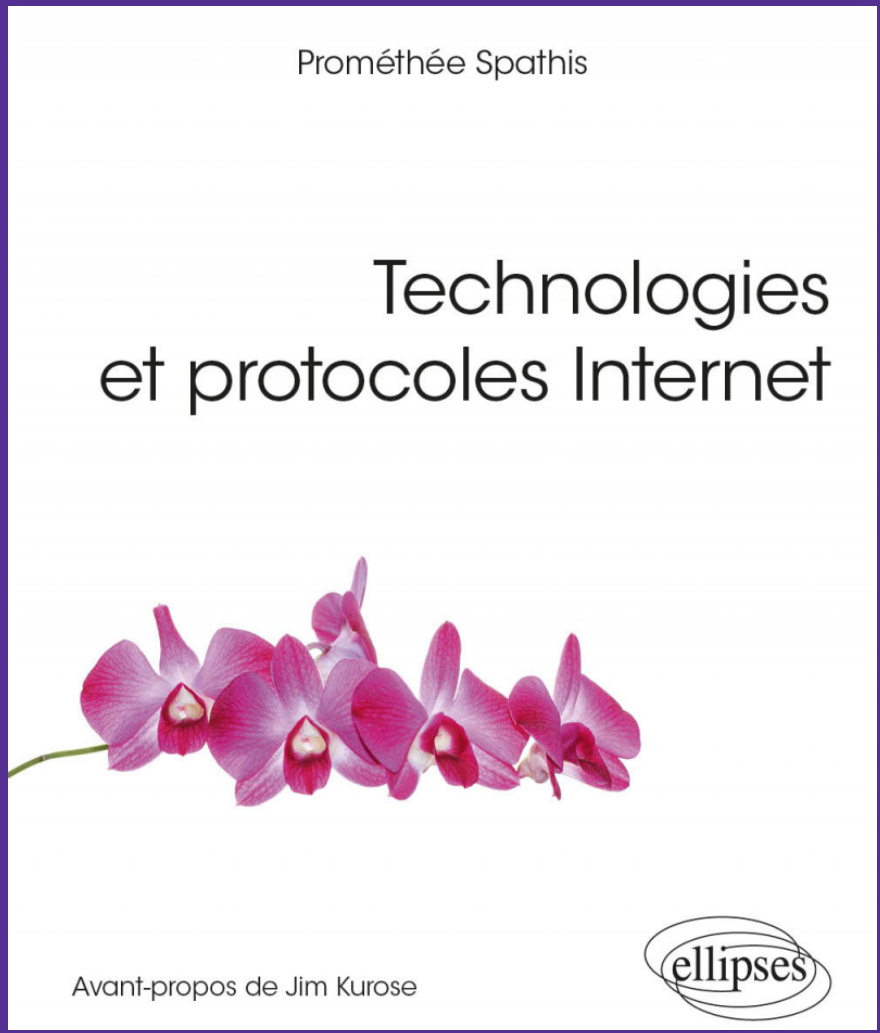
Chap 7 - DHCP, ARP & NAT

Ces transparents sont mis à disposition de tous (étudiants, enseignants, lecteurs).

En contrepartie, merci de bien vouloir :

- mentionner leur source,
- préciser la mention de copyright.

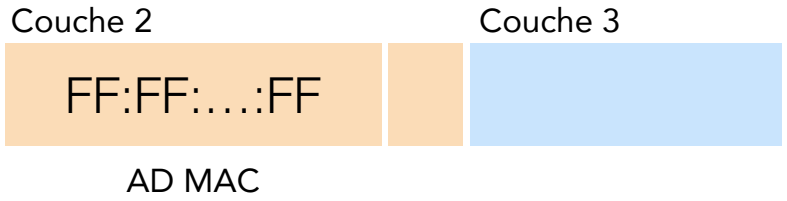
Merci et bon cours !

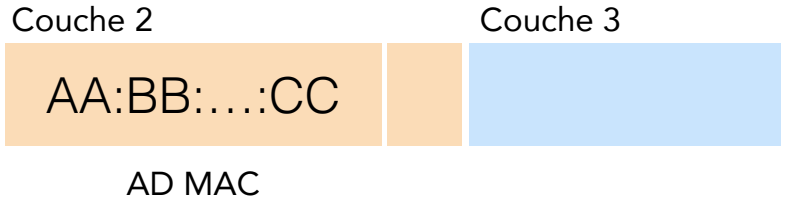


Plan du cours

- Acheminement direct vs indirect
  - Encapsulation IP dans Ethernet
  - Concordance entre adresses IP et adresses Ethernet
- Découverte et configuration des paramètres réseau
  - Statique manuelle
  - A la demande : protocole DHCP
  - ICMPv6 et DHCPv6
- Découverte de l'adresse MAC des machines voisines
  - Protocole et tables ARP
  - Découverte de voisins ICMPv6
- Adresses IP privées et NAT (Network Address Translation)
  - Plusieurs machines partagent une même adresse IP publique
  - Dissimulation des adresses privées au moyen de boîtiers NAT

Rappel sur Ethernet





Adresse Ethernet de broadcast :

- Toutes les stations du réseau local reçoivent la trame
- Toutes les stations passent le paquet encapsulé à leur couche réseau indépendamment de l'adresse IP destination

Adresse Ethernet unicast :

- Toutes les stations du réseau local reçoivent la trame
- Seule la station destinatrice passe le paquet encapsulé à sa couche réseau
- Les autres stations suppriment la trame

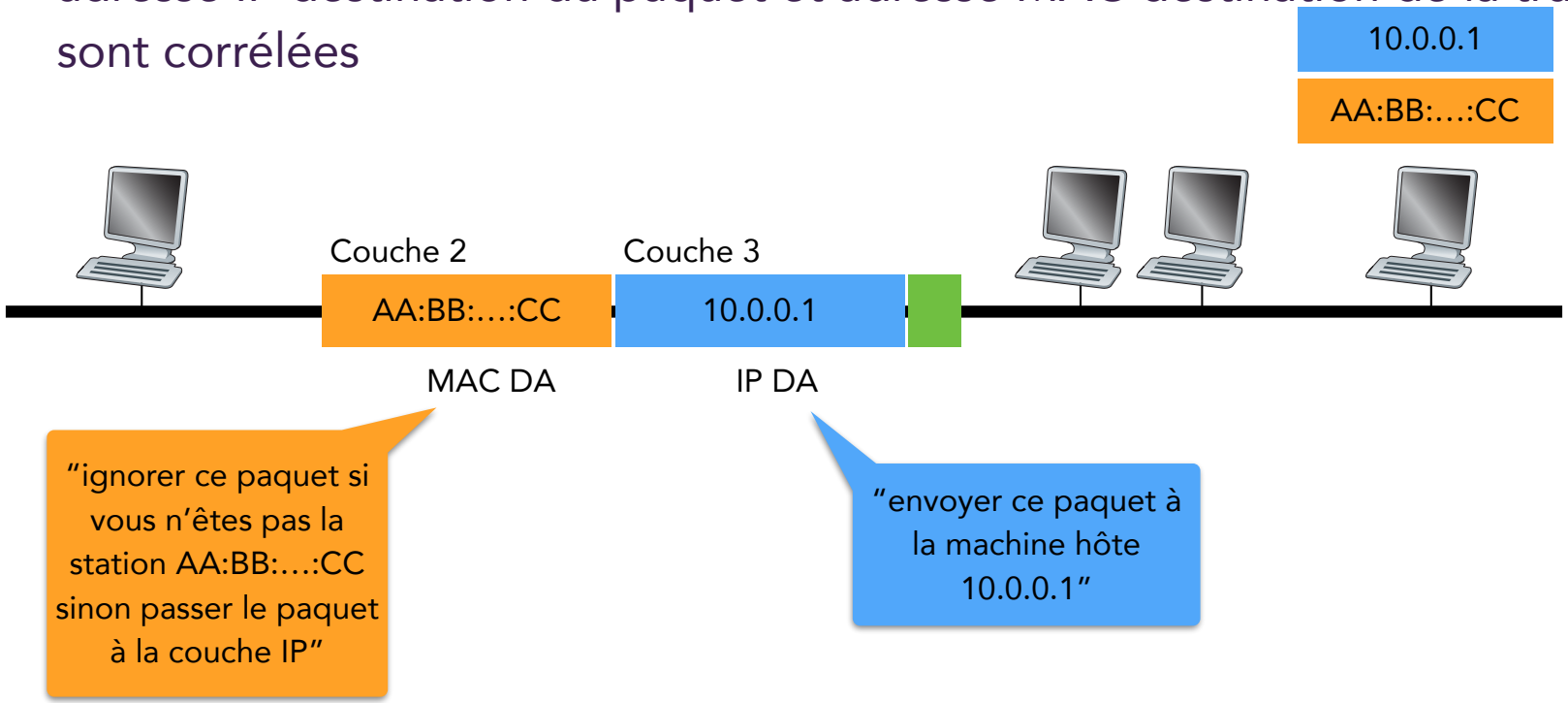
- Couche 3 (logiciel) :
  - la suppression des paquets consomme CPU et mémoire
- Couche 2 (matériel) :
  - la suppression des trames ne consomme pas de ressources logicielles

Suppression anticipée des paquets si adresses MAC et adresses IP correspondent

Envoi de paquets IP sur un lien Ethernet

Acheminement direct

- Les paquets sont encapsulés dans des trames Ethernet :
  - adresse IP destination du paquet et adresse MAC destination de la trame sont corrélées

