démarrage
    - Windows : control-panel->network->configuration->tcp/ip->properties
    - MAC OS : /System/Applications/System Settings.app
    - UNIX : /etc/rc.config







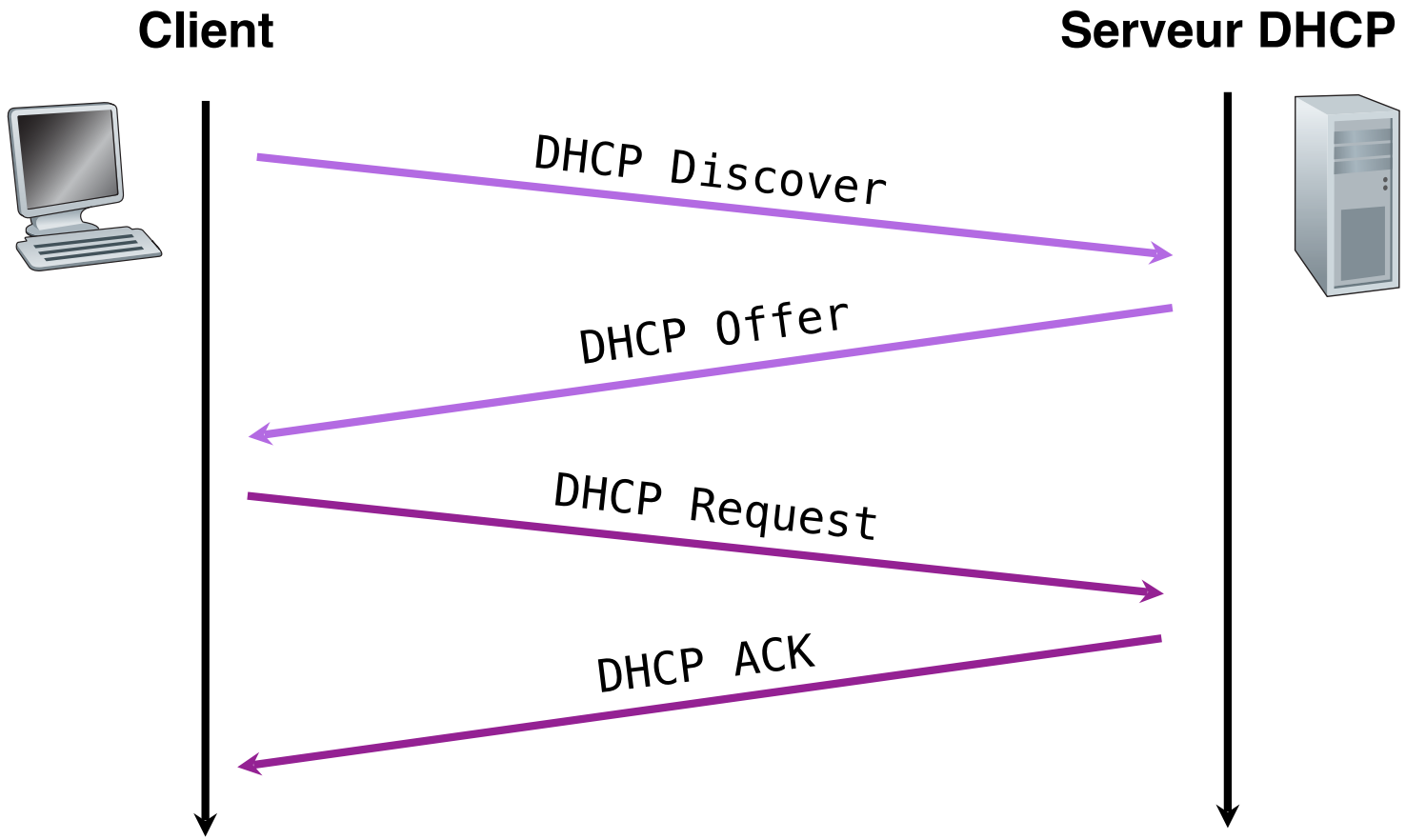
DHCP

- *Dynamic Host Configuration Protocol*
- Pour éviter la configuration manuelle
- Remplace le protocole BOOTP (*Boostrap Protocol*)
- Une machine hôte qui « apparaît » sur un réseau contacte un serveur DHCP afin d'obtenir ses paramètres réseau
  - son adresse IP
  - le masque du sous-réseau sur lequel elle est connectée
  - l'adresse de la *gateway*
  - les adresses IP du serveur DNS local (primaire et secondaire)
- Tous ces paramètres sont obtenus pour une certaine durée : bail (*lease time*)
  - avant l'issue du bail
    - la machine peut demander son renouvellement
  - à l'issue du bail
    - l'adresse IP peut être allouée à une autre machine
  - à tout moment une machine peut décider de libérer son adresse IP

