

RESEAUX : Internetworking

- ***Repeater, Bridge, Switch***
- **100 Mbit/s, 1Gbit/s, 10 Gbit/s, ...**
- ***Full duplex***

- ***Router, Subnet mask***
- **Routages statique et dynamique**
- ***Routing Information Protocol***

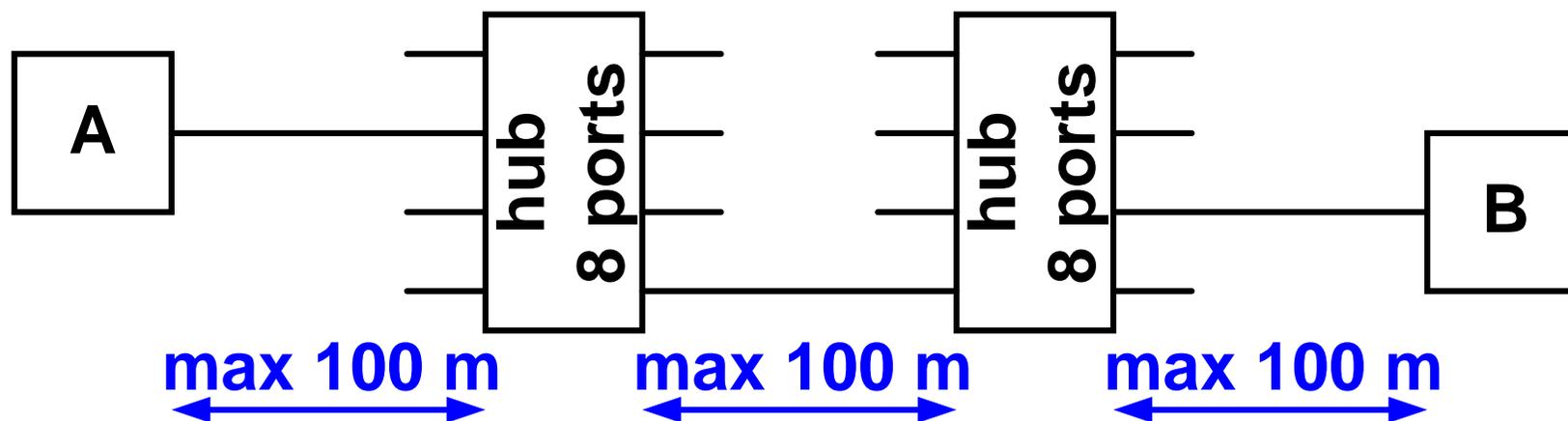
- ***Internet Control Message Protocol, Traceroute***

- **Configuration dynamique : DHCP**

- **Livres et URLs**

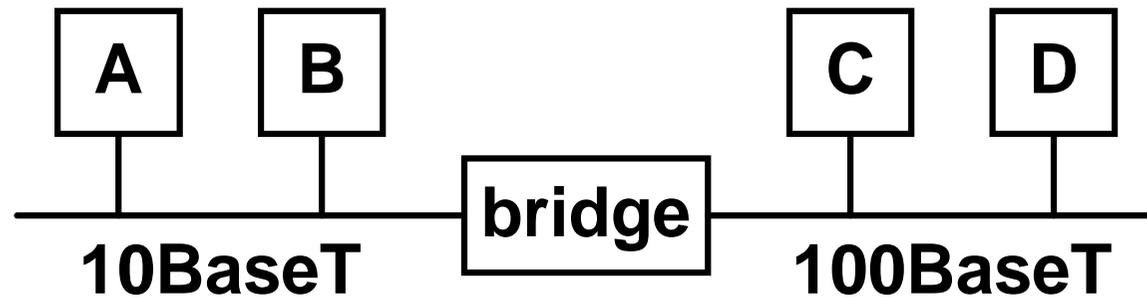
Repeater (répéteur)

- Fonction de niveau 1 (couche physique)
- Régénérer le signal :
 - 500 m avec 10Base5
 - 200 m avec 10Base2
 - 100 m avec 10BaseT



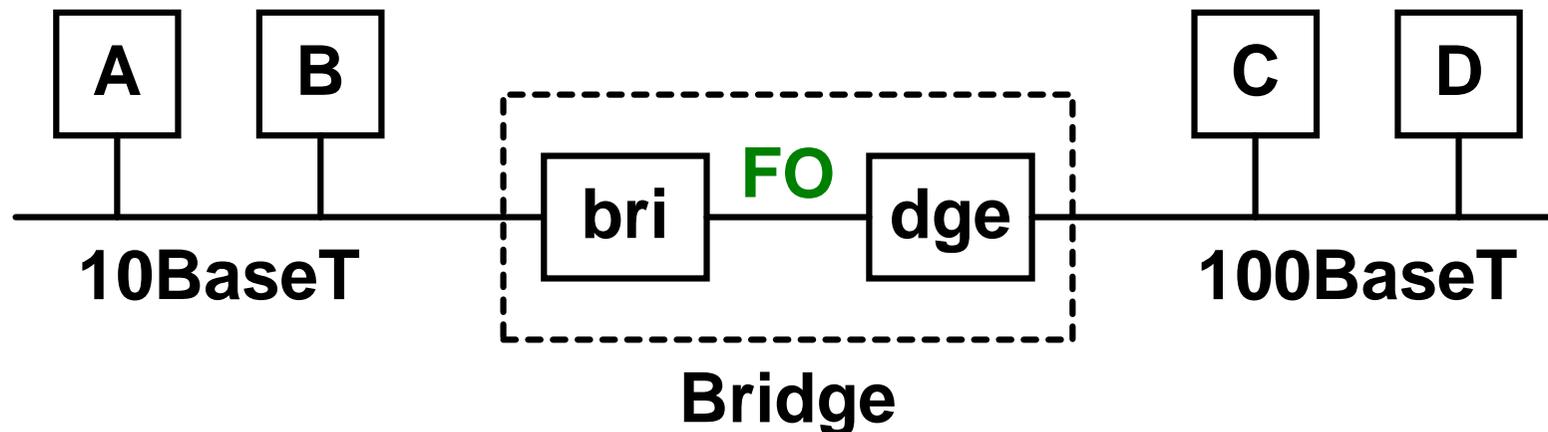
- Interfaces électriques :
 - connecteur AUI (15 pins)
 - connecteur BNC
 - connecteur RJ45

- **Subdiviser** un réseau en sous-réseaux (**segments**) à partir des **adresses de niveau 2 ou MAC** (*Medium Access Control*)



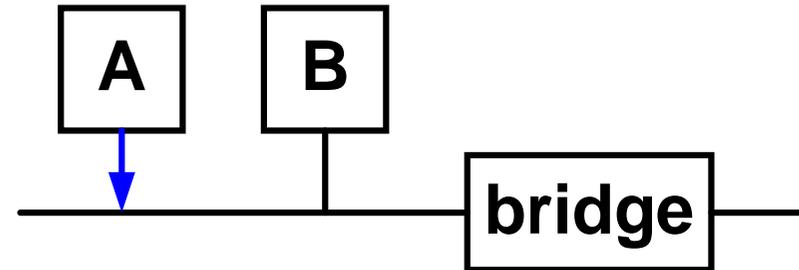
- **Local bridge** relie 2 LANs

- **Remote bridge** utilise une liaison point à point Cu ou **FO**



1 Mise sous tension du *bridge*

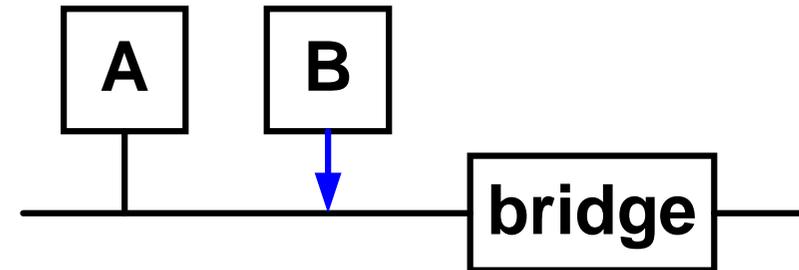
2 A émet une trame à B



3 *Bridge learns* : A se trouve sur le segment gauche

4 *Bridge forwards* la trame sur le segment de droite

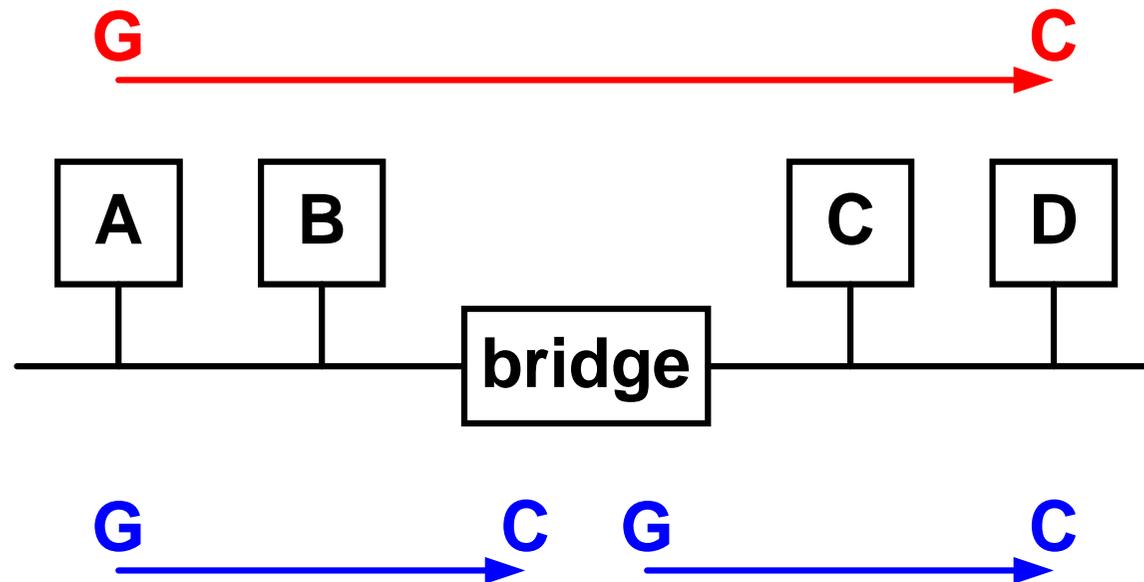
5 B répond à A



6 *Bridge learns* : B se trouve sur le segment gauche

7 *Bridge filters* cette trame

- Certains *bridges* transmettent ce CRC
→ Mécanisme d'extrémité à extrémité (*end to end*)



- D'autres *bridges* gèrent ce CRC
→ Les trames avec erreur de CRC sont ignorées
→ Mécanisme en cascade

Ethernet à 100 Mbit/s (1)

- La norme **100 Base T** (*Fast ethernet*), apparue en 1994, reste compatible avec les réseaux *ethernet* à 10 Mbit/s
- Elle conserve l'accès non déterministe, défini dans la norme IEEE 802.3 (CSMA/CD) et permet une distance maximale de **100 m** sur paire torsadée entre nœud et *hub*
- Le temps de propagation max aller et retour (*RTD : Round Trip Delay*) est cette fois de 5,1 μ s (51 μ s à 10 Mbit/s) alors que l'*interframe gap* = 0,96 μ s (9,6 μ s à 10 Mbit/s) correspond toujours à 12 octets
- Variantes :

| | |
|-------------|--------------------|
| 100 Base TX | 2 paires torsadées |
| 100 Base T4 | 4 paires torsadées |
| 100 Base FX | 2 fibres multimode |

Ethernet à 100 Mbit/s (2)

- **Détection automatique** (*auto negotiation*)

Certains *hubs auto sensing* sont capables de détecter le type de nœud : 10 Base T, 100 Base TX, 100 Base T4

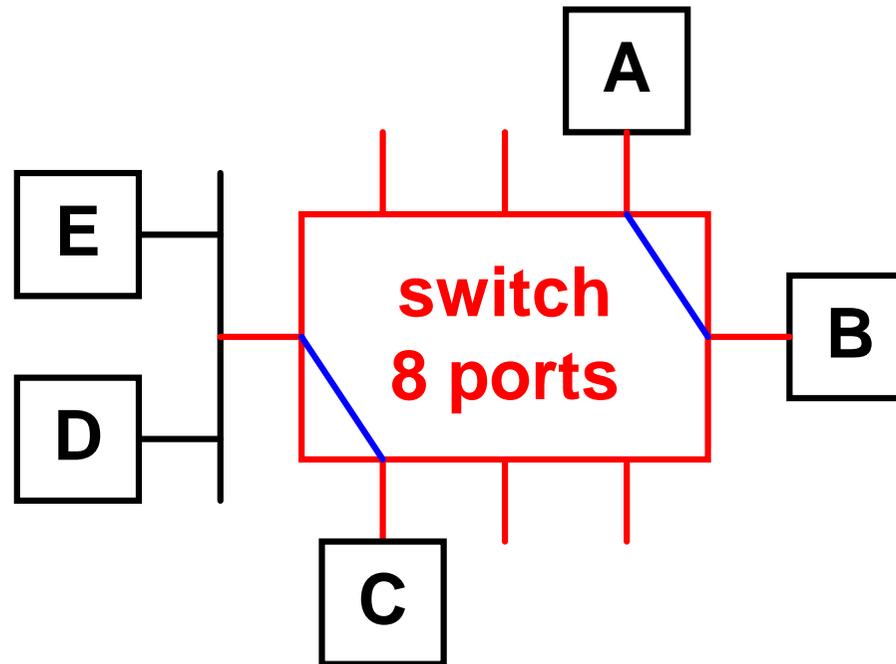
- **Réseau mixte 10/100 Mbit/s ?**

L'introduction de nœuds 100 Base T se fait de façon assez naturelle car elle ne remet pas en cause le câblage existant

- La migration s'effectue progressivement avec des *hubs hybrides 10/100 Base T* → voir Ex 2