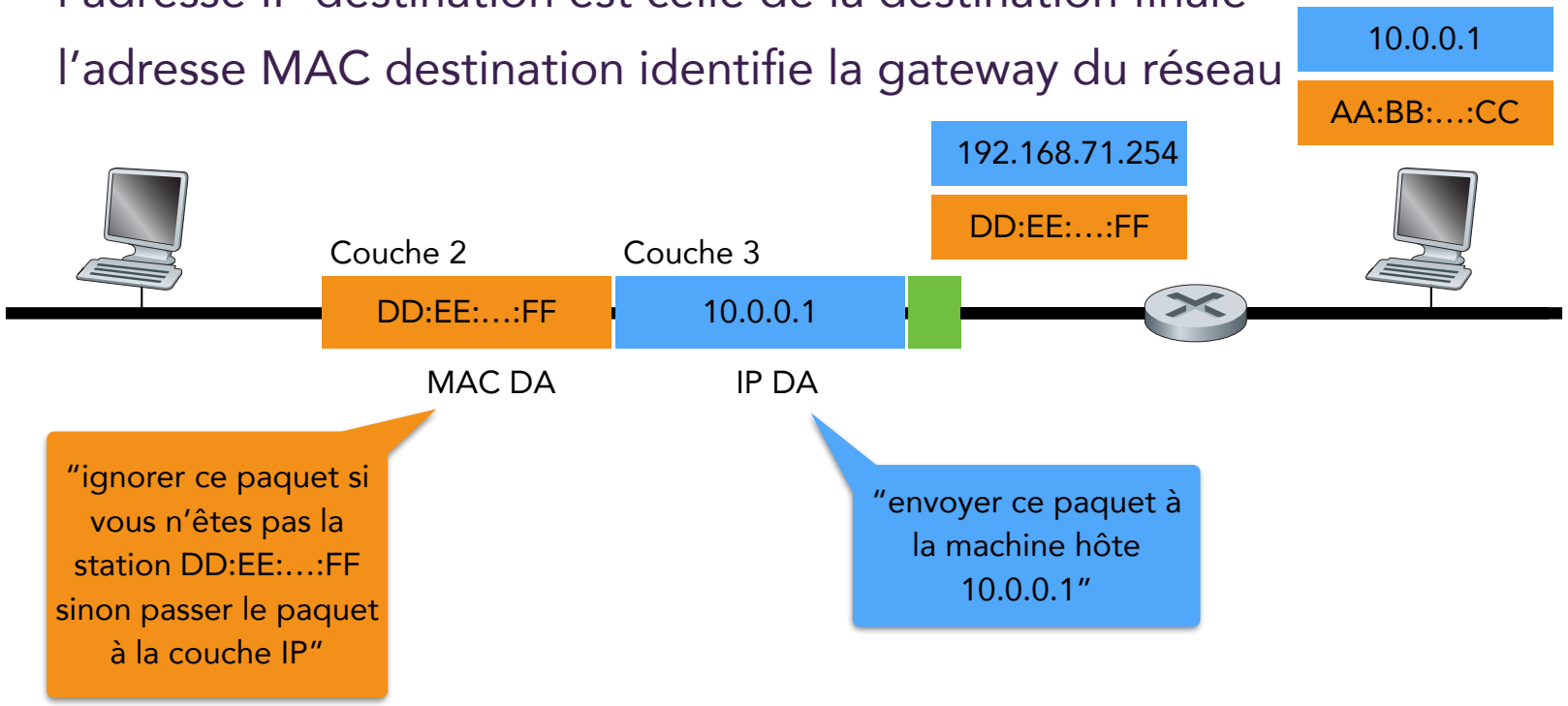


Comment fait la source pour connaitre l'adresse MAC de la destination ?

Envoi de paquets IP sur un lien Ethernet

Acheminement indirect

- Les paquets sont encapsulés dans des trames Ethernet :
  - l'adresse IP destination est celle de la destination finale
  - l'adresse MAC destination identifie la gateway du réseau



Comment fait la source pour connaitre les adresses IP et MAC du premier saut ?

Acheminement de paquet encapsulation IP dans Ethernet

Acheminement direct

Source et destination connectées au même réseau :

- adresses IP source et destination partagent le même préfixe
- l'entête IP contient les adresses IP
  - de la source
  - de la destination finale
- l'entête Ethernet contient l'adresse MAC
  - de la source
  - de la destination finale

Acheminement indirect

Source et destination connectées à des réseaux différents :

- adresses IP source et destination ont des préfixes différents
- l'entête IP contient les adresses IP
  - de la source
  - de la destination finale
- l'entête Ethernet contient l'adresse MAC
  - de la source sur le réseau initial ou du saut précédent sinon
  - de la destination finale sur le dernier réseau ou du saut suivant sinon

Comment fait la source pour savoir si une destination est voisine ?

Paramètres réseau

Les paramètres réseau qu'une machine doit connaitre pour communiquer sur Internet sont :

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 sa 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 (si communiqués par l'administrateur local)
  - dynamiquement (DHCP)

  (*) l'adresse MAC est codée en dur sur sa carte réseau

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 gateway (configuration manuelle ou DHCP)
  - l'adresse MAC de la gateway (ARP)
- Protocoles impliqués :
  - DNS : résolution des noms
  - ARP : résolution des adresses IP
  - DHCP : découverte des paramètres réseau

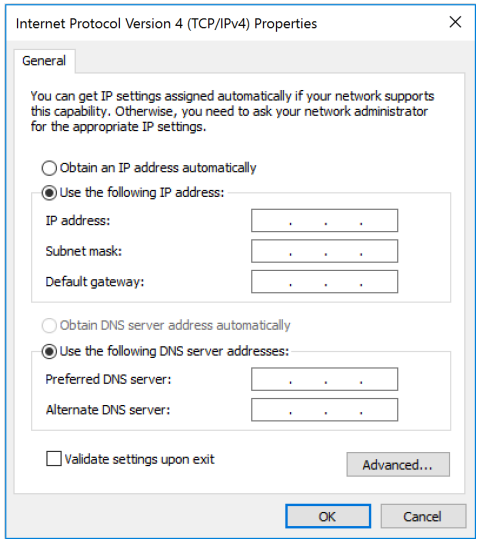
Mécanismes de résolution d'adresses

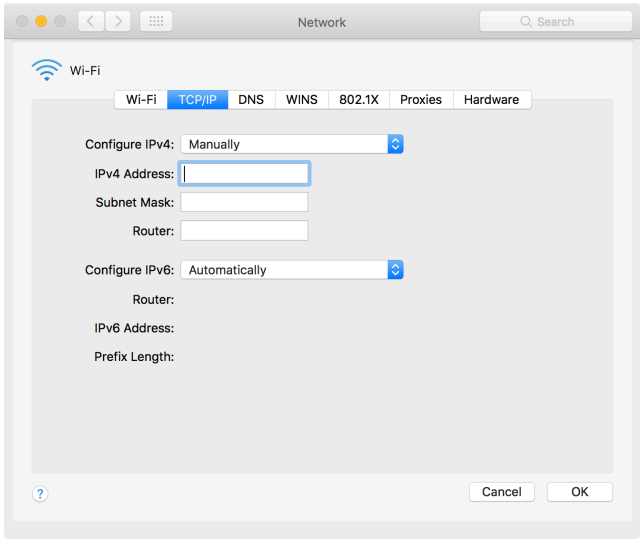
- Dynamic Host Configuration Protocol (DHCP)
  - Découvrir mon adresse IP
    - l'adresse source de mes paquets
  - … et d'autres paramètres sur le réseau local
    - masque du sous-réseau, adresse de la passerelle par défaut, adresses du serveur DNS local
- Address Resolution Protocol (ARP)
  - Découvrir l'adresse MAC d'une destination locale sachant son adresse IP
    - l'adresse MAC de la passerelle par défaut
- Domain Name System (DNS)
  - Découvrir l'adresse IP d'une destination sachant son nom
  - … et inversement.

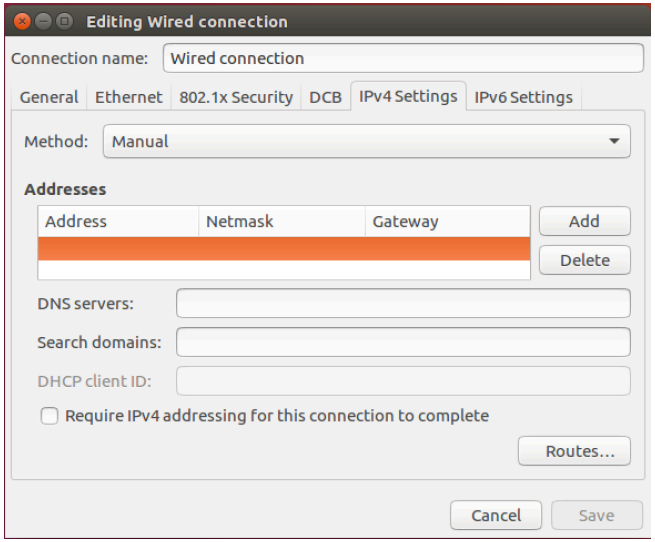
DHCP
Configuration dynamique des machines hôtes

Configuration manuelle des paramètres réseau

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







Eviter la configuration manuelle

- Dynamic Host Configuration Protocol (DHCP)
  - La machine hôte contacte un serveur qui lui communique ses paramètres réseau :
    - adresse IP (utilisable pour une durée limitée appelée bail)
    - masque du sous-réseau
    - adresse de la gateway
    - adresses IP du serveur DNS local (primaire et secondaires)
    - durée du bail
  - Comment contacter le serveur DHCP sans connaître son adresse IP ?
- Address Resolution Protocol (ARP)
  - Une machine hôte découvre l'adresse MAC d'une machine voisine dont elle connait l'adresse IP
  - Comment contacter la destination avant de connaître son adresse MAC ?
- Domain Name System (DNS)
  - Une machine hôte découvre l'adresse IP d'une machine hôte destination dont elle connait le nom