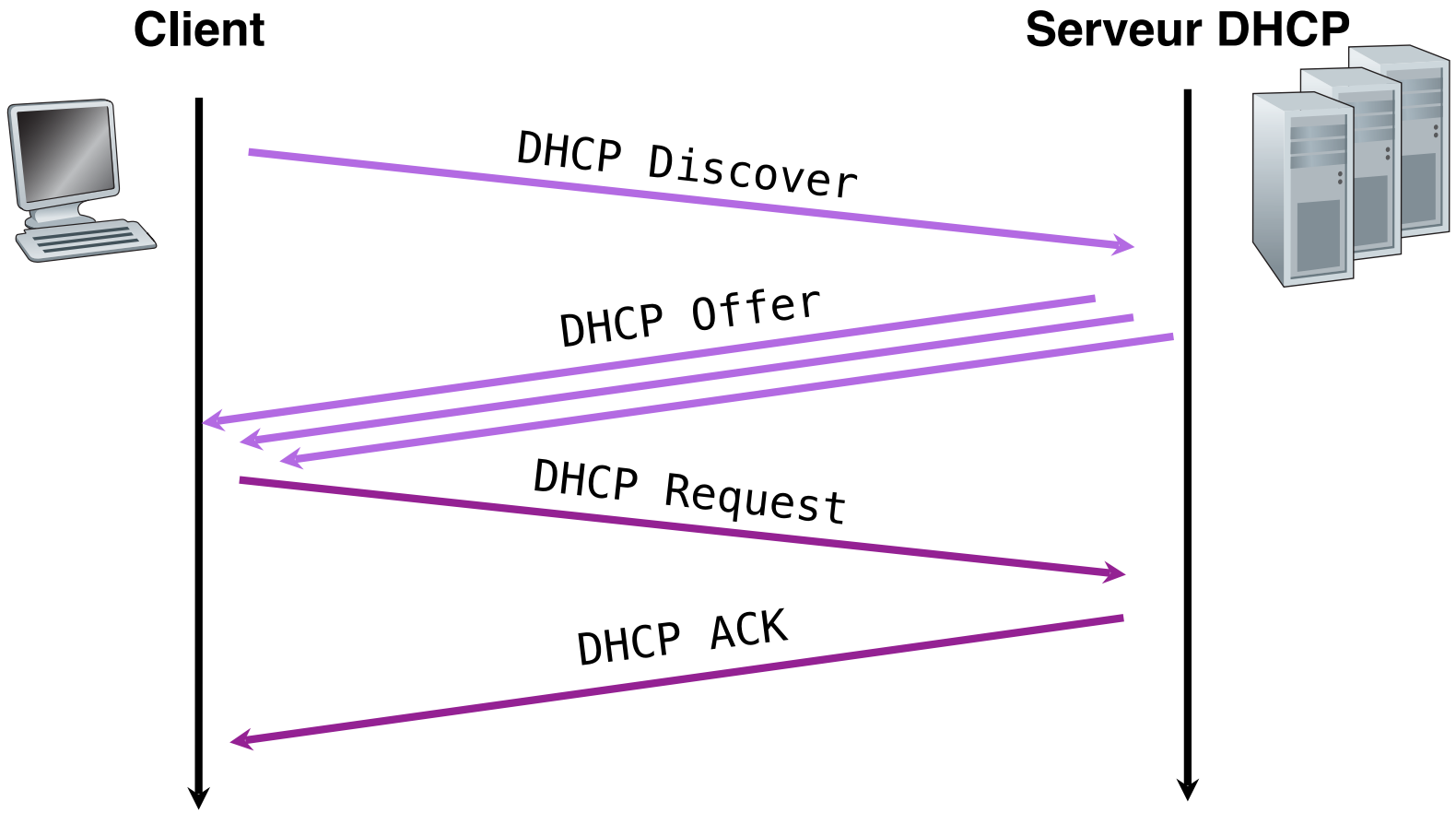
Echange DHCP initial

- La machine hôte diffuse un message « DHCP Discover »
  - pour localiser un serveur DHCP
- Le(s) serveur(s) DHCP répond(ent) avec un message « DHCP Offer » contenant
  - les paramètres réseau (adresse IP, masque, gateway, DNS locaux, ...)
  - la durée du bail associé (durée de validité de ces paramètres)
- La machine hôte choisit une offre et envoie un message « DHCP Request » au serveur correspondant
  - contenant les paramètres proposés dans l'offre qu'il a acceptée
- Le serveur DHCP sélectionné confirme son offre en envoyant un message « DHCP ACK »
  - pour finaliser l'offre
  - les autres serveurs comprennent que leur offre n'a pas été retenue
- Encapsulation des messages DHCP
  - DHCP ⊂ UDP ⊂ IP ⊂ Ethernet
- Les 4 messages sont diffusés (au niveau MAC et au niveau IP)

Echange DHCP initial



Echange DHCP initial

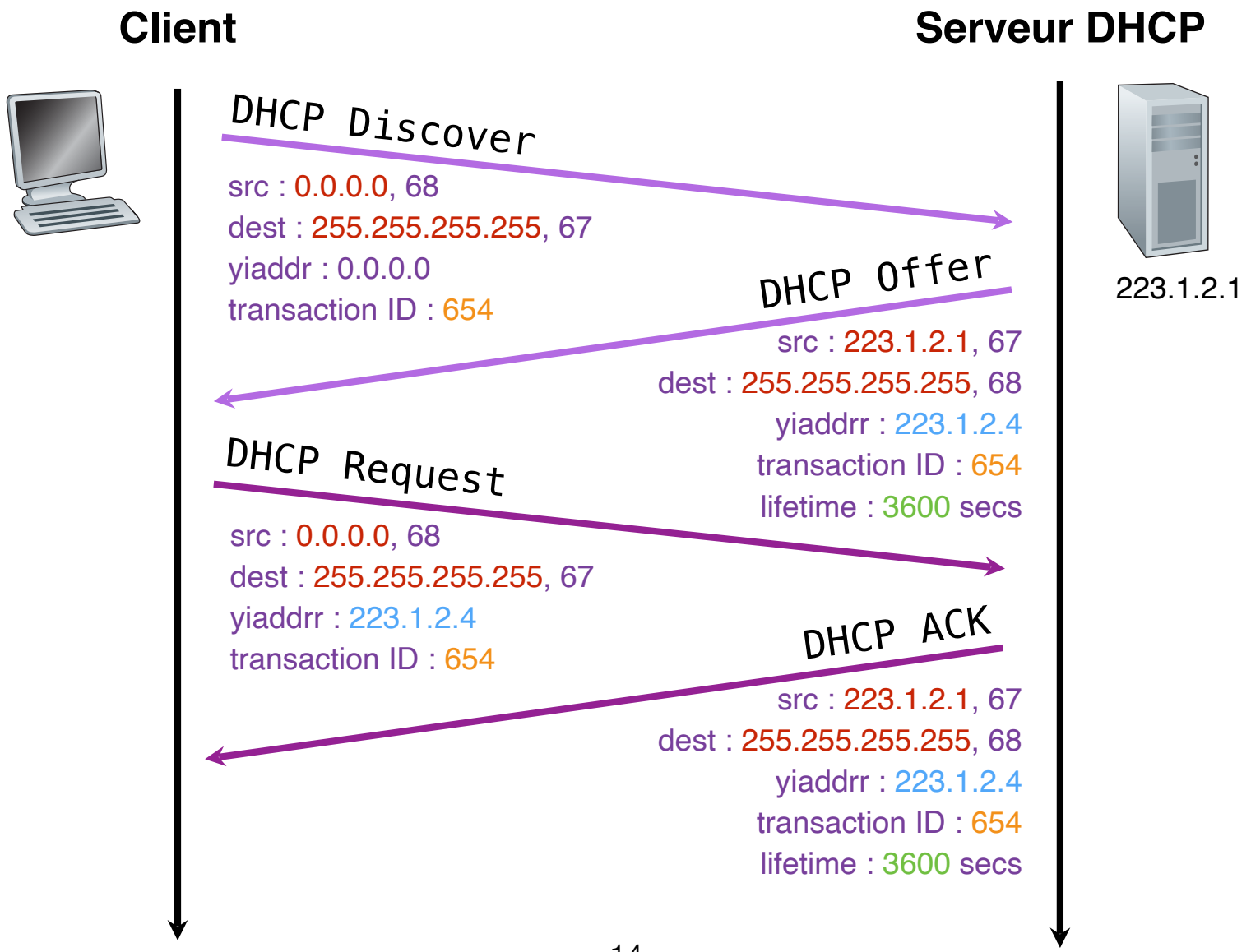


- Plusieurs serveurs peuvent répondre
  - plusieurs serveurs sur un même réseau physique pour palier aux pannes
  - le client choisit une des offres proposées par les différents serveurs