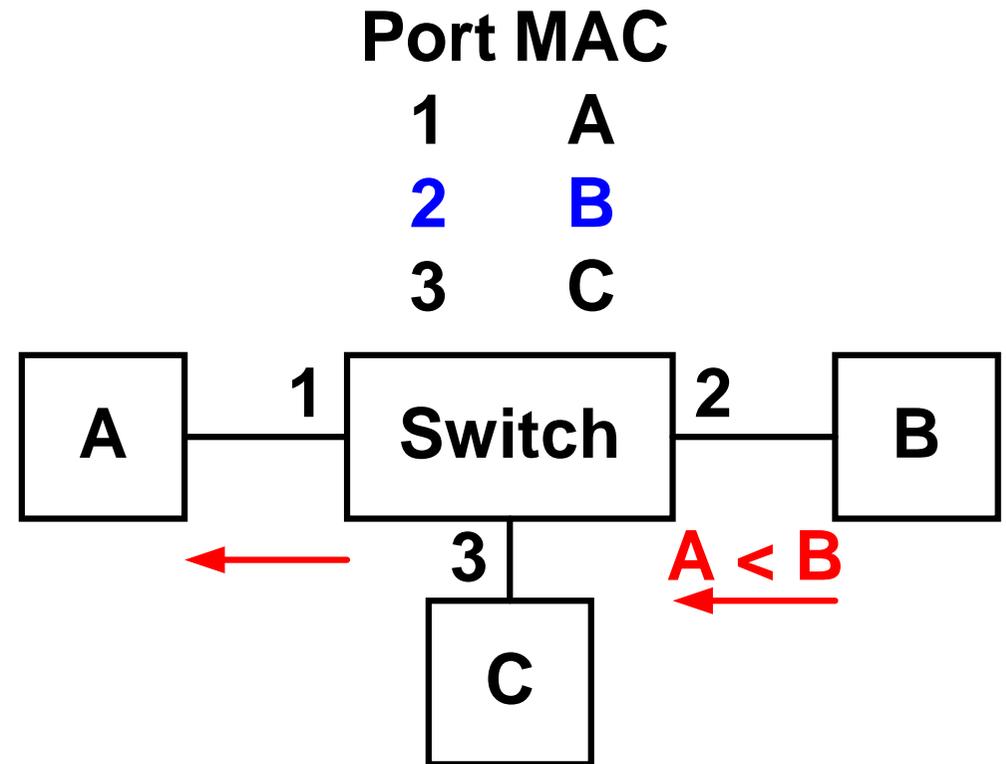
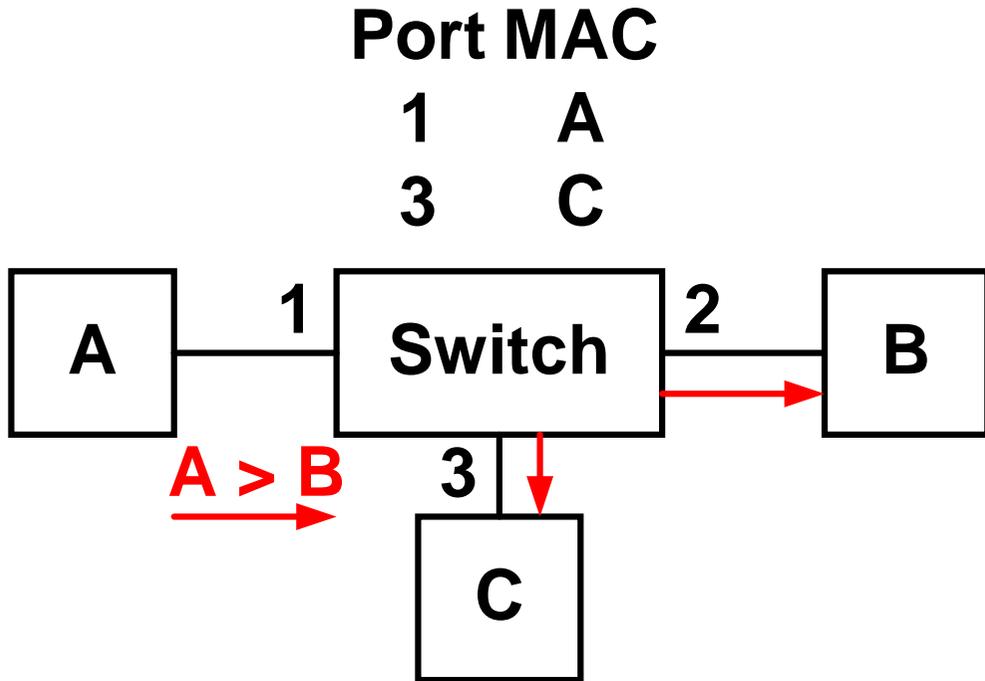
Switch (commutateur)

- Ce commutateur (*switch*), à ne pas confondre avec un *hub*, fonctionne sur le principe du *multiport bridge*



- Il teste chaque trame (adresse de destination) et ouvre au besoin un **canal** entre ces 2 ports; plusieurs **canaux** pouvant être actifs simultanément (4 au maximum dans l'exemple)

Switch : Table

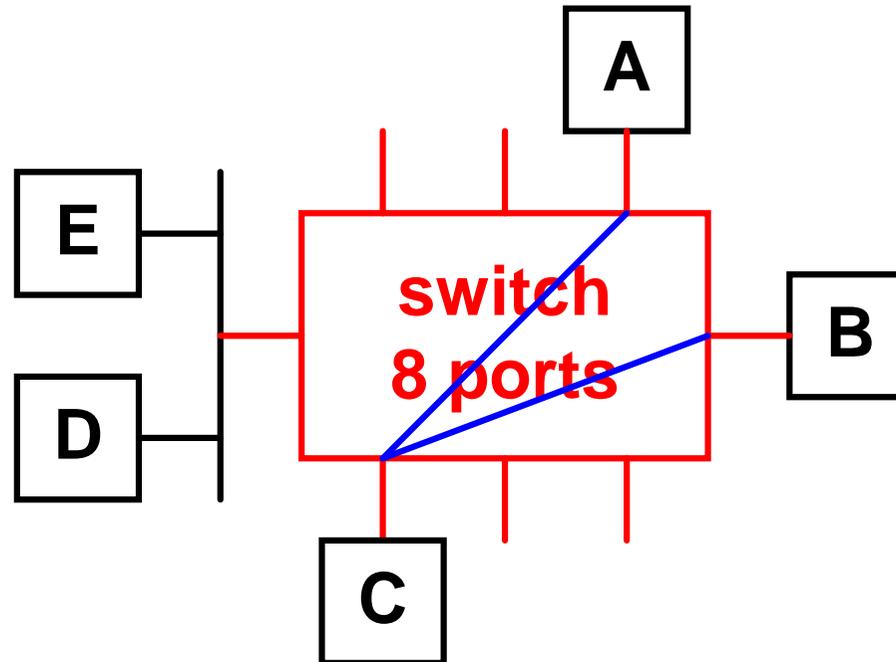


CAM (Cisco)
Content Addressable Memory
Max 8000 MAC addr (2950)

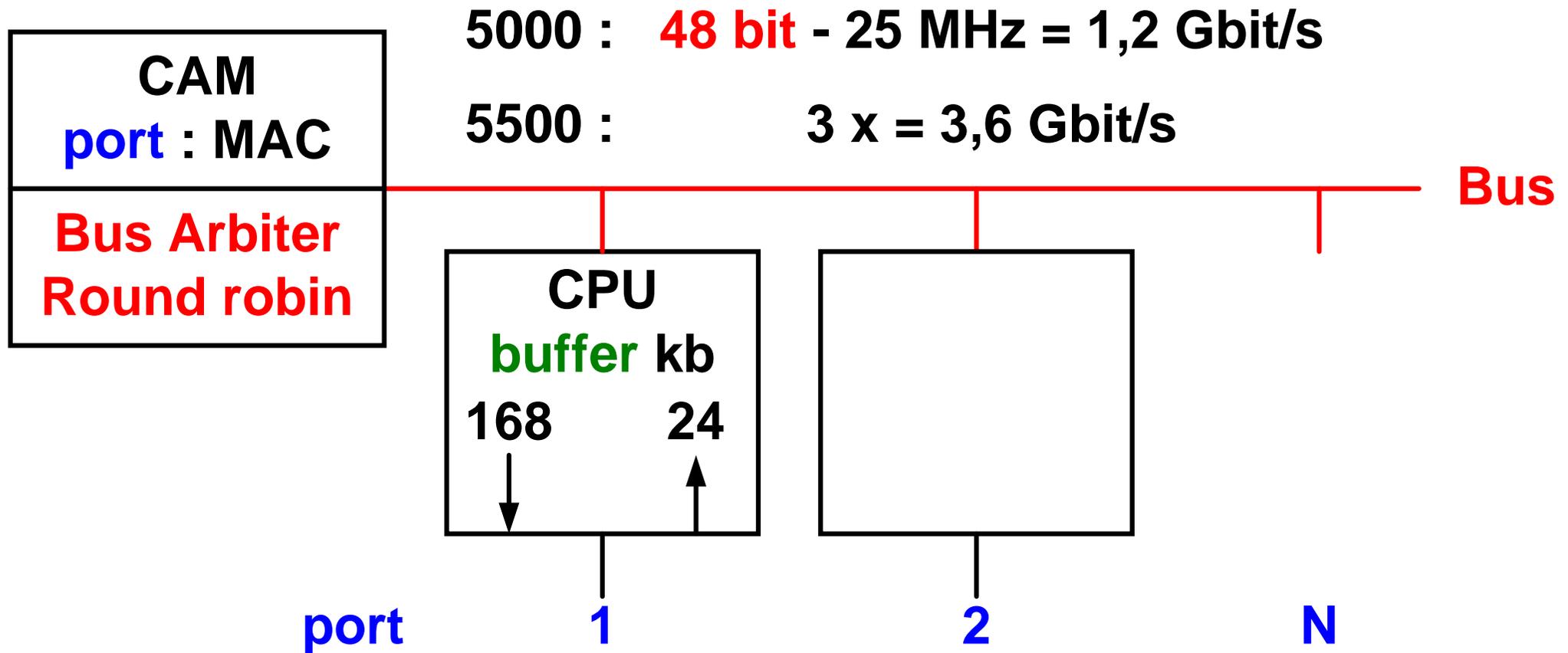
Principe de fonctionnement (1)

- **Le commutateur mémorise l'adresse source MAC de chaque trame dans sa table de filtrage**
- **Si l'adresse de destination de la trame est inconnue; la trame est diffusée sur tous les ports**
- **Chaque commutateur dispose d'une certaine capacité de mémorisation**
- **La capacité de transmission à l'intérieur du commutateur doit être suffisante pour écouler plusieurs trames simultanées → Transmission en parallèle sur un bus**

- Que se passe-t-il si A et B émettent simultanément une trame destinée à C ?

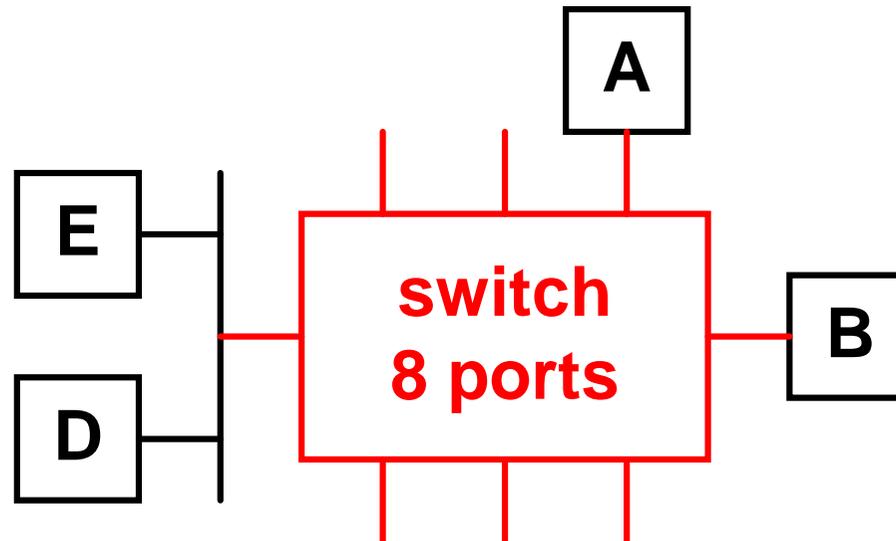


- Le commutateur dispose de mémoire tampon (FIFO)
- FIFO plein → perte de trame



- *Frame transmitted to all port - Instruct non destination port*
- *Latency = 10 μ s + length of frame (store & forward)*
- Catalyst 2950 (**labo**) : 24 ports 10/100 – 3,6 Mpps (64 byte)

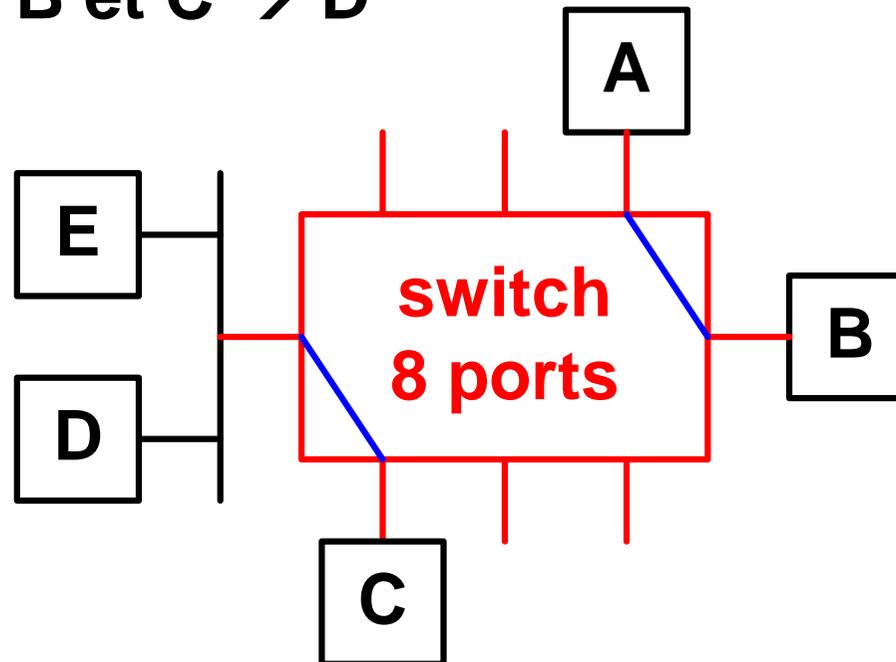
- Dans cet exemple, les éventuelles collisions sur le segment des nœuds D et E ne sont pas visibles sur les autres ports du commutateur