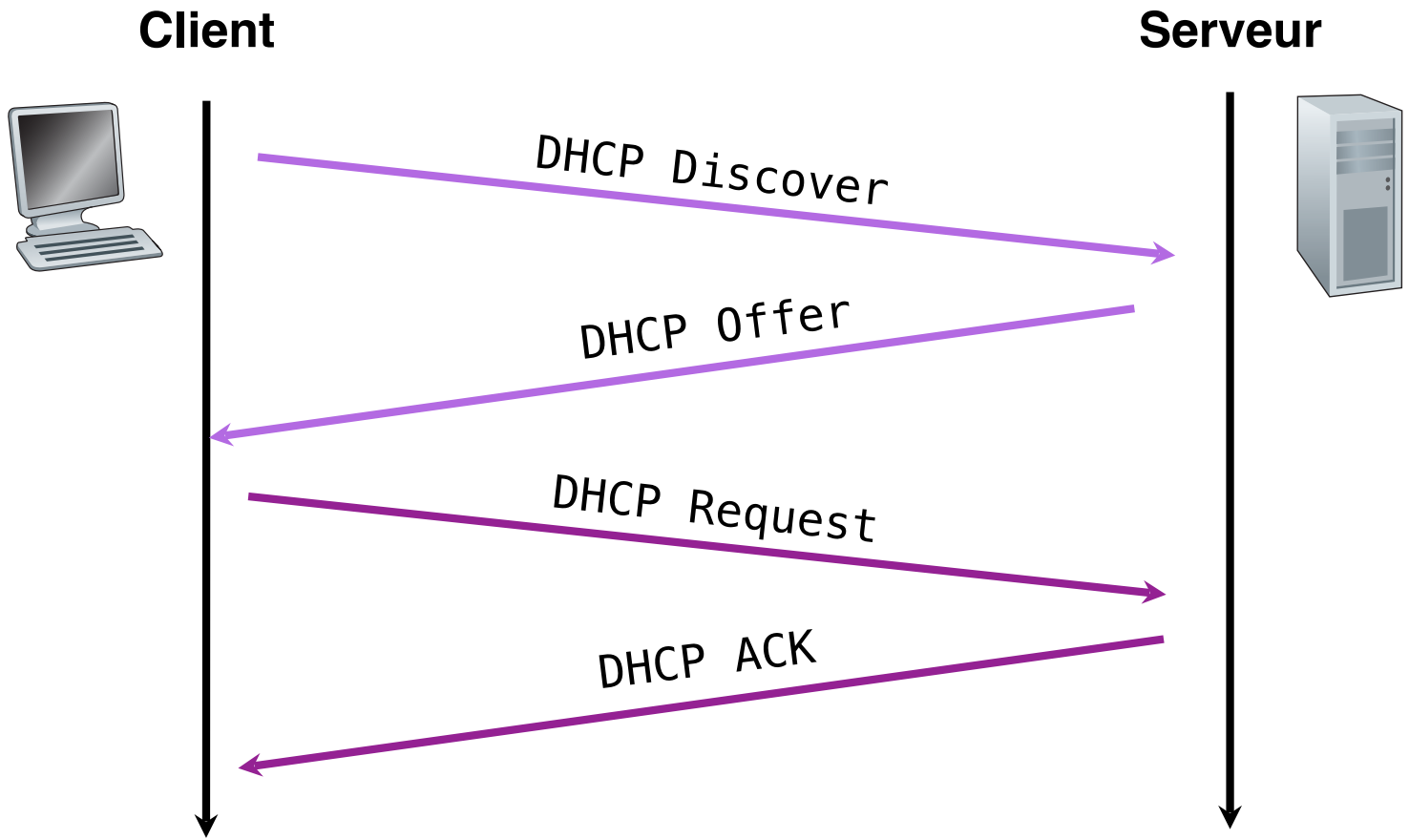
Principes communs à ARP et DHCP

- Les réseaux locaux sont des réseaux à diffusion naturelle :
  - Les requêtes ARP ou DHCP sont encapsulées dans une trame envoyée à l'adresse MAC de diffusion FF:FF:…:FF
  - Toutes les stations du réseau local inspectent le contenu de la trame
    - en cas de requête DHCP, seuls les serveurs DHCP répondent
    - en cas de requête ARP, seule la destination visée répond
- La diffusion est coûteuse :
  - Consommation des resources en réception de l'ensemble des stations du réseau local
  - Mémoriser les 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

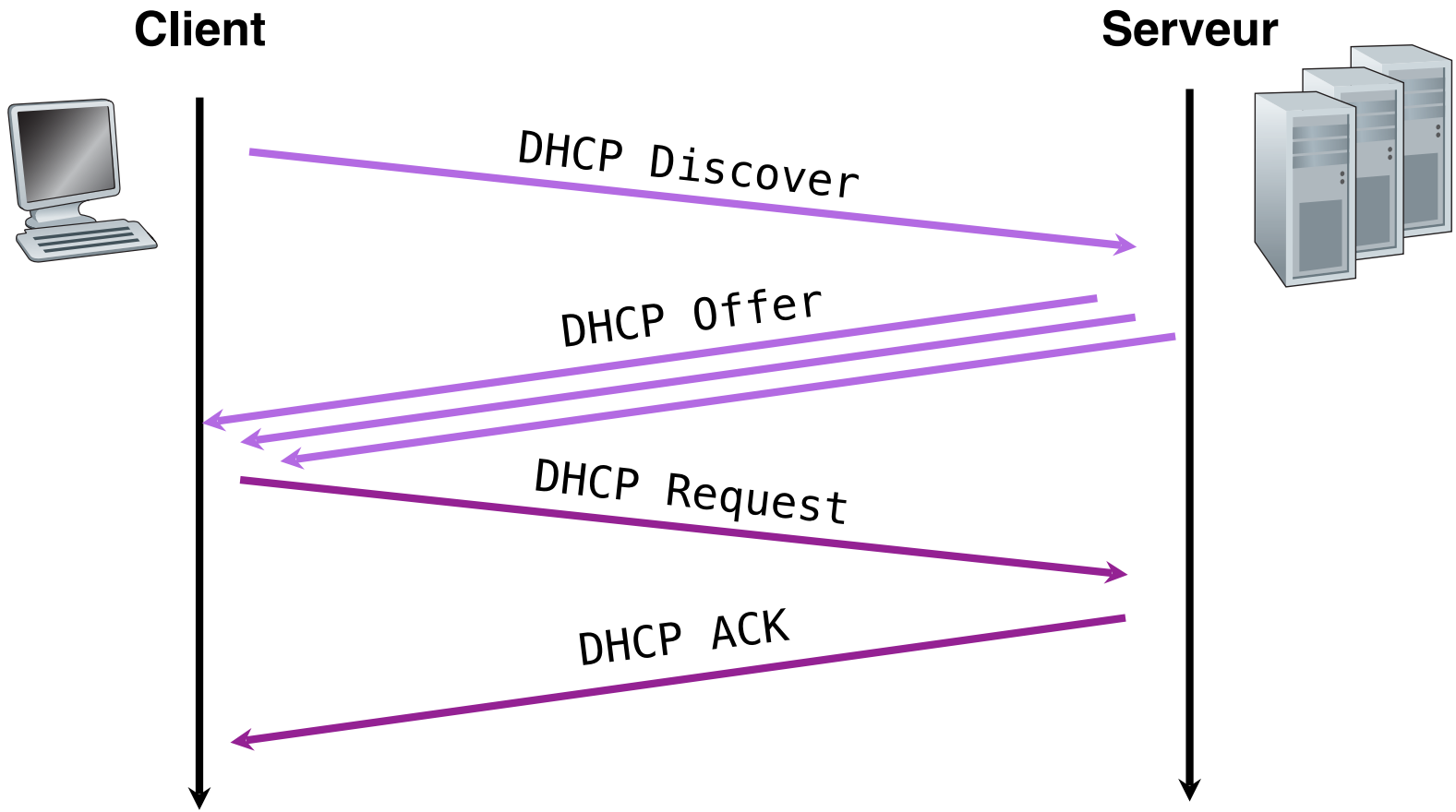
DHCP: Dynamic Host Configuration Protocol

- Une machine hôte obtient, à sa demande, les paramètres réseau tels que son adresse IP :
  - à l'issue du bail :
    - l'adresse IP peut être allouée à une autre machine
    - le bail de l'adresse IP peut être renouvelé
- Echange DHCP :
  - la machine hôte diffuse un message "DHCP discover"
  - les serveurs DHCP répondent avec un message "DHCP offer"
  - la machine hôte choisit une des offres et diffuse un message "DHCP request"
  - Le serveur DHCP sélectionné confirme que son offre tient toujours en envoyant un message "DHCP ack"

