ARP

Introduction

- Toute machine reliée sur un réseau se charge d'aiguiller les paquets à émettre en fonction de leur destination :
- Si le destinataire est sur le réseau local, le datagramme est directement envoyé à la machine cible.
- Si le destinataire est sur un réseau différent, les données sont envoyées au routeur du réseau local.

Nécessité de la résolution d’adresse

- la transmission doit se faire en utilisant le service de la couche hôte-réseau (réseau physique)
- la couche hôte-réseau (niveau trame) n'utilise pas les adresses IP (niveau réseau) mais des adresses physiques (adresses MAC)
- la résolution d'adresse est le mécanisme permettant à une station d'obtenir l'adresse physique (de l'interface/carte réseau) d'une station possédant une certaine adresse IP dans le même réseau

Méthode possibles pour la résolution d'adresse

résolution directe

- l'adresse physique est déterminée comme une fonction de l'adresse IP
- méthode simple à mettre en œuvre si les adresses physiques sont configurables

interrogation d'un serveur

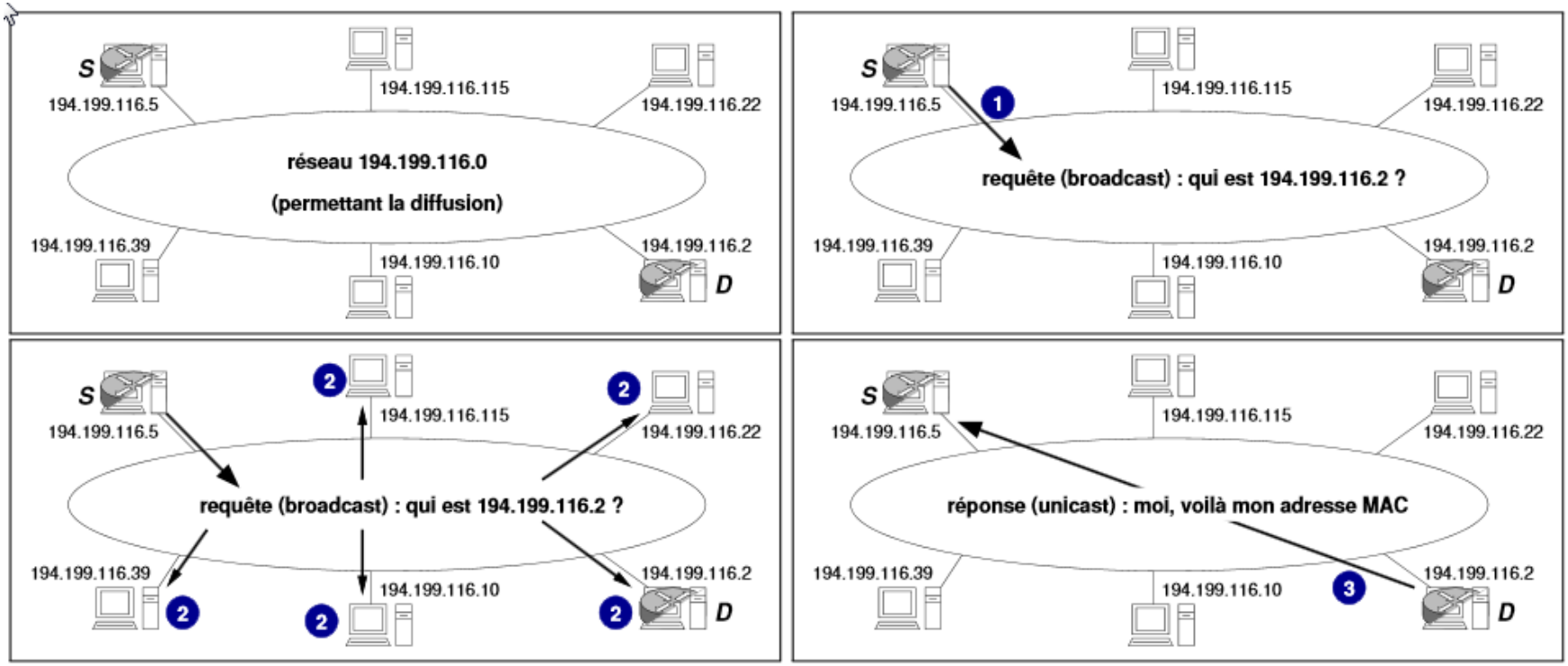
- un serveur est chargé de collecter les adresses physiques et IP des hôtes du réseau
- les stations interrogent le serveur pour résoudre les adresses
- méthode souvent utilisée lorsque le réseau ne permet pas la diffusion
- mais la résolution n'est plus possible si le serveur devient injoignable. . .

Résolution dynamique par ARP (Address Resolution Protocol)

- ARP a l'avantage d'être à la fois dynamique et décentralisé :
  - les changements d'association adresse IP/adresse MAC sont automatiquement et rapidement pris en compte
  - aucun serveur n'est nécessaire et une panne d'une station n'a aucun impact global

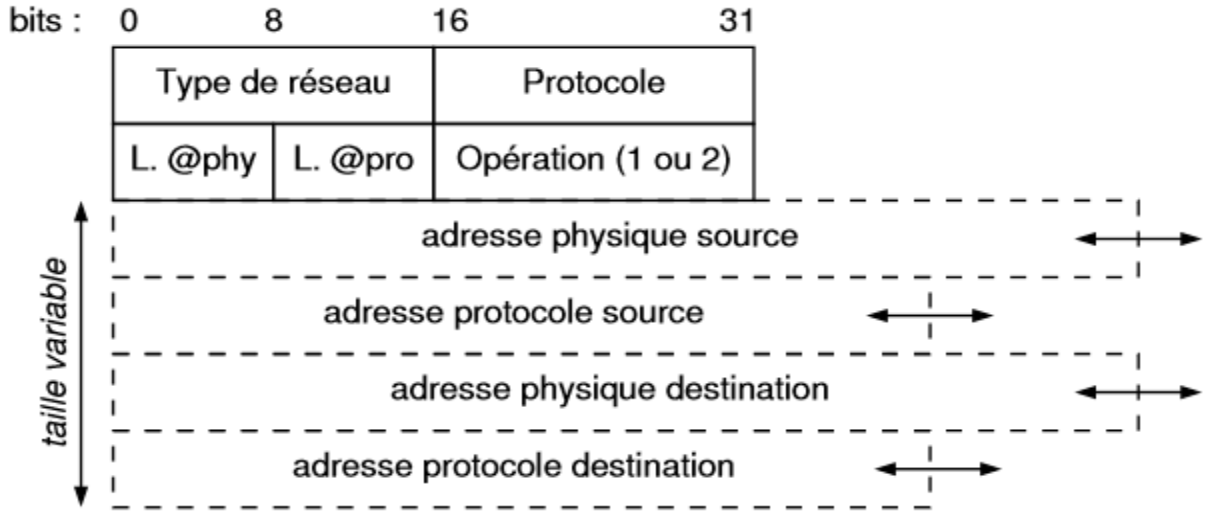
- ARP a été originellement défini pour IP et Ethernet.
  Mais il est plus général et peut être utilisé sur tout type de réseau permettant la diffusion, pour le compte de différents protocoles réseau (dont IP)

Principe de résolution par ARP



1. S envoie en **broadcast** une **requête ARP** signifiant qu'il souhaite obtenir l'adresse physique correspondant à D
2. la requête est reçue et traitée par toutes les stations du réseau
3. seule la station d'adresse D répond en envoyant en **unicast** à S une **réponse ARP** contenant l'adresse physique demandée

Format du datagramme ARP



- la taille du datagramme ARP dépend des protocoles concernés :
  - la taille (en octets) des adresses physiques (comme Ethernet) est indiquée par le champ *Longueur adresses physiques* (L. @phy)
  - la taille (en octets) des adresses protocole (comme IP) est indiquée par le champ *Longueur adresses protocole* (L. @pro)
- les requêtes et les réponses ont le même format ; le champ *Opération* indique s'il s'agit d'une requête (*Opération* vaut 1) ou d'une réponse (*Opération* vaut 2)