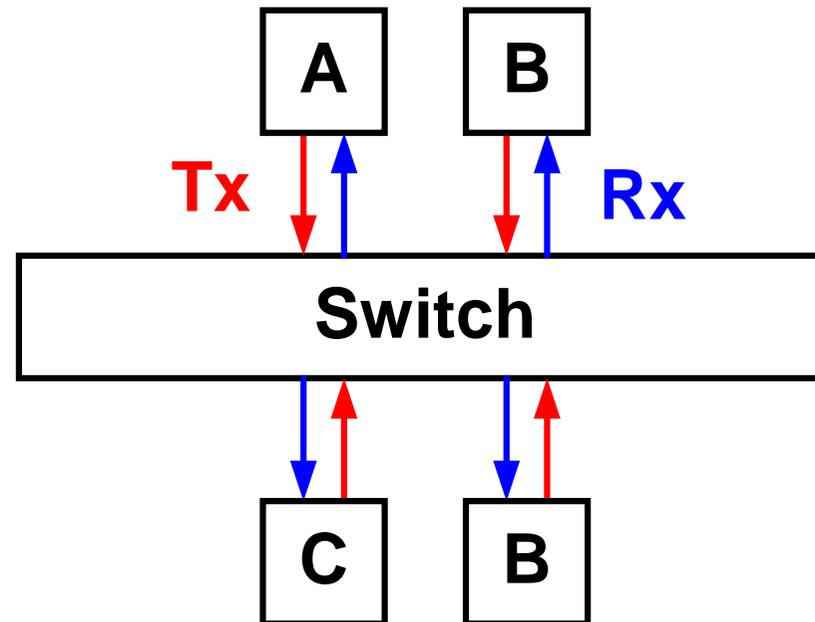
- Chaque port constitue donc son **propre domaine de collisions**
- L'adresse de diffusion (FFFFFFFFFFFF) est propagée sur tous les autres ports
→ **Un seul domaine de diffusion** (*broadcast domain*)

Shared versus switched LAN

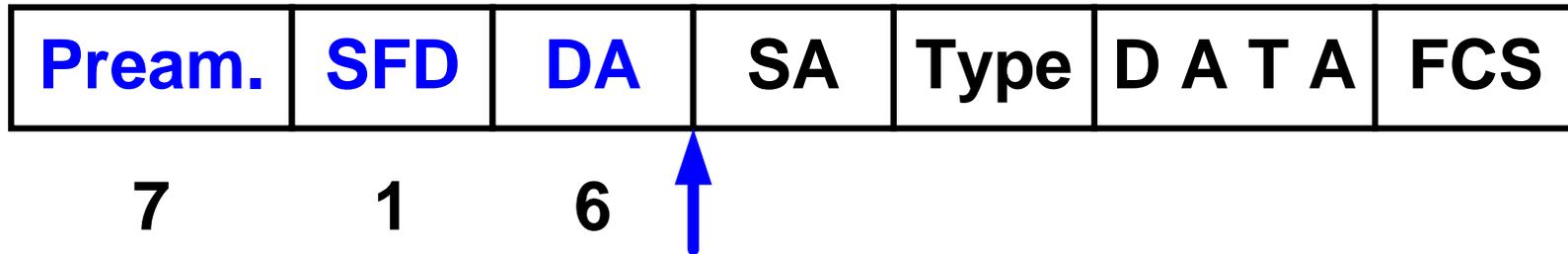
- Un réseau 10 Base T composé de *hubs* partage une bande passante de 10 Mbit/s → *shared LAN*
- Un **commutateur** 10 Base T permet l'émission de plusieurs trames simultanées → *switched LAN*
- Exemple : A → B et C → D



- La majorité des **commutateurs 100 Base T** autorisent l'émission et la réception simultanées

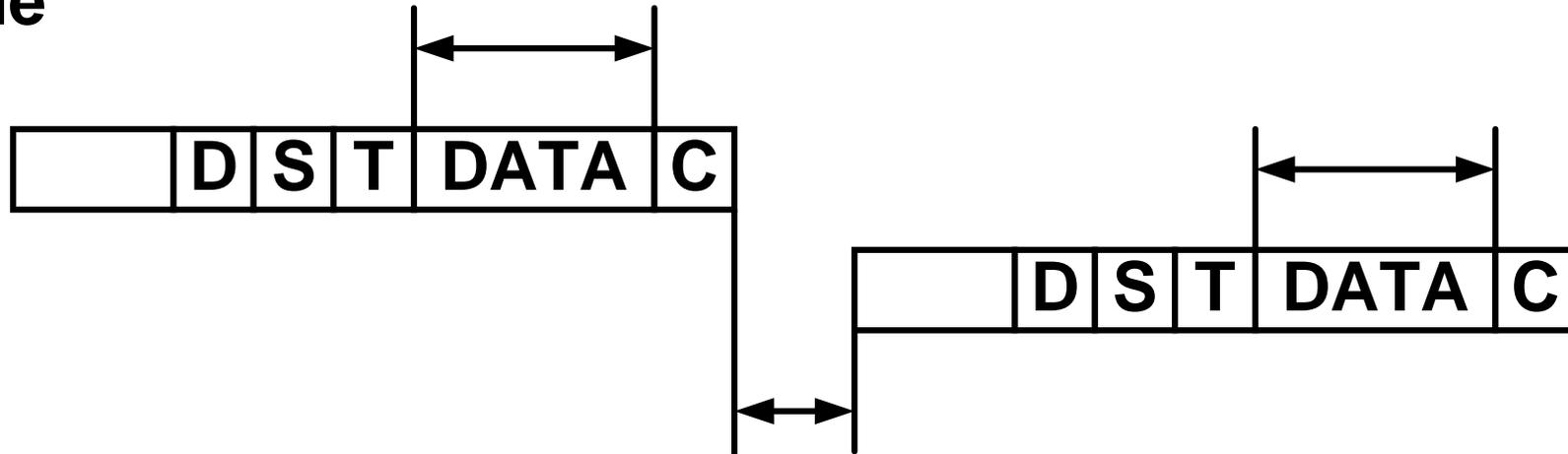


- Il commute la trame dès qu'il a reçu l'adresse de destination



- Temps de latence minimum ($\sim 15 \text{ ns}$) indépendant de la longueur de trame pour $D = 10 \text{ Mbit/s}$
- Retransmission des erreurs (CRC, trame trop courte)
- Même débit \rightarrow débits 10 - 100 Mbit/s pas possibles
- Commutation au niveau matériel (*switch fabric, ASIC = Application Specific Integrated Circuit*)

- La trame n'est commutée que lorsqu'elle a été complètement reçue



- Temps de latence dépendant de la longueur de la trame
- Erreurs sont filtrées (CRC, trame trop courte)
- Adaptation possible de débit 10 - 100 Mbit/s
- Commutation au niveau logiciel (CPU, RISC)
- Mises à jour possibles du logiciel

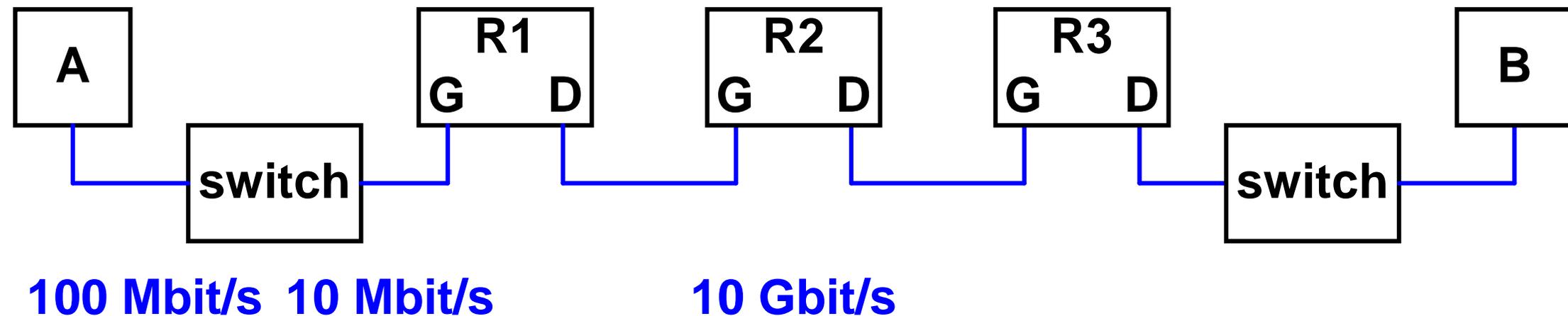
Gigabit ethernet (1)

- Cette norme, apparue en 1999, conserve le format de trames *ethernet*
- Elle est principalement utilisée en mode **full duplex** où la **méthode d'accès CSMA/CD est désactivée**
- La charge théorique max est alors de 1,488 Mio trame/s
- 802.3z :

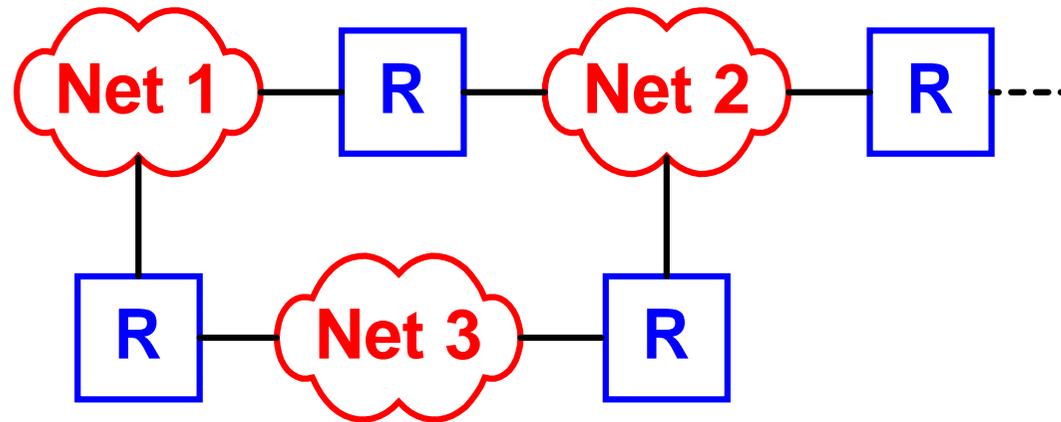
| | | |
|--------------|-------|---------------------------------|
| 1000 Base CX | 25 m | <i>shielded balanced copper</i> |
| 1000 Base SX | 550 m | fibres optiques multimode |
| 1000 Base LX | 3 km | fibres optiques monomode |
- 802.3ab 1000 Base T 100 m UTP cat. 5 (4 paires)

- La méthode d'accès CSMA/CD, active qu'en *half duplex*, a été modifiée afin de permettre une distance suffisante
- La durée minimale d'émission de la trame est fixée à 512 octets permettant ainsi une domaine de collision de 200 m
- Le contrôleur *ethernet*, qui doit émettre une trame de longueur inférieure, génère un signal particulier tout en détectant les collisions (*carrier extension*)
- Le débit utile, dans le cas le plus défavorable (émission de trames de 64 octets), atteint ainsi 120 Mbit/s !

- Ratification du standard en 2002
- Extension *full duplex*
- 100 m à 40 km selon la fibre (monomode, multimode)
- Intéresser les opérateurs (ISP) !



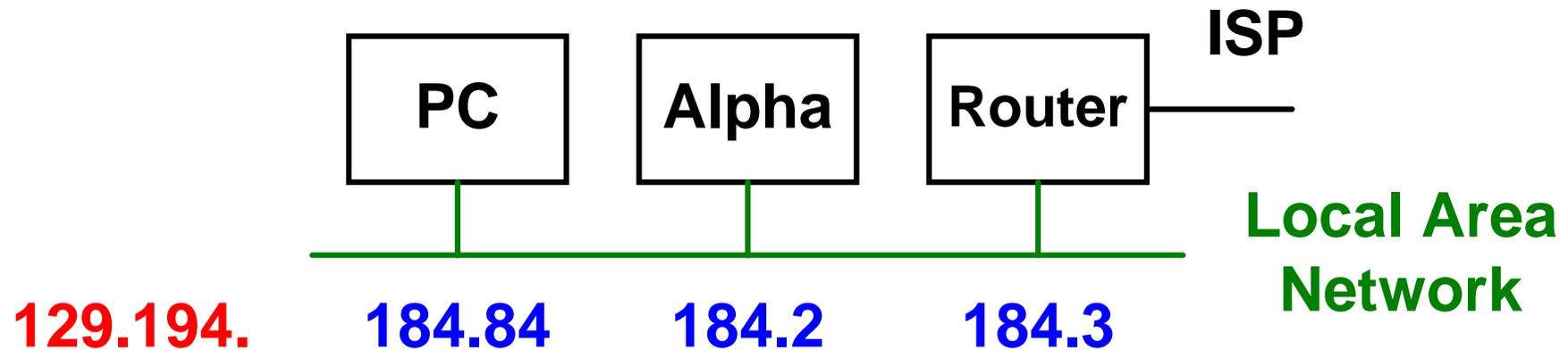
- *Internet* est constitué de réseaux (**Network**) reliés par des routeurs (**Router**)



- Adresse IP (32 bits) = **network** + **host**
Serveur Alpha de l'EIG = 129.194.184.2
 - adresse de classe B
 - **network = 129.194**
 - **host = 184.2**

Configuration de mon PC

- UniGE dispose de la classe B **129.194.H.H**



- PC *IP address* **129.194.184.84** Adresse IP
 Subnet mask 255.255.0.0 Masque
 Router **129.194.184.3** Routeur
 DNS **129.194.4.6** Serveur DNS

Subnet Mask (1)

- Valeur par défaut (adresse de classe B dans notre cas)

255.255.0.0

| | | | |
|----------|----------|----------|----------|
| 255 | 255 | 0 | 0 |
| 11111111 | 11111111 | 00000000 | 00000000 |

- Ce masque permet de distinguer, parmi toutes les destinations possibles, entre **destination directe** ou **indirecte**
- Notation Cisco : 129.194.184.0/16 (16 bits à 1)

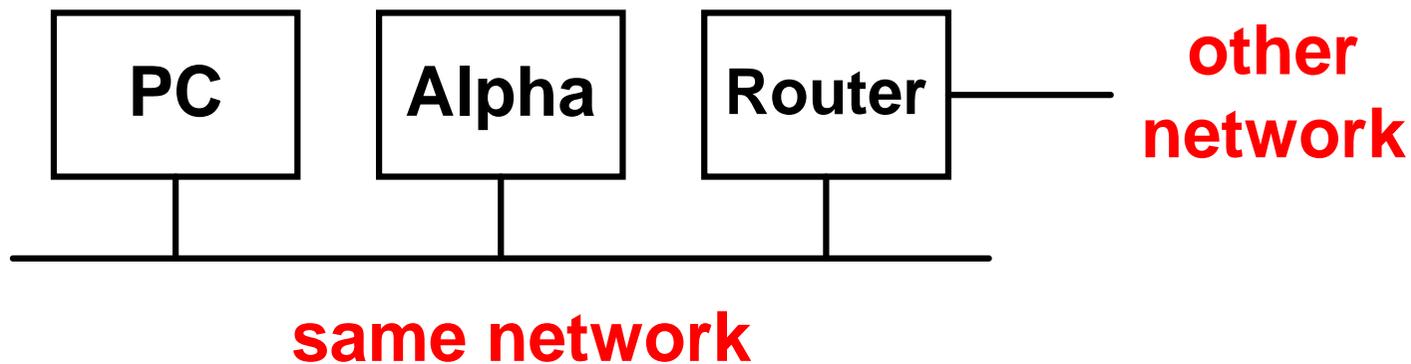
Subnet Mask (2)

