

**Ministère de l'enseignement supérieur et de la recherche scientifique**

**École supérieure en informatique de Sidi Bel Abbès**



**Module: RÉSEAUX I**

**Chapitre 5: Adressage et Routage**

# Partie 5 : IP - Plan

1. Interconnexion IP
2. Relayage et routage IP
3. Adressage IP
4. Datagramme IP
5. Fragmentation
6. ICMP

# IP - Plan

## 1. **Interconnexion IP**

- ✓ concept d'interconnexion
- ✓ rôle de IP
- ✓ service de IP

## 2. Relayage et routage IP

## 3. Adressage IP

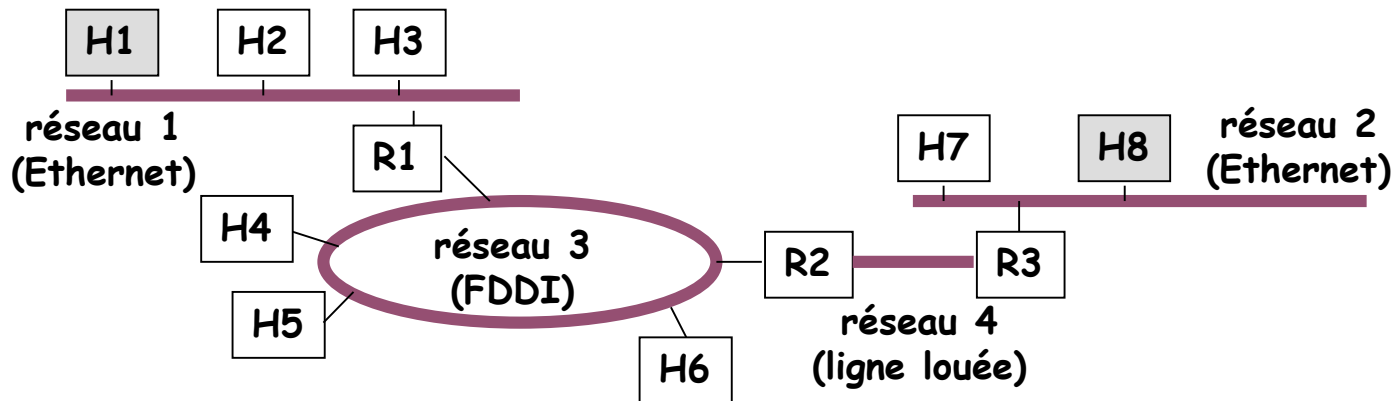
## 4. Datagramme IP

## 5. Fragmentation

## 6. ICMP

# Interconnexion

- une concaténation de réseaux
  - à l'intérieur d'un réseau, les nœuds utilisant la technologie spécifique de leur réseau



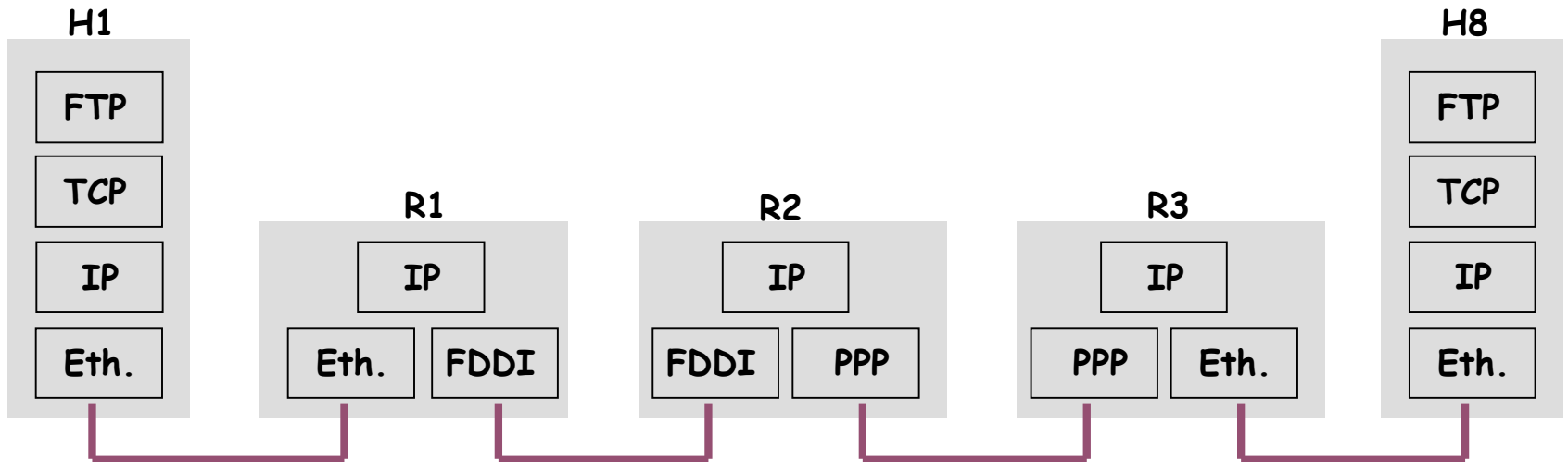
- l'**interconnexion** consiste à faire transiter des informations depuis une machine sur un réseau vers une autre machine sur un autre réseau
  - les différences entre tous les réseaux ne doivent pas apparaître à l'utilisateur

# Interconnexion

- Principe
  - mise en œuvre d'une couche réseau
    - masquant les détails de la communication physique du réseau
    - détachant les applications des problèmes de routage
- le logiciel d'interconnexion
  - fait apparaître l'ensemble des réseaux disparates comme un seul et unique réseau
  - offre un service commun à toutes les applications

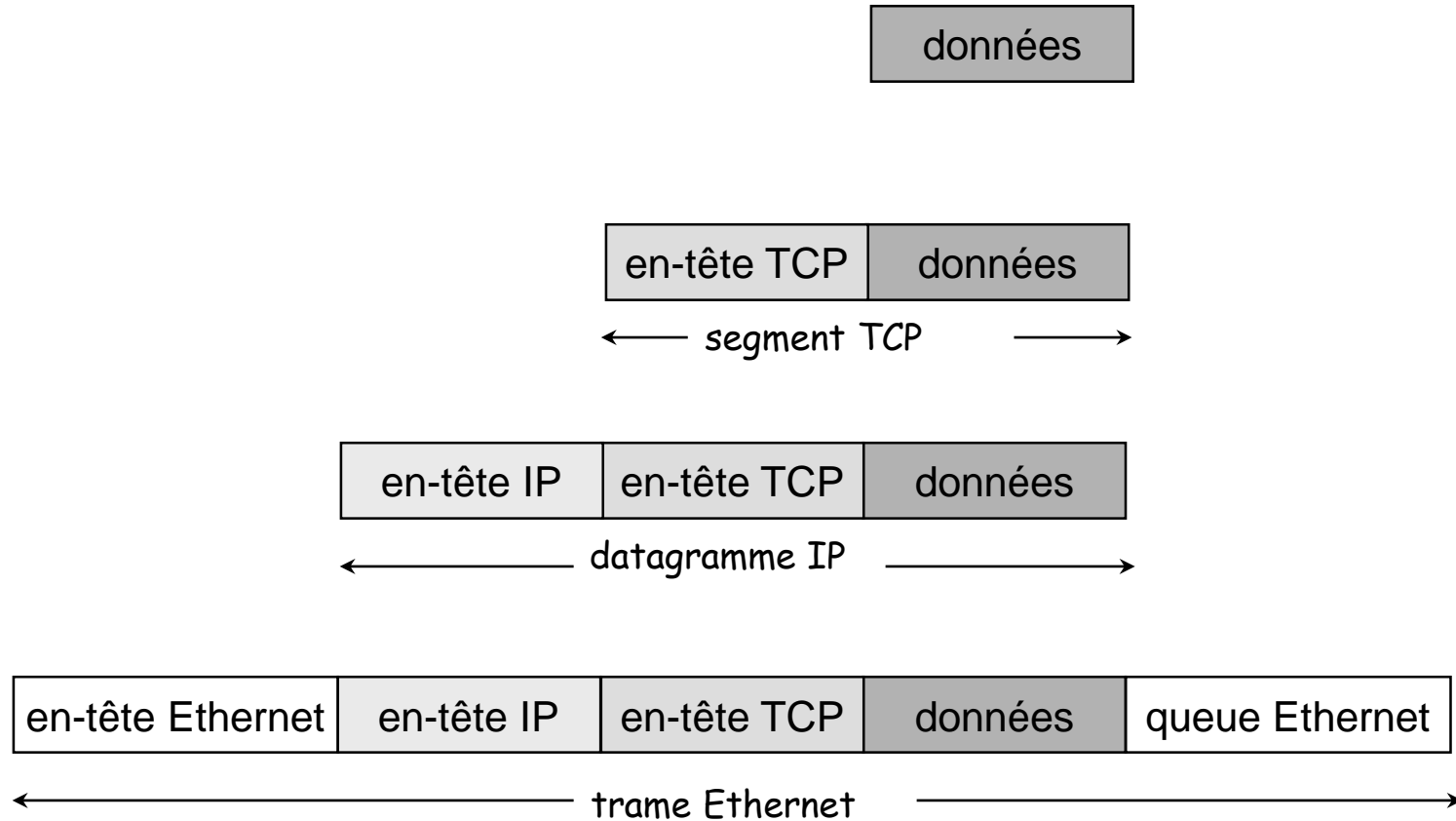
# Interconnexion IP

- la glue qui lie l'Internet : le protocole **IP** (*Internet Protocol*)
- une pile de protocoles