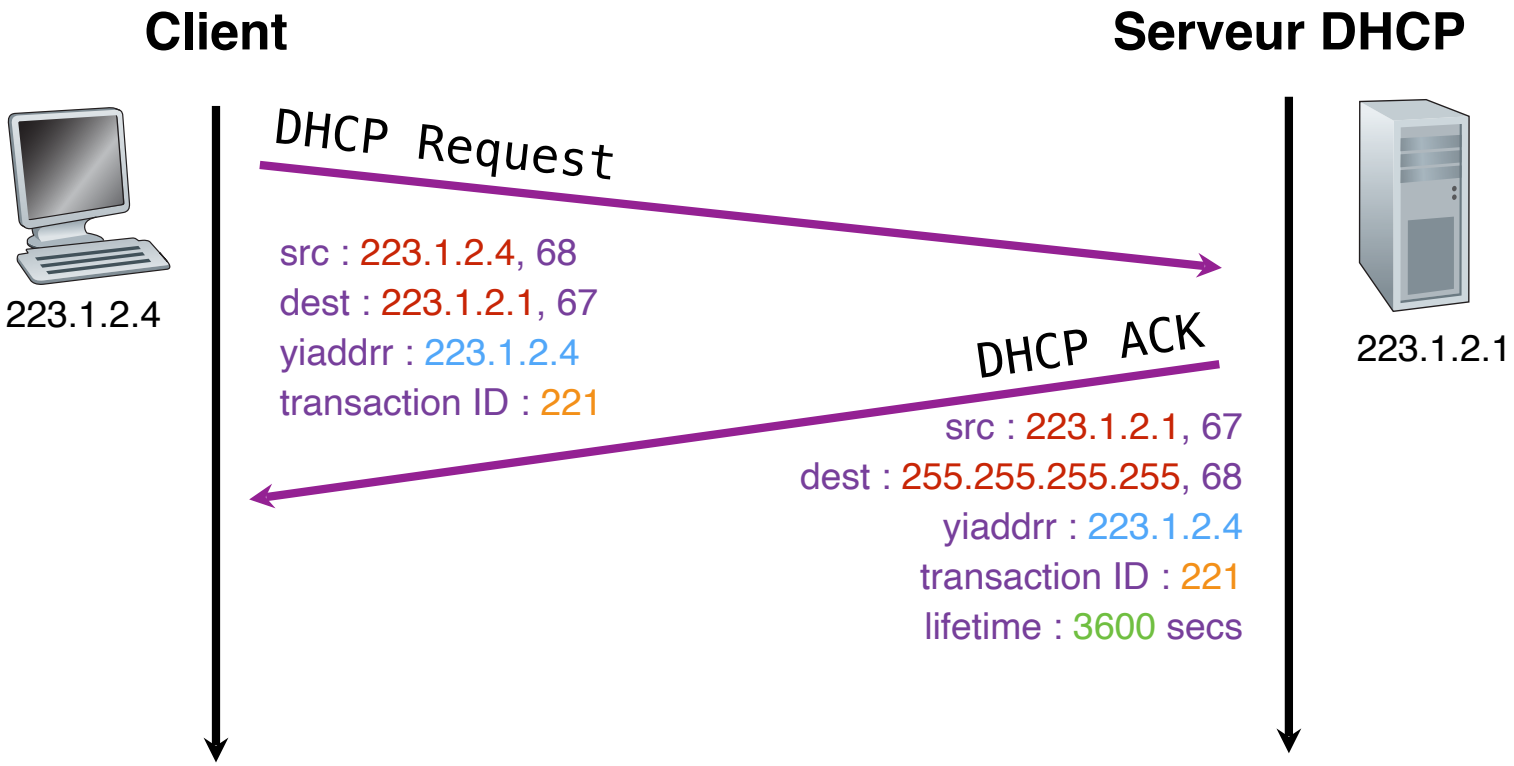
Allocation d'adresses IP

- Afin d'attribuer des adresses IP aux machines, DHCP dispose d'un pool d'adresses
  - plage d'adresses (*address range*)
  - il est possible de définir plusieurs plages
- Lors de l'utilisation de plusieurs serveurs DHCP, l'intersection des plages d'adresses des différents serveurs doit être vide
- Les adresses qui ne figurent dans aucune plage peuvent faire l'objet d'affectations statiques
  - machines nécessitant une adresse IP invariable dans le temps
    - serveurs, routeurs, imprimantes réseau, …
  - DHCP attribuera toujours la même adresse IP à une machine possédant une adresse MAC connue