- **Direct destination**

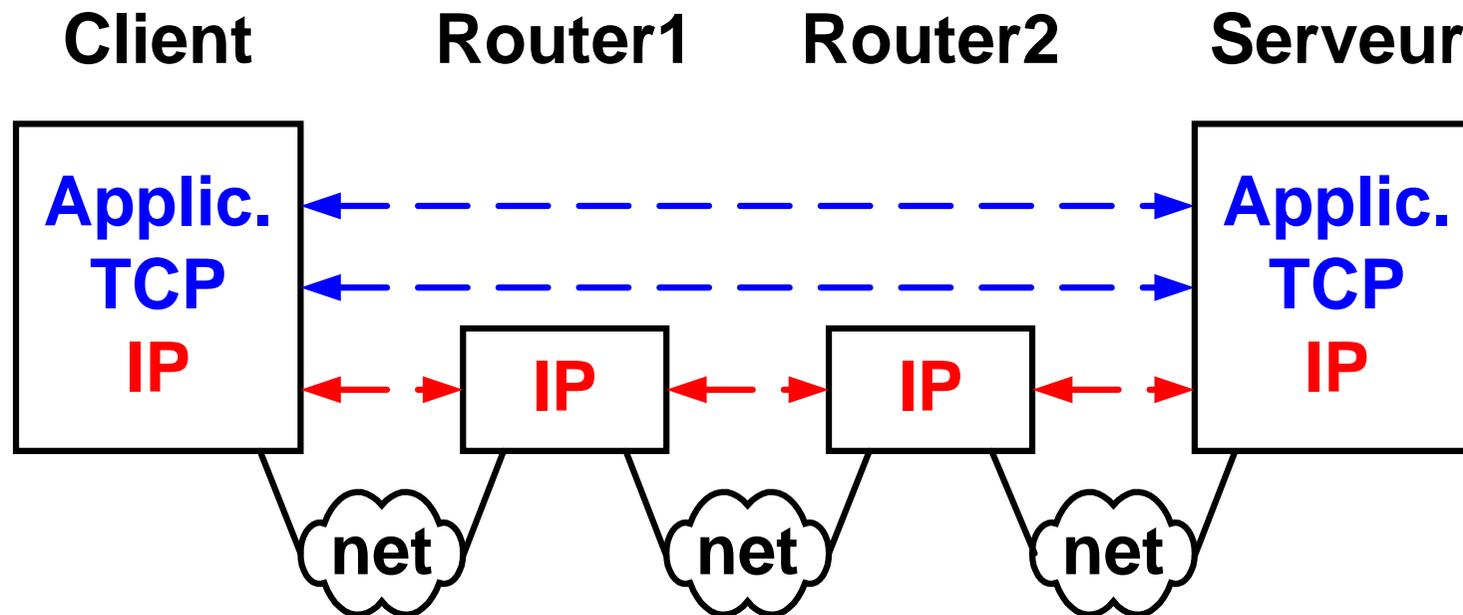
ping 129.194.184.2
subnet mask 255.255.0.0 → **same network**

- **Indirect destination**

ping 130.59.1.40
subnet mask 255.255.0.0 → **other network**
router = 129.194.184.3

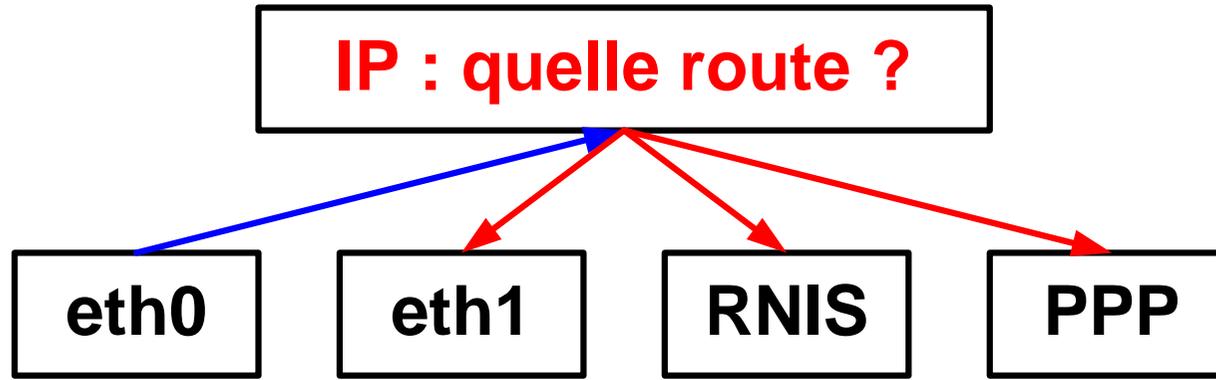


- Les routeurs ne gèrent que le protocole **IP**



- Les couches **Application** et **TCP** ont une signification d'extrémité à extrémité (*end to end protocol*) alors que les **protocoles IP sont en cascade**

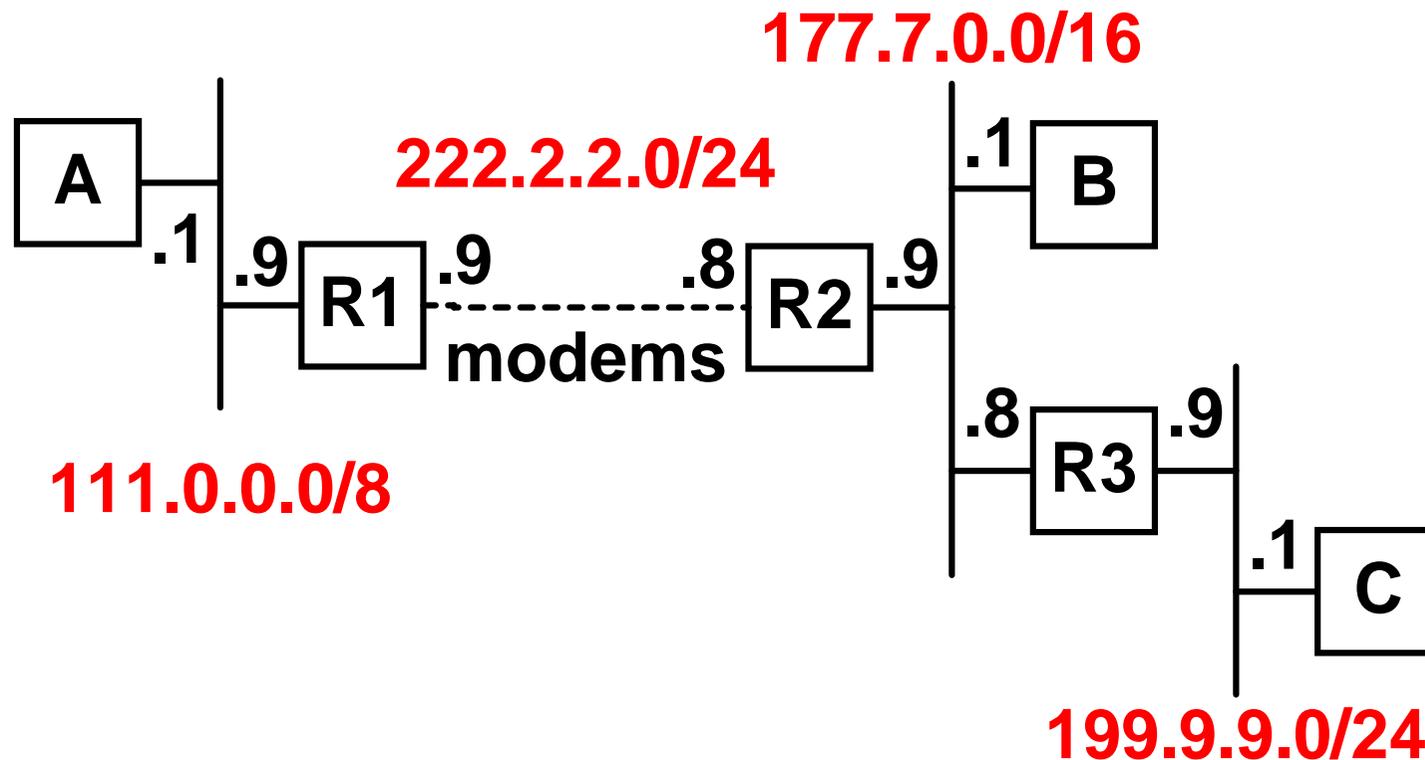
- Chaque **datagramme reçu** doit être **acheminé sur le bon interface**



- Couche IP, **orientée sans connexion** (*best effort*) ne fonctionne pas sur le principe du *Switched Virtual Circuit* X.25 ou du label *Multi Protocol Label Switching*

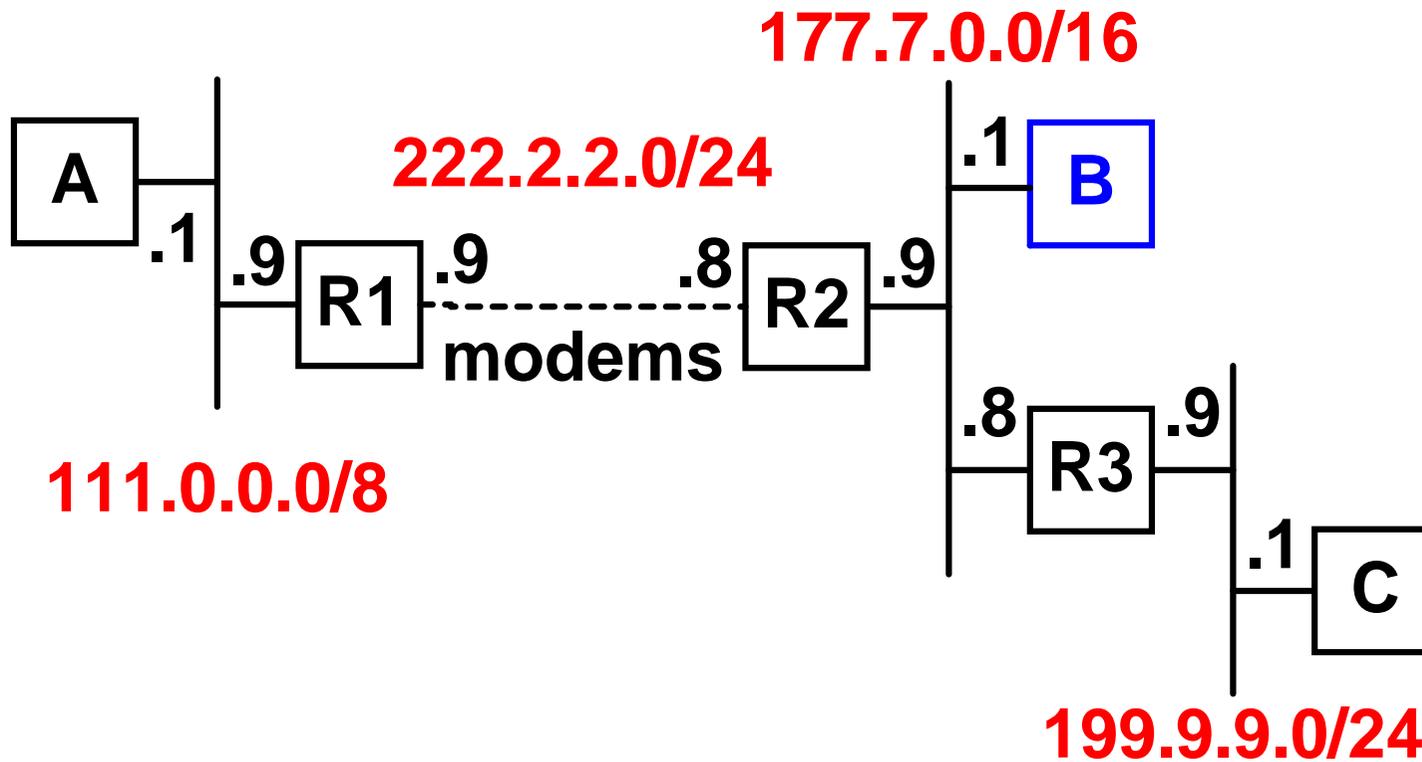
Routage statique

- Dans cet exemple, chaque équipement est configuré **manuellement** (commandes Unix)



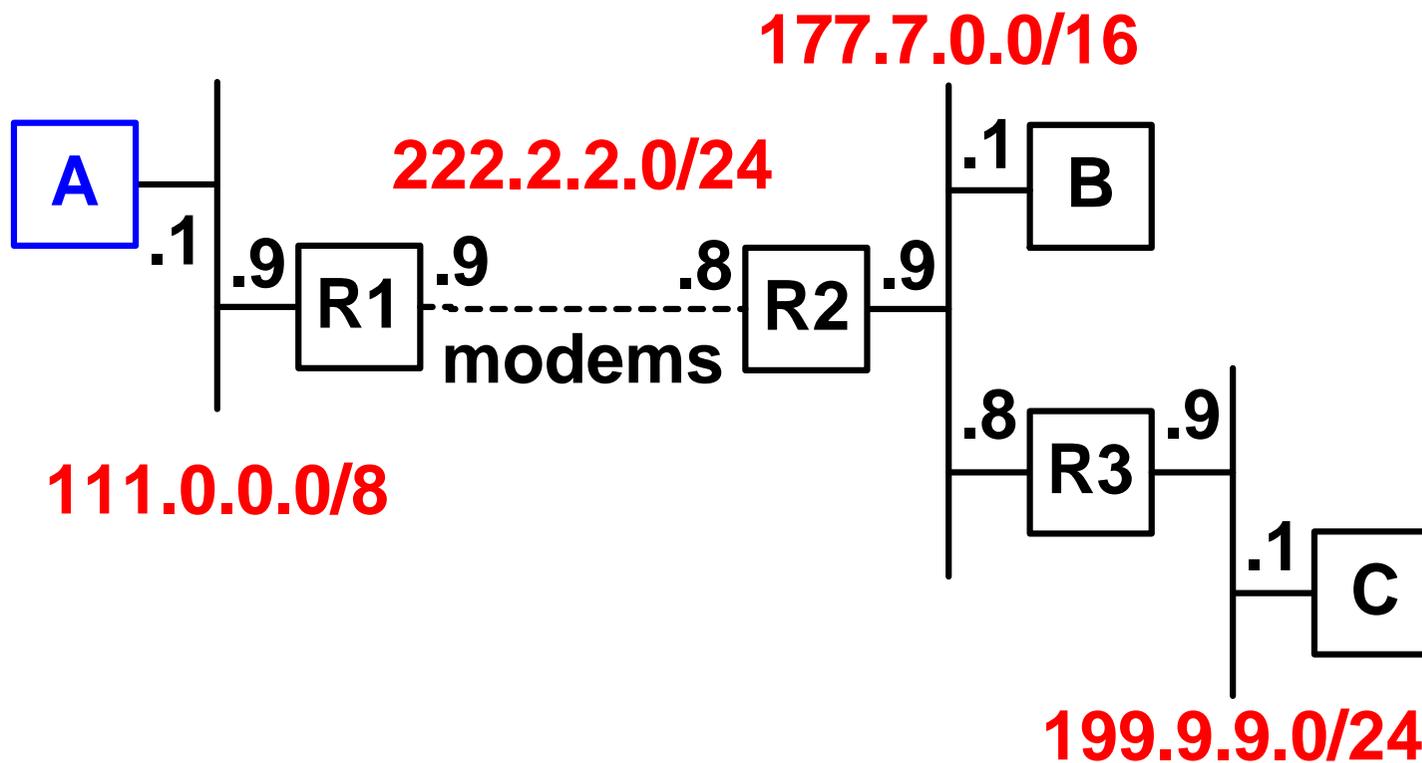
Sur la machine B

- `ifconfig eth0 177.7.0.1 mask 255.255.0.0`
- `route add 111.0.0.0 177.7.0.9`
- `route add 199.9.9.0 177.7.0.8`