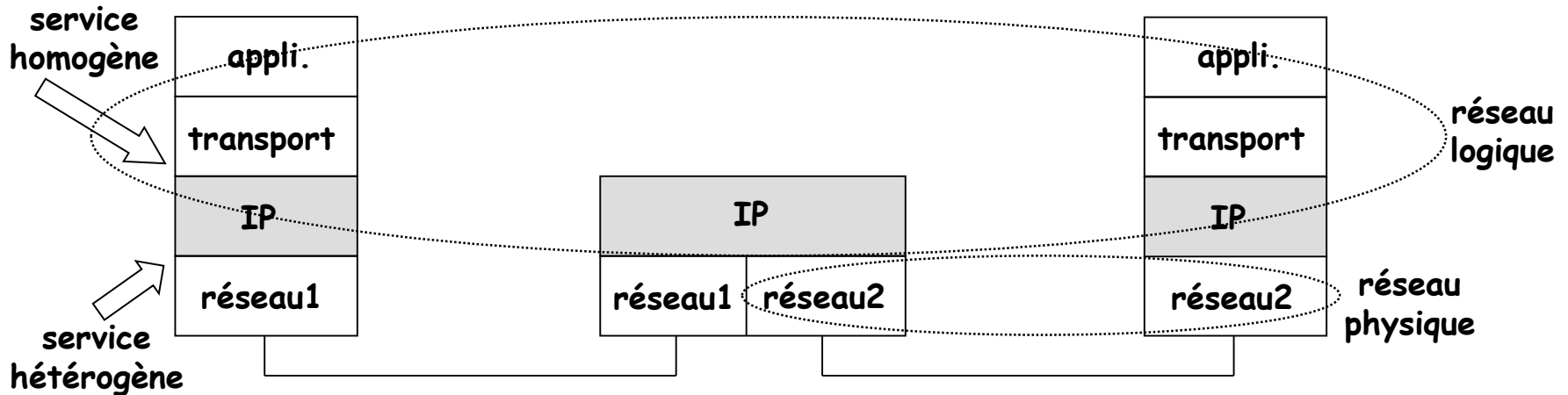
# Encapsulations successives

- cas application / TCP / IP / Ethernet



# Internet Protocol (IP)

- protocole de la couche d'interconnexion



- caractéristiques de l'interface IP
  - adresse unique et homogène
  - transfert par blocs (datagrammes)
  - service sans connexion
  - service *best effort* (les datagrammes ne sont pas éliminés sans raison)
- fonctions de IP
  - adressage
  - routage
  - fragmentation



# Service IP

- utilise un service minimum
  - envoi d'une unité de transfert d'un point à ses voisins
  - voisin : partage la même connexion physique
- rend un service minimum
  - service en mode non connecté
    - absence d'états dans les routeurs
    - transmission de datagrammes
  - remise *best effort*
    - service non fiable
  - service de connectivité
- avantages
  - ☺robustesse
  - ☺efficace pour les échanges brefs
  - ☺simplicité d'utilisation

# Primitives de service IP

## **SEND (**

adresse source

adresse destination

TCP ou UDP: protocole supérieur

indicateurs de QOS: high ou normal

rapidité: de remise demandée

priorité: traitement d'abord

débit:

sécurité:

identificateur du paquet courant

indicateur de fragmentation: oui ou non

durée de vie

longueur des données

données optionnelles: sécurité (mot de passe pour une passerelle), routage/ source, enregistrement du chemin, estampillage (enregistrement de l'heure de chaque passage)

données )

## **DELIVER (**

adresse source

adresse destination

TCP ou UDP: protocole supérieur

indicateurs de QOS: high ou normal

longueur des données

données optionnelles et données )

# IP - Plan

1. Interconnexion IP
2. **Relayage et routage IP**
  - relayage IP
  - routage IP
3. Adressage IP
4. Datagramme IP
5. Fragmentation
6. ICMP

# Relayage vs. routage

- relayage (*forwarding*)

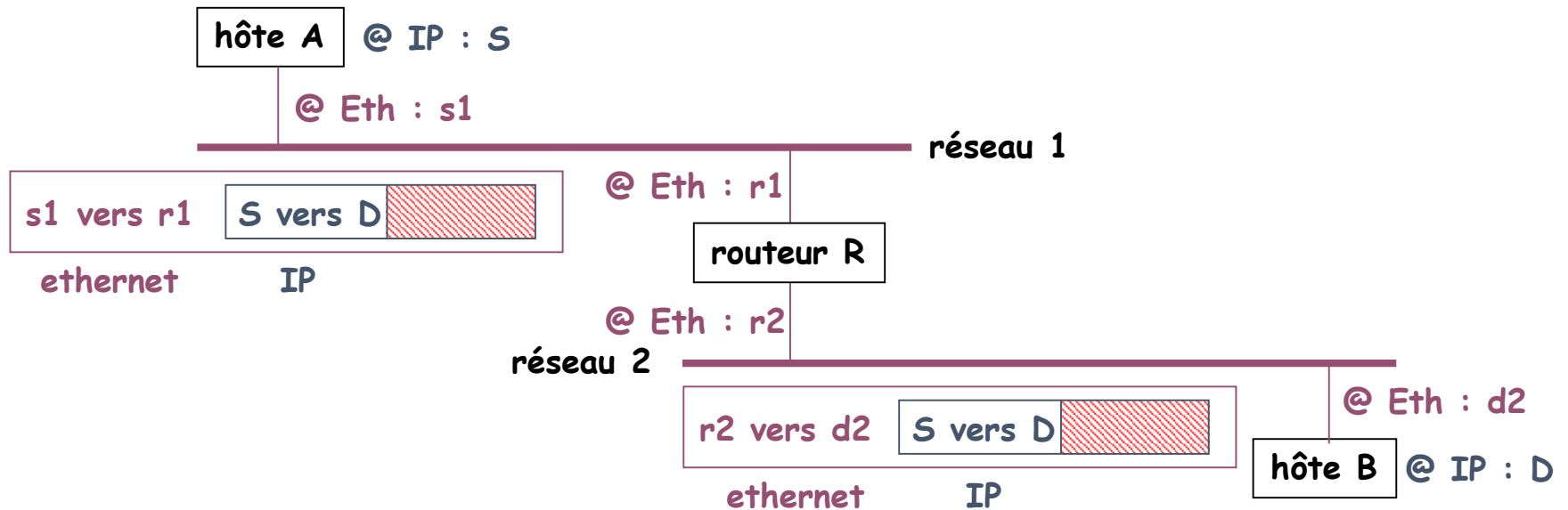
- action de retransmettre sur une interface un datagramme reçu sur une autre interface et n'étant pas arrivé à destination

- routage

- action de chercher (1) l'interface sur laquelle transmettre un datagramme, et (2) le destinataire immédiat
- interface (réseau) : point d'accès au réseau (physique)

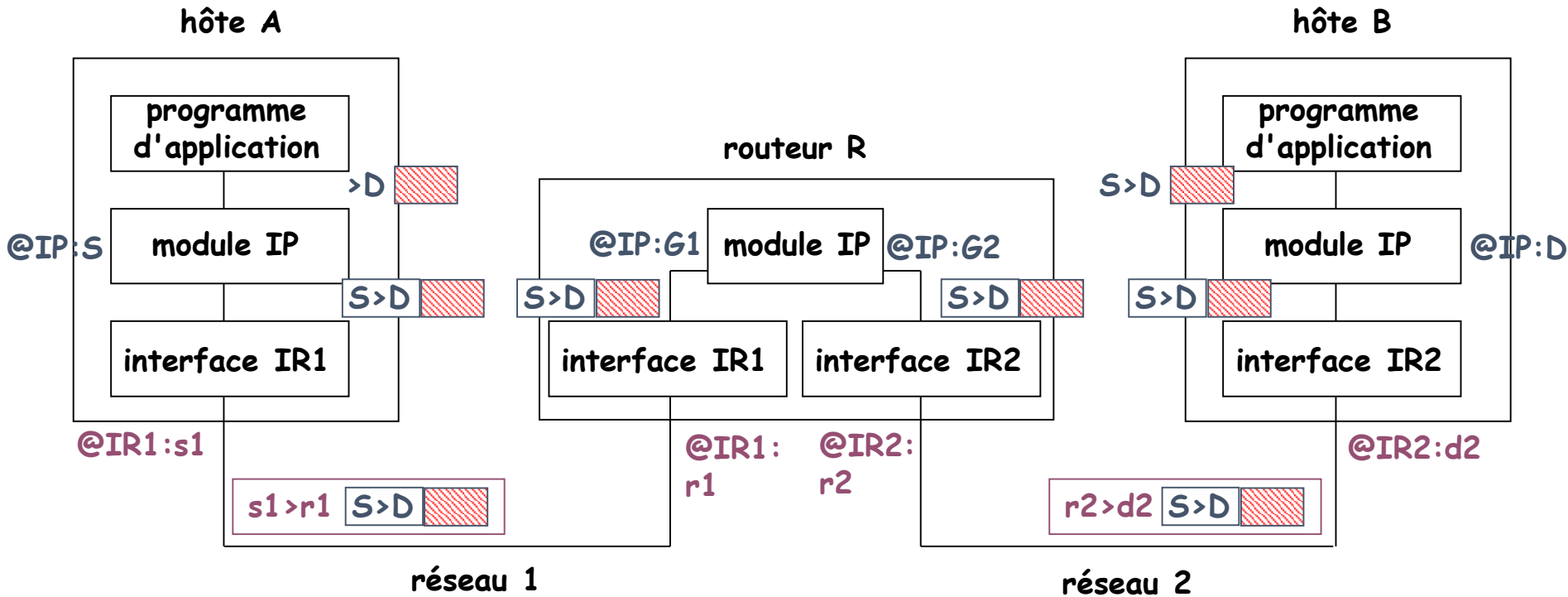
# Relayage par IP

- Vue topologique



# Relayage par IP

- Vue architecturale



# Que fait un routeur ?

Pour chaque datagramme IP qui traverse le routeur, IP :