Datagramme ARP : Adresse

- qu'il s'agisse d'une requête ou d'une réponse :
  - *adresse physique source* contient l'adresse physique (MAC) de l'émetteur du datagramme
  - *adresse protocole source* contient son adresse réseau (IP)
- *adresse physique destination* :
  - dans requête : inconnue (à 0, soit 00:00:00:00:00:00 pour Ethernet)
  - dans réponse : adresse MAC du destinataire
- *adresse protocole destination* contient l'adresse réseau (IP) du destinataire (dans une requête, c'est l'adresse à résoudre)

Requête ARP sur Ethernet V2

adresses de l'émetteur

IP : 194.199.116.5

ethernet : 08:00:05:0e:ab:51

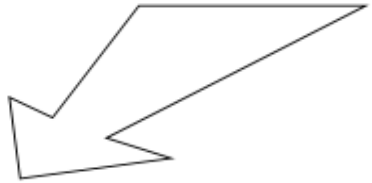
adresses de la cible

IP : 194.199.116.2

ethernet (recherchée)

- Trame Ethernet V2 (en hexadécimal) :

	destination	*source*	*type*	*données*	
préambule	ff:ff:ff:ff:ff:ff	08:00:05:0e:ab:51	**08 06**	**Datagramme ARP (requête)**	CRC
	(broadcast)				



- Requête ARP (en binaire) :

Type réseau : Ethernet (1)	Protocole : IP (0x0800)	L. @ phy : 6	L. @ pro : 4	Opération : requête (1)	
0000000000000001	0000100000000000	00000110	00000100	0000000000000001	
0000100000000000000010100001110101010111010100001					← Ethernet source (08:00:05:0e:ab:51)
11000010110001110111010000000101					← IP source (194.199.116.5)
000000000000000000000000000000000000000000000000					← Ethernet destination (inconnue)
11000010110001110111010000000010					← IP destination (194.199.116.2)

Réponse ARP pour IP sur Ethernet v2

émetteur de la réponse

IP : 194.199.116.2

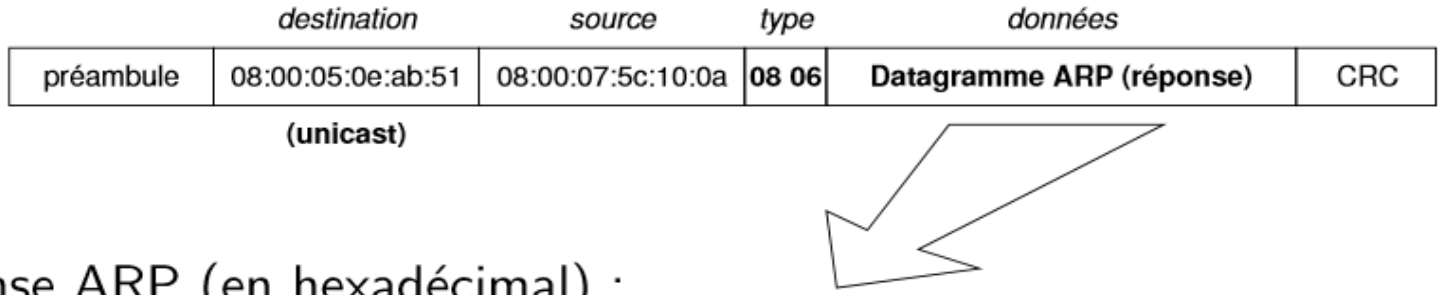
ethernet : **08:00:07:5c:10:0a**

destinataire de la réponse

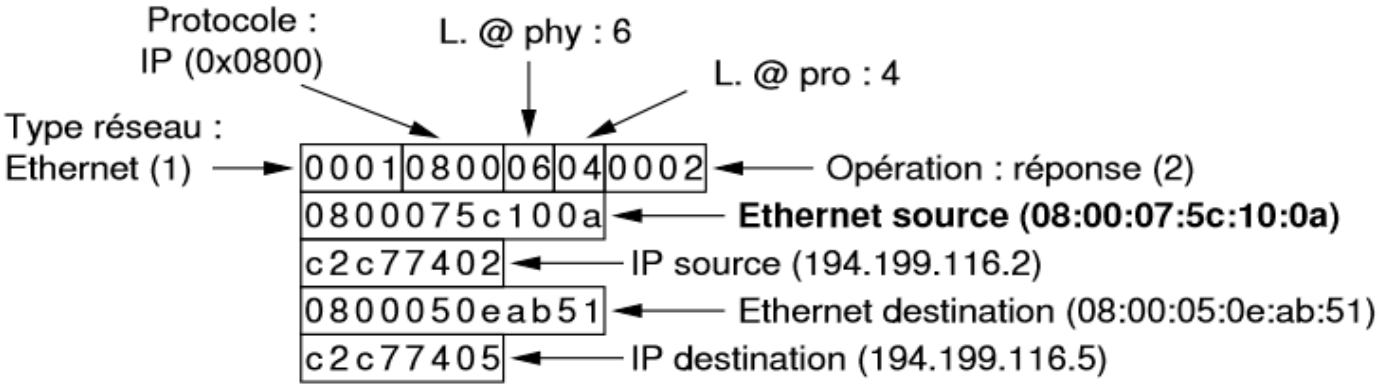
IP : 194.199.116.5

ethernet : 08:00:05:0e:ab:51

- Trame Ethernet V2 (en hexadécimal) :



- Réponse ARP (en hexadécimal) :



Optimisation d'ARP

- **cache** (mémoire temporaire) ARP obligatoire stocké sur les hôtes :
  - contient une liste d'associations $\prec$ adresse MAC, adresse IP $\succ$
  - évite d'émettre une nouvelle requête lorsque l'association a déjà été obtenue
  - une association a une durée de vie (TTL) limitée, variable selon les systèmes (1 min, 20 min, ...)
  - chaque fois qu'une association est confirmée, sa durée de vie est remise à son max
  - les associations dont la durée de vie expire sont supprimées
- traitement de la **requête** :
  - les requêtes étant envoyées en broadcast, toutes les stations les traitent
  - or elles incluent l'adresse MAC et l'adresse IP de l'émetteur
  - en recevant une requête, les stations *peuvent* mettre à jour leur cache avec les infos sur l'émetteur
- *possibilité* d'émission d'une **requête ARP fictive** si changement de carte (et donc d'adresse MAC) :
  - en plaçant sa propre adresse IP comme celle recherchée
  - personne ne répondra, mais en recevant la requête les stations *peuvent* mettre à jour leur cache

Quelques commandes

- Linux
  - **arp** (affichage de la table arp)
  - **ping** (interroge une carte réseau et exprime le temps aller-retour en mili secondes)
    ping localhost
    ping @ip
    ping -v nom-hôte-distant
  - **route** (programme de gestion de la table de routage IP)
  - **ifconfig** (programme de configuration des interfaces réseaux, c'est à dire des cartes réseaux)
  - **netstat** (affiche les informations sur les connexions réseaux)
  - **nslookup** ("name server", programme d'interogation des serveurs de noms de domaines)
- Windows
  - **ipconfig** –all
  - **arp** –a
  - **ping** IP

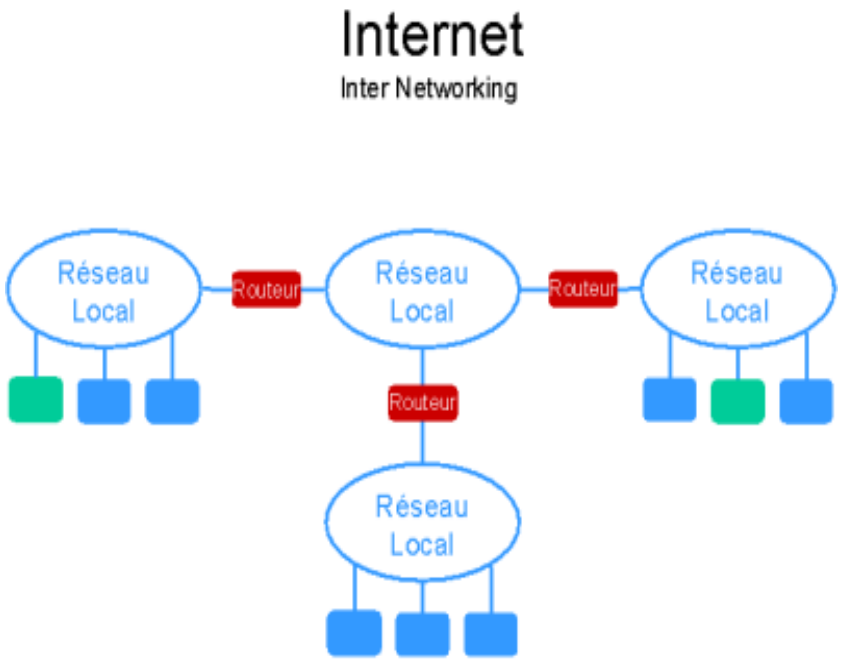
Routage
Slides tirés du cours de
C. Pain-Barre