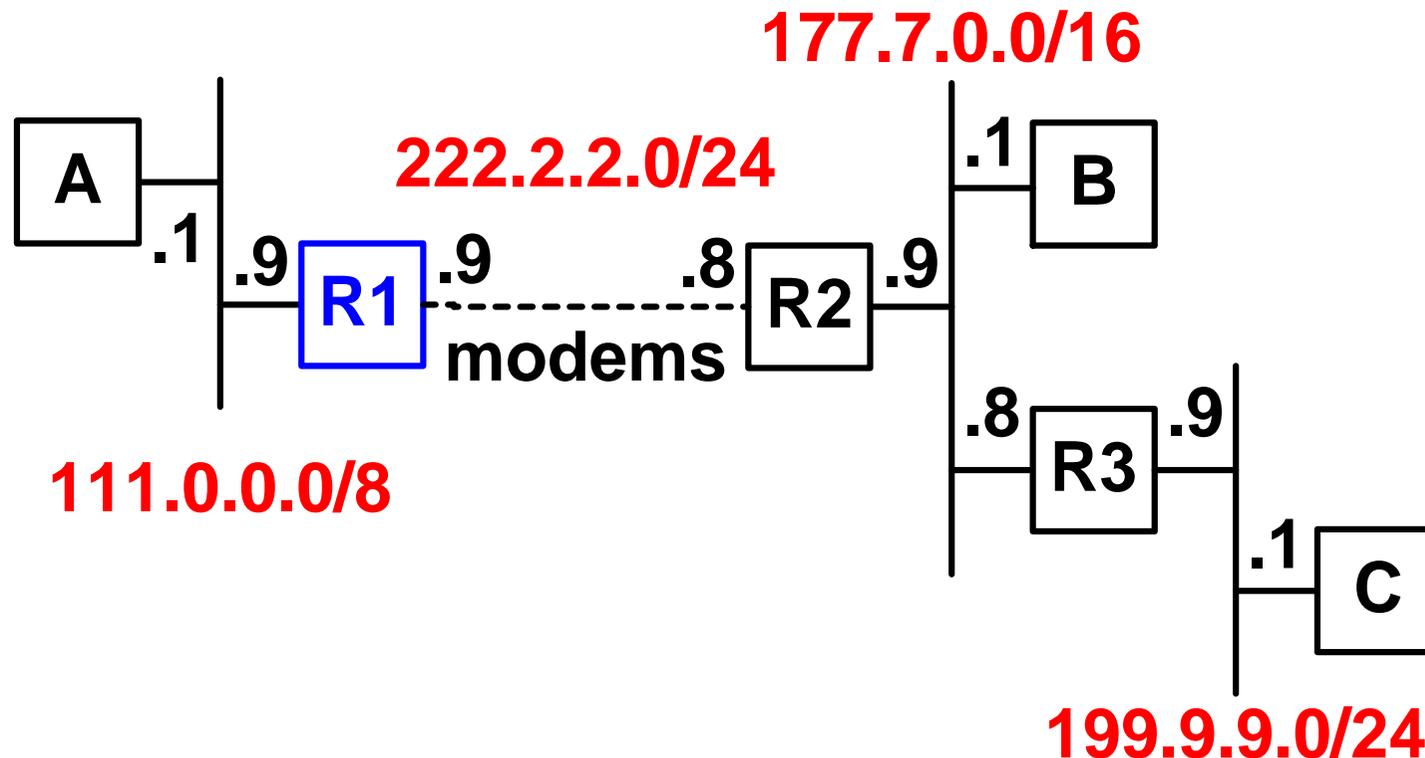
Sur la machine A

- `ifconfig eth0 111.0.0.1 mask 255.0.0.0`
- `route add default 111.0.0.9`



Sur le routeur R1

- `ifconfig eth0 111.0.0.9 mask 255.0.0.0`
- `ifconfig le0 222.2.2.9 mask 255.255.255.0`
- `route add default 222.2.2.8`



- Chaque routeur gère une **table de routage IP** (*IP routing table*) qu'il **consulte à chaque fois qu'il reçoit un datagramme**

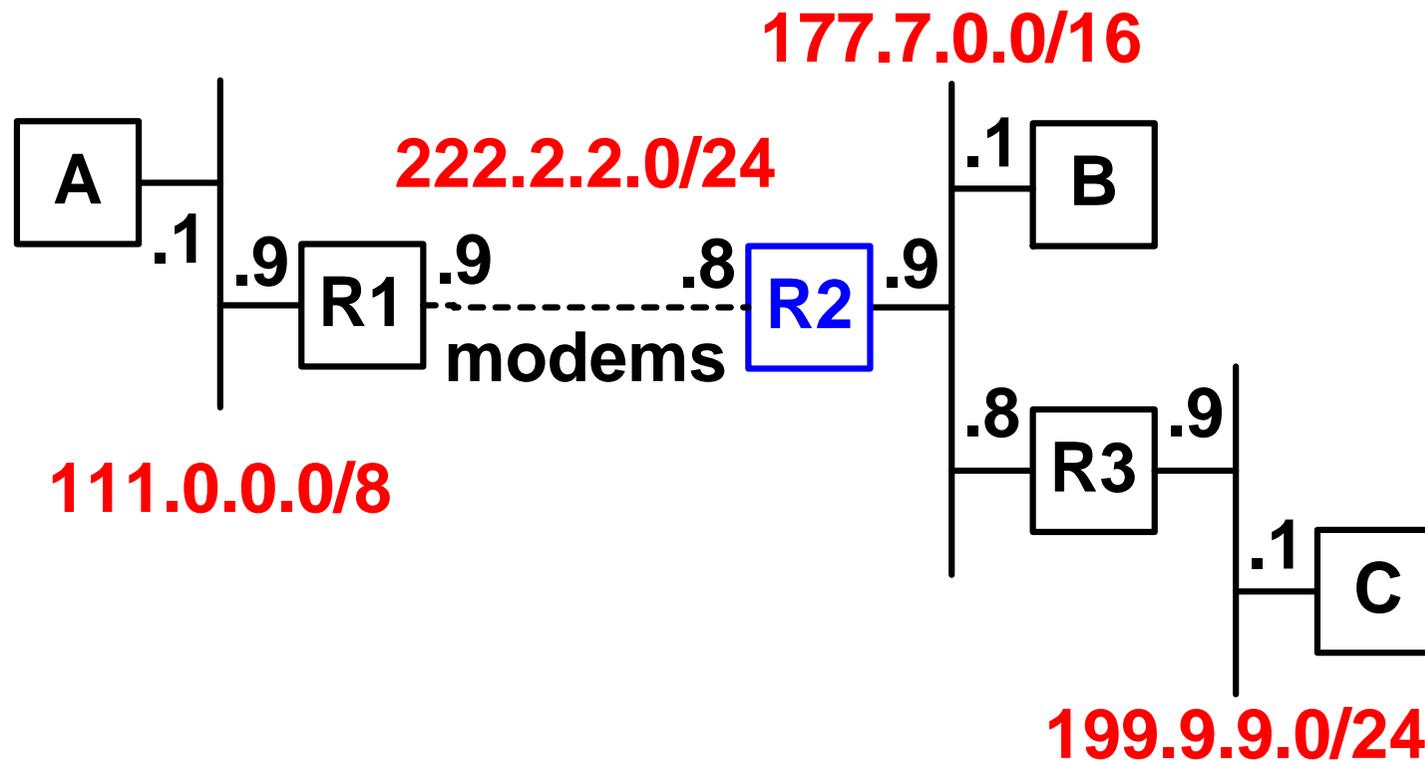
- Pour R1

| Destination | Routeur | Interface |
|----------------|------------------|-----------|
| 111.0.0.0 | connecté | eth0 |
| 222.2.2.0 | connecté | le0 |
| 0.0.0.0 | 222.2.2.8 | |

- Chaque routeur possède généralement une **route par défaut**

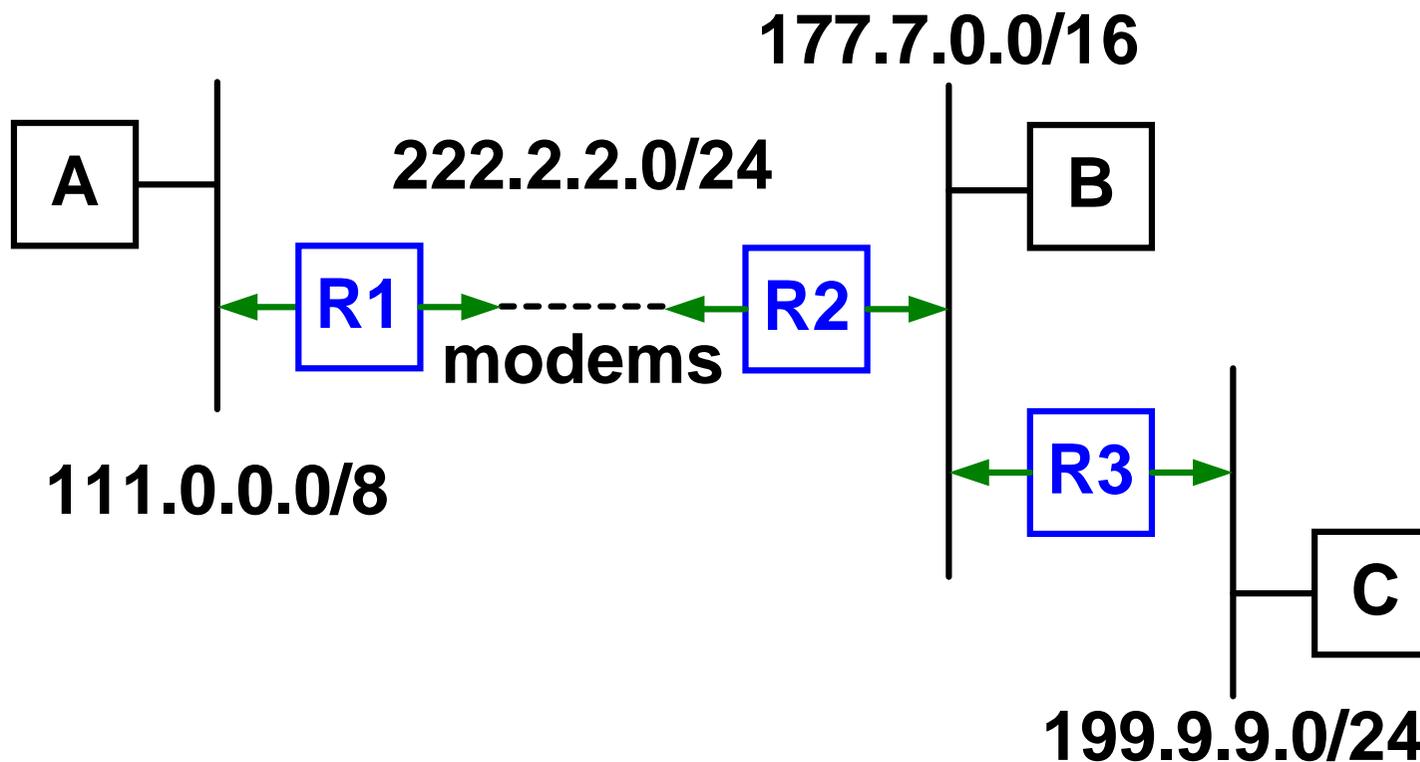
Sur le routeur R2

- `ifconfig eth0 177.7.0.9 mask 255.255.0.0`
- `ifconfig le0 222.2.2.8 mask 255.255.255.0`
- `route add 111.0.0.0 222.2.2.9`
- `route add 199.9.9.0 177.7.0.8`



Routage dynamique

- Le routage dynamique met en œuvre un **protocole de communication inter-routeurs** (protocole de routage, RIP, ...)
- Chaque routeur informe son(s) voisin(s)