- vérifie le checksum, si faux → destruction du datagramme
- détermine si ce sont des données *utilisateur* ou de *contrôle* destinées au routeur
- décrémente la durée de vie, si nulle → destruction du datagramme
- **décide du routage**
- **fragmente** le datagramme si nécessaire
- **reconstruit l'en-tête IP** avec les champs mis à jour
- transmet le(s) datagramme(s) au protocole d'accès de l'interface réseau de sortie avec **l'adresse de sous-réseau correspondante**

A réception dans l'hôte destinataire, IP :

- vérifie le checksum
- s'il y a eu fragmentation, mémorise puis **réassemble**
- **délivre au niveau supérieur** les données et les paramètres par la primitive DELIVER

# Routage

- fonction déterminant un chemin vers une adresse destinataire

## ↳ table de routage

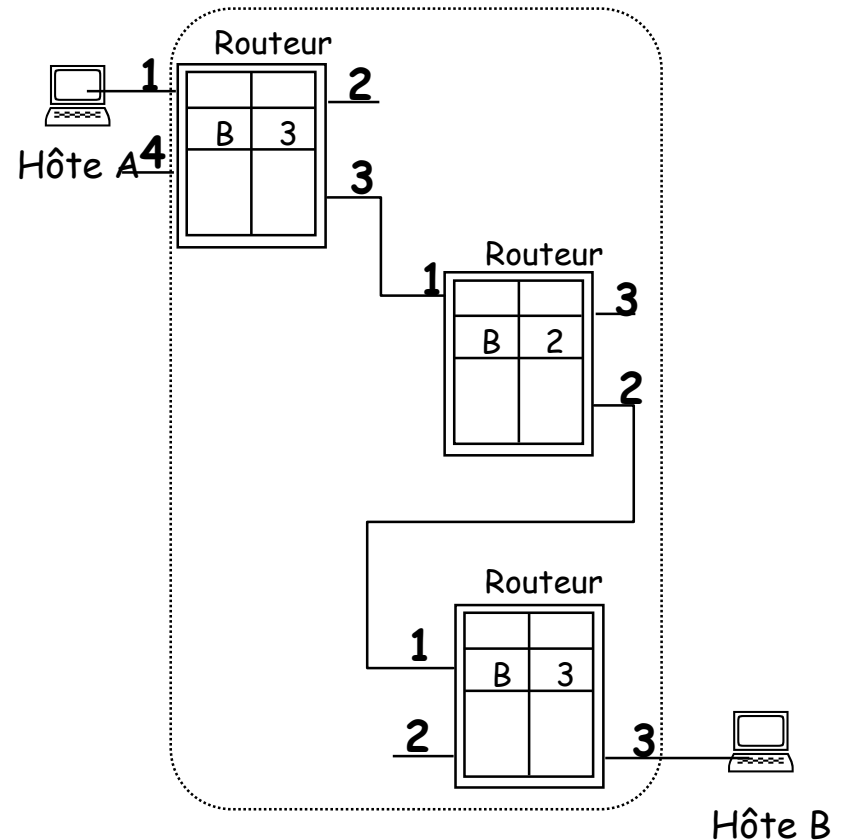
- informations nécessaires pour atteindre le prochain nœud

## ↳ algorithme de routage

- calcul d'un chemin optimal pour atteindre une adresse destinataire

## ↳ protocole de routage

- échange d'informations de routage
- dépend du domaine dans lequel se trouve le routeur
- ex : RIP, OSPF, ...





# Tables de routage

- contiennent 3 informations

- destination

- réseau
- sous-réseau
- machine
- default

- chemin

- interface locale à la machine
- un routeur intermédiaire

- coût ou *métrique*

- nombre de hops
- débit ...

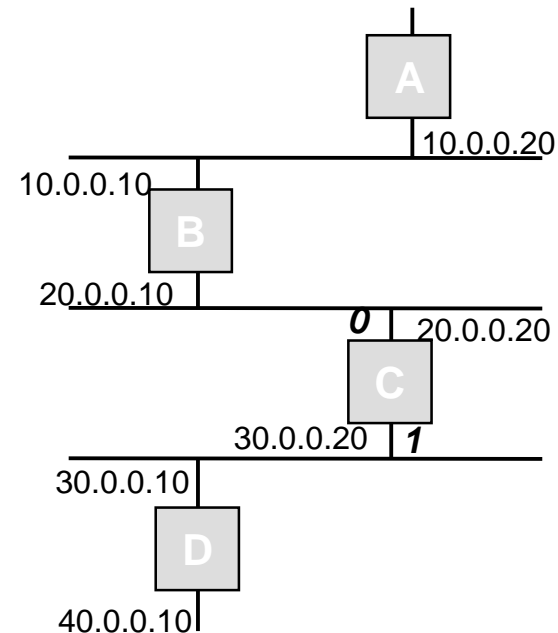


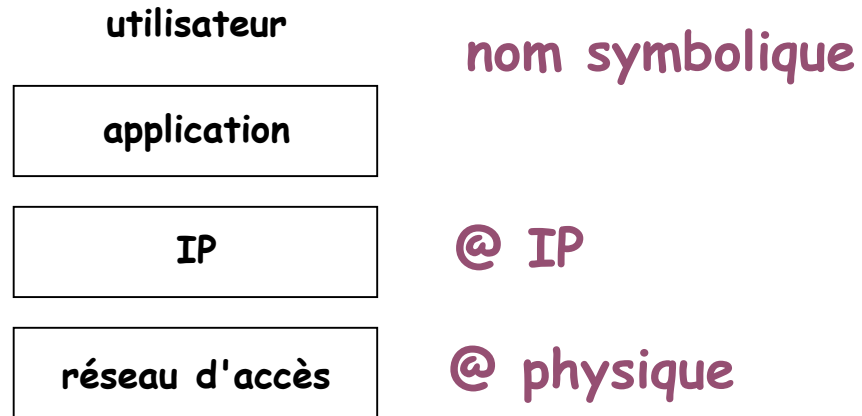
Table du nœud C

Préfixe @destinataire	@routeur par où passer
10.0.0	20.0.0.10
20.0.0	<i>eth0</i>
30.0.0	<i>eth1</i>
40.0.0	30.0.0.10

# Routage direct/indirect

- le module IP examine l'adresse de destination du datagramme et détermine si la destination est sur un même réseau physique
  - si oui : **routage direct**
    - la destination étant sur un même réseau physique, le datagramme est transmis directement
      - ↳ l'adresse physique suivante est celle de la destination
  - si non : **routage indirect**
    - la destination étant sur un réseau physique différent, le datagramme est transmis au routeur suivant
      - ↳ l'adresse physique suivante est celle du routeur suivant

# Différentes "adresses"

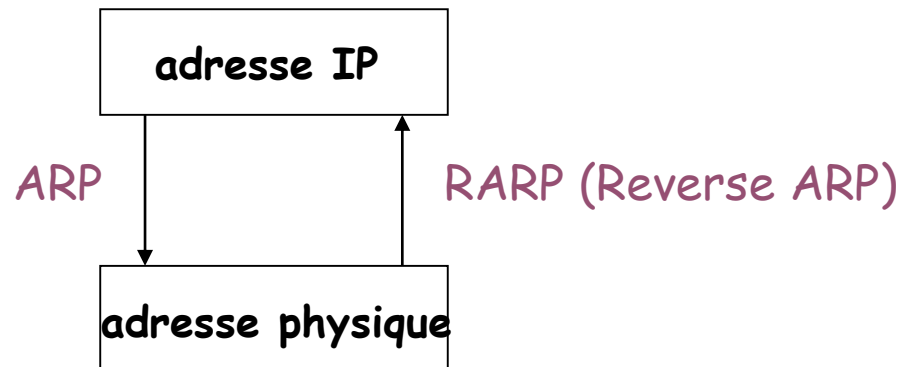


↪ 2 niveaux de conversion

- nom ⇔ adresse IP
- adresse IP ⇔ adresse physique

# Adressage physique

- Principe
  - adresse propre au système de transmission
  - identifie le périphérique
  - multitude d'espaces d'adressage
  - exemples
    - @ Ethernet : sur 6 octets, adressage absolu
    - @ ATM : sur 20 octets, adressage hiérarchique
- besoin d'une glue : Address Resolution Protocol