Dynamic Host Configuration Protocol

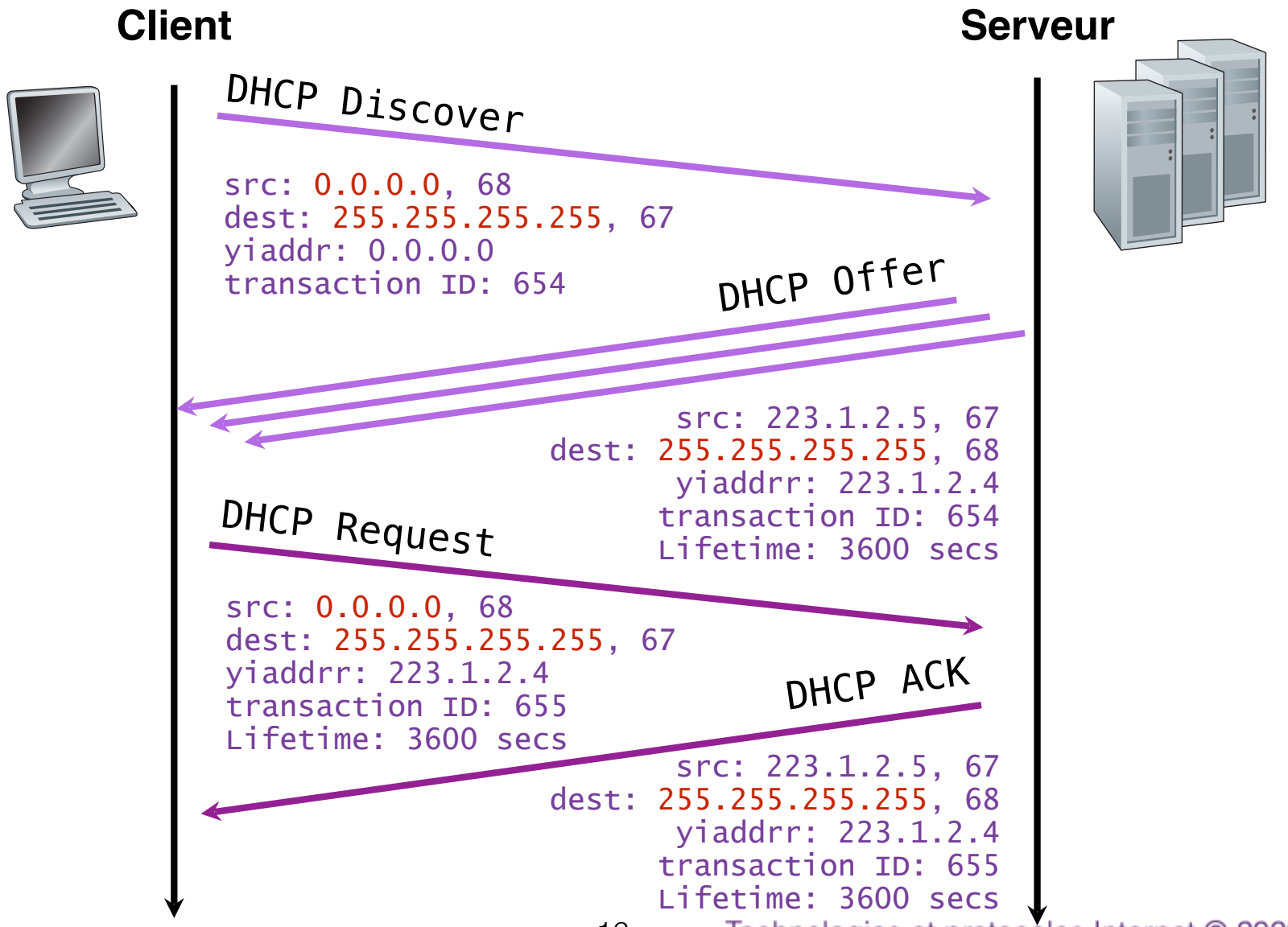


Dynamic Host Configuration Protocol

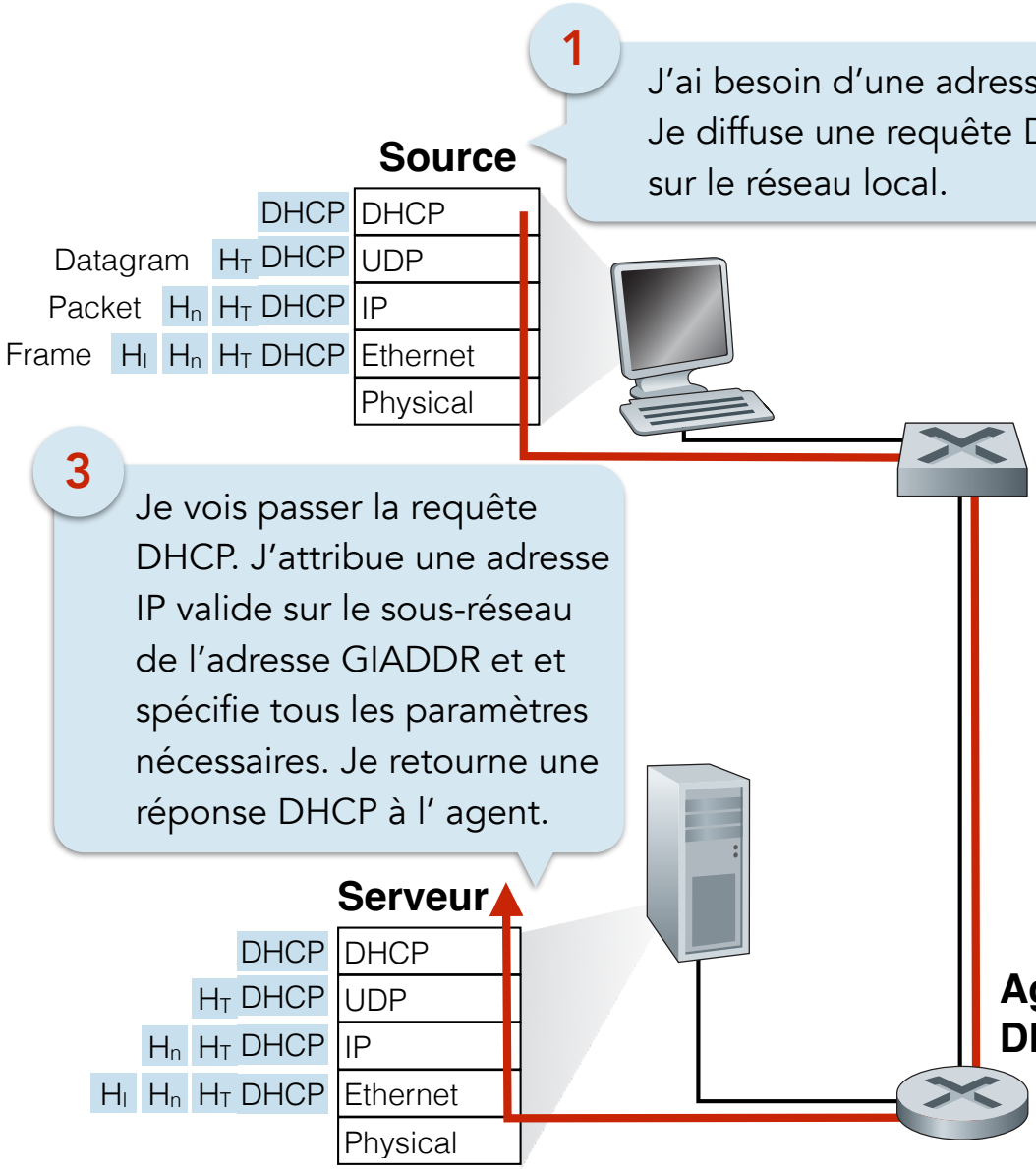


- Les quatre messages sont diffusés
- Les deux premiers servent à localiser un des serveurs DHCP
  - inutiles pour renouveler le bail d'une adresse IP

Dynamic Host Configuration Protocol



Agent Relais DHCP



- Agent relais DHCP
  - Installé si le serveur DHCP est sur un sous-réseau différent
  - Configuré avec l'adresse IP du serveur DHCP
  - Réachemine en unicast les requêtes DHCP au serveur DHCP en précisant son adresse IP dans le champ GIADDR des messages DHCP
- Serveur DHCP
  - Utilise GIADDR pour determiner le sous-réseau de l'agent relais
  - Attribue une adresse IP valide sur ce sous-réseau et spécifie les autres paramètres
  - Transmets l'adresse IP et les autres paramètres à l'agent relais en utilisant la valeur de GIADDR

Serveur DHCP

- Le message “DHCP offer” contient :
  - les paramètres réseau à configurer (IP adresse, masque, gateway, serveurs DNS locaux, ...)
  - La durée du bail (durée de validité de ces paramètres)
- Plusieurs serveurs peuvent répondre :
  - Plusieurs serveurs sur un même réseau physique pour palier aux pannes
  - Le client choisit un des serveurs en acceptant son offre
- Le client diffuse un message “DHCP request”contenant :
  - Les paramètres contenus dans l’offre qu’il a acceptée
  - Le serveur DHCP à l’origine de cette offre envoie un message “DHCP ack”
  - Les autres serveurs comprennent que leur offre n'a pas été retenue

Configuration des adresses IPv6

Type d'adresse	Methode	ICMPv6 Router advertisement Type 134		Préfixe réseau	Identifiant d'Interface	DNS
		M Flag	O Flag			
Link Local	Dynamique sans état (SLAAC)	-	-	FFE80:/64	Manuelle, aléatoire, EUI-64, MAC-48, cryptographique	-
Global Unicast	Statique (manuelle)	0	0	Manuelle	Manuelle	Manuelle
	Dynamique avec état (DHCPv6)	1	1	DHCPv6	DHCPv6	DHCPv6
	Dynamique sans état (SLAAC)	0	1	ICMPv6	Manuelle, aléatoire, EUI-64, MAC-48, cryptographique	DHCPv6
			0			Manuelle