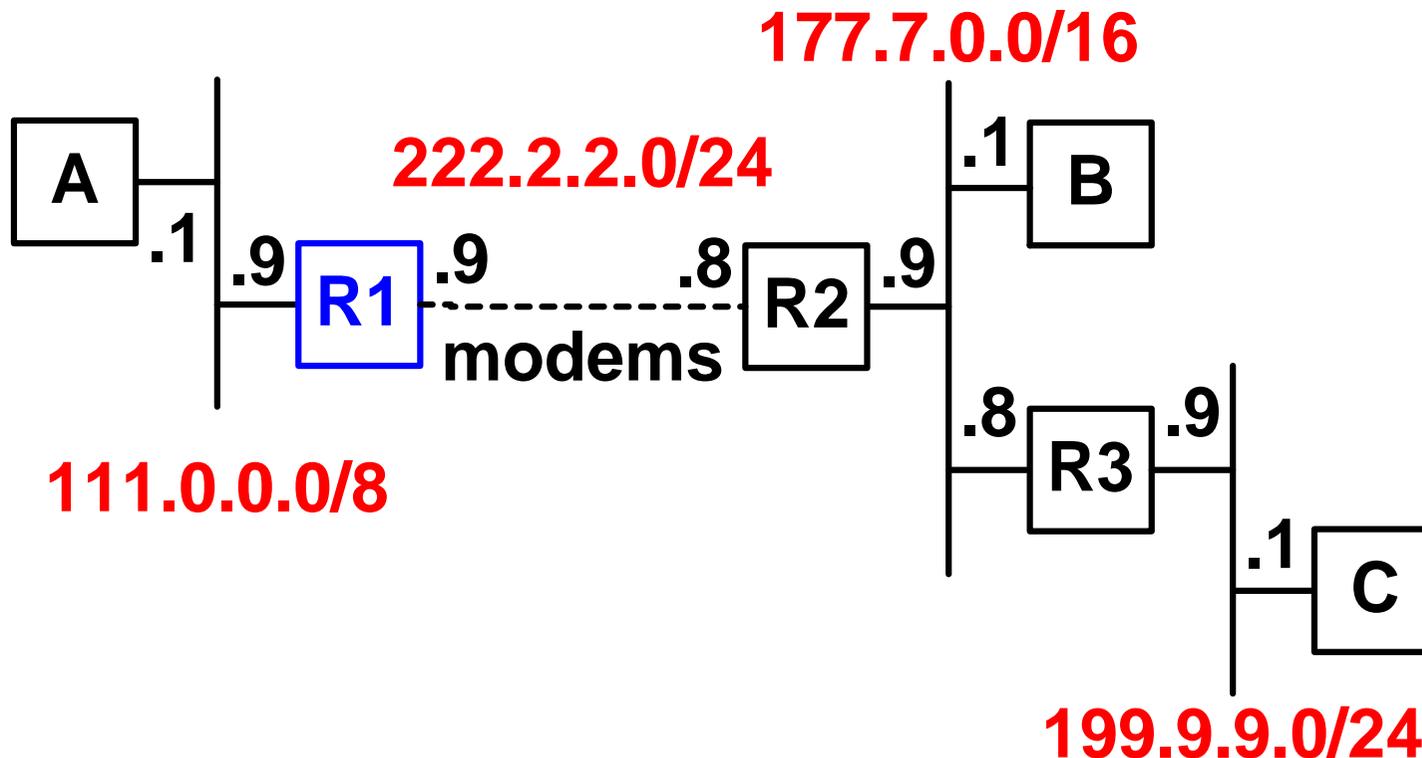


Configuration de R1

- Interface LAN

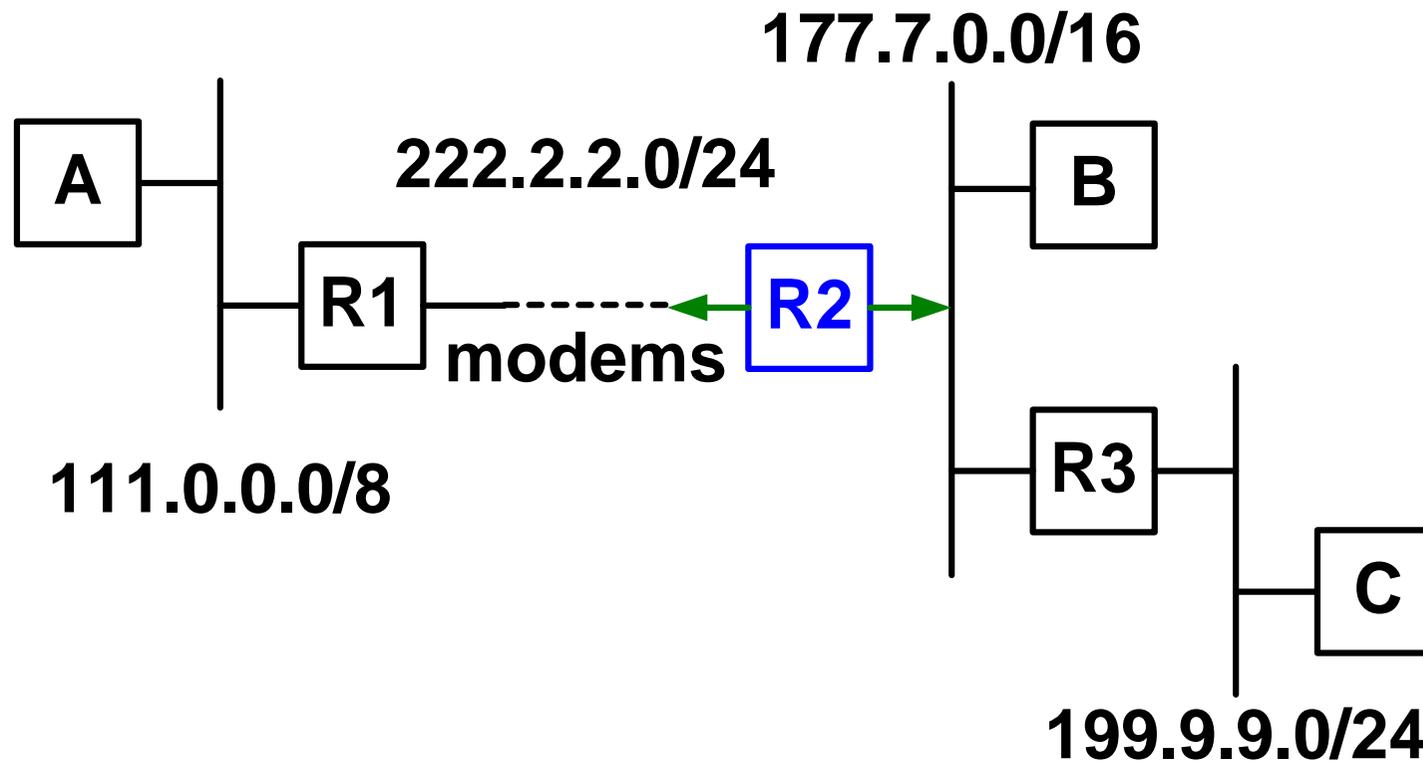
| | | |
|--------------------|-----------|----------|
| <i>IP address</i> | 111.0.0.9 | classe A |
| <i>subnet mask</i> | 255.0.0.0 | |
| <i>router</i> | | |
- Interface WAN

| | | |
|--------------------|---------------|----------|
| <i>IP address</i> | 222.2.2.9 | classe C |
| <i>subnet mask</i> | 255.255.255.0 | |
| <i>router</i> | 222.2.2.8 | |

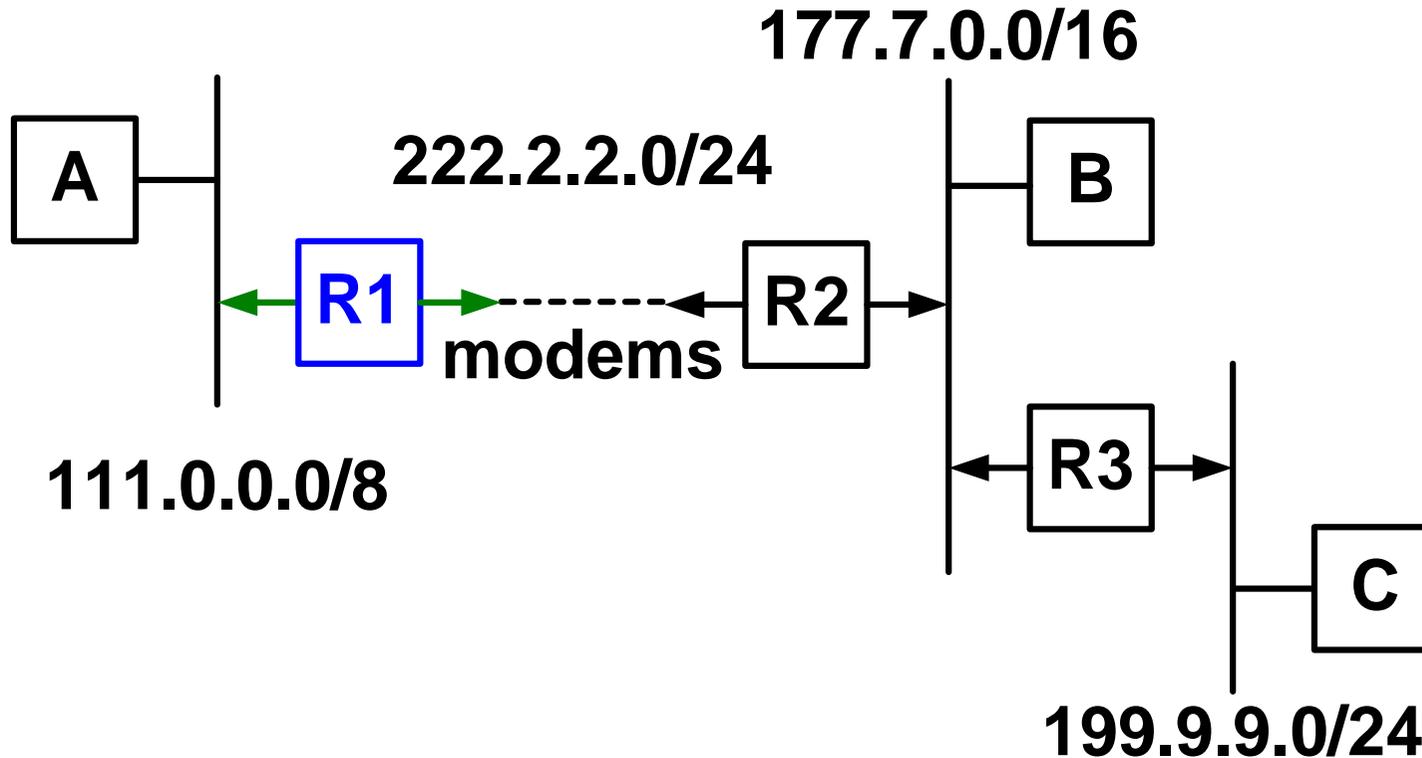


- Un routeur **diffuse** (*broadcast*) toutes les 30 secondes la liste des réseaux qu'il peut atteindre avec leur **distance** (*metric*)
- **Distance** = nb de routeurs à traverser
- Le routeur transmet une copie de sa table de routage avec le protocole RIP (*Routing Information Protocol*)
- Les messages RIP sont contenus dans des datagrammes
UDP port = 520

- **R2** envoie à ses voisins : 222.2.2.0 d=1
177.7.0.0 d=1



- **R1** envoie à ses voisins : 111.0.0.0 d=1
222.2.2.0 d=1



- **R3** envoie à ses voisins : 177.7.0.0 d=1
199.9.9.0 d=1

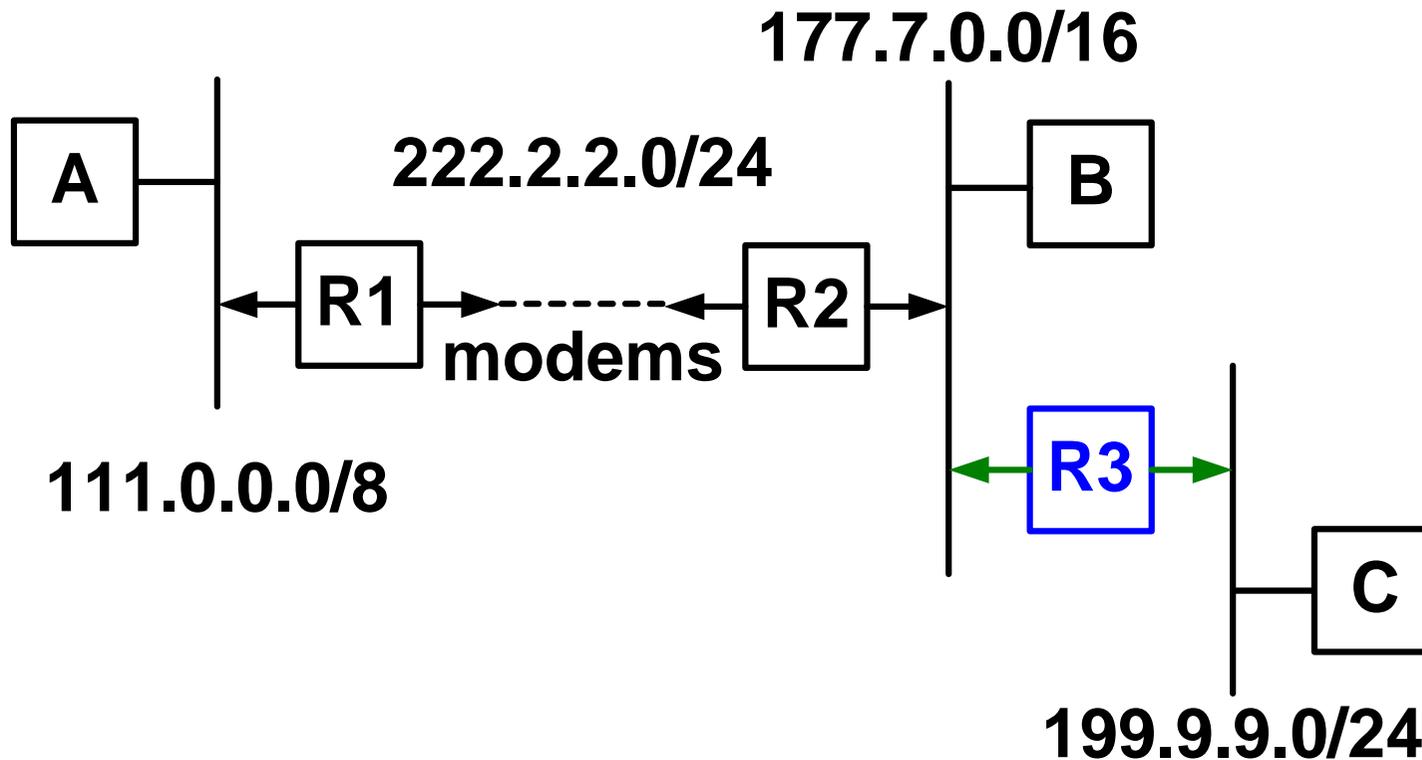


Table de routage de R2

- Pour R2
 - 222.2.2.0 d=1
 - 177.7.0.0 d=1
 - 111.0.0.0 d=2
 - 222.2.2.0 d=2 sans intérêt
 - 177.7.0.0 d=2 sans intérêt
 - 199.9.9.0 d=2

- Pour R2

| Destination | Distance | Routeur |
|-------------|----------|-----------|
| 222.2.2.0 | 1 | connecté |
| 177.7.0.0 | 1 | connecté |
| 111.0.0.0 | 2 | 222.2.2.9 |
| 199.9.9.0 | 2 | 177.7.0.8 |