# IP - Plan

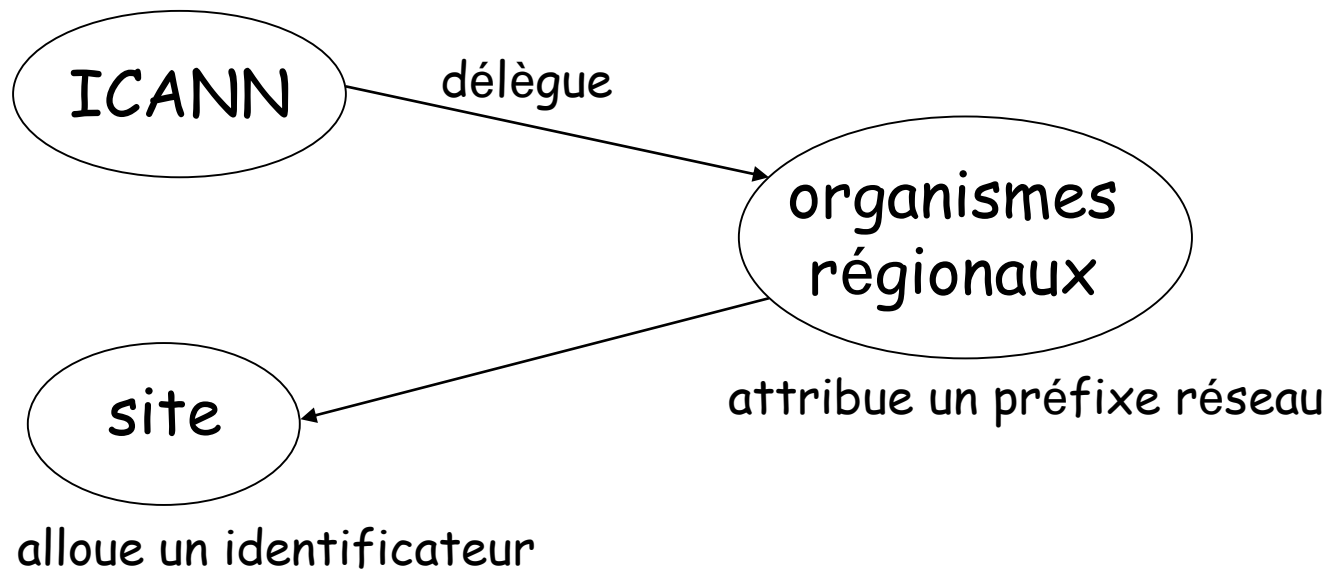
1. Interconnexion IP
2. Relayage et routage IP
3. **Adressage IP**
  - classes d'adresses
  - subnetting
4. Datagramme IP
5. Fragmentation
6. ICMP

# Adressage IP

- adressage
  - pour l'identification d'un équipement réseau
  - pour le routage
- plan d'adressage homogène
  - format : 4 octets ➔ 4,3 milliards d'adresses ???
  - notation décimale pointée : x1.x2.x3.x4
- adresse globalement unique et hiérarchique
- format : <réseau> <machine>
  - localisateur ou préfixe réseau : identificateur de réseau
  - identificateur : identificateur de machine