Rôles des routeurs

- Les routeurs actuels sont pour la plupart des matériels dédiés à la tâche de routage, se présentant généralement sous la forme de serveurs.
- On envoie la requête au routeur le plus proche, c'est-à-dire à la passerelle réseau sur lequel il se trouve. Ce routeur va ainsi déterminer la prochaine machine à laquelle les données vont être acheminées de manière à ce que le chemin choisi soit le meilleur.
- Pour y parvenir, les routeurs tiennent à jour des tables de routage, véritable cartographie des itinéraires à suivre en fonction de l'adresse visée. Il existe de nombreux protocoles dédiés à cette tâche.
- les routeurs permettent de manipuler les données circulant sous forme de datagrammes afin d'assurer le passage d'un type de réseau à un autre
- les routeurs sont chargés de fragmenter les paquets de données pour permettre leur libre circulation

Routeur

- Un **routeur** est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règle (Wikipedia)



Les premiers routeurs étaient de simples ordinateurs ayant plusieurs cartes réseau, dont chacune était reliée à un réseau différent.

Algorithme de routage

- le logiciel IP de **A** doit envoyer un datagramme à (l'adresse IP de) **B**, situé quelque part dans l'inter-réseau

- routage = prise de décision pour l'envoi
- question : la destination appartient-elle au même réseau ?
  - oui : la remise est **directe**.

    A peut envoyer directement le datagramme à **B**, en utilisant le service d'envoi de leur réseau

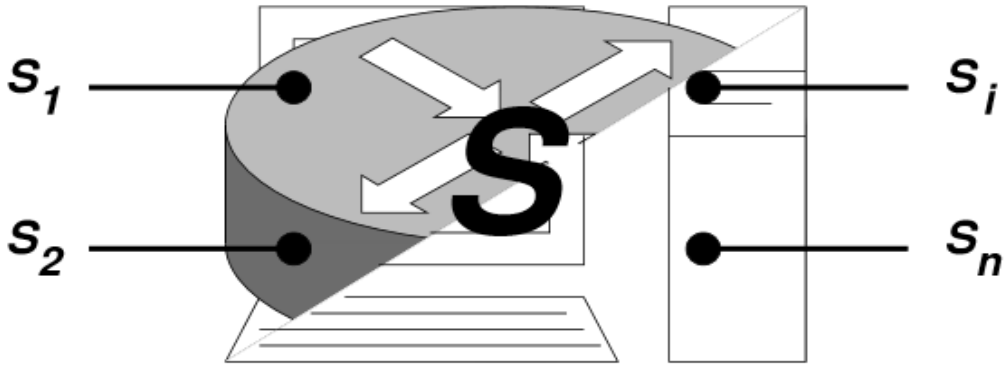
  - non : la remise est **indirecte**.

    A ne peut qu'envoyer le datagramme à un routeur. À son tour, le routeur devra appliquer le même algorithme

dans ce cas, le choix du routeur est prépondérant

Test d'appartenance au même réseau

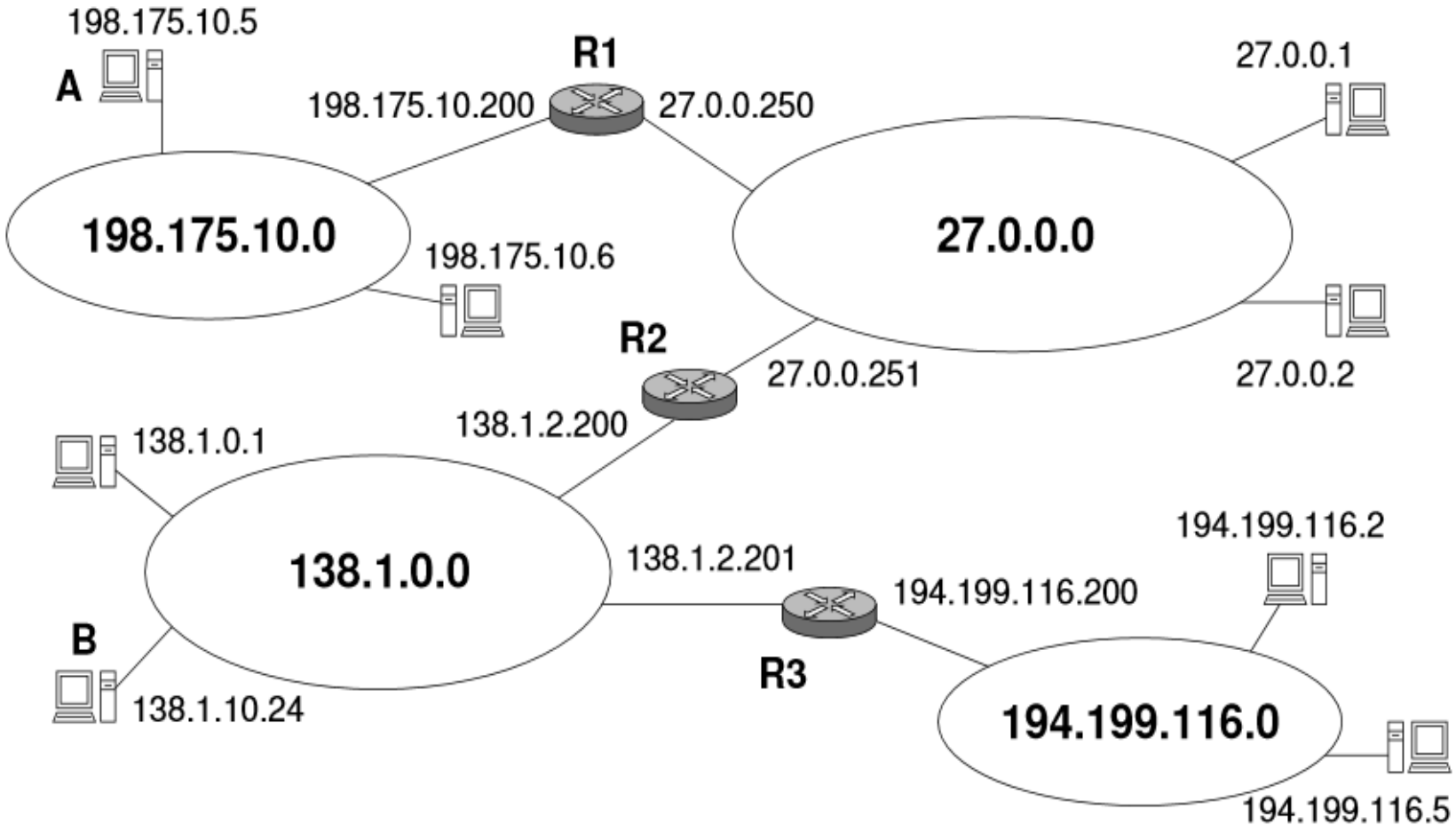
- une station (ou un routeur) S dispose d'une ou plusieurs interfaces, chacune avec une adresse IP S_i



- S doit envoyer un datagramme à une IP de destination D
- pour savoir si D appartient à un réseau connecté à S :
  1. de D **et de sa classe**, en déduire l'adresse du réseau de D, qu'on notera $R(D)$
  2. pour chaque adresse IP S_i de S :
     a) extraire son adresse de réseau $R(S_i)$
     b) si $R(S_i) = R(D)$ alors S et D appartiennent au même réseau