ARP
Découverte des adresses MAC des machines IPv4 voisines

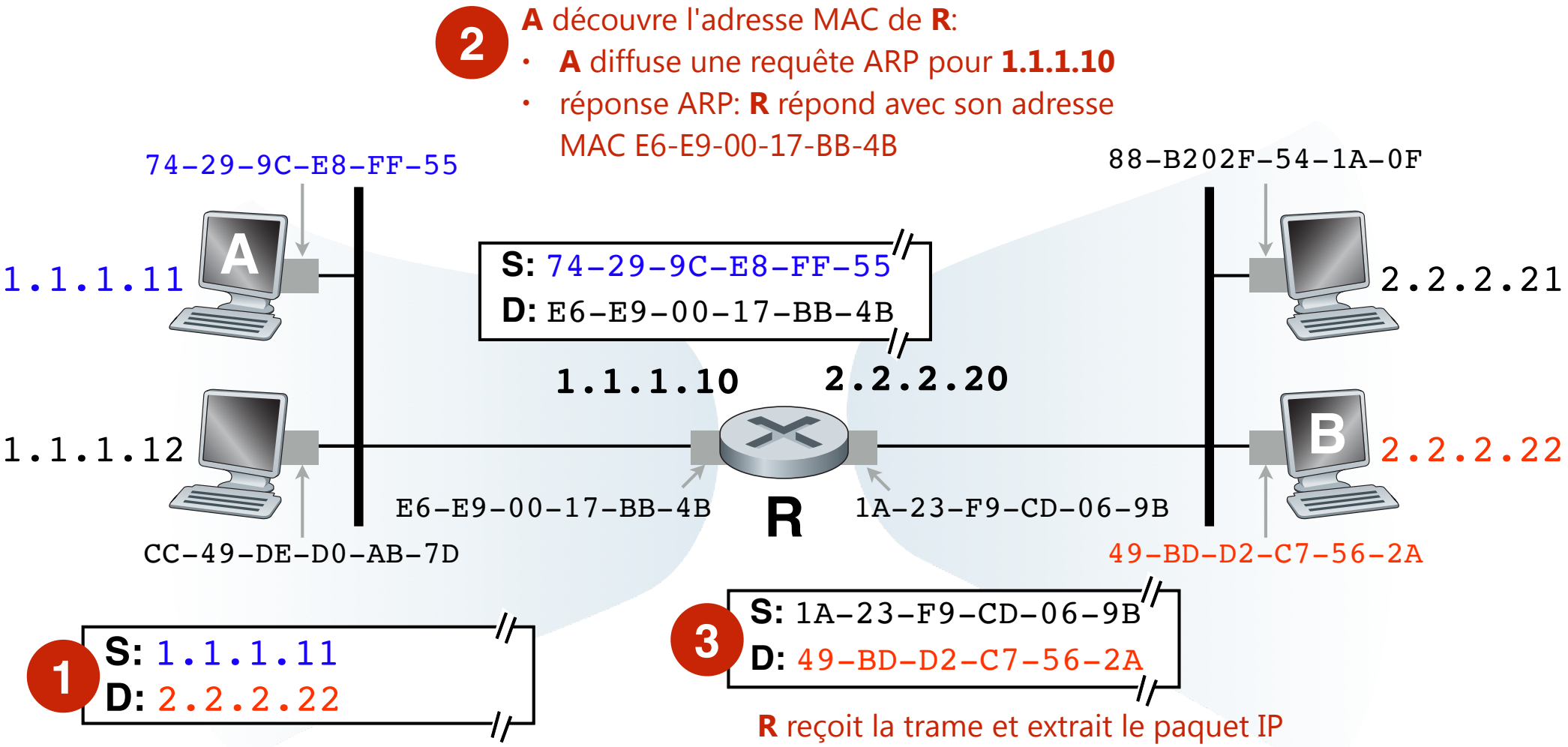
Address Resolution Protocol (ARP)

- Les machines hôtes maintiennent une table ARP :
  - Une correspondance (IP adresse, MAC adresse) par entrée
  - Entrées configurées manuellement ou découvertes par envoi de requêtes ARP
- Une machine hôte qui souhaite envoyer un paquet IP consulte sa table ARP :
  - Si une entrée est trouvée pour l'adresse IP destination du paquet :
    - Encapsuler le paquet IP dans une trame destinée à l'adresse MAC spécifiée par cette entrée
  - Sinon :
    - Diffuser une requête ARP contenant l'adresse IP à résoudre
    - La cible retourne une réponse ARP contenant son adresse MAC
    - Encapsuler le paquet IP dans une trame destinée à l'adresse MAC retournée
    - Créer une nouvelle entrée dans la table ARP pour cette cible

Format des messages ARP

- Protocol Type
  - IPv4 = 0x0800
- Hardware Type
  - Ethernet = 1
  - HDLC = 17
- HLEN (longueur adresse physique)
  - Ethernet = 48
- PLEN (longueur adresse logique)
  - IPv4 = 32
- Operations
  - Requête ARP = 1
  - Réponse ARP = 2

Hardware type		Protocol type
HLEN (n)	PLEN (m)	Operations
Source Hardware Address: n		
Source Protocol Address: m		
Destination Hardware Address: n		
Destination Protocol Address: m		



A désire envoyer un paquet à **B**
Les préfixes de **A** et **B** sont différents
A doit envoyer son paquet à la gateway **R**
(acheminement indirect)

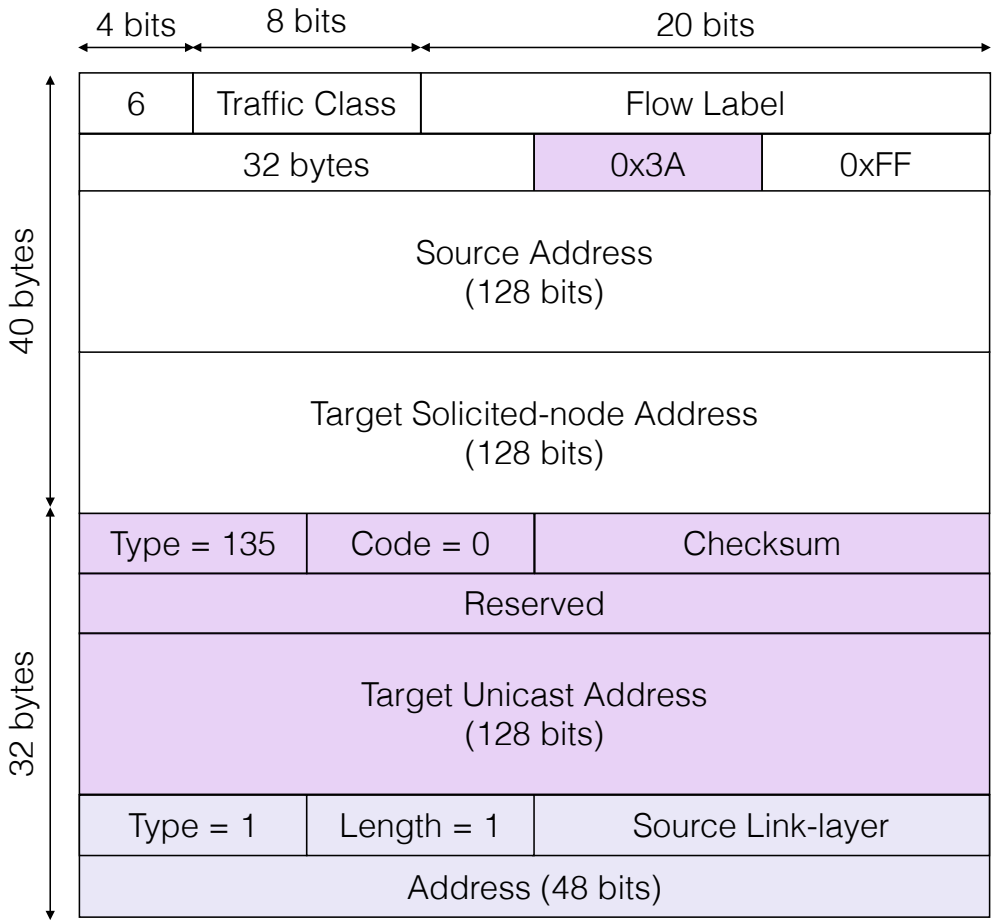
R reçoit la trame et extrait le paquet IP
R cherche dans sa table de routage l'interface sortante pour 2.2.2.22
R diffuse une requête ARP pour 2.2.2.22
B répond avec l'adresse MAC 49-BD-D2-C7-56-2A
R encapsule le paquet dans une trame qu'il envoie à **B**

On suppose les tables ARP de A et R vides

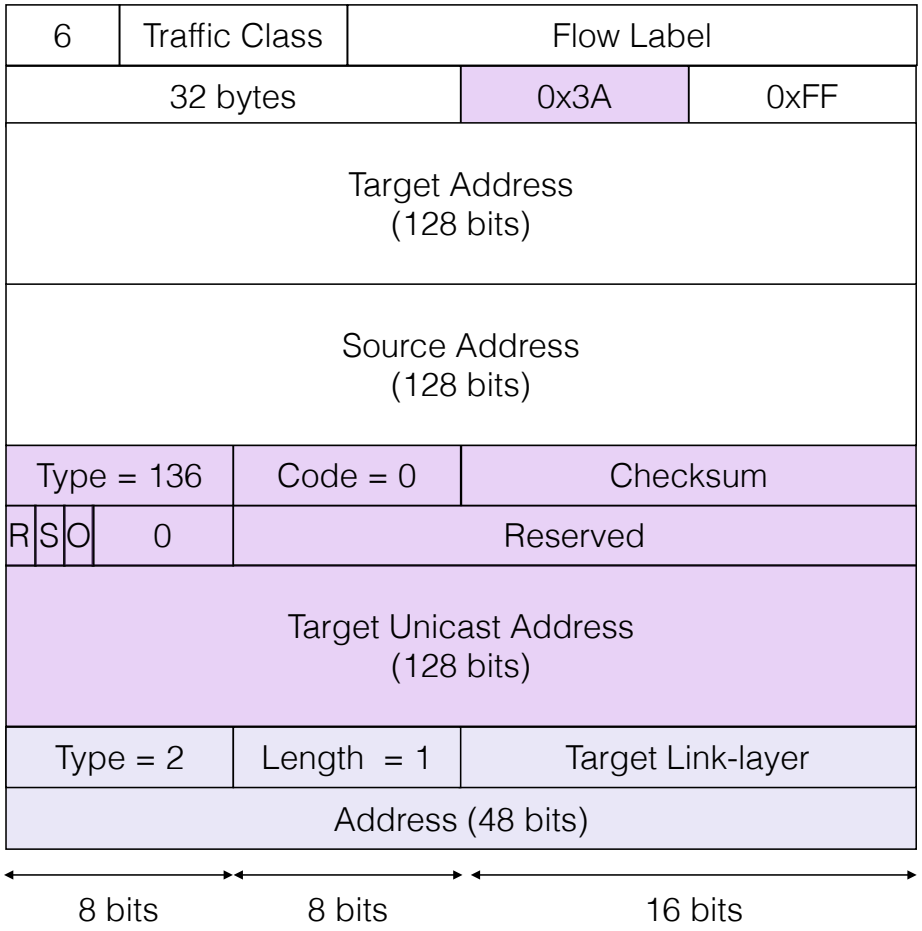
ICMPv6 et Découverte de voisins
Découverte des adresses MAC des machines IPv6 voisines