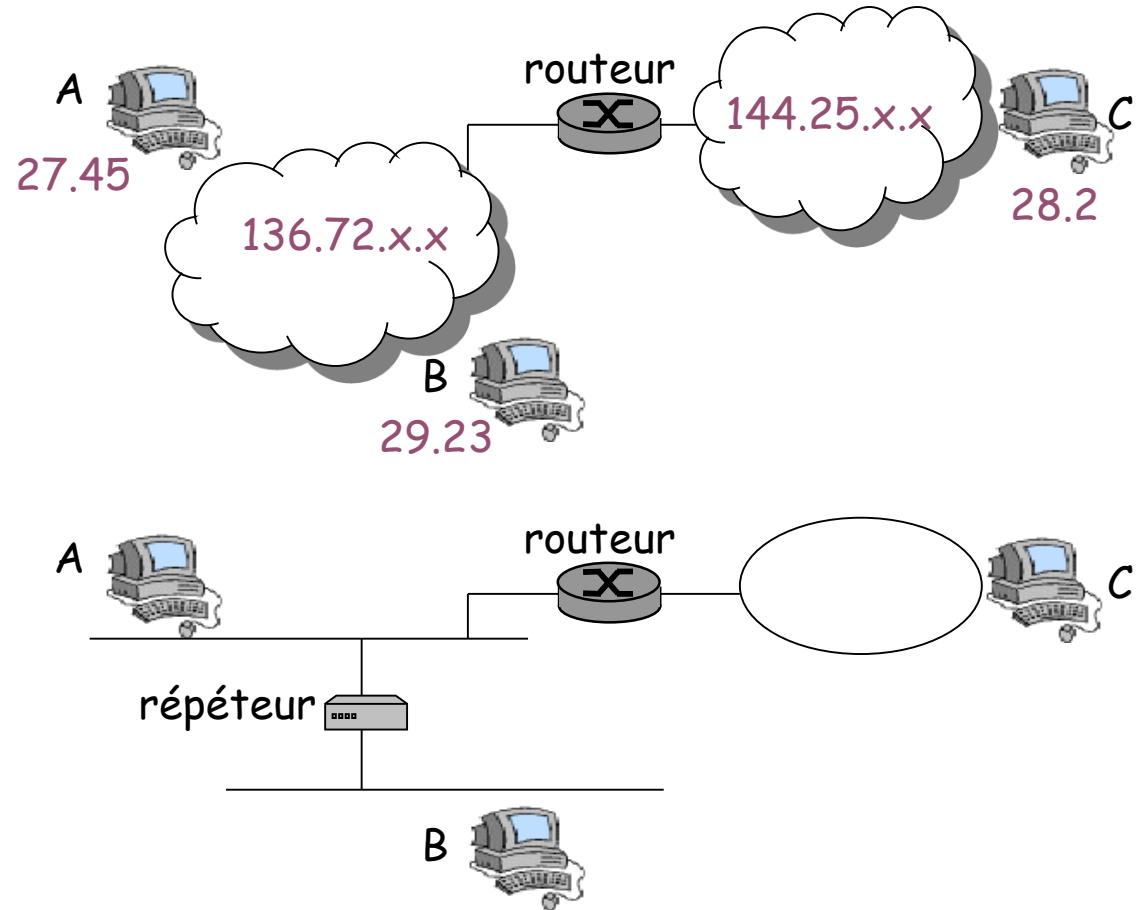


# Attribution des adresses



# Adressage réseau

- un préfixe réseau par réseau physique
  - au niveau IP

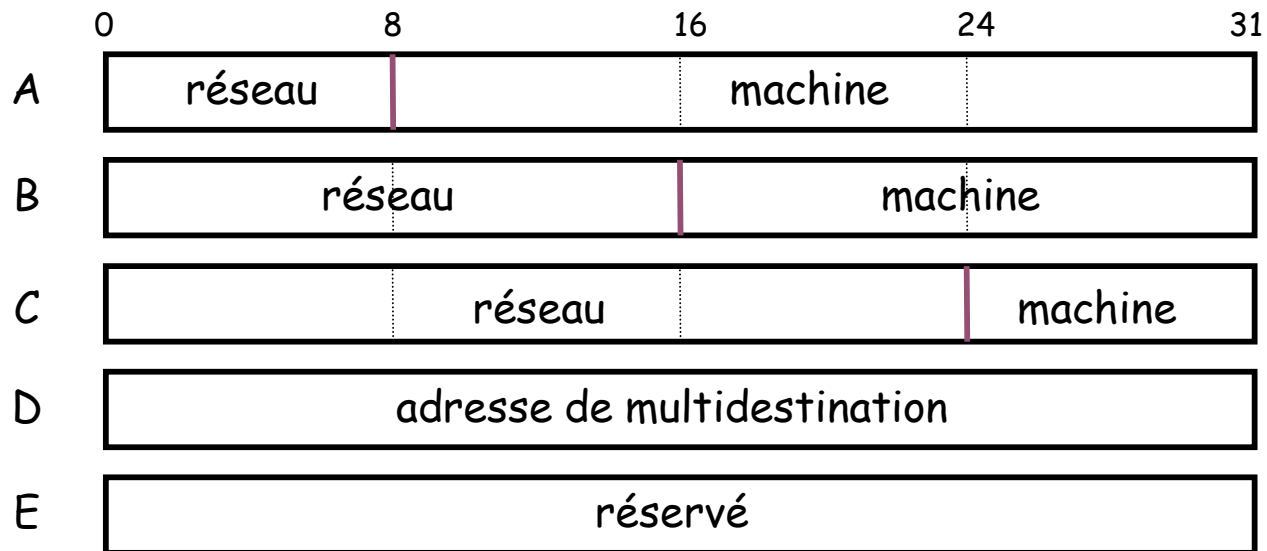




# Classes d'adresses

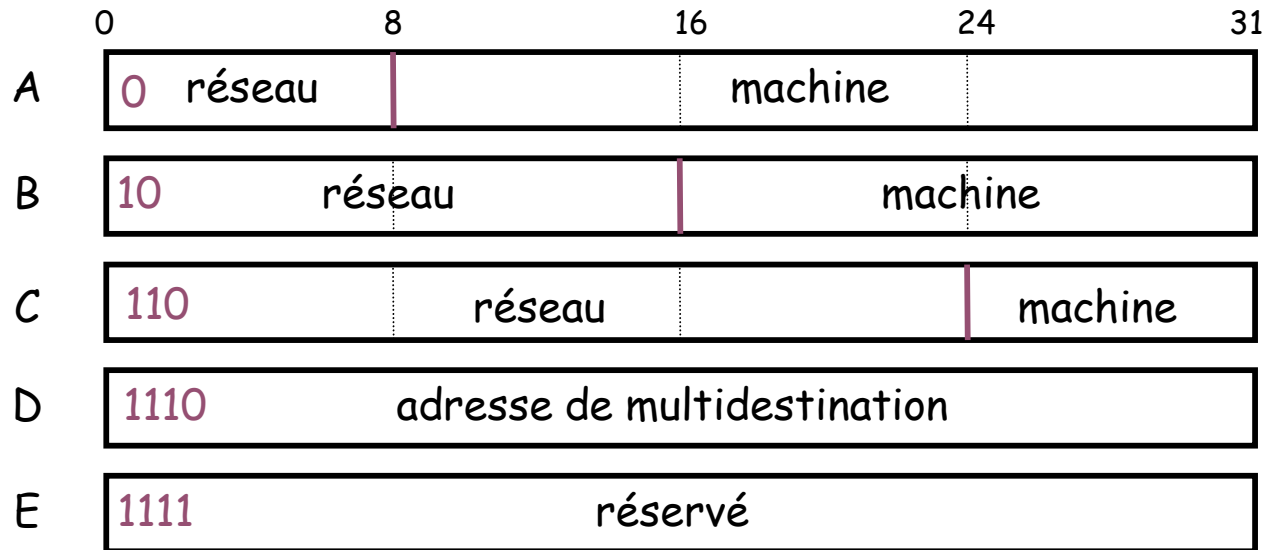
- le découpage <réseau> / <machine> n'est pas fixe

↳ 5 classes d'adresses



- comment reconnaître ces classes ?

# Classes d'adresses



# Classes d'adresses

- **classe A** :  $2^7$  réseaux (128)
  - réservé: 0.0.0.0 et 127.0.0.0
  - disponible: 1.0.0.0 à 126.0.0.0
    - 126 réseaux classe A et 16 777 214 machines/réseau
- **classe B** :  $2^{14}$  réseaux (16 384)
  - réservé: 128.0.0.0 et 191.255.0.0
  - disponible 128.1.0.0 à 191.254.0.0
    - 16 382 réseaux classe B et 65 534 machines/réseau
- **classe C** :  $2^{21}$  réseaux (2 097 152)
  - réservé 192.0.0.0 et 223.255.255.0
  - disponible 192.0.1.0 à 223.255.254.0
    - 2 097 150 réseaux classe C et 254 machines/réseau

# Les adresses particulières



↳ une adresse IP dont la valeur hostid ne comprend que des 1 ne peut être attribuée à une machine réelle

- c'est une **adresse de diffusion dirigée**

↳ une adresse IP dont la valeur hostid ne comprend que des 0 ne peut être attribuée à une machine réelle

- c'est une **adresse de réseau**

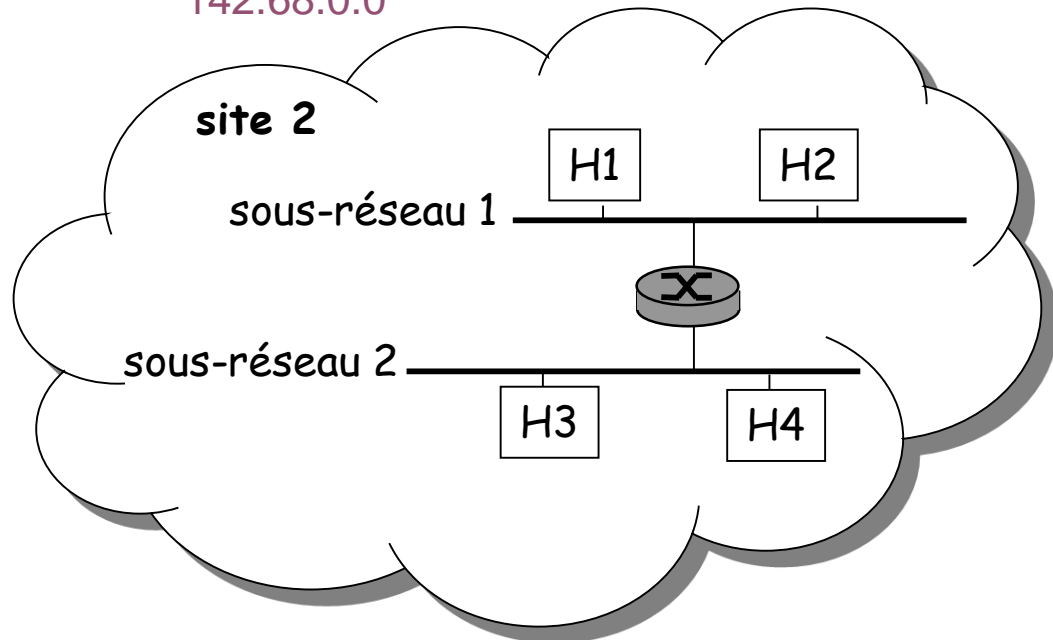
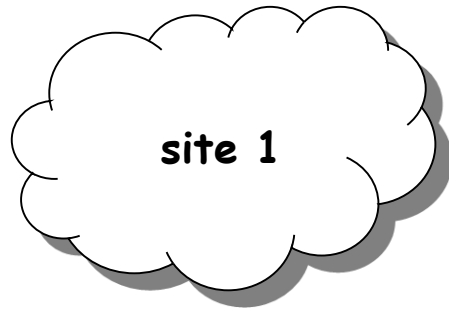
# Subnetting

- Problème

- distinction <réseau> / <hôte> insuffisante en pratique

140.201.0.0

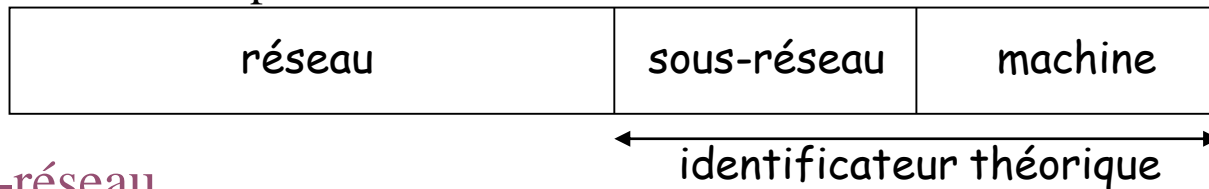
142.68.0.0



# Sous-adressage

- Principe

- ajout d'un niveau hiérarchique dans l'adressage
  - adresse de sous-réseau
- subdivision de la partie <hôte>



- le sous-réseau

- est un réseau physique (i.e. un réseau IP connexe) du réseau de site
- a une visibilité purement interne

# Le masque de sous-réseau

- le masque indique la frontière entre la partie <sous-réseau> et la partie <machine>
- le masque est propre au site
- le masque est de 32 bits
- bits du masque de sous-réseau (*subnet mask*)
  - positionnés à 1 ➔ partie réseau
  - positionnés à 0 ➔ partie machine
- exemple
  - 11111111 11111111 11111111 00000000  
↳ 3 octets pour le champ réseau, 1 octet pour le champ machine
- notations
  - décimale pointée
    - exemple : 255.255.255.0
  - adresse réseau/masque
    - exemple : 193.49.60.0/27 (27 = nombre de bits contigus du masque)

# Masque de sous-réseau

- classe utilisation

réseau	machine
--------	---------

interne  
au site

masque réseau
---------------

&&

réseau	ss-réseau	machine
--------	-----------	---------

- exemple

- le réseau 142.68.0.0 (classe B!) a comme masque 255.255.255.0
- soit l'hôte d'@IP 142.68.2.6

$$\begin{array}{rcl}
 & 10001110.01000100.00000010.00000110 & 142.68.2.6 \\
 \&\& & 11111111.11111111.11111111.00000000 & 255.255.255.0 \\
 \hline
 = & 10001110.01000100.00000010.00000000 & 142.68.2.0
 \end{array}$$