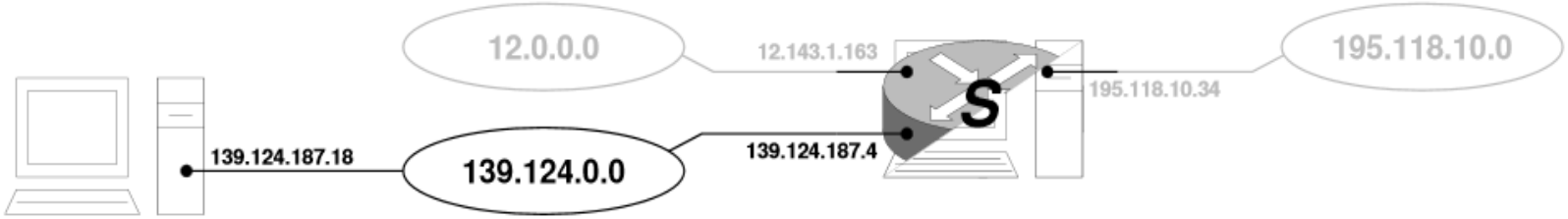
Exemple

Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté



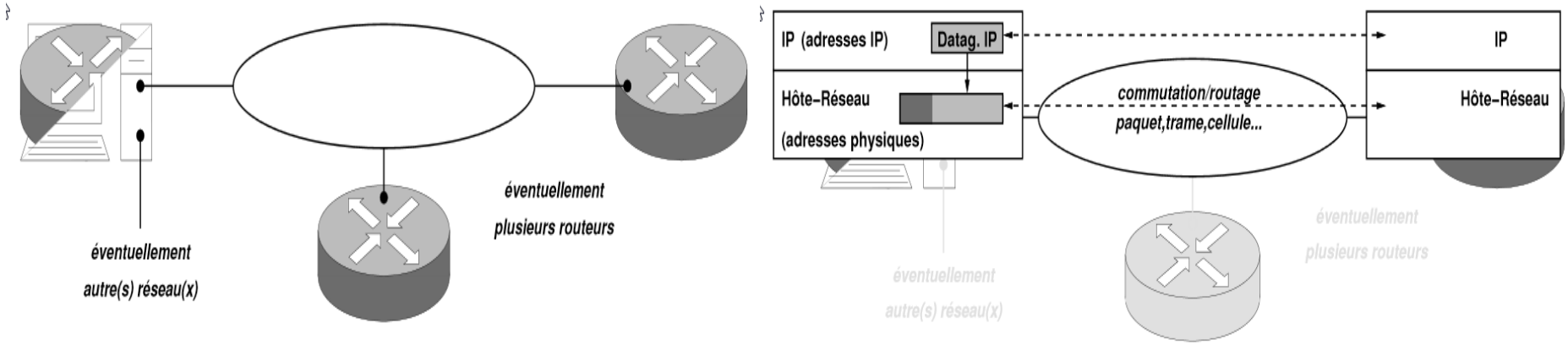
Test d'appartenance au même réseau

- soient S avec 3 interfaces (S_1, S_2 et S_3) et une destination $D_1 = 139.124.187.18$:



  - $S_1 = 12.143.1.163$ (classe A) $\Longrightarrow R(S_1) = 12.0.0.0$
  - $S_2 = 139.124.187.4$ (classe B) $\Longrightarrow R(S_2) = 139.124.0.0$
  - $S_3 = 195.118.10.34$ (classe C) $\Longrightarrow R(S_3) = 195.118.10.0$
- l'adresse de D_1 est de classe B $\Longrightarrow R(D_1) = 139.124.0.0$
- puisque $R(D_1) = R(S_2)$, alors D_1 et S appartienent à un même réseau
- S peut envoyer directement un datagramme à D_1 en utilisant l'interface (et le réseau) associée à S_2

Remise indirecte



- **Méthode**
  1. déterminer l'adresse IP du routeur à solliciter par consultation de la table de routage
  2. transmettre le datagramme au routeur
     a. Déterminer son adresse physique (résolution d'adresse)
     b. Utiliser le service du réseau pour lui transmettre le datagramme

Test d'appartenance au même réseau

- le même S (avec 3 interfaces) doit envoyer à une destination $D_2 = 195.118.11.35$:

  - $S_1 = 12.143.1.187$ (classe A) $\Longrightarrow R(S_1) = 12.0.0.0$
  - $S_2 = 139.124.187.4$ (classe B) $\Longrightarrow R(S_2) = 139.124.0.0$
  - $S_3 = 195.118.10.34$ (classe C) $\Longrightarrow R(S_3) = 195.118.10.0$
- l'adresse de D_2 est de classe C $\Longrightarrow R(D_2) = 195.118.11.0$
- $R(D_2)$ est différent de tous les $R(S_i)$, alors D_1 et S appartienent à des réseaux différents
- pour envoyer un datagramme à D_2, S doit passer par un routeur connecté à l'un de ses réseaux

Traitement du datagramme reçu

- Traitement par un routeur
  - Si le datagramme est destiné au routeur, l'accepter
  - Sinon le routeur est utilisé comme nœud de transfert et doit relayer le datagramme (si aucun route , message ICMP renvoyé)
- Traitement par une station
  - Si le datagramme est destiné à la station , l'accepter
  - Sinon le datagramme est détruit et un message ICMP est envoyé

Remarque : une station, même disposant de plusieurs interfaces, n'assure pas systématiquement la fonction de routeur, il faut qu'elle soit configurée

Table de routage

- chaque station ou routeur dispose de sa propre table de routage
- une table contient autant d'entrées que de destinations (réseaux) connues de l'hôte
- une entrée est un couple (adresse réseau, adresse du saut suivant (routeur))
- pour une destination donnée, la table n'indique pas le chemin à suivre, seulement le routeur à qui confier le datagramme

➔ le chemin est une information répartie

- ce routeur doit être directement accessible (situé sur un réseau commun) et c'est son adresse dans ce réseau qui est utilisée
- une destination dont l'adresse de réseau ne figure pas dans la table est inaccessible