Résolution des adresses IPv6-MAC

Neighbor Solicitation



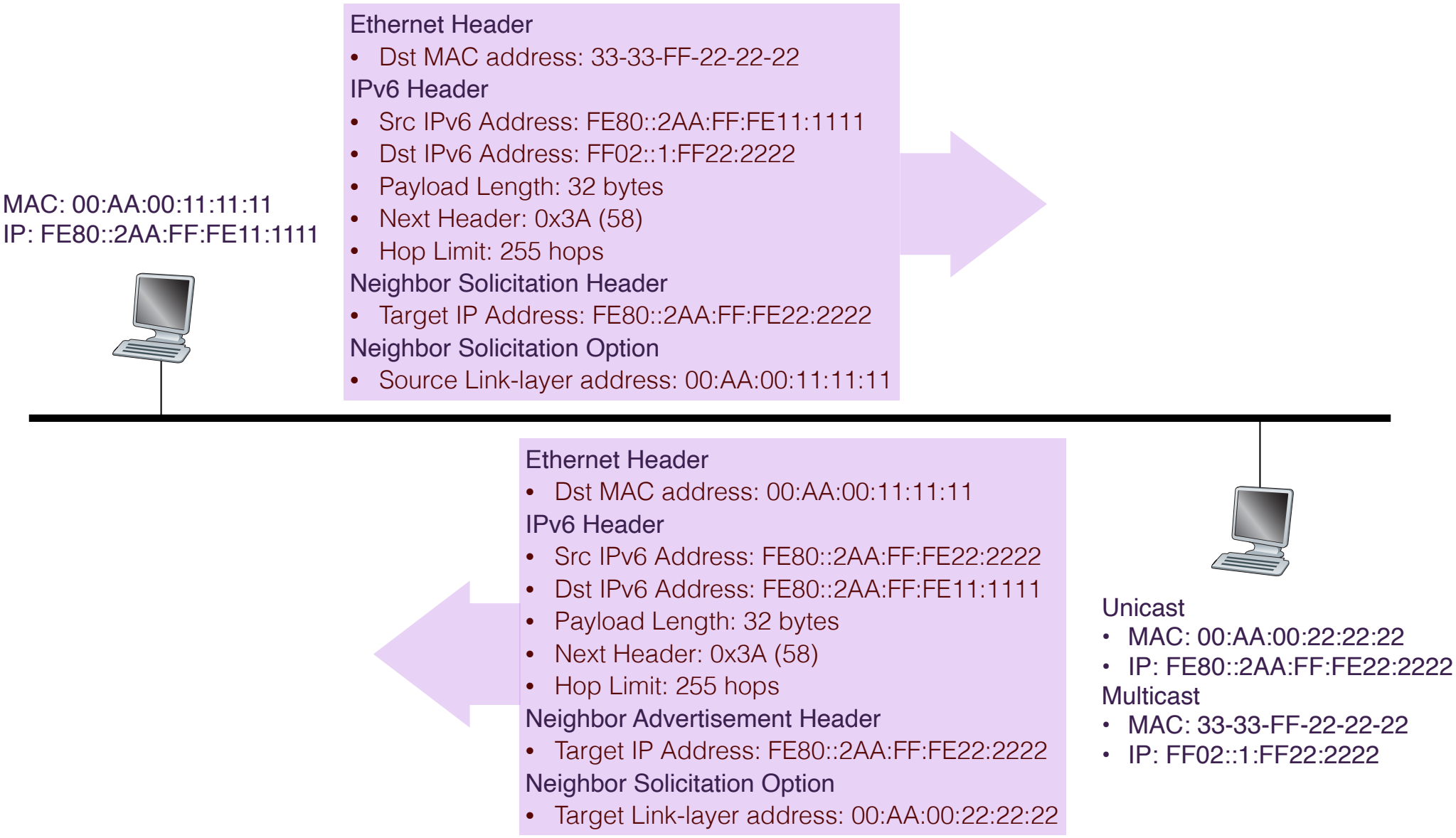
Neighbor Advertisement



Résolution des adresses IPv6 vers MAC

- Neighbor Solicitation (NS)
  - Pour découvrir l'address physique d'un voisin, la source :
    - envoie un NS contenant son adresse physique (Link-Layer Address option Type 1)
    - le NS est encapsulé dans un paquet IPv6 envoyé à l'adresse de nœud sollicitée déduite de l'adresse IP de la cible
    - le paquet IPv6 est encapsulé dans une trame envoyée à l'adresse MAC multicast correspondant à l'adresse de nœud sollicitée de la cible
- Neighbor Advertisement (NA)
  - Sur réception du message NS, la cible :
    - met à jour sa table de voisins avec la correspondance adresses IPv6-MAC de la source
    - envoie un NA en unicast contenant l'adresse physique de la cible (Link-Layer Address option Type 2)
  - Drapeaux RSO flags:
    - Drapeau Router – positionné à 1 si la cible est un routeur et à 0 sinon
    - Drapeau Solicited – positionné à 1 pour indiquer que le NA est retourné en réponse à un NS
    - Drapeau Override – positionné à 1 pour indiquer que l'adresse physique dans l'option Target Link-Layer Address doit écraser l'adresse physique si présente dans la table de voisins

Résolution des adresses IPv6-MAC



Conclusion

- La notion d'adresses IP a changé depuis leur apparition :
  - Une adresse IP identifie plusieurs machines au cours du temps
  - Une machine hôte est identifiée par différentes adresses IP selon le réseau qu'elle visite
- Le protocole IPv4 dépend des capacités de diffusion de la couche 2
  - DHCP : découverte des paramètres réseau
  - ARP : découverte de l'adresse MAC de machines voisines
- Le protocole IPv6 permet la configuration dynamique sans état des machines hôtes
  - Auto-configuration de l'identifiant d'interface
  - Annonces de routeur ICMPv6 pour configurer le préfixe (TTL et MTU locale)
  - DHCPv6 pour configurer les serveurs DNS
  - Sollicitations de voisin ICMPv6 pour découvrir l'adresse physique d'une machine IPv6 voisine

Adresses IP privées et NAT

l'Internet en pratique

- Nomadicité des machines hôtes
  - L'adresse IP d'une machine hôte change selon sa position : DHCP
- Déperdition des adresses IPv4
  - Attribution des adresses IP à la demande : DHCP
  - Utilisation d'adresses IP privées : NAT
- Sécurisation des réseaux
  - Détecter les paquets suspects IDS
  - Bloquer les paquets malveillants ou indésirables : firewall
- Préservation des ressources
  - Contrôler l'utilisation de la bande passante : régulateur de trafic
  - Mettre en mémoire les contenus populaires à proximité des clients : proxy cache

Box Internet

- Les box sont des dispositifs intermédiaires
  - équipements interposés entre les machines hôtes
  - souvent à leur insu
  - qui interceptent le trafic qu'ils voient passer

- Exemples :
  - NAT Translateur d'adresses réseau (Network address translators)
  - Pare-feu (firewalls)
  - Régulateur de trafic (traffic shapers)
  - IDS Système de détection d'intrusion (intrusion detection system)
  - Cache Web transparent (proxy cache)

Network Address Translation

- Epuisement des adresses IPv4
  - Prédit depuis le début des années 90
  - Date de début des travaux sur le successeur à IPv4
- Solution intermédiaire :
  - Réutiliser 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

Network Address Translation

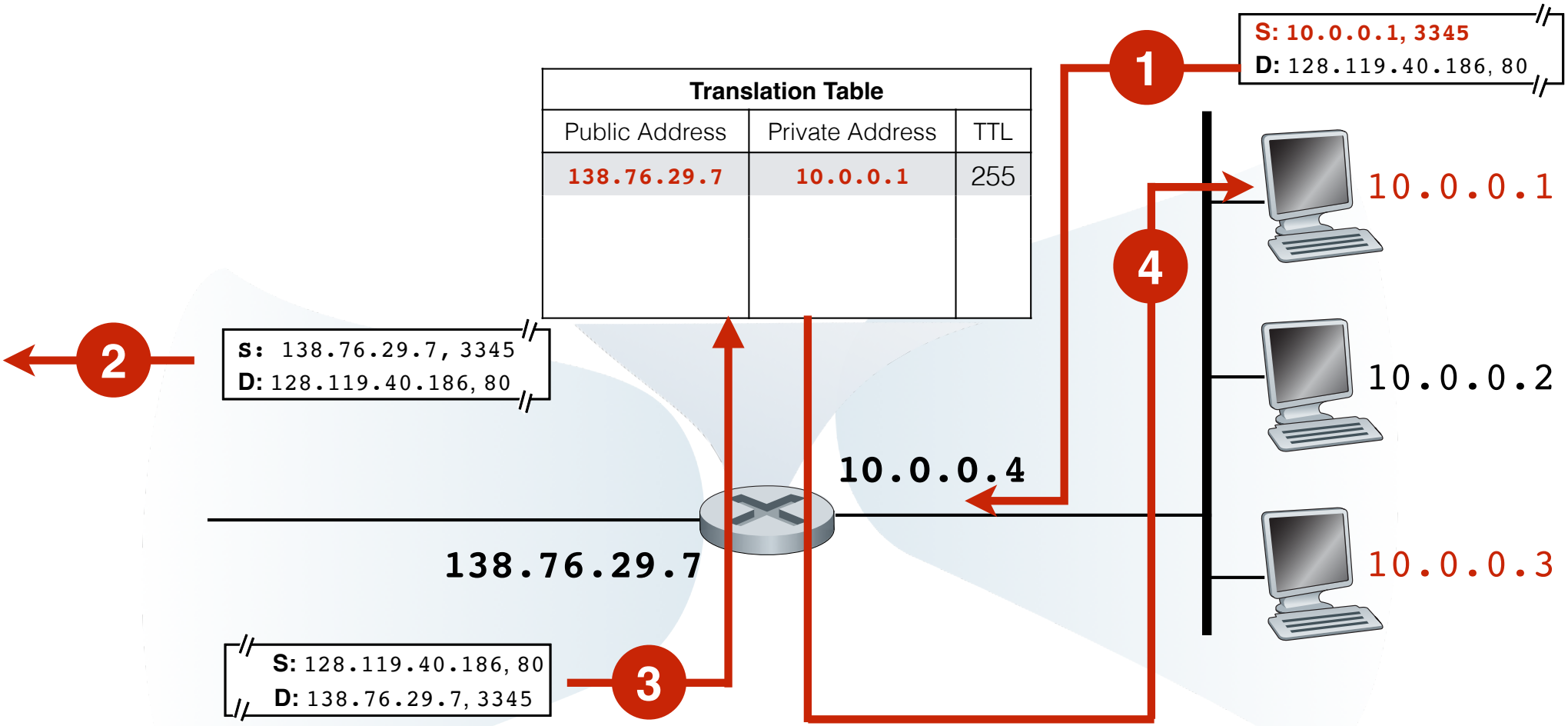
- NAT est destiné aux organisations de taille modérée
  - les adresses IP allouées par leur ISP, appelées publiques, ne suffisent pas
  - le NAT consomme une adresse IP publique visible de l'extérieur
- Numérotation des machines internes
  - l'organisation utilise en interne des adresses IP arbitraires, appelées privées
  - les adresses privées sont invisibles de l'extérieur
- Réutilisation des adresses IP publiques
  - NAT remplace l'adresse source des paquets sortants par une adresse publique
  - NAT remplace l'adresse destination des paquets entrants par une adresse privée
- Filtrage des paquets entrants
  - NAT laisse passer les paquets entrants uniquement si précédemment sollicités par un paquet sortant
  - nécessité d'états maintenus par paquet entrant