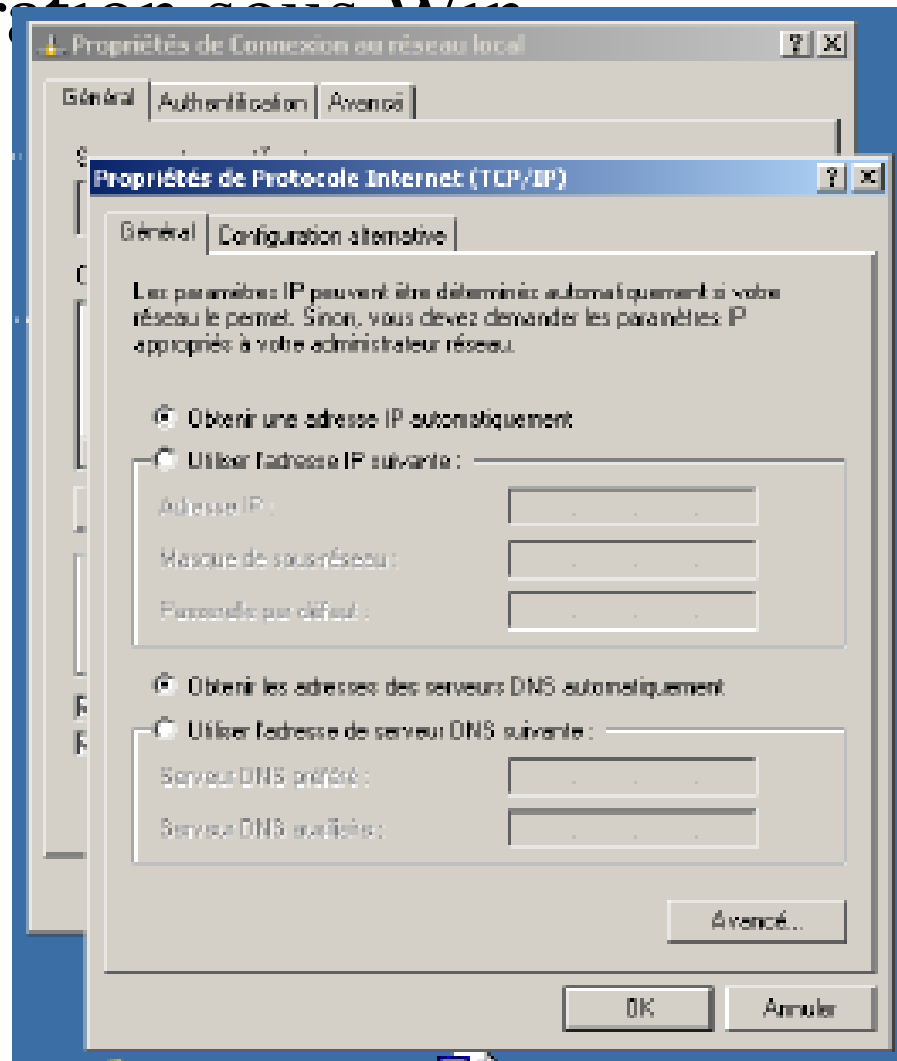
↳ l'hôte est sur le sous-réseau numéro «3, et a comme identificateur 6



# Le masque de sous-réseau

- Le choix du découpage <réseau> / <hôte> dépend des perspectives d'évolution du site
  - exemple **classe B** :
    - 8 bits pour la partie sous réseau ➔ 256 sous réseaux de 254 machines
    - 3 bits pour la partie sous réseau ➔ 8 sous-réseaux de 8190 machines
  - exemple **classe C** :
    - 4 bits pour la partie sous-réseau ➔ 16 sous-réseaux de 14 machines

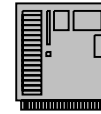
# Configuration sous Windows



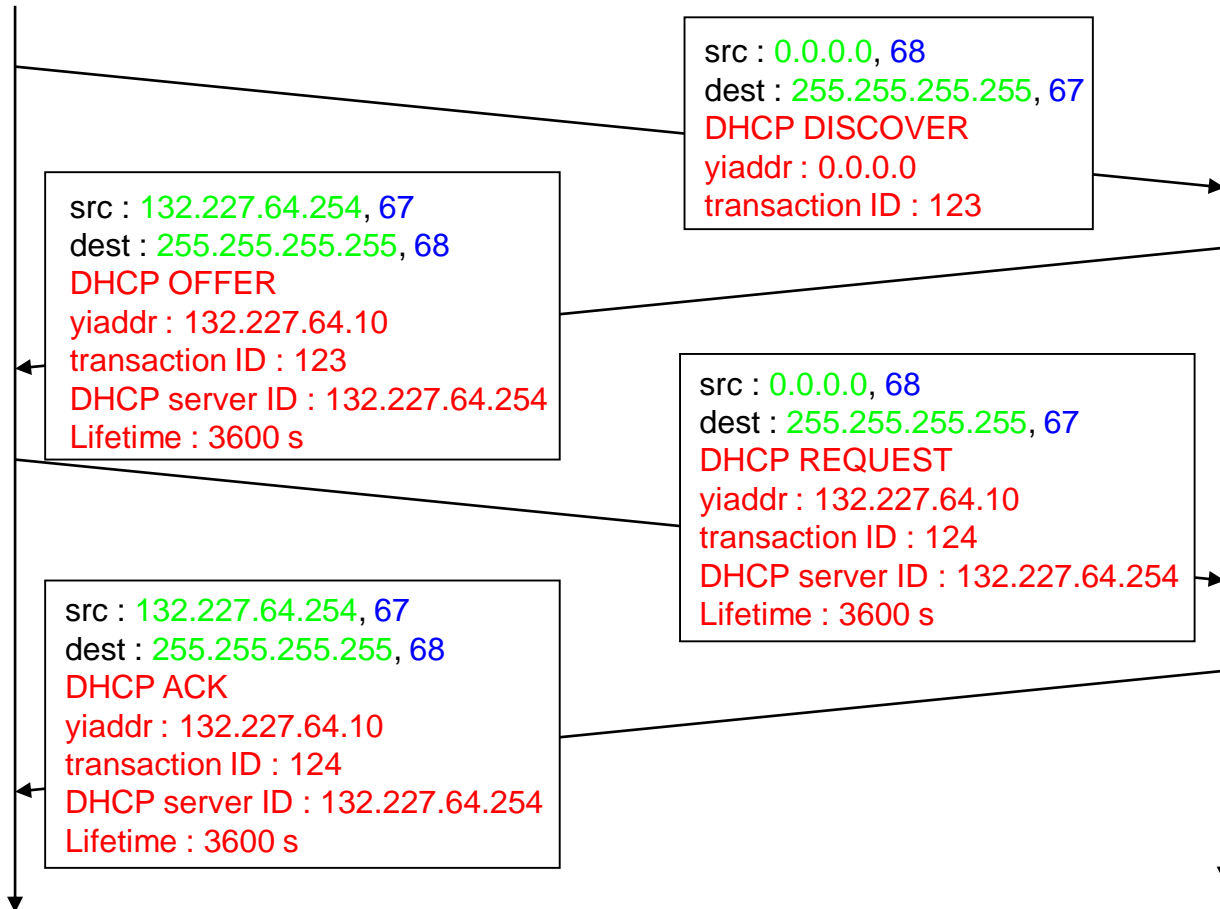
# Adresse dynamique : DHCP



@IP : ???



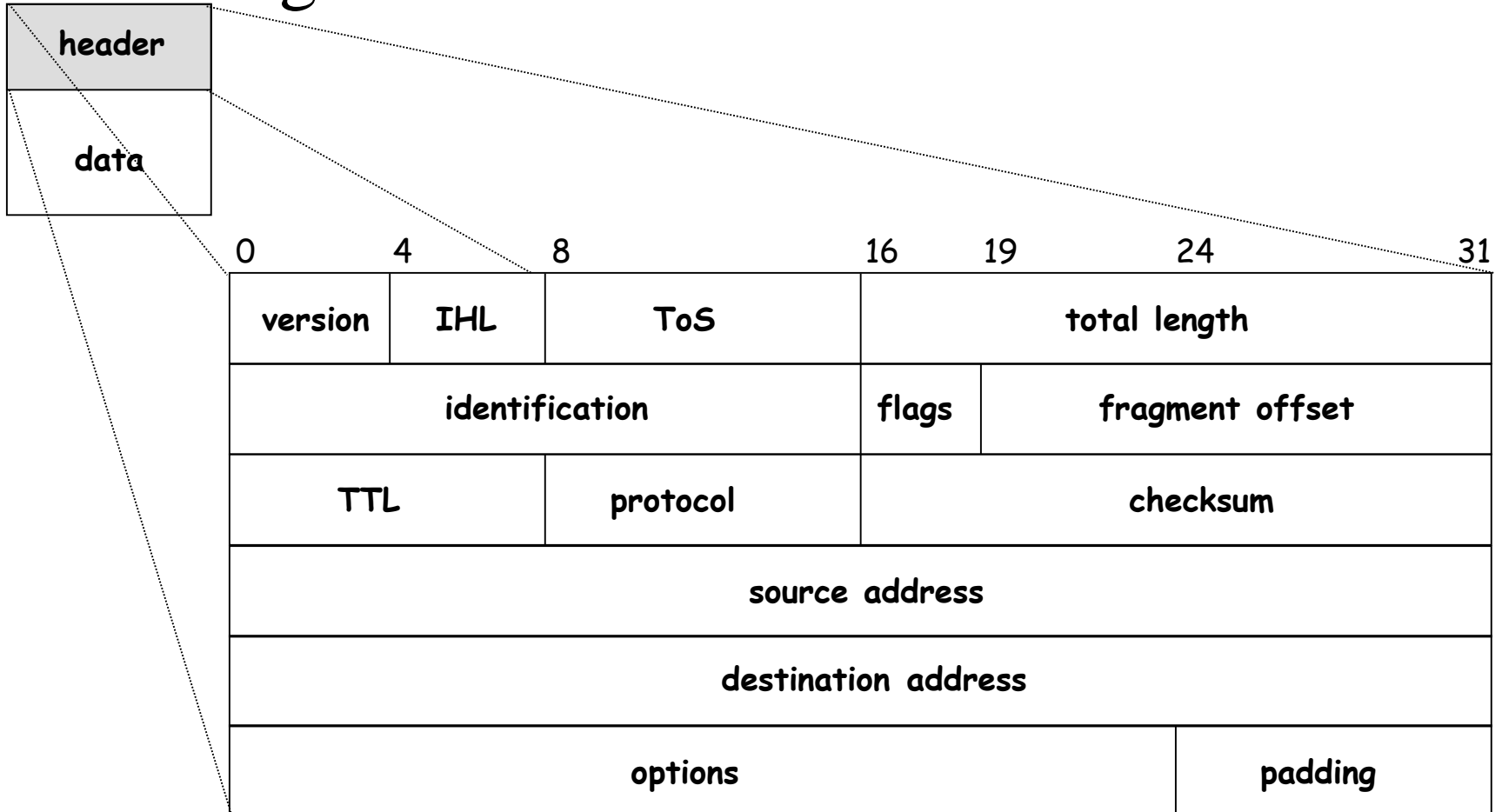
@IP : 132.227.64.254



# IP - Plan

1. Interconnexion IP
2. Relayage et routage IP
3. Adressage et nommage
4. Adressage IP
- 5. Datagramme IP**
6. Fragmentation
7. ICMP