Exemple

Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté

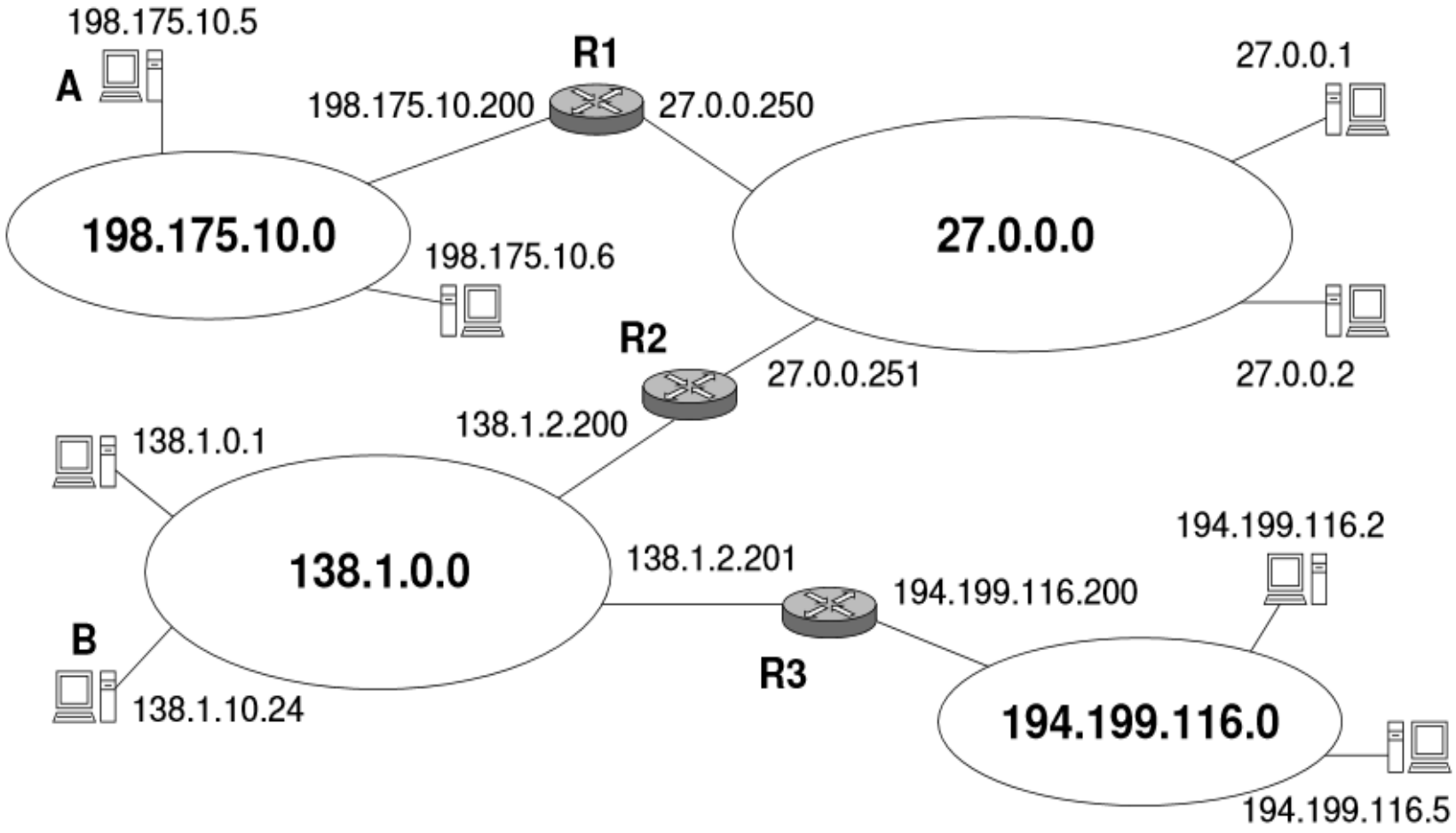


Table de routage

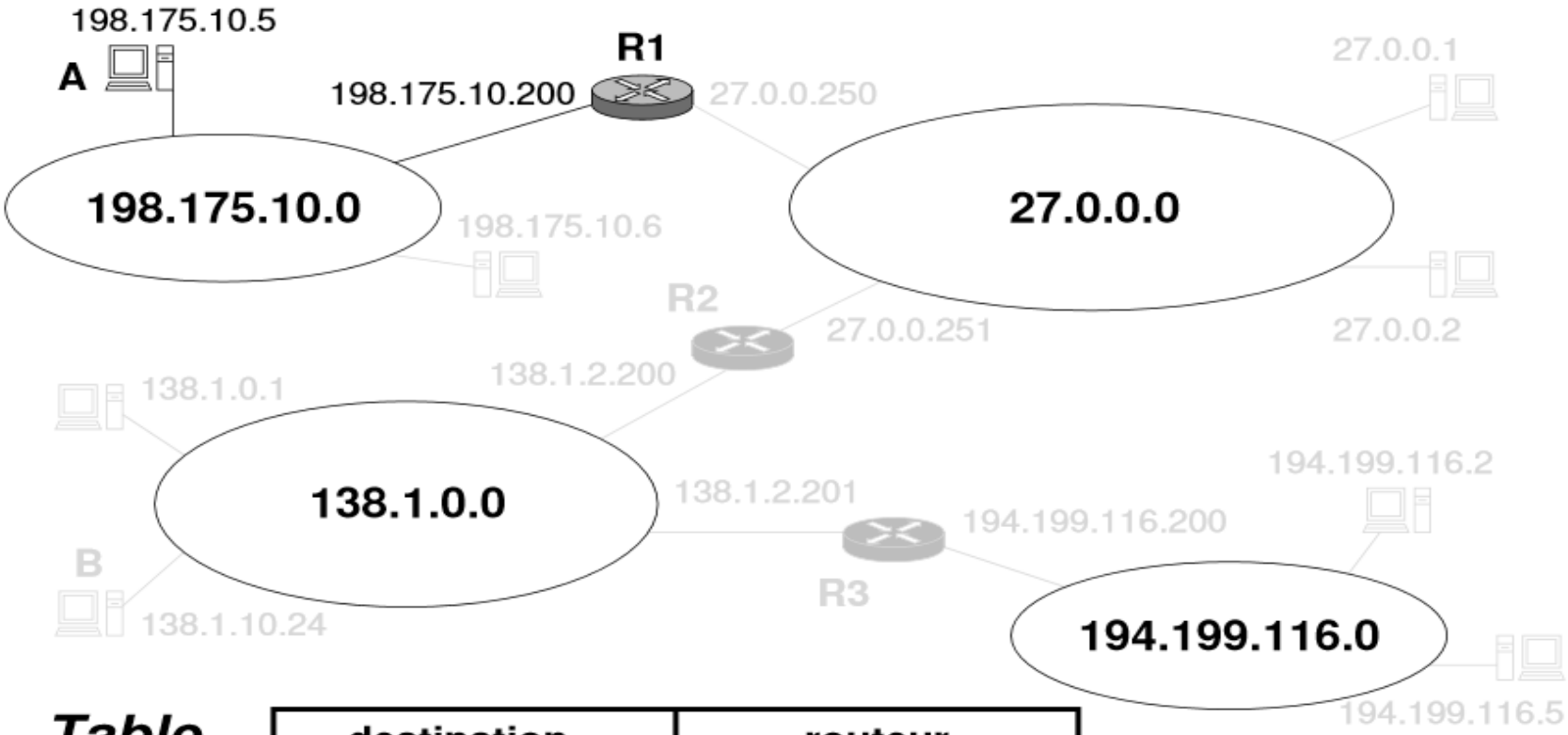


Table de A :

destination	routeur	
198.175.10.0	0.0.0.0	*remise directe*
27.0.0.0	198.175.10.200	
138.1.0.0	198.175.10.200	*remise indirecte*
194.199.116.0	198.175.10.200	

Table de routage

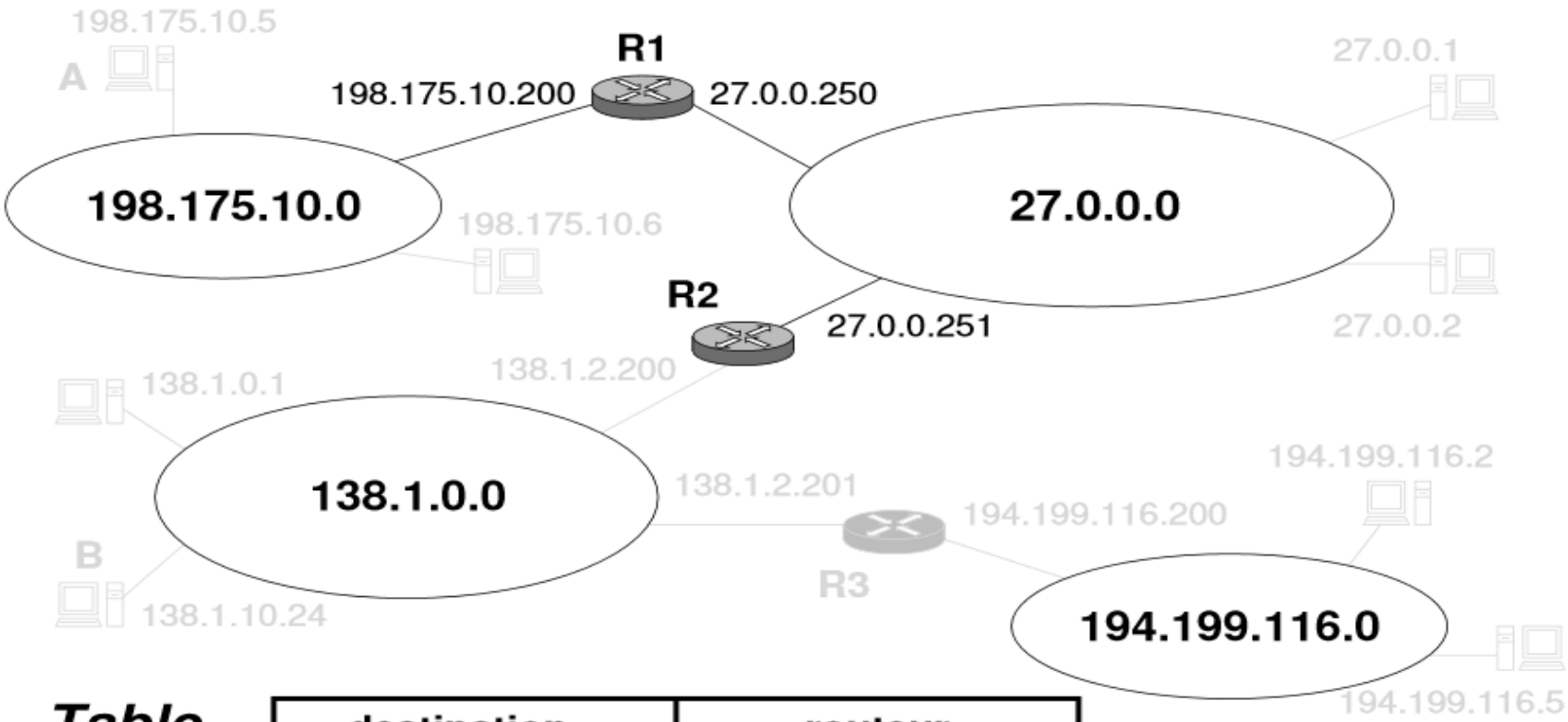


Table de R1 :