Echange DHCP initial

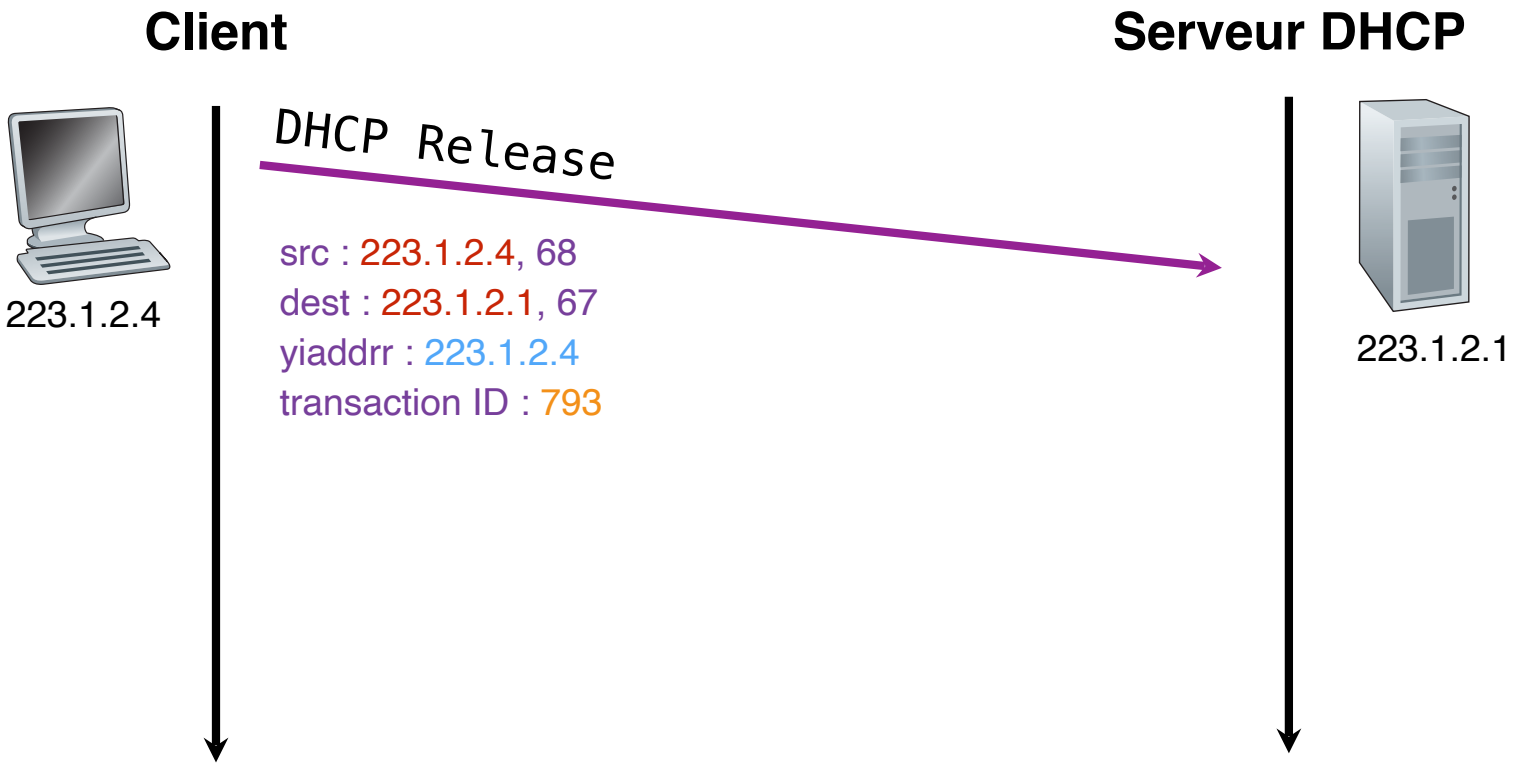


Renouvellement de bail



- Avant l'expiration du bail, une machine peut demander son renouvellement
  - le client envoie un message "DHCP Request" au serveur ayant proposé l'offre initiale
  - généralement à la moitié du bail

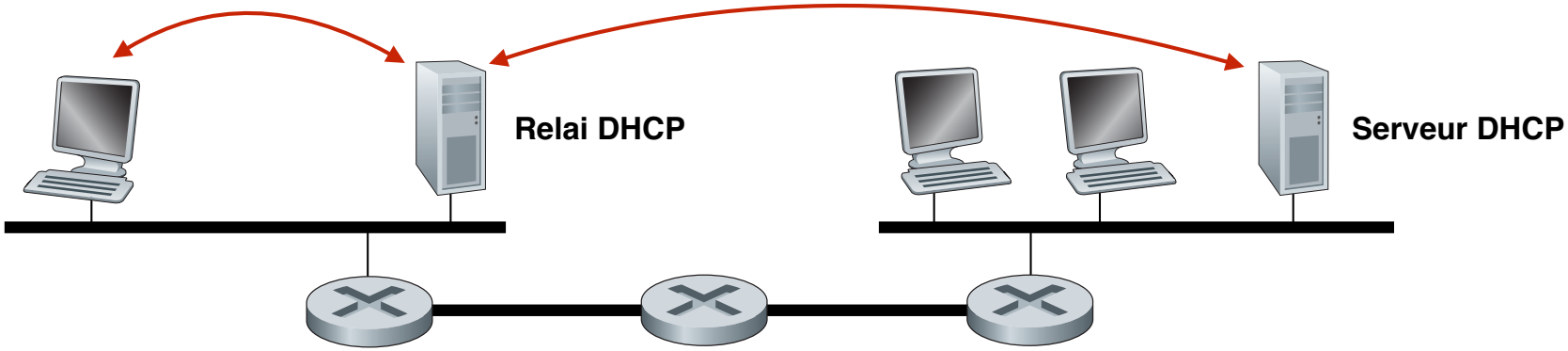
Libération de bail



- A tout moment, une machine peut libérer son adresse IP
  - le client envoie un message “DHCP Release“ au serveur ayant proposé l’offre initiale
  - l’adresse IP est alors utilisable par une autre machine

Relai DHCP

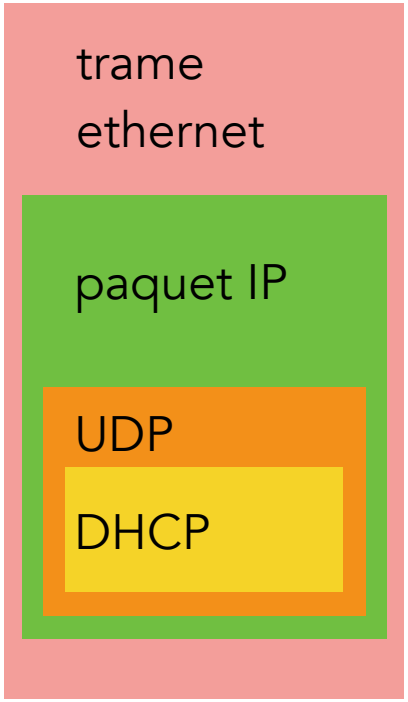
- Un serveur DHCP ne peut répondre qu'à une machine hôte connectée sur le même réseau physique que lui
- Un réseau local peut être constitué de différents sous-réseaux connectés par des routeurs
  - un routeur ne réachemine pas les messages IP broadcastés
- Afin d'éviter la multiplication des serveurs DHCP
  - un relai DHCP est installé sur chaque sous-réseau
    - machine dédiée ou fonction prise en charge par un routeur
  - le relai intercepte les messages DHCP des clients et les retransmet au serveur
    - de façon totalement transparente pour le client



Encapsulation

- DHCP est un protocole de niveau applicatif (5)
- Les messages DHCP utilisent le protocole de transport UDP
  - numéro de port coté serveur : 67
  - numéro de port coté client : 68
- Format des messages

op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
cidaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options			



Principes communs à DHCP et ARP

- Les réseaux locaux sont des réseaux à diffusion naturelle
  - Les requêtes DHCP ou ARP sont encapsulées dans une trame envoyée à l'adresse MAC de diffusion FF:FF:FF:FF:FF:FF
  - Toutes les stations du réseau local inspectent le contenu de la trame
    - pour une requête DHCP, seuls les serveurs (et les relais) DHCP répondent
    - pour une requête ARP, seule la destination visée répond
- La diffusion est coûteuse
  - Consommation de resources en réception pour l'ensemble des stations du réseau local
  - Mémorisation des réponses : installation d'états
- Suppression et mise à jour des informations stockées
  - Limiter la durée de vie (TTL) des informations mises en mémoire
    - suppression des informations à l'expiration du TTL
  - Le TTL assure la cohérence des états installés dans le réseau et en limite le nombre