Translation d'adresses

- Les adresses locales à un réseau ne sont pas uniques :
  - Exemple : adresses IP privées (10.0.0.0/8)
- Un NAT remplace les adresses IP des paquets sortants ou entrants
  - Les machines d'un réseau local sont vues comme une adresse IP publique unique
  - … le NAT change l'entête en conséquence
- Trafic sortant
  - L'adresse source des paquets est remplacée par l'adresse IP publique
- Trafic entrant
  - L'adresse IP destination est remplacée par l'adresse IP privée de la machine destination
- Recalcul d'autres champs d'entête
  - checksum, …

NAT

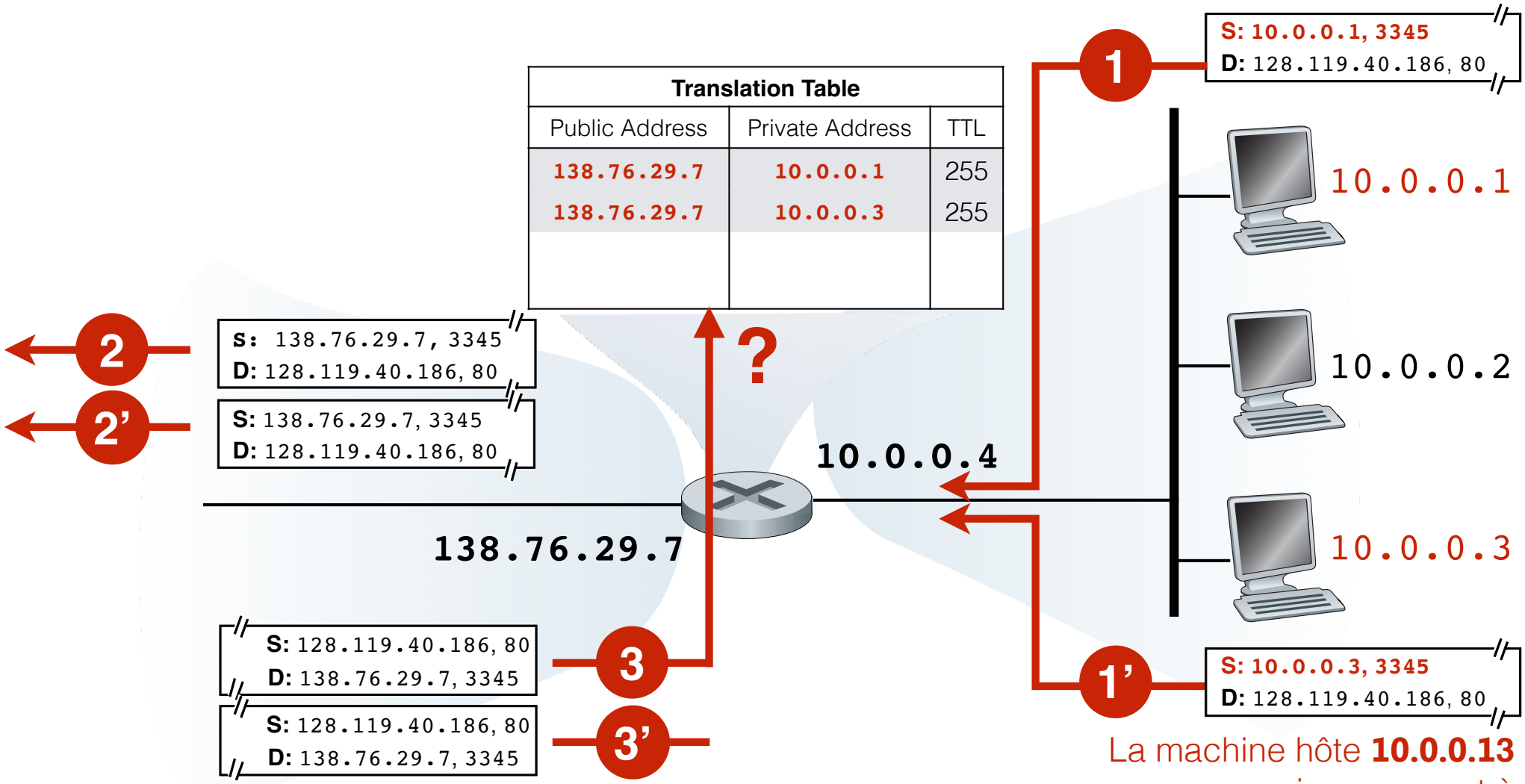
La machine hôte **10.0.0.1** envoie un paquet à **128.119.40.186**, **80**



Adresse et port destination **138.76.29.7**, **3345**

NAT

La machine hôte **10.0.0.1** envoie un paquet à **128.119.40.186, 80**



Adresse et port destination **138.76.29.7, 3345**

La machine hôte **10.0.0.13** envoie un paquet à **128.119.40.186, 80** avec le même numéro de port que 10.0.0.1

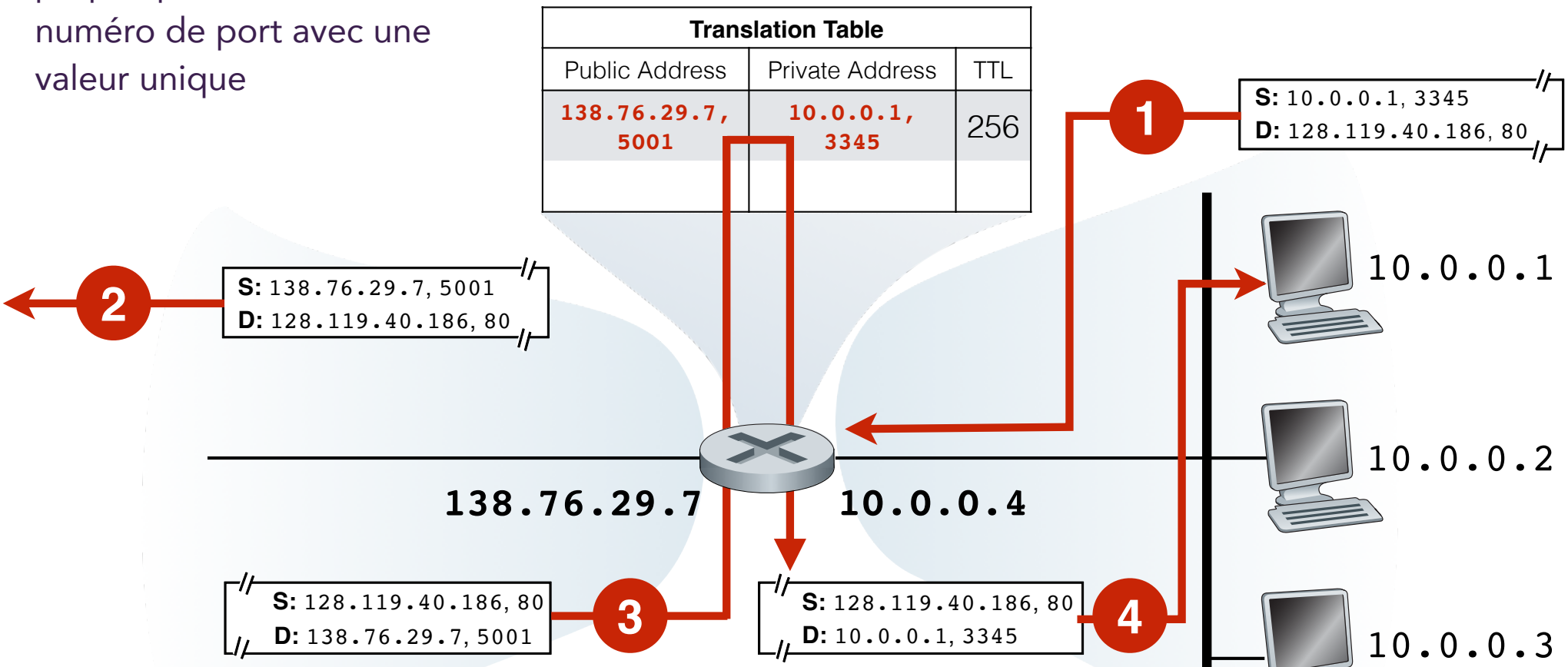
Si deux machines hôtes cherchent à contacter le même serveur ?