destination	routeur	
198.175.10.0	0.0.0.0	*remise directe*
27.0.0.0	0.0.0.0	
138.1.0.0	27.0.0.251	*remise indirecte*
194.199.116.0	27.0.0.251	

Table de routage

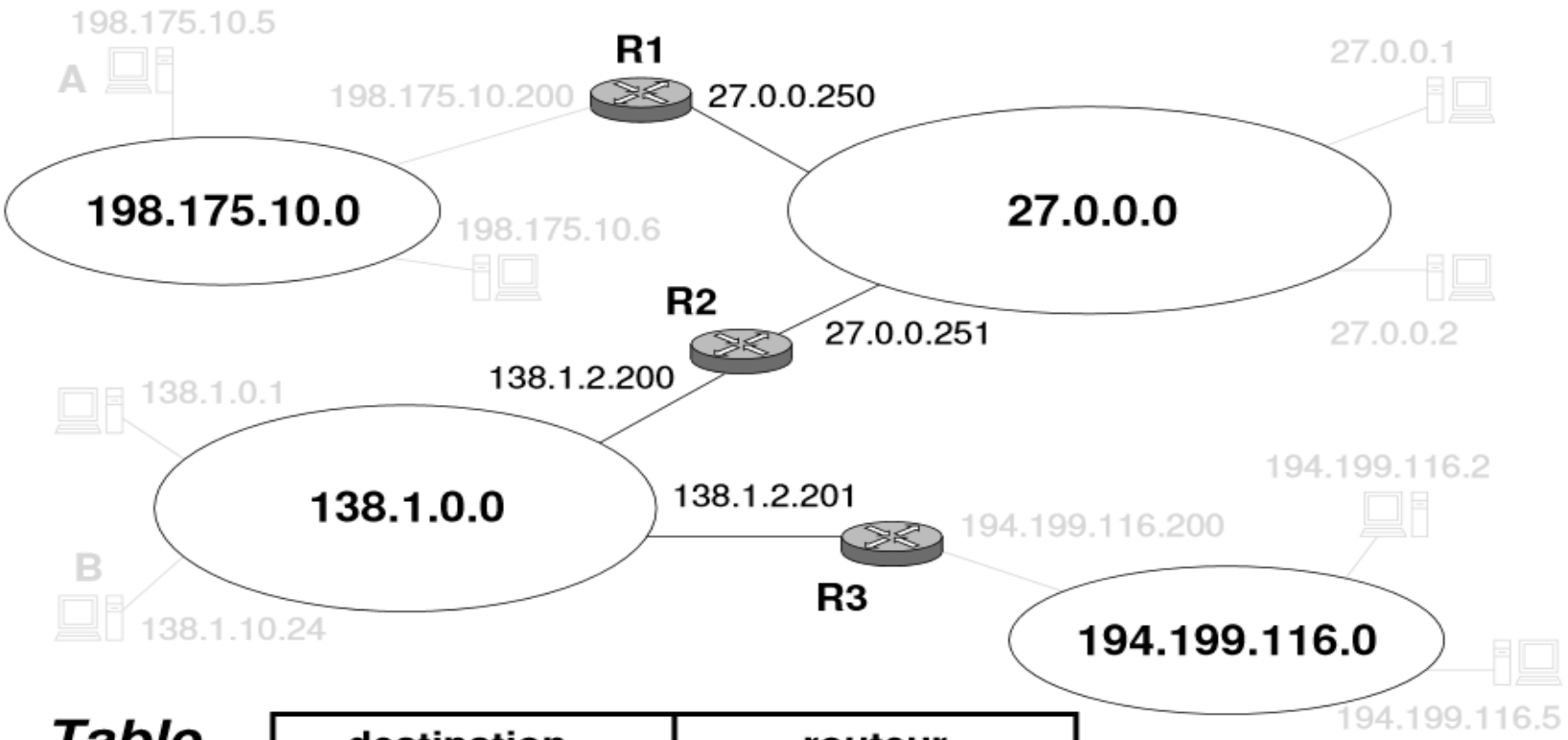
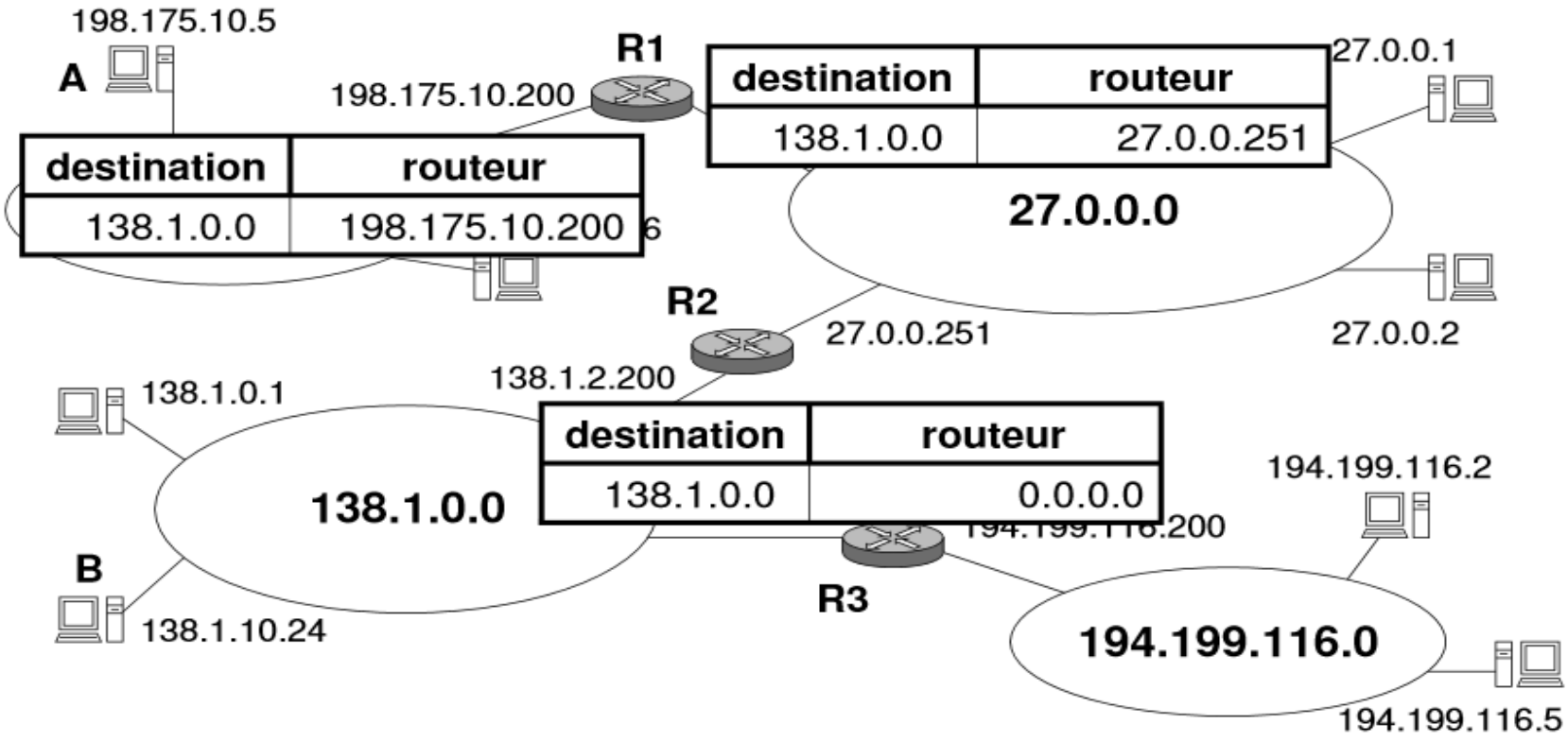