Adresses IP privées et NAT

Network Address Translation

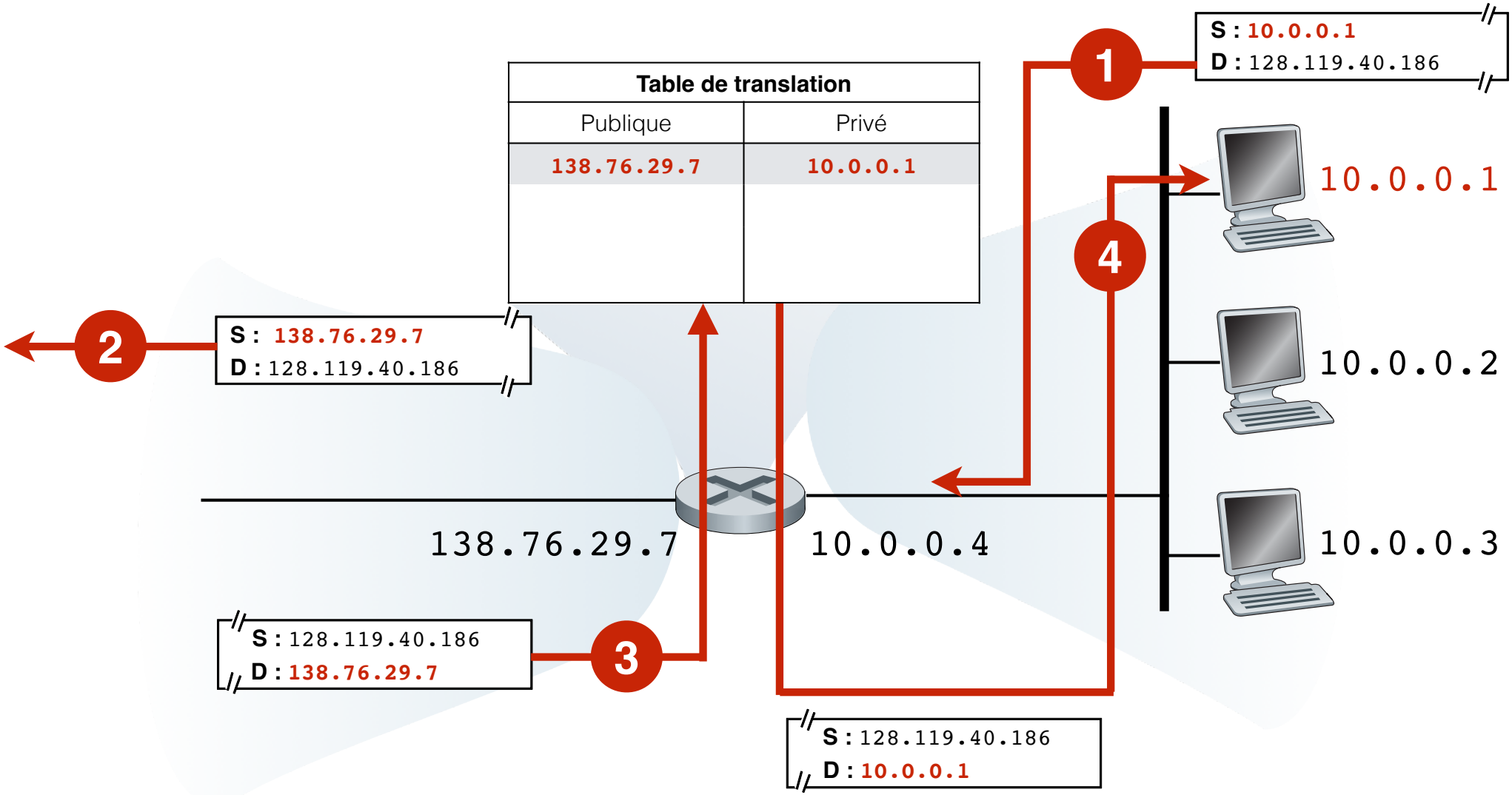
- Répond au problème d'épuisement des adresses IPv4
  - prédit depuis le début des années 90
  - date de début des travaux sur IPv6
- Solution intermédiaire
  - réutilisation d'une même adresse IP pour identifier plusieurs machines
  - … sans modifier le comportement des machines hôtes
- Proposé comme une solution à court/moyen terme
  - NAT est largement déployé
  - … largement plus que IPv6

Translation d'adresses

- NAT utilise des adresses IP privées
  - Classe A : 10.0.0.0 à 10.255.255.255
  - Classe B : 172.16.0.0 à 172.31.255.255
  - Classe C : 192.168.0.0 à 192.168.255.255
  - non routables sur internet
  - réutilisables
- NAT remplace les adresses IP des paquets sortants ou entrants
  - Les machines d'un réseau local sont vues comme une adresse IP publique unique
  - … NAT modifie l'entête en conséquence
- Trafic sortant
  - L'adresse IP source des paquets est remplacée par l'adresse IP publique du réseau
- Trafic entrant
  - L'adresse IP destination est remplacée par l'adresse IP privée de la machine de destination
- Nécessite le recalcul d'autres champs d'entête
  - checksum, …

