

Chapitre 5

La couche réseau

Haïfa Touati

Plan

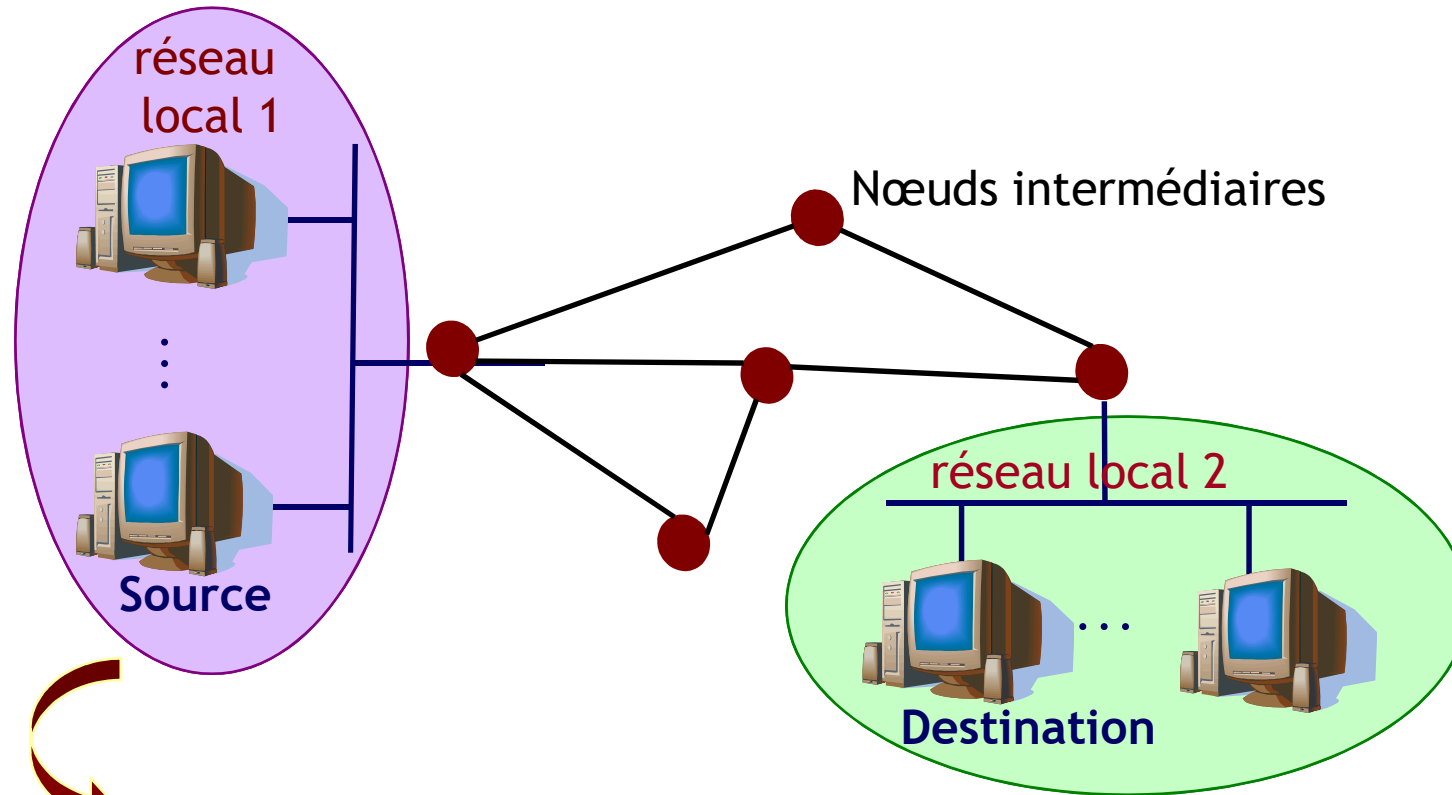
1- Introduction

2- L'adressage

3- Le routage

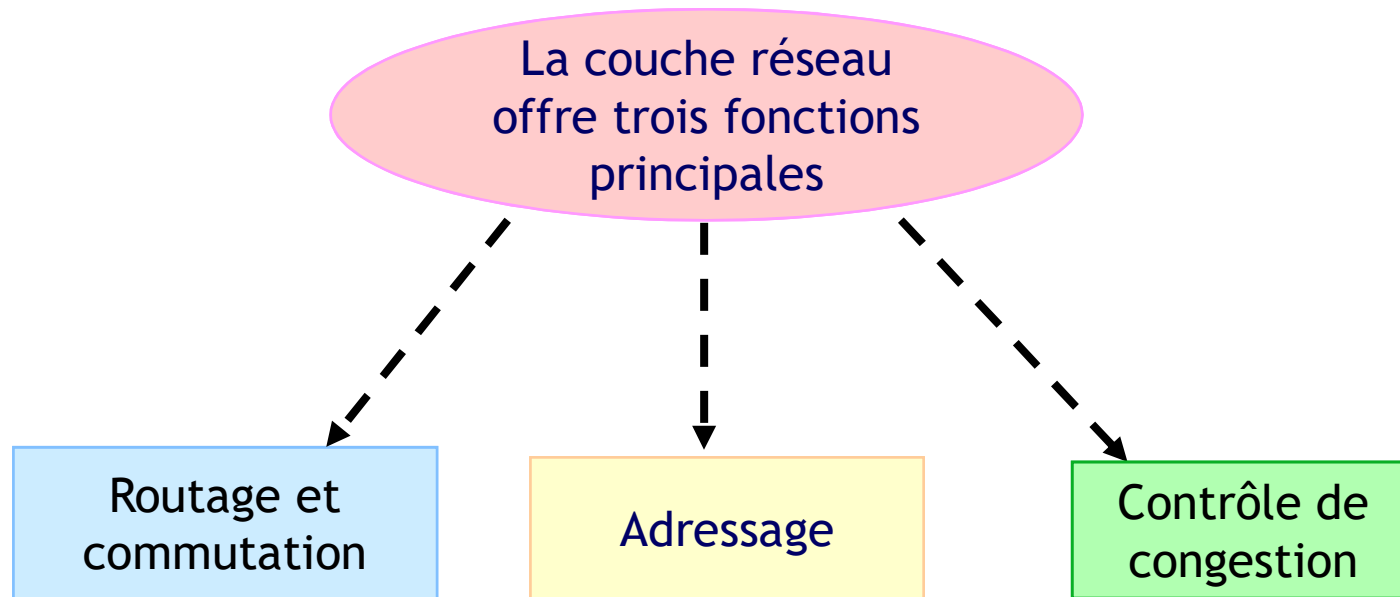
4- Exemple : le protocole IPv4

Introduction



Cette couche permet la transmission entre 2 machines qui ne sont pas nécessairement directement connectées