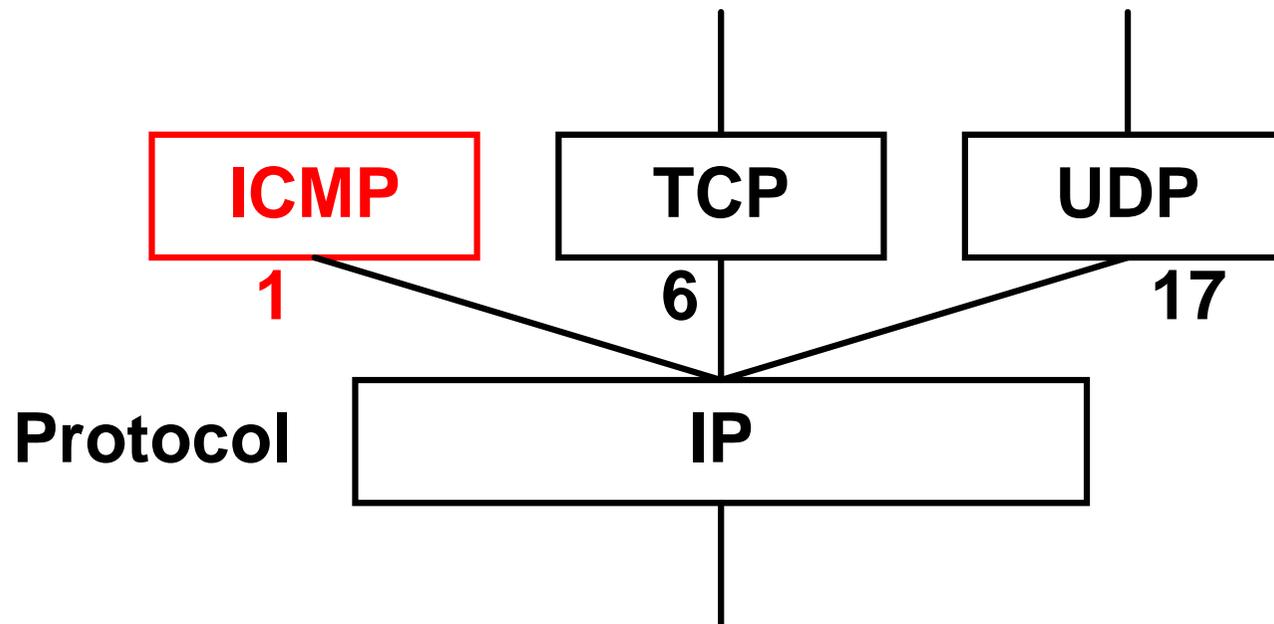
- Commandes Cisco show ip route
Unix netstat, route

Caractéristiques de RIP

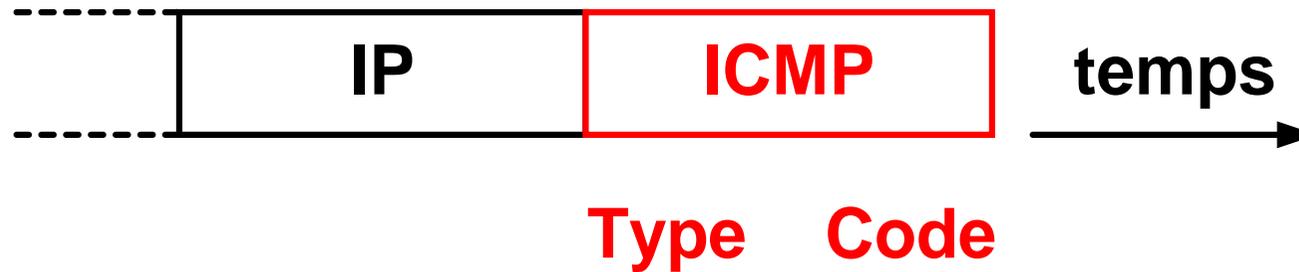
- **Protocole de routage très simple**
- **Distance est une information sommaire**
- **Distance max = 15**
- **Pas de garantie sur l'origine des informations**
- **Convient pour de petits réseaux**

- Un algorithme comme RIP, de type *distance vector*, exprime la distance en nombre de sauts (*hops count*)
- Un saut est représenté par un routeur reliant 2 segments
- Chaque routeur construit sa table de routage à partir des informations diffusées par les autres
- Ce **mécanisme d'apprentissage progressif n'est pas immédiat** et n'aboutit à une description complète du réseau qu'**après un temps de convergence** de l'algorithme
- Intérêt du champ TTL (couche IP)

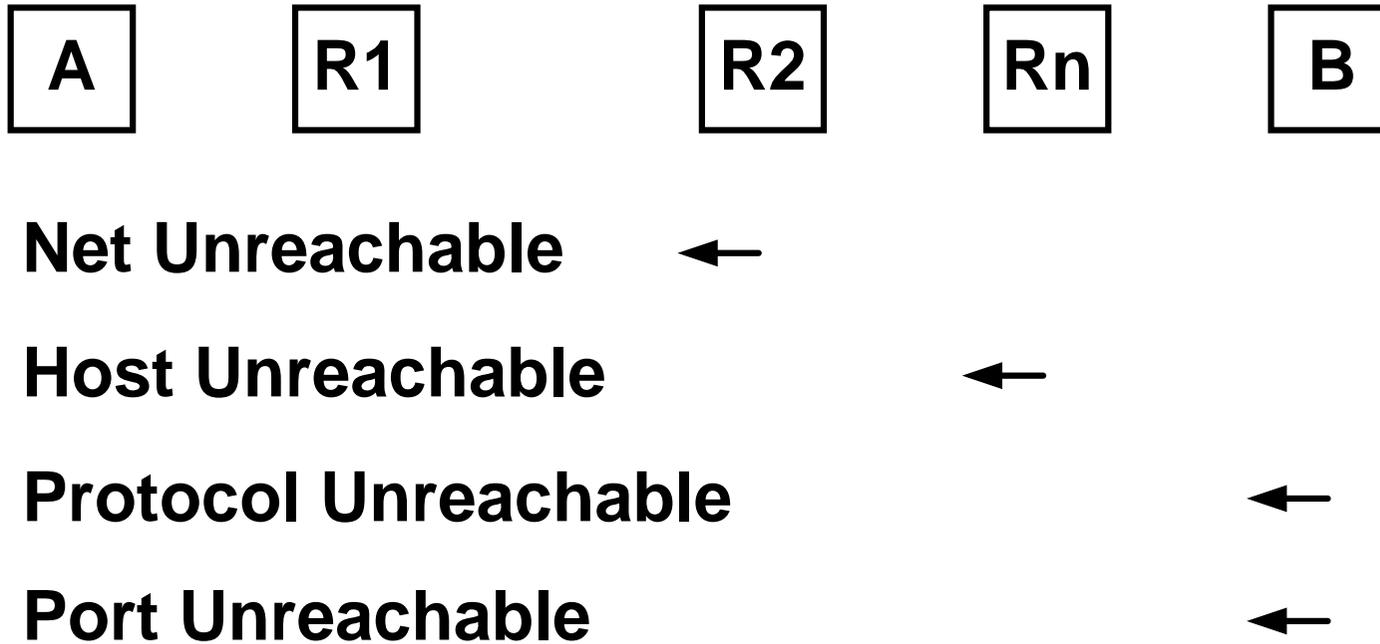
- IP : service datagramme sans connexion → *best effort*
- **ICMP** : messages d'erreur et de diagnostic → adm. Réseau



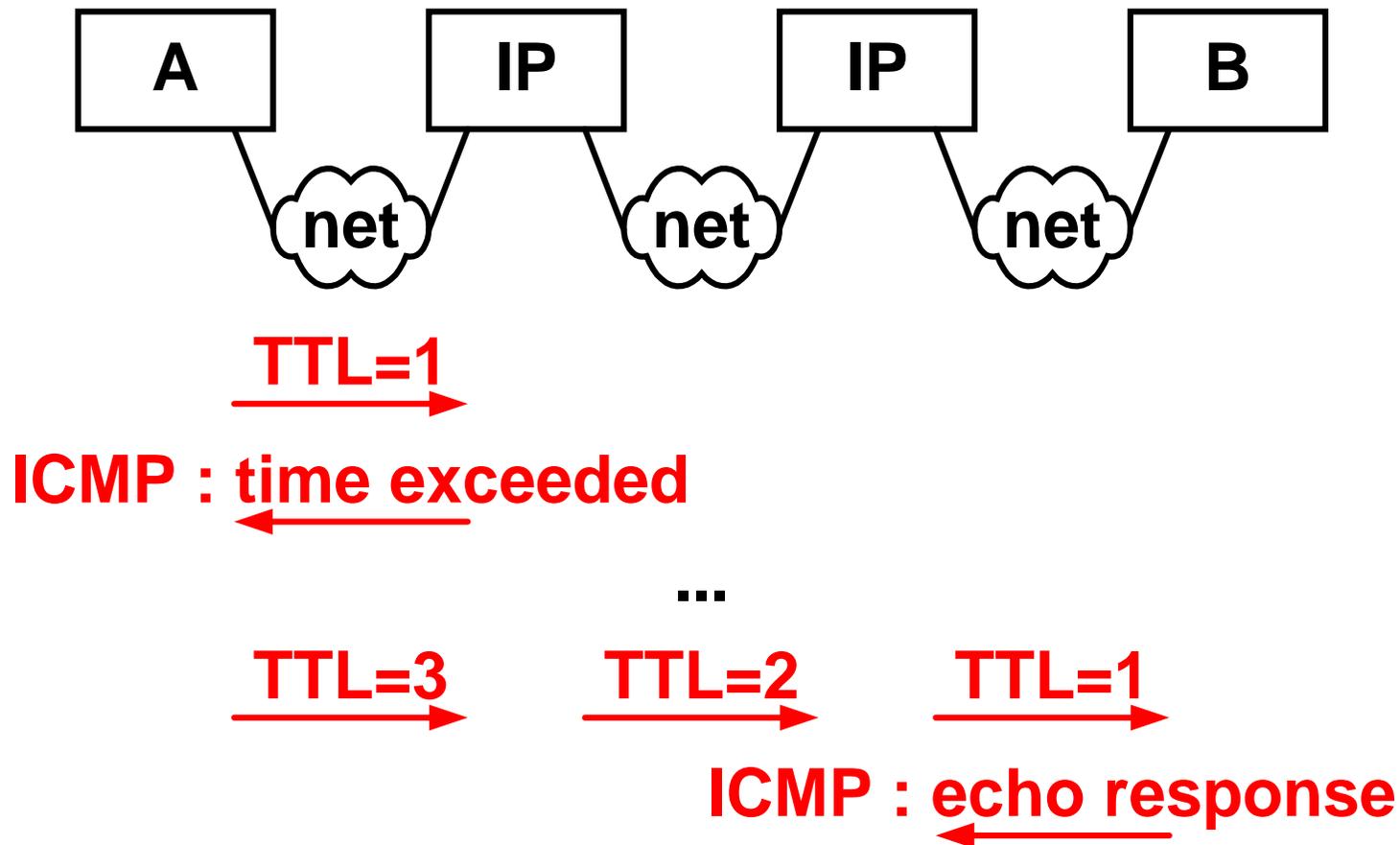
- Rfc 792



| Type | Code | |
|----------------------------|----------------------------------|-------------|
| 0 <i>Echo Reply</i> | 0 | |
| 3 <i>Dest. Unreachable</i> | 0 <i>Net Unreachable</i> | Router |
| | 1 <i>Host Unreachable</i> | last Router |
| | 2 <i>Protocol Unreachable</i> | Host |
| | 3 <i>Port Unreachable</i> | Host |
| 5 <i>Redirect</i> | | |
| 8 <i>Echo</i> | 0 | |
| 11 <i>Time Exceeded</i> | 0 <i>TTL exceeded in transit</i> | |



- La commande **Traceroute** permet de localiser chaque routeur situé sur le chemin en envoyant des datagrammes successifs avec le champ TTL égal à 1, 2, ...



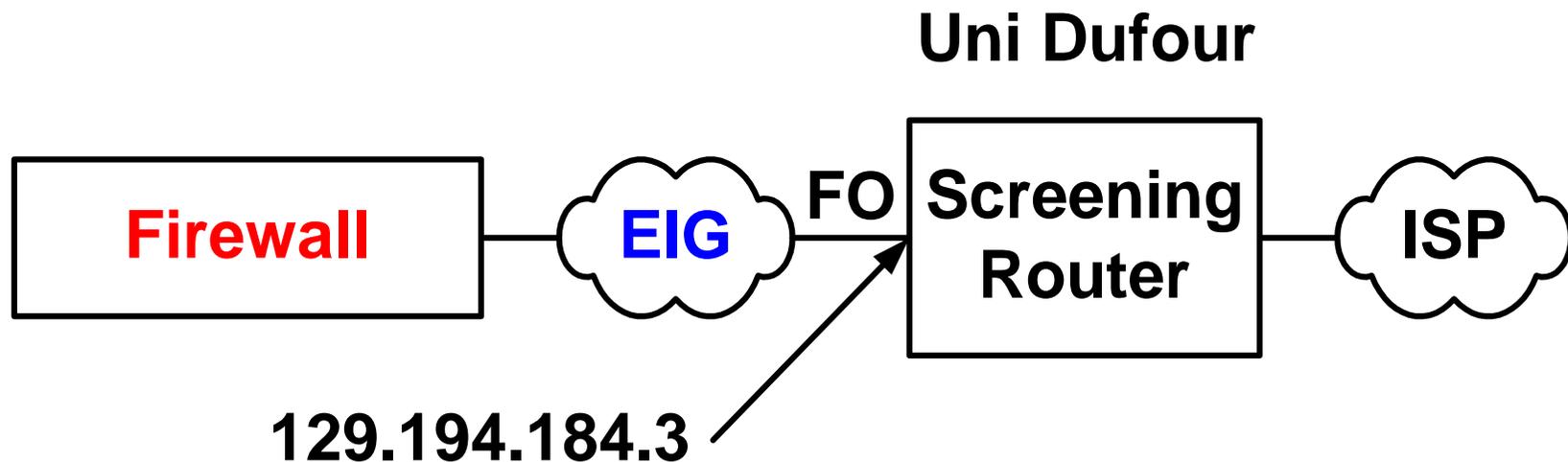
Traceroute (2)

```
tracert www.luth.se
```