NAT

La machine hôte **10.0.0.1** envoie un paquet à **128.119.40.186**

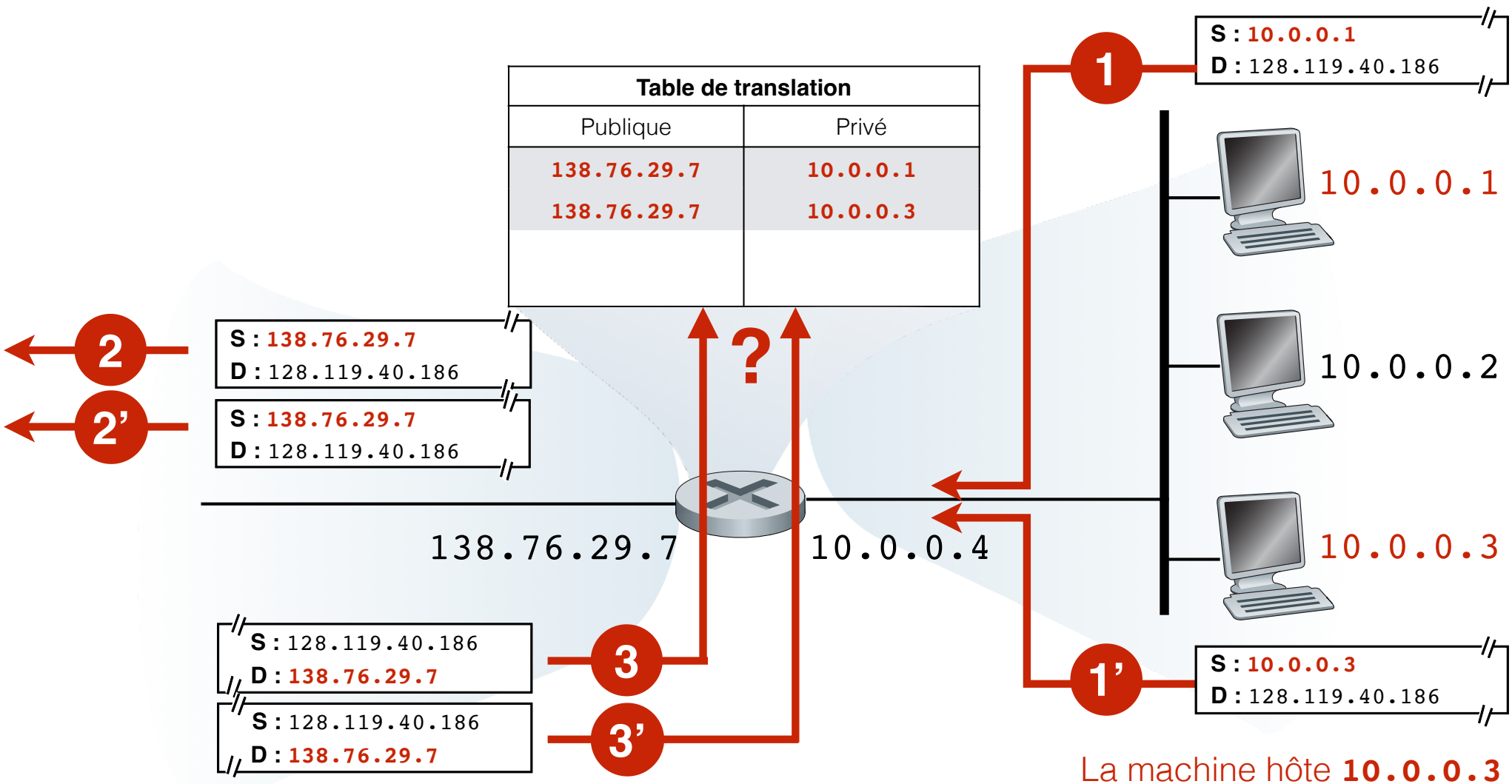


Problème

- Si deux machines hôtes tentent de se connecter au même serveur
  - l'adresse IP destination des deux paquets émis est identique
- Le protocole NAT remplace l'adresse source des paquets sortants par la même adresse IP publique
  - L'adresse IP source des deux paquets sortants est identique
- Problèmes
  - Comment différencier les deux sources côté serveur ?
  - Comment faire parvenir les réponses du serveur à la machine hôte adéquate ?

NAT

La machine hôte **10.0.0.1** envoie un paquet à **128.119.40.186**



La machine hôte **10.0.0.3** envoie un paquet à **128.119.40.186**

Solution

- Utiliser des numéros supplémentaires
  - numéros de port
  - utilisés par UDP/TCP pour identifier les applications
  - inclus dans l'entête des messages UDP/TCP (couche 4)
- Le protocole NAT remplace les numéros de port en même temps que les adresses IP
  - remplace le numéro de port source des paquets sortants par un numéro aléatoire
    - mémorisation de la correspondance dans la table NAT
  - restitue le numéro de port destination des paquets entrant initial
    - par inspection de la table NAT