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

NAT

Le boîtier NAT :

- mémorise l'adresse IP source et le numéro de port source des paquets sortants
- remplace l'adresse IP source du paquet par son adresse et le numéro de port avec une valeur unique



le numéro de port 5001 identifie une entrée unique dans la table de translation

le NAT remet les valeurs originales dans l'entête des paquets entrants

Gestion des tables de translation

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

  (adresse IP source privée, numéro de port orignal,
  adresse IP publique, numéro de port translaté)

  - le numéro de port translaté sert de clé pour trouver une entrée en particulier
- Suppression des entrées obsolètes
  - si aucun paquet n'est reçu pendant un certain temps (TTL)
  - supprimer l'état correspondant et libérer le numéro de port translaté
- Nouvel exemple d'état mou (soft state)
  - suppression sans nécessité d'intervention extérieure explicite

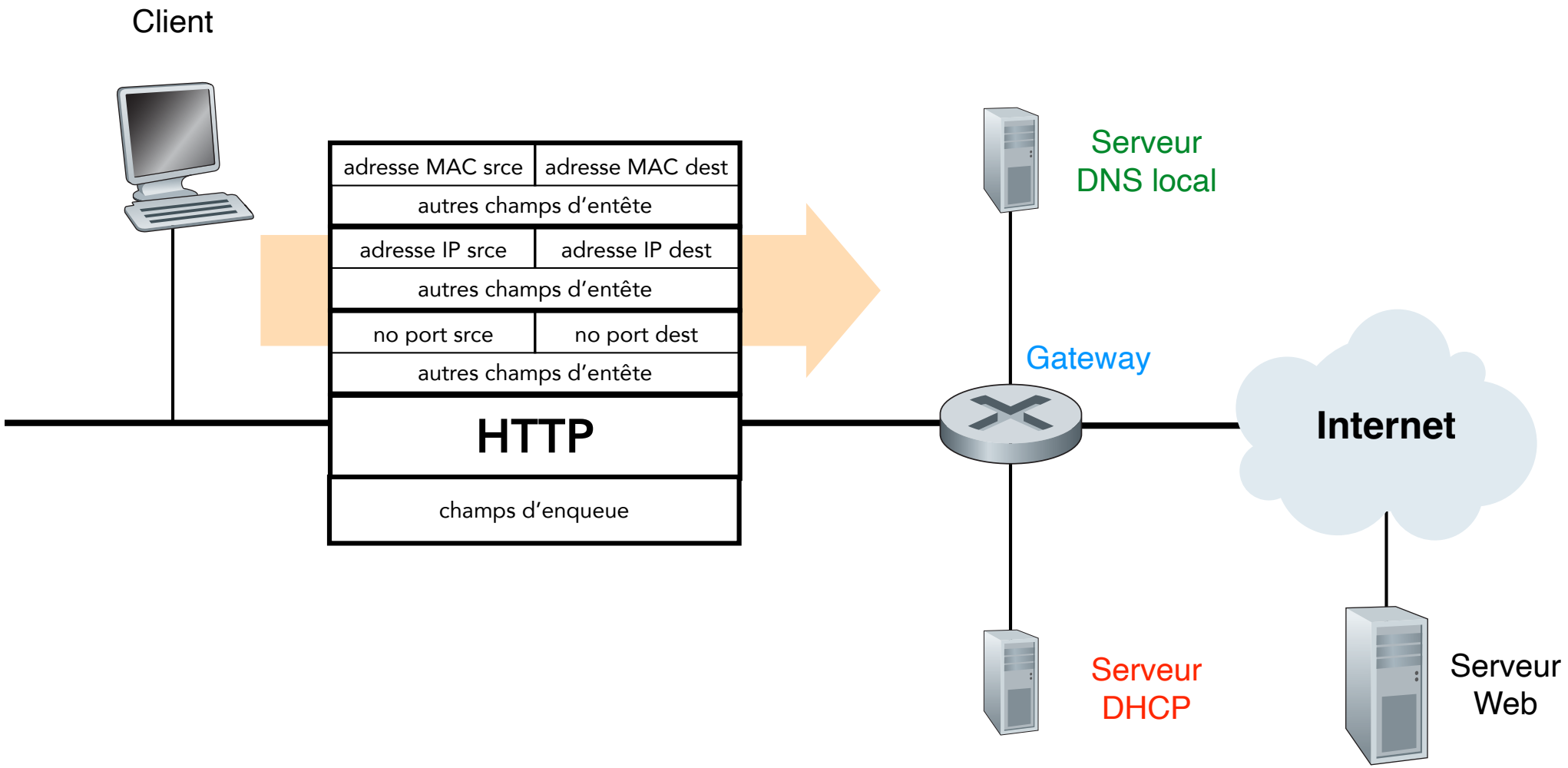
Les critiques vis-à-vis de NAT

- NAT ajoute une nouvelle signification au numéro de port (source)
  - Les numéros de port sont censés identifier les processus exécutés sur une même machine hôte
  - NAT l'utilise pour identifier les machines locales 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
  - … encore moins le modifier
  - Le réseau n'est pas censé modifier les adresses source ou destination des paquets IP
- NAT introduit des états dans le réseau
  - Le protocole IP a été conçu en mode non connecté (stateless)

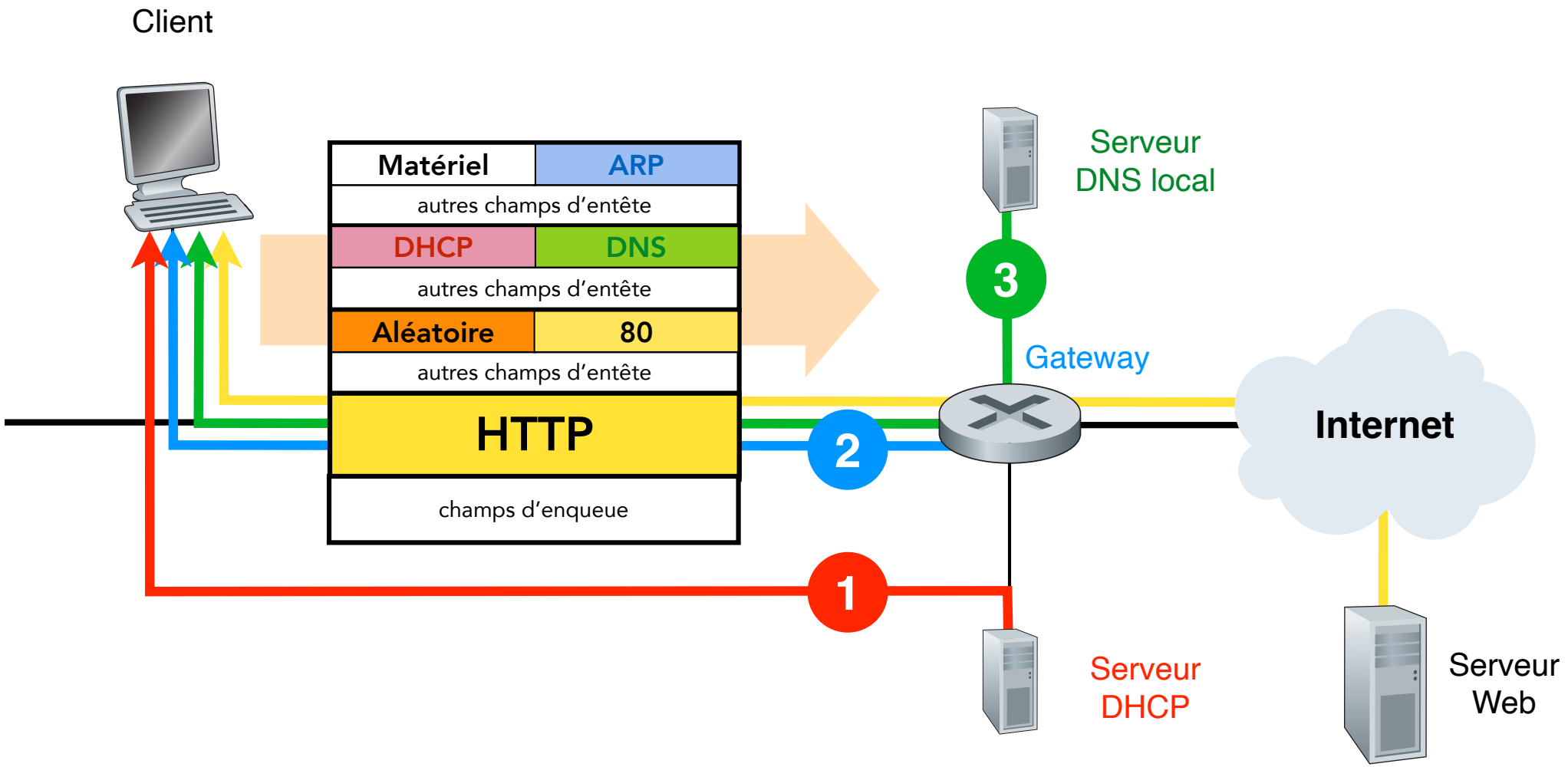
Où trouve-t-on les fonctions NAT ?

- Réseaux domestiques
  - Une box Internet cumule les fonctions de gateway, serveur DHCP, NAT, firewall (…)
  - consomme la seule adresse IP publique attribuée par votre fournisseur d'accès Internet
  - … masque la présence de plusieurs machines hôtes
- Universités ou réseau d'entreprise
  - NAT est 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 case de changement de fournisseur d'accès
- IPv6 est LA solution
  - qui tarde à s'imposer

Remplissage des entêtes



Remplissage des entêtes



Conclusion

- Une machine hôte est identifiée par plusieurs identifiants :
  - nom d'hôte
  - adresse IP
  - adresse MAC
- Une machine hôte doit découvrir ses identifiants et ceux des destinations
  - DHCP : son adresse IP, le masque du réseau local, l'adresse de la gateway, les adresses des serveurs DNS locaux, …
  - DNS : adresse IP des destinations
  - ARP : adresse MAC des machines locales (gateway ou destinations locales)
- Un NAT dissimule l'existence de plusieurs machines hôtes :
  - NAT s'interpose entre les machines hôtes d'un réseau identifié par une adresse IP privée et le reste de l'Internet
  - NAT modifie les entêtes des paquets à l'insu de leur source
  - NAT rompt la chaine d'acheminent entre source original d'un paquet et destination finale du paquet