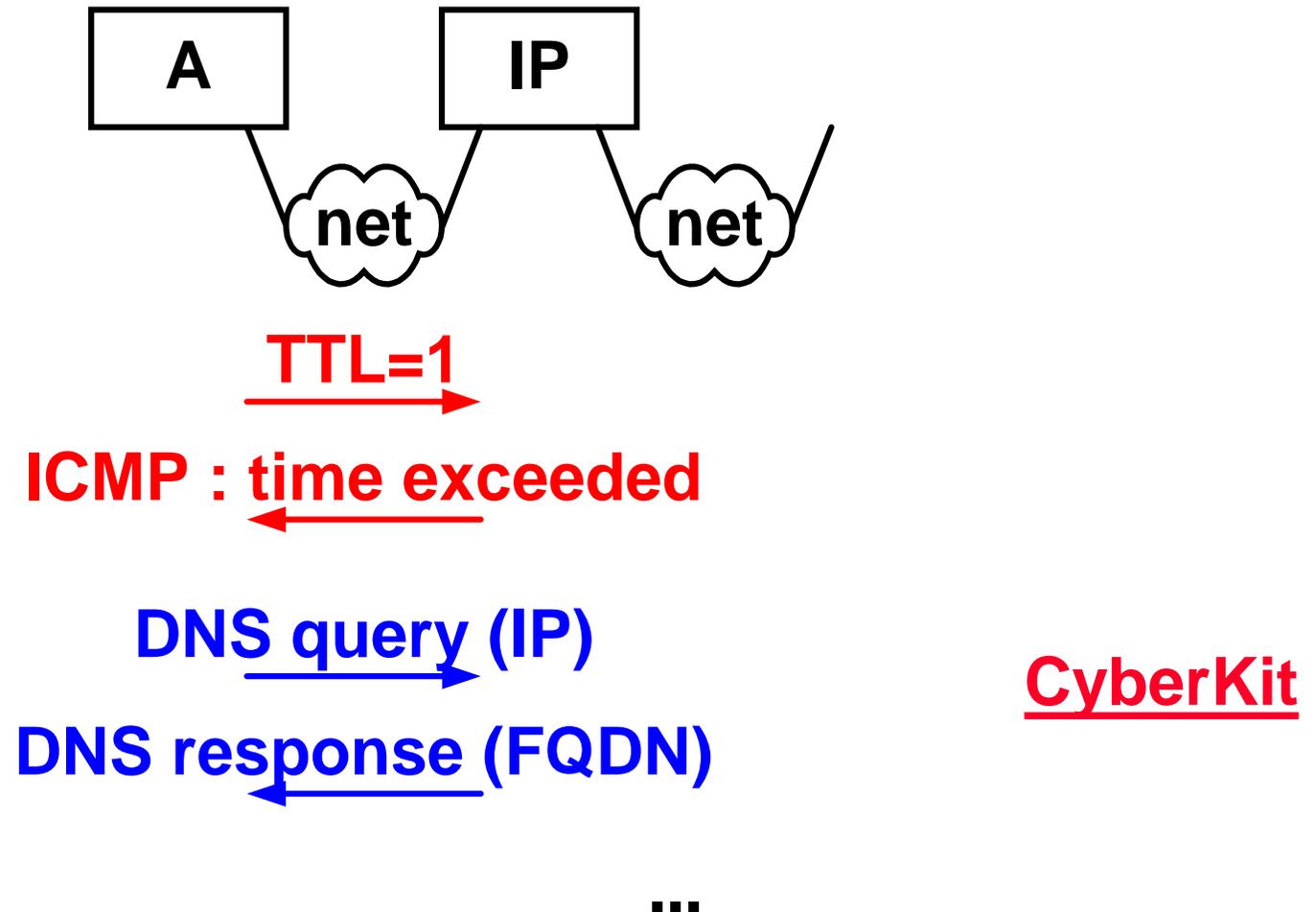
| # | Address | Response Time |
|----|-----------------|---------------|
| 1 | 129.194.184.3 | 4 ms |
| 2 | 129.194.12.3 | 2 ms |
| 3 | 192.33.214.3 | 2 ms |
| 4 | 130.59.33.45 | 3 ms |
| 5 | 212.1.192.169 | 4 ms |
| 6 | 212.1.192.46 | 58 ms |
| 7 | 212.1.192.154 | 53 ms |
| 8 | 193.10.252.178 | 54 ms |
| 9 | 130.242.200.10 | 58 ms |
| 10 | 130.242.200.126 | 66 ms |
| 11 | 130.242.202.116 | 68 ms |
| 12 | 130.240.42.42 | 69 ms |

Screening router

- Les attaques basées sur l'envoi de requêtes ICMP *echo request* sont fréquentes
- La plupart des routeurs disposent de fonction de filtrage au niveau adresse IP, type de protocole (ICMP, ...), numéro de port, ...
- Première ligne de défense contre les intrusions



- Cette option produit des **requêtes DNS inverses**



CyberKit

Traceroute avec option DNS (2)

```
tracert www.luth.se
```

| # | Address | Host Name | Response Time |
|----|-----------------|---------------------------|---------------|
| 1 | 129.194.184.3 | Unavailable | 4 ms |
| 2 | 129.194.12.3 | unige-gw.unige.ch | 2 ms |
| 3 | 192.33.214.3 | swige1.unige.ch | 2 ms |
| 4 | 130.59.33.45 | swiCE1-A4-0-0-2.SWITCH.ch | 3 ms |
| 5 | 212.1.192.169 | switch.ch.ten-155.NET | 4 ms |
| 6 | 212.1.192.46 | ch-se.se.ten-155.NET | 58 ms |
| 7 | 212.1.192.154 | sw-gw.nordu.NET | 53 ms |
| 8 | 193.10.252.178 | STK-BB-1.SUNET.SE | 54 ms |
| 9 | 130.242.200.10 | SVL-BB-1.SUNET.SE | 58 ms |
| 10 | 130.242.200.126 | lulea-pos.SUNET.SE | 66 ms |
| 11 | 130.242.202.116 | Unavailable | 68 ms |
| 12 | 130.240.42.42 | www.luth.se | 69 ms |

Adressage de sous-réseaux

- Adresse IP (32 bits) = **network** + **host**

Le champ **host** peut identifier des **sous-réseaux**

- L'Université de Genève, qui dispose d'une adresse IP de classe B (**network = 129.194**) a décidé de subdiviser son réseau en **64 sous-réseaux** (*subnet*)

6 bits étant nécessaires, chaque nœud IP du réseau de l'Université doit être configuré avec le masque de sous-réseau suivant :

255.255.252.0

| | | | |
|-----------------|-----------------|-----------------|-----------------|
| 255 | 255 | 252 | 0 |
| 11111111 | 11111111 | 11111100 | 00000000 |

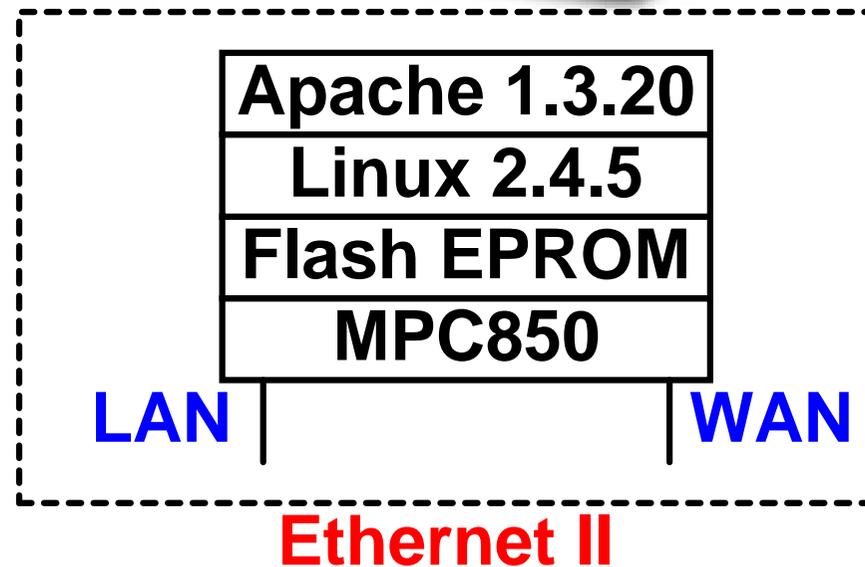
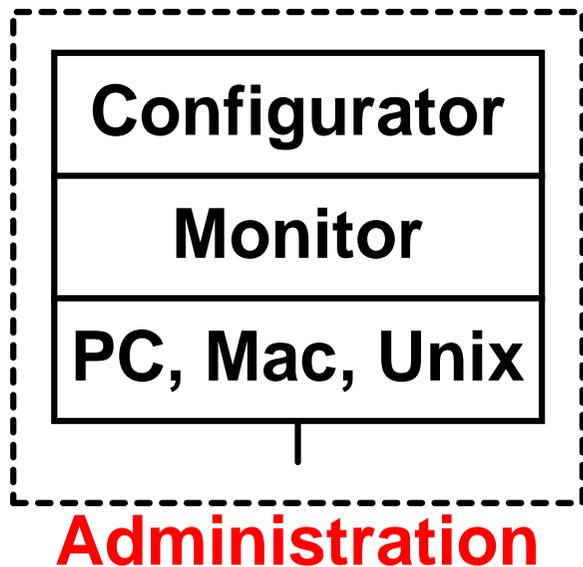
- Chaque *subnet* ne peut plus contenir que 1024 ordinateurs
- Cette subdivision n'est pas visible à l'extérieur du réseau

- **Labo C1**

`ipconfig`, `ping`, `tracert`, `netstat`,
Analyse des protocoles ARP, IP, ICMP

- **Labo C2**

Configuration d'un routeur



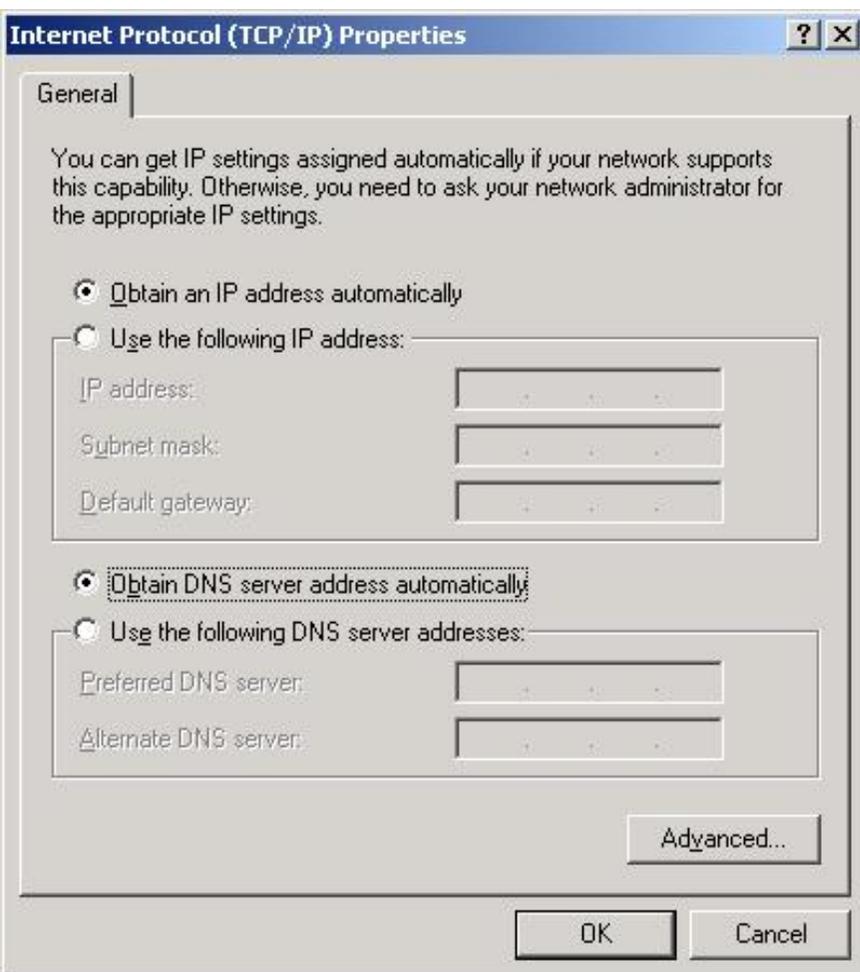
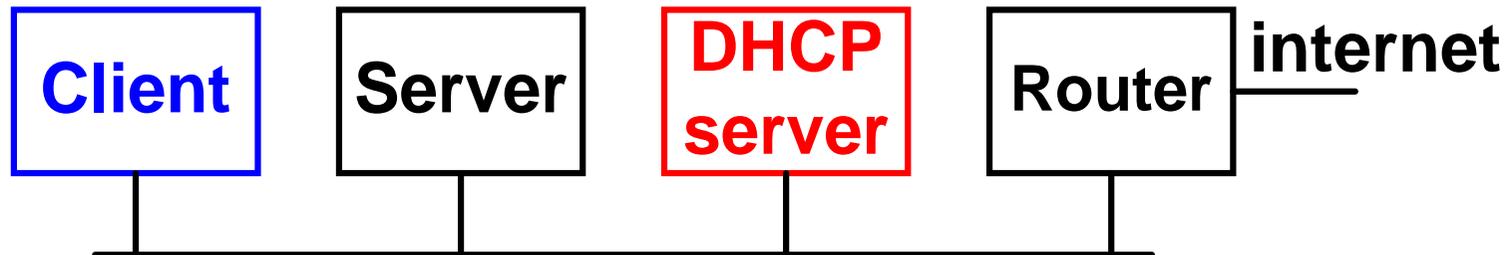
Configuration dynamique : motivation

- La configuration d'un nœud IP demande des **connaissances spécifiques** que certains utilisateurs n'ont pas
- L'essor d'**équipements grand public** comme portable, *mobile IP*, *phone IP*, *thin client*, ... exige une procédure de configuration dynamique (automatique)
- Certaines entreprises **changent** d'ISP (*Internet Service Provider*) tous les ans

- ***Reverse Address Resolution Protocol - RFC 903***
- **Ce protocole de résolution d'adresse inverse permet à un système minimum sans disque de demander l'adresse IP correspondant à l'adresse physique transmise**
- **Le serveur RARP contient le fichier d'équivalence entre adresse physique (MAC) et adresse logique (IP)**
- ***Bootstrap Protocol - RFC 951***
- **Alternative à RARP en offrant des informations supplémentaires comme le masque de sous-réseau, l'adresse IP du routeur, l'adresse IP du serveur DNS, ...**

Configuration dynamique : DHCP (1)

- *Dynamic Host Configuration Protocol* - RFC 2131
- Un **serveur DHCP** va **allouer dynamiquement les adresses IP** dans l'espace qu'il gère sans connaître l'adresse physique du nœud
- Il transmet également les **informations supplémentaires** décrites précédemment
- Le **client** doit être dans le mode (par défaut de Win2000) : *Obtain an IP address automatically*
- La configuration présente une certaine **durée de vie** (*lease time*)



ip addr 10.0.0.1
Mask 255.0.0.0
range 10.0.0.10 – 10.0.0.254
lease time 3600

→ DHCP Discover

← DHCP Offer

→ DHCP Request

← DHCP Ack

...

lease time

→ DHCP Request

← DHCP Ack

- TCP/IP illustré – Les protocoles W. Richard Stevens
Versions anglaise et française
- <http://www.cisco.com/univercd/cc/td/doc/>
- Command : ping, tracert, ipconfig, netstat, ...
- Cyberkit <http://www.gknw.com/mirror/cyberkit/>