NAT

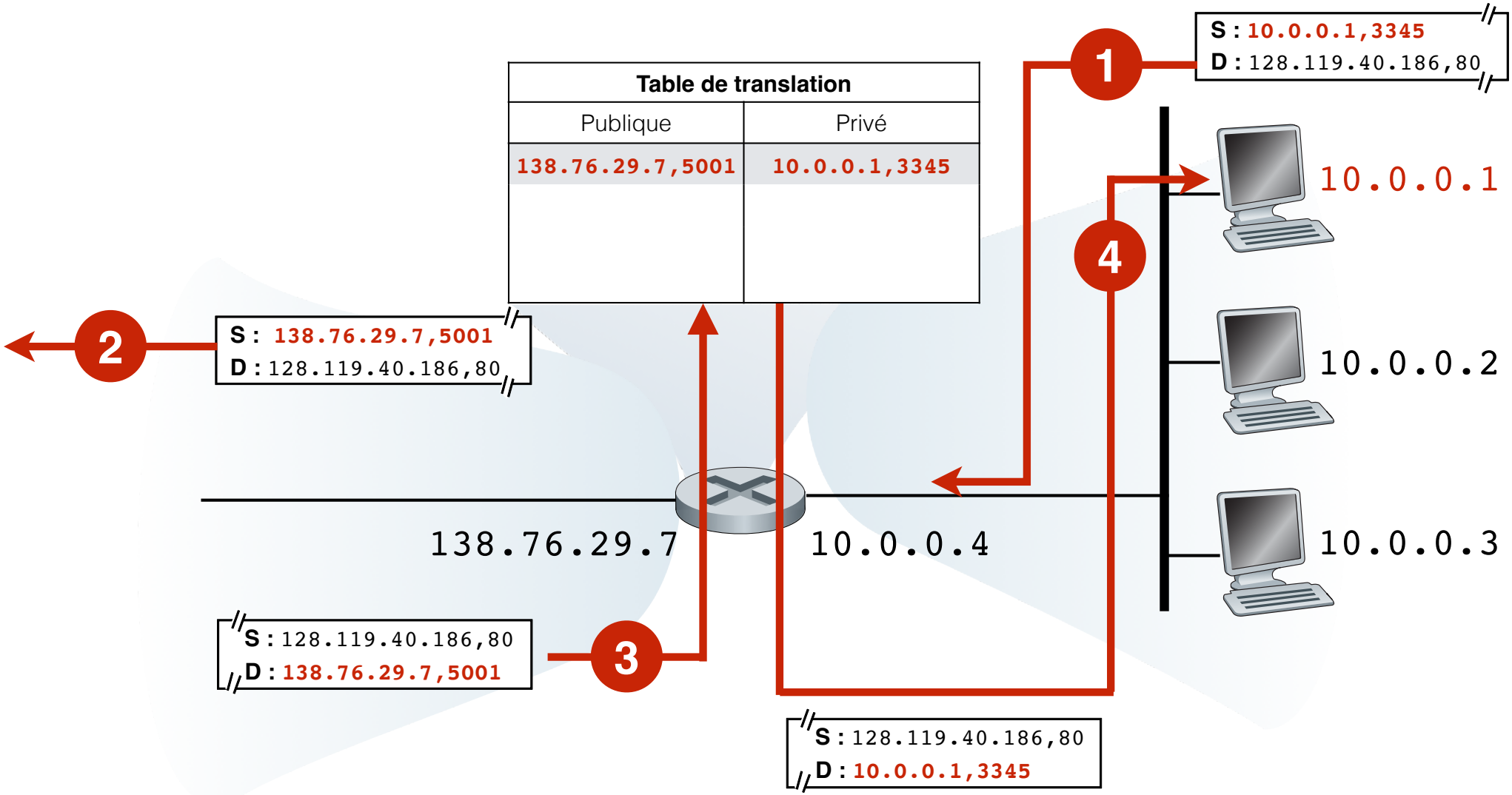


Table de translation
Publique
Privé
138.76.29.7,5001
10.0.0.1,3345
1
S : 10.0.0.1,3345
D : 128.119.40.186,80
2
S : 138.76.29.7,5001
D : 128.119.40.186,80
3
S : 128.119.40.186,80
D : 138.76.29.7,5001
4
S : 128.119.40.186,80
D : 10.0.0.1,3345
10.0.0.1
10.0.0.2
10.0.0.3
138.76.29.7
10.0.0.4

NAT

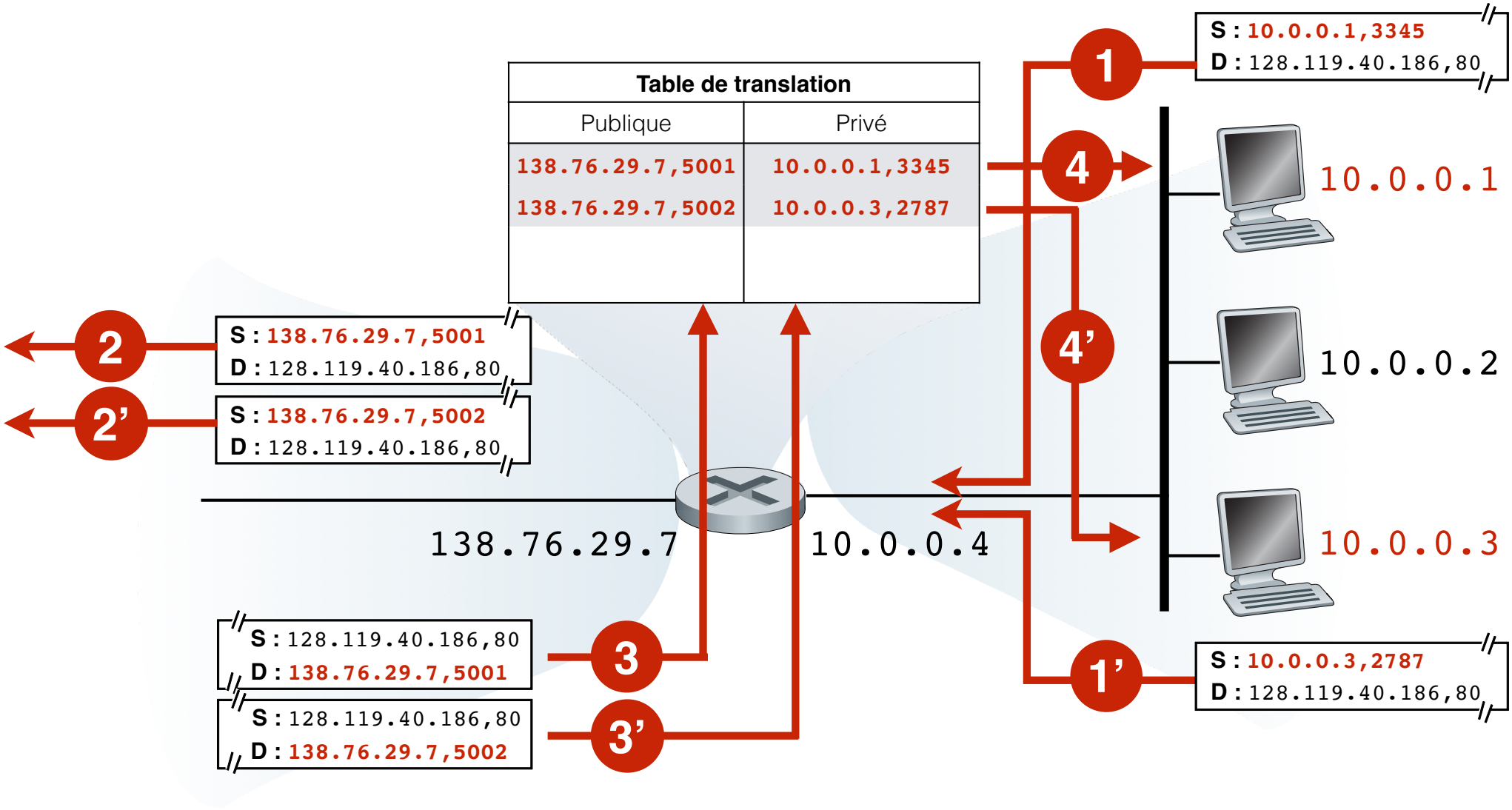


Table de translation
Publique
Privé
138.76.29.7,5001
10.0.0.1,3345
138.76.29.7,5002
10.0.0.3,2787
1
S : 10.0.0.1,3345
D : 128.119.40.186,80
4
4'
10.0.0.1
10.0.0.2
10.0.0.3
2
S : 138.76.29.7,5001
D : 128.119.40.186,80
2'
S : 138.76.29.7,5002
D : 128.119.40.186,80
138.76.29.7
10.0.0.4
3
S : 128.119.40.186,80
D : 138.76.29.7,5001
3'
S : 128.119.40.186,80
D : 138.76.29.7,5002
1'
S : 10.0.0.3,2787
D : 128.119.40.186,80