# Le datagramme IP



# Les champs de l'en-tête IP

- **version** : identification de la version courante du protocole (4 pour IPv4)
- 4 Ipv4 et 6 IPv6
- **IHL** (*IP Header Length*) : longueur de l'en-tête IP (en mots de 32 bits)
- Par défaut 5mots
- **TOS** (*Type Of Service*) : type de service à appliquer au paquet en fonction de certains paramètres comme le délai de transit, la sécurité, QOS
  - 3bit priorité exemple prioritaire, urgent, très urgent, critique .....
  - 1bit délai normal ou bas
  - 1bit débit normal ou haut
  - 1bit fiabilité normal ou haute
  - 1bit coût normal ou faible
  - 1bit MBZ 0
- **total length** : longueur totale du datagramme (en octets)
- **identification** : valeur fournie par la source aidant la destination au réassemblage des différents fragments du datagramme
- **flags** : utilisé par la fragmentation et composé de
  - réservé
  - DF (*Don't Fragment*) valeur 1
  - MF (*More Fragment*) 1 existe autre fragment
- **offset** : déplacement par rapport au datagramme
  - Premier fragment 0

# Les champs de l'en-tête IP

- **TTL** (*Time To Live*) : limite supérieure du temps de vie d'un datagramme
- **protocol** : protocole utilisé pour le champ de données
  - 1 pour ICMP
  - 6 pour TCP
  - 17 pour UDP
- **checksum** : zone de contrôle d'erreur portant uniquement sur l'en-tête du datagramme
- **source address** : @ IP de la source du datagramme
- **destination address** : @ IP de la destination du datagramme
- **options** : fonctions de contrôle utiles dans certaines situations (sécurité, routage particulier, etc.)
- **padding** : pour aligner l'en-tête sur 32 bits

# IP - Plan

1. Interconnexion IP
2. Relayage et routage IP
3. Adressage et nommage
4. Adressage IP
5. Datagramme IP
- 6. Fragmentation**
7. ICMP



# Fragmentation et réassemblage

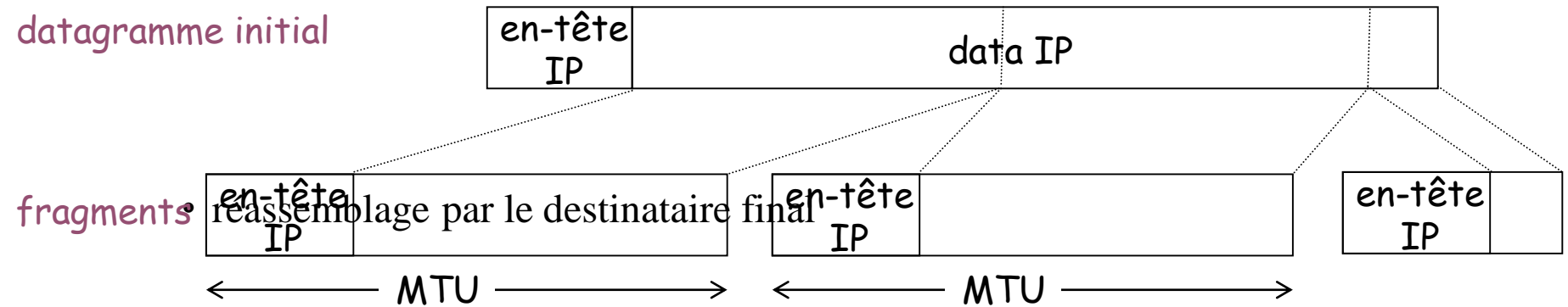
- Motivations

- l'Internet est par nature hétérogène
- le MTU (Maximum Transmission Unit) varie selon la technologie
- certains protocoles de niveau supérieur génèrent des datagrammes de longueur supérieure au MTU

↳ adaptation de la taille du datagramme au MTU

# Fragmentation et réassemblage

- Principe
  - découpage de la charge utile et duplication de l'en-tête



□ MTU = 1500 bytes

several smaller datagrams

1480 bytes in  
data field

offset =  
 $1480/8$

	length =1500	ID =x	fragflag =1	offset =0
	length =1500	ID =x	fragflag =1	offset =185
	length =1040	ID =x	fragflag =0	offset =370

émission d'un message  
de 5000 octets →  
A fragmente

Ethernet

R2



R2 n'a pas besoin de fragmenter

FDDI

B



B réassemble

# IP Fragmentation and Reassembly

## Example

- ❑ 4000 byte datagram
- ❑ MTU = 1500 bytes

	length	ID	fragflag	offset	
	=4000	=x	=0	=0	

One large datagram becomes several smaller datagrams

1480 bytes in data field

offset =  
 $1480/8$

	length	ID	fragflag	offset	
	=1500	=x	=1	=0	

	length	ID	fragflag	offset	
	=1500	=x	=1	=185	

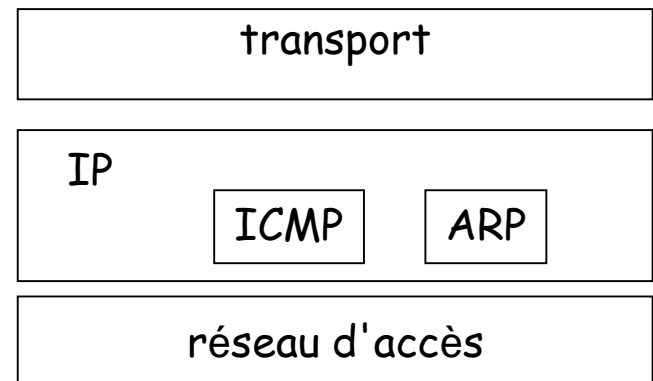
	length	ID	fragflag	offset	
	=1040	=x	=0	=370	

# IP - Plan

1. Interconnexion IP
2. Relayage et routage IP
3. Adressage et nommage
4. Adressage IP
5. Datagramme IP
6. Fragmentation
7. **ICMP & ARP**

# Protocole de contrôle ICMP

- Motivation
  - pas de signalisation dans IP
    - pas de retour d'information
    - pas de messages d'anomalies
- **ICMP** (Internet Control Message Protocol)
  - instrumentation et test
  - signalisation d'anomalies
  - mise en œuvre obligatoire
  - messages ICMP encapsulés dans des datagrammes IP
  - même si :



# Messages ICMP

- format

- les messages ICMP ont tous le même format pour le premier mot de 32 bits

type	code	checksum
------	------	----------

- champ type

Type	Message	Objet
0	Echo Reply	Réponse en écho.
3	Destination Unreachable	Destination inaccessible.
4	Source Quench	Interruption de la source.
5	Redirect	Redirection, changement de route.
8	Echo	Demande d'écho.
11	Time Exceeded	Temps de vie d'un datagramme dépassé.
12	Parameter Problem	Datagramme mal formé.
13	Timestamp	Demande de date d'estampillage.
14	Timestamp Reply	Réponse à une demande d'estampillage.
15	Information Request	Demande d'information.
16	Information Reply	Réponse à une demande d'information.
17	Address Mask Request	Demande de masque d'adresse.
18	Address Mask Reply	Réponse à une demande de masque d'adresse.

# Outil ping

- Principe

- exploite la fonction d'écho de ICMP
- un routeur ou un hôte recevant un "echo request" retourne un "echo reply"

↳ permet de

- tester l'accessibilité d'une machine
- obtenir des statistiques sur la qualité de la route