Table de R2 :

destination	routeur	
27.0.0.0	0.0.0.0	*remise directe*
138.1.0.0	0.0.0.0	
198.175.10.0	27.0.0.250	*remise indirecte*
194.199.116.0	138.1.2.201	

Table de routage



le chemin qui mène de A à B est une information répartie :

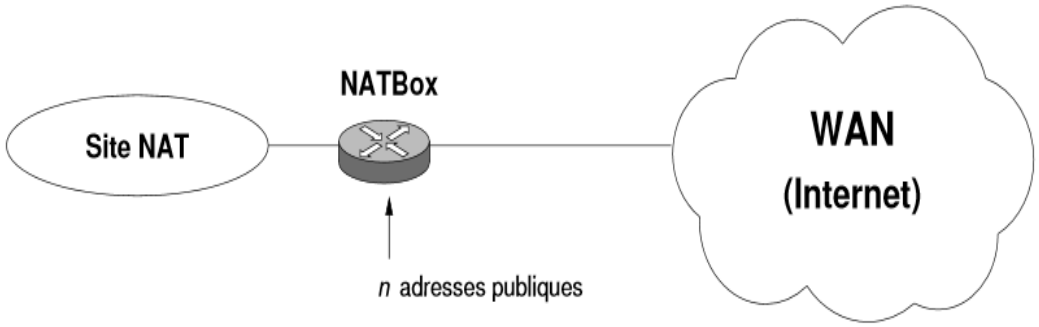
aucun hôte ne le connaît en totalité

Network Address Translation (NAT)

- C’est un système qui fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables.
- Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.
- La fonction NAT dans un routeur de service intégré (ISR) traduit une adresse IP source interne en adresse IP globale.

Principe de la traduction d'adresse

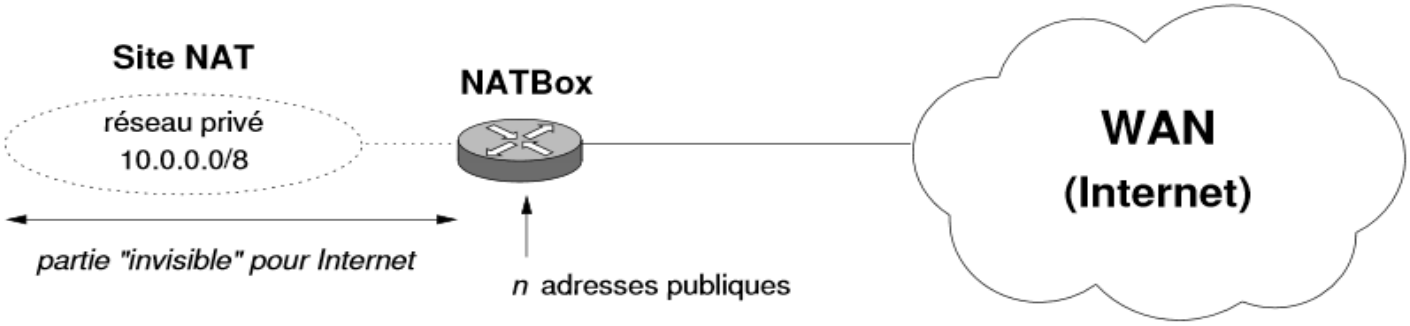
- Permettre à n adresses publiques d'être partagées par un grand nombre m de stations (périphériques réseau)



- il faut placer une NATBox qui doit être le seul point de passage entre le Site NAT (réseau de l'organisation) et le WAN (Internet)
- la NATBox est la seule qui possède et gère les n adresses publiques

Quelques précisions

- une NATBox est un routeur avec les fonctionnalités NAT (la plupart des routeurs, et les **box* des FAI)
- les stations du Site NAT n'ont pas connaissance des adresses publiques de la NATBox et ne les utilisent pas
- mais ont des **adresses privées** qu'il est fortement conseillé de prendre dans les plages définies par la RFC 1918 :
  - 10.0.0.0/8 soit 16 777 216 adresses (de 10.0.0.0 à 10.255.255.255)
  - 172.16.0.0/12 soit 1 048 576 adresses (de 172.16.0.0 à 172.31.255.255)
  - 192.168.0.0/16 soit 65 536 adresses (de 192.168.0.0 à 192.168.255.255)



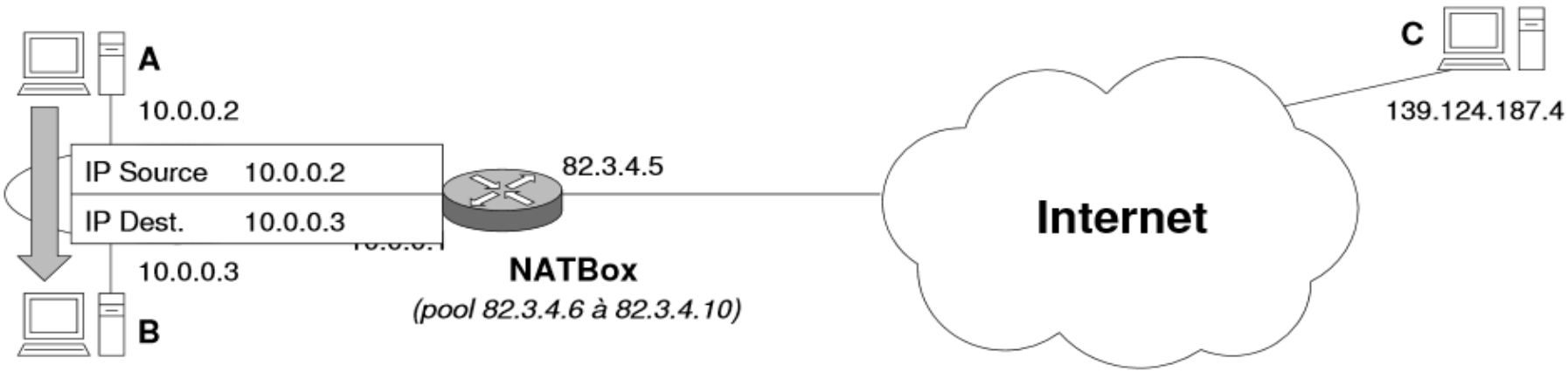
Remarque : Pour les stations du WAN, seules les n adresses de la NATBox existent et le Site NAT avec ses adresses privées est invisible

Quelques précisions

- A l’intérieur du Site NAT, les stations communiquent entre elles en utilisant leurs adresses privées
- sans le NAT, un message envoyé à l'extérieur ne pourrait avoir de réponse car les adresses privées ne sont pas routables dans le WAN
- la NATBox doit traduire (remplacer) dans un tel message, l'adresse privée par une adresse publique, et inversement pour la réponse