Gestion des tables de translation

- Création d'une entrée sur réception d'un paquet sortant

  @ IP source privée, port orignal, @IP publique, port translaté

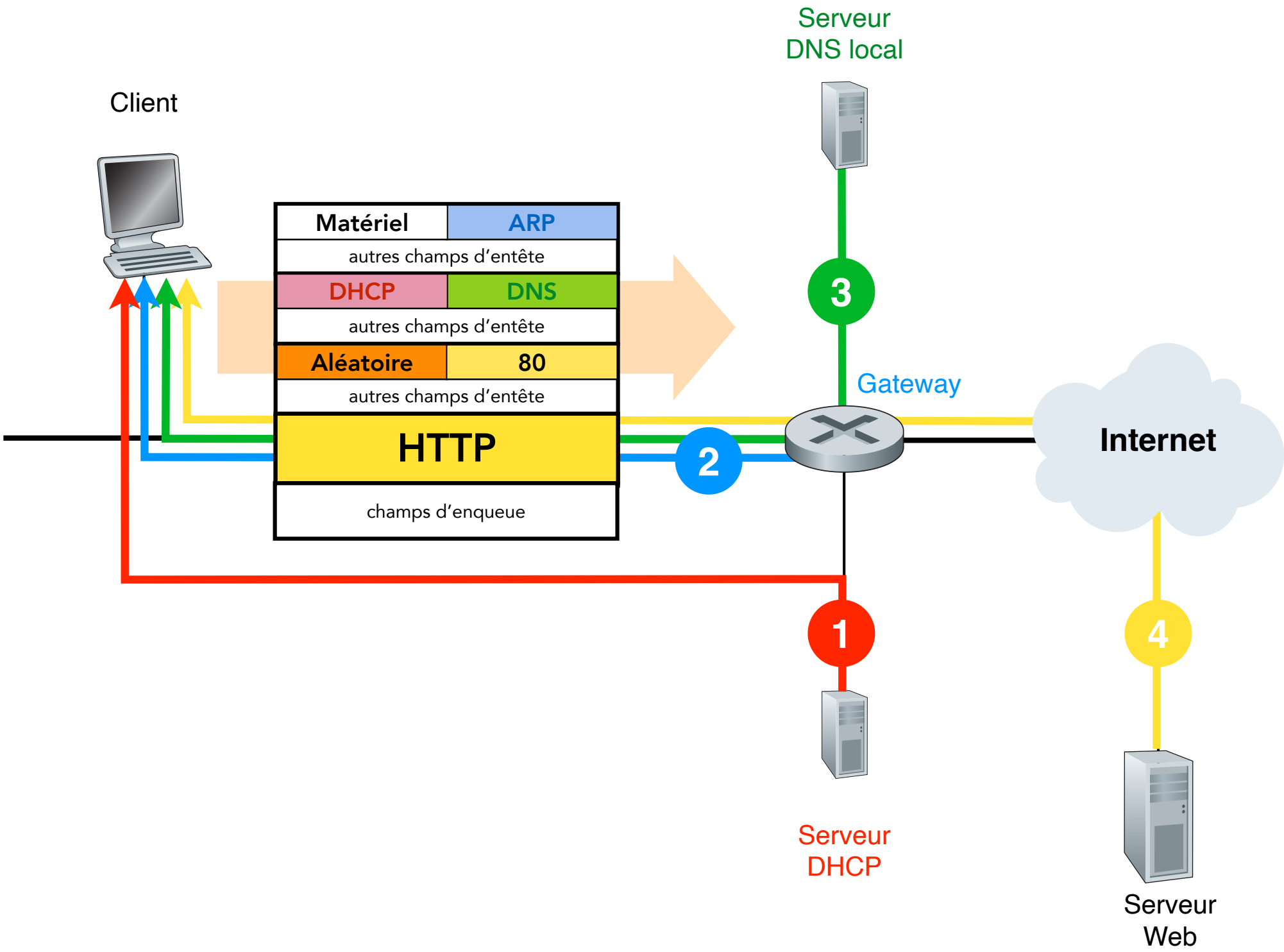
  - le numéro de port translaté sert de clé pour trouver une entrée dans la table
  - à chaque entrée est associée une durée de vie (*aging timer*)
- Suppression des entrées obsolètes de la table
  - si aucun paquet n'est reçu pendant un certain temps
  - permet de « libérer » le numéro de port translaté
- Nouvel exemple d'état « mou » (*soft state*)
  - suppression sans nécessité d'intervention extérieure explicite

Les critiques vis-à-vis de NAT

- NAT ajoute une nouvelle signification aux numéros de port (client)
  - Les numéros de port sont censés identifier les processus exécutés sur une même machine hôte
  - NAT l'utilise pour identifier les machines d'un réseau local privé
- NAT bloque les demandes de connexions entrantes
  - Comment installer un serveur sur un réseau « NATé » ?
- NAT est en porte-à-faux avec le principe de bout-en-bout
  - Le réseau n'est pas censé inspecter le contenu des paquets IP ou des messages UDP/TCP
  - … encore moins le modifier
- NAT introduit des états dans le réseau
  - Le protocole IP a été conçu en mode non connecté (*stateless*)

Où trouve-t-on les fonctions NAT ?

- Réseaux domestiques
  - une box Internet cumule les fonctions de gateway, serveur DHCP, NAT, firewall, …
  - consomme la seule adresse IP publique attribuée par le fournisseur d'accès Internet
  - … masque la présence de plusieurs machines hôtes
- Universités ou réseau d'entreprise
  - NAT est généralement situé à la jonction avec l'Internet
  - dispose d'un ensemble d'adresses IP publiques que NAT partage parmi les machines du réseau
  - évite la complexité découlant de la renumérotation des machines hôtes et des routeurs en cas de changement de fournisseur d'accès
- IPv6 est LA solution
  - … qui tarde à s'imposer


Serveur
DNS local
Client
Matériel
ARP
autres champs d'entête
DHCP
DNS
autres champs d'entête
Aléatoire
80
autres champs d'entête
HTTP
champs d'enqueue
3
Gateway
2
Internet
1
4
Serveur
DHCP
Serveur
Web

Conclusion

- DHCP permet à une machine d'obtenir automatiquement tous ses paramètres réseau
  - son adresse IP, le masque du réseau local, l'adresse de la gateway, les adresses des serveurs DNS locaux, …
- NAT identifie les machines d'un réseau local à l'aide d'adresses IP privées
  - vues de l'extérieur (le reste de l'internet) comme une seule et même adresse IP publique
  - NAT modifie les entêtes des paquets à l'insu des machines du réseau
  - NAT rompt la chaîne d'acheminent entre source originale d'un paquet et destination finale du paquet
- DHCP et NAT travaillent souvent de concert
  - DHCP utilise un pool d'adresses IP fournies par NAT

A faire

- Cours 7
  - à relire attentivement
- Devoir 7 sur Moodle
  - date de rendu : dimanche 22 octobre