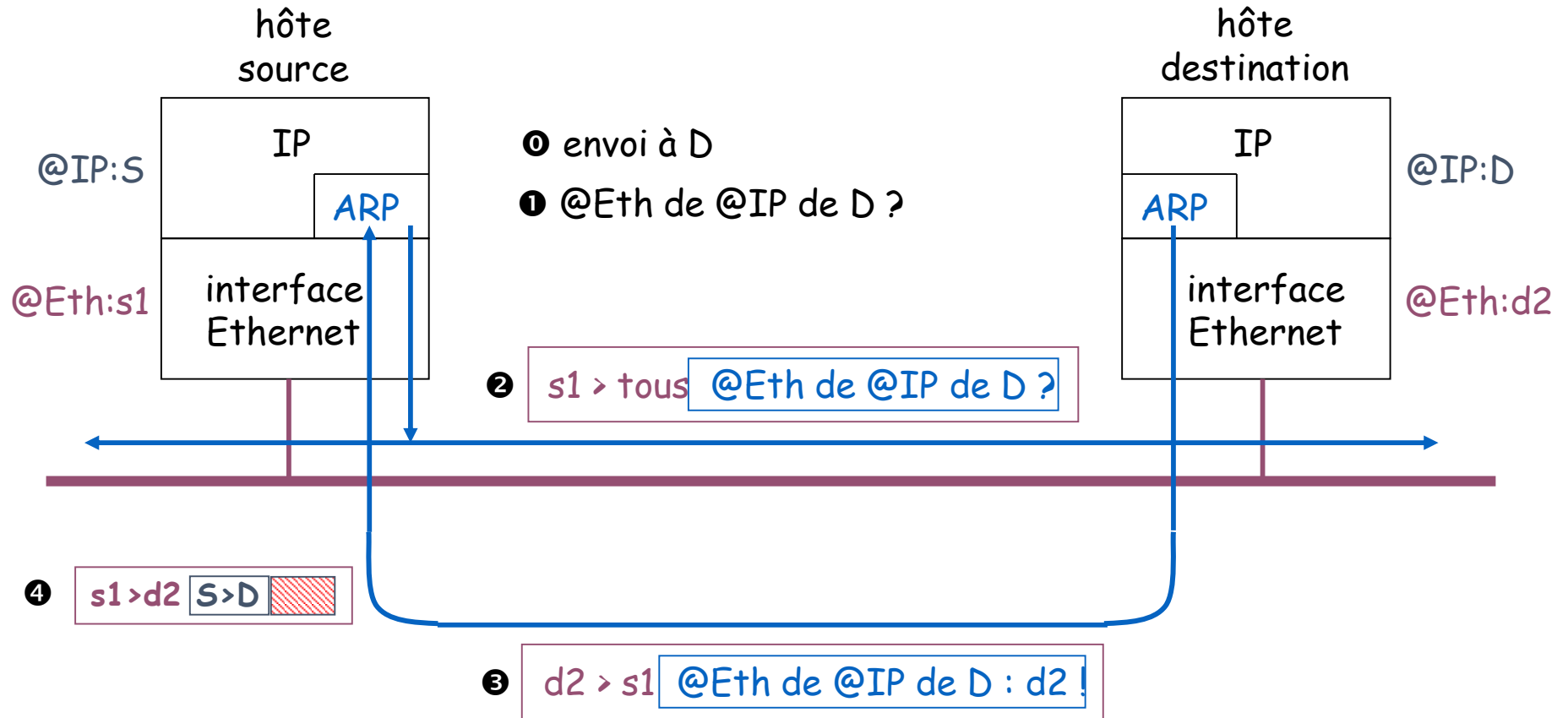
- Exemple

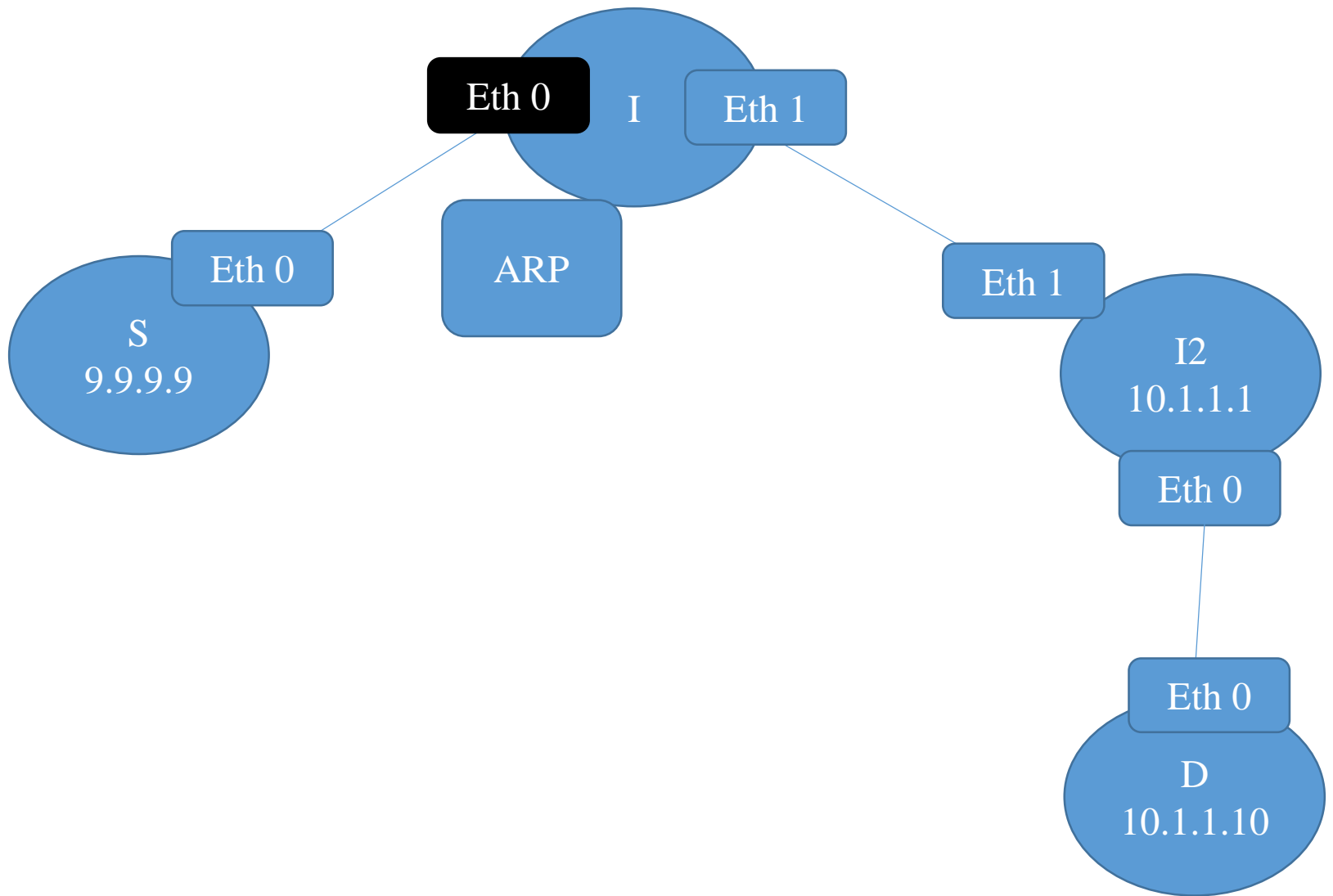
- Ping 192.168.1.1

```
$ ping castor.univ-reunion.fr
PING castor.univ-reunion.fr (194.199.73.51): 56 data bytes
64 bytes from 194.199.73.51: icmp_seq=0 ttl=246 time=570.800 ms
64 bytes from 194.199.73.51: icmp_seq=1 ttl=246 time=581.364 ms
64 bytes from 194.199.73.51: icmp_seq=2 ttl=246 time=571.022 ms
64 bytes from 194.199.73.51: icmp_seq=3 ttl=246 time=572.722 ms
64 bytes from 194.199.73.51: icmp_seq=4 ttl=246 time=579.121 ms
64 bytes from 194.199.73.51: icmp_seq=5 ttl=246 time=571.619 ms
^C
----castor.univ-reunion.fr PING Statistics----
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 570.800/574.441/581.364/4.598 ms
```



# Résolution des adresses





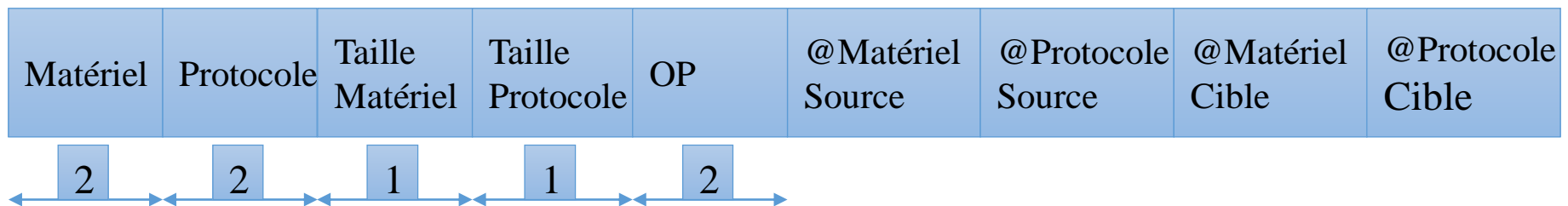
Matériel	Protocole	Taille Matériel	Taille Protocole	OP	@Matériel Source	@Protocole Source	@Matériel Cible 00000	@Protocole Cible
2	2	1	1	2				

# Protocole ARP

- Broadcaste un appel à l'aide...

- @source.ethernet = @émetteur
- @destination.ethernet = FF-FF-FF-FF-FF-FF
- Type = 0x 0800

**FF FF FF FF FF FF 00 04 80 5F 68 00 08 06 00 01  
 08 00 06 04 00 01 00 04 80 5F 68 00 89 C2 A2 03  
 00 00 00 00 00 00 89 C2 A2 F3 00 00 00 00 00 00  
 00 00 00 00 00 00 00 00 00 00 00 00 00 00**



## ■ Réponse :

- Même trame, champs remplis par machine cible

- FF FF FF FF FF FF 00 04 80 5F 68 00 08 06 00 01
- 08 00 06 04 00 01 00 04 80 5F 68 00 89 C2 A2 03
- 00 00 00 00 00 00 89 C2 A2 F3 00 00 00 00 00 00
- 00 00 00 00 00 00 00 00 00 00 00 00 00 00