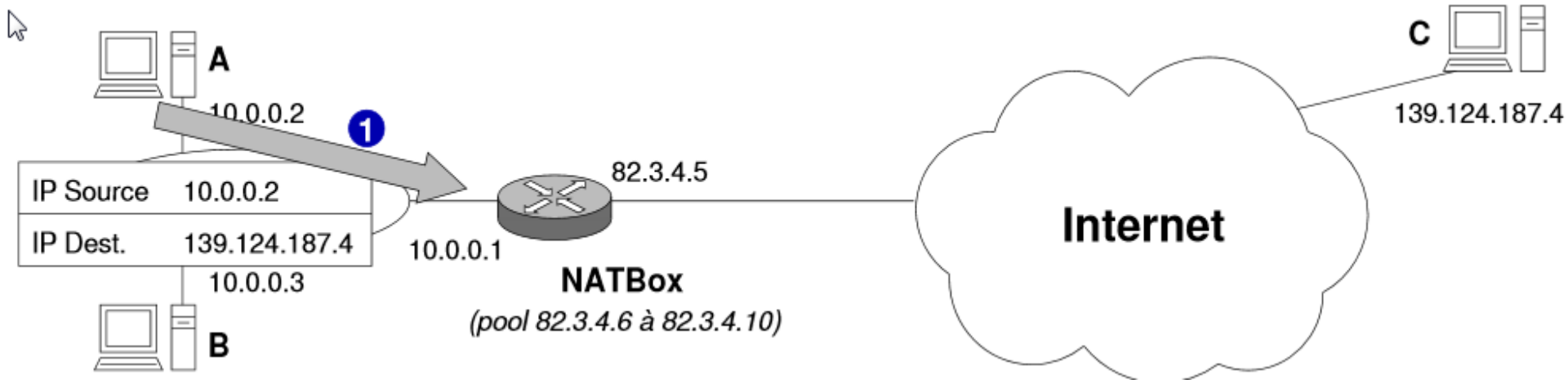
NAT et la discussion interne

- La station A (10.0.0.2) veut discuter avec la station B (10.0.0.3) :
  - le dialogue étant interne, la NATBox n'est pas concernée par ce trafic
  - les datagrammes contiennent les adresses de A et de B



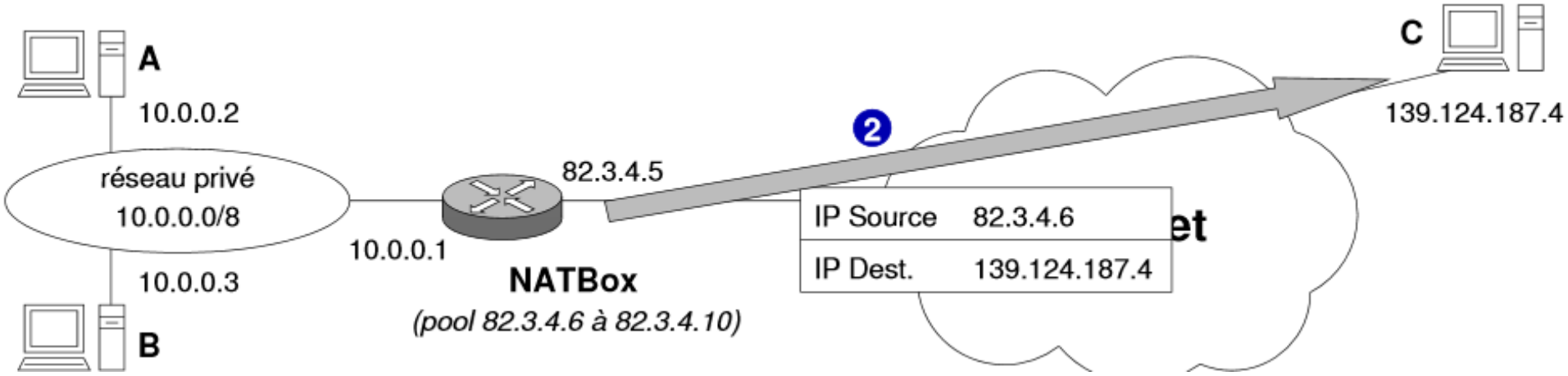
NAT et la discussion extérieur

- A (10.0.0.2) veut discuter avec la station externe C (139.124.187.4) :
  1. A envoie le datagramme qui parvient au routeur (NATBox)



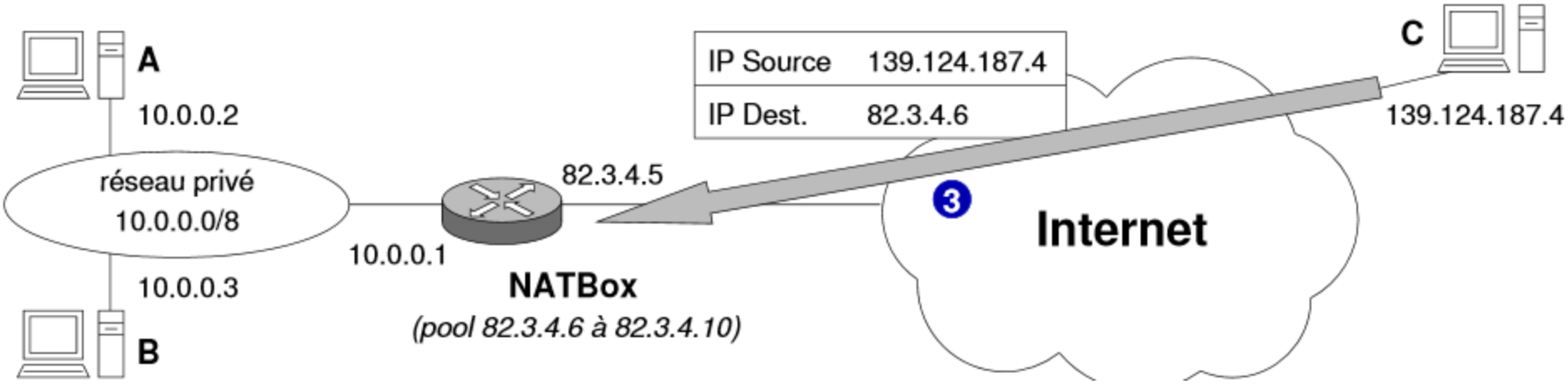
NAT et la discussion extérieur

- 2. La NATBox remplace l'adresse source (privée) par une adresse publique disponible (82.3.4.6), enregistre une association (82.3.4.6, 10.0.0.2) dans sa table de traductions , et transmet le datagramme vers C



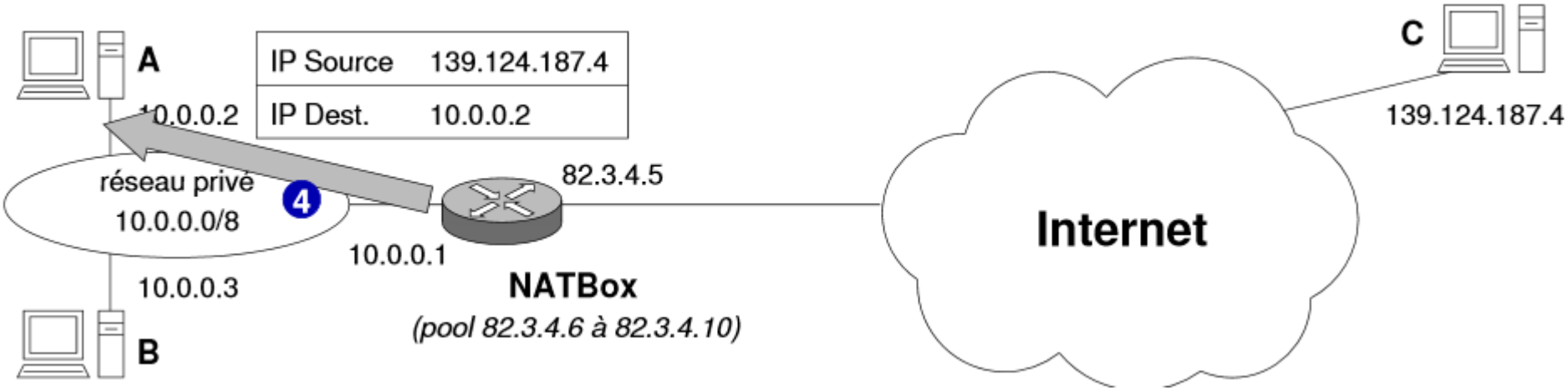
NAT et la discussion extérieur

3. C répond a l'adresse source du datagramme (82.3.4.6)



NAT et la discussion extérieur

- 4. la NATBbox reçoit le datagramme, consulte sa table de traductions, trouve l'association (82.3.4.6, 10.0.0.2), remplace l'adresse destination par 10.0.0.2 et retransmet le datagramme à A



Prochains cours

- Serveur de domaine DNS (*Domain Name System*).
- Protocole DHCP signifie **Dynamic Host Configuration Protocol**. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir *dynamiquement* (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau).
- Serveur HTTP

Source

- Slides tirés du cours de C. Pain-Barre