Introduction



Plan

1- Introduction

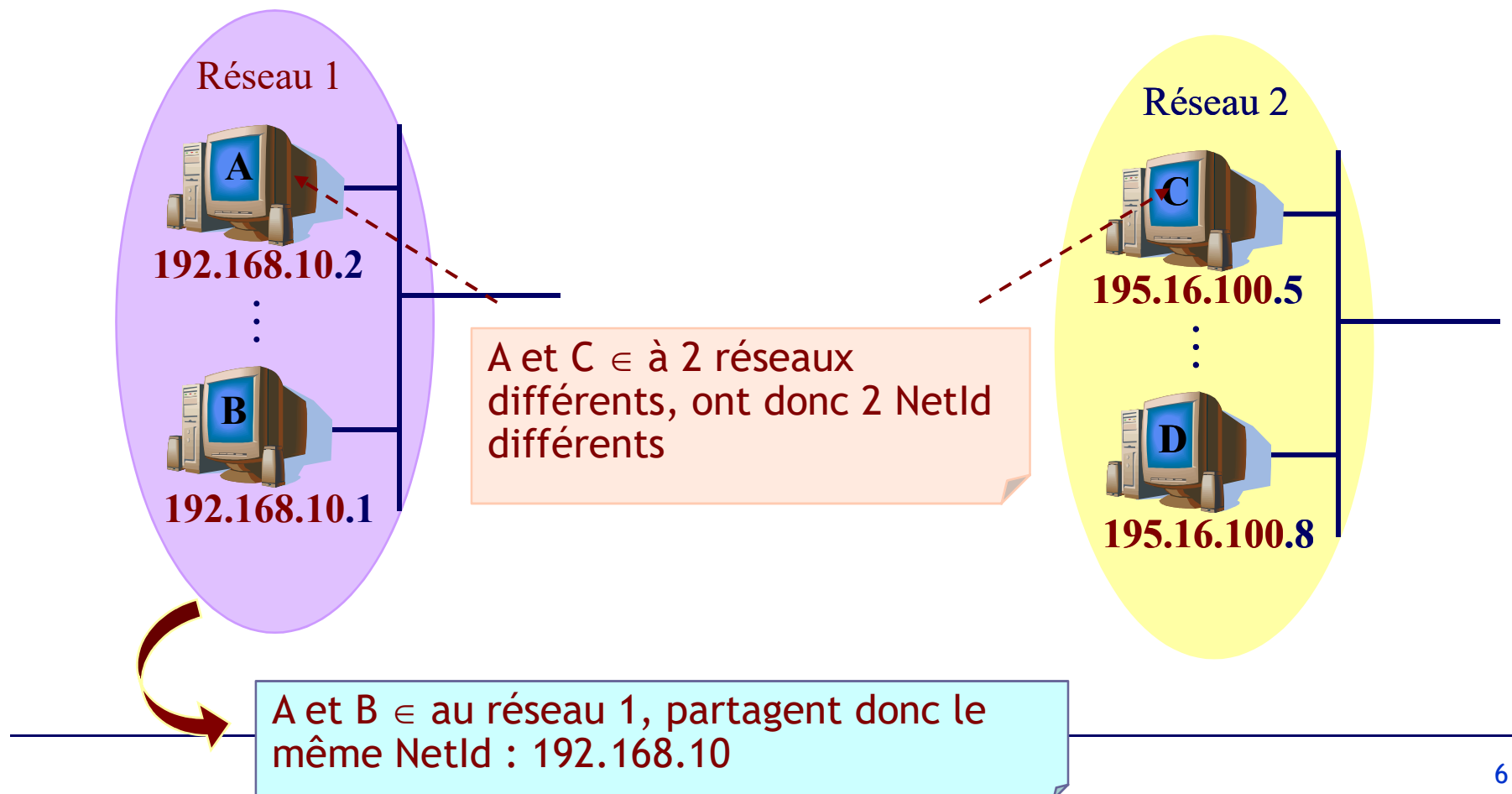
2- L'adressage

3- Le routage

4- Exemple : le protocole IPv4

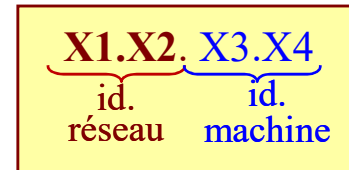
L'adressage : L'adressage IP

- Les machines d'un même réseau doivent avoir le même identificateur réseau (NetId)



Adressage IPv4

- Le protocole IP fonctionne en **mode non connecté** => chaque paquet IP est envoyé indépendamment des autres => contient donc toujours l'adresse IP du destinataire
- Une adresse IP est constituée de deux parties :
 - un identificateur de réseau (NetId)
 - un identificateur de machine (HostId)
- Toute adresse IP est associée à un **masque réseau** qui sert à déterminer la portion de l'adresse réservée à l'hôte et celle réservée au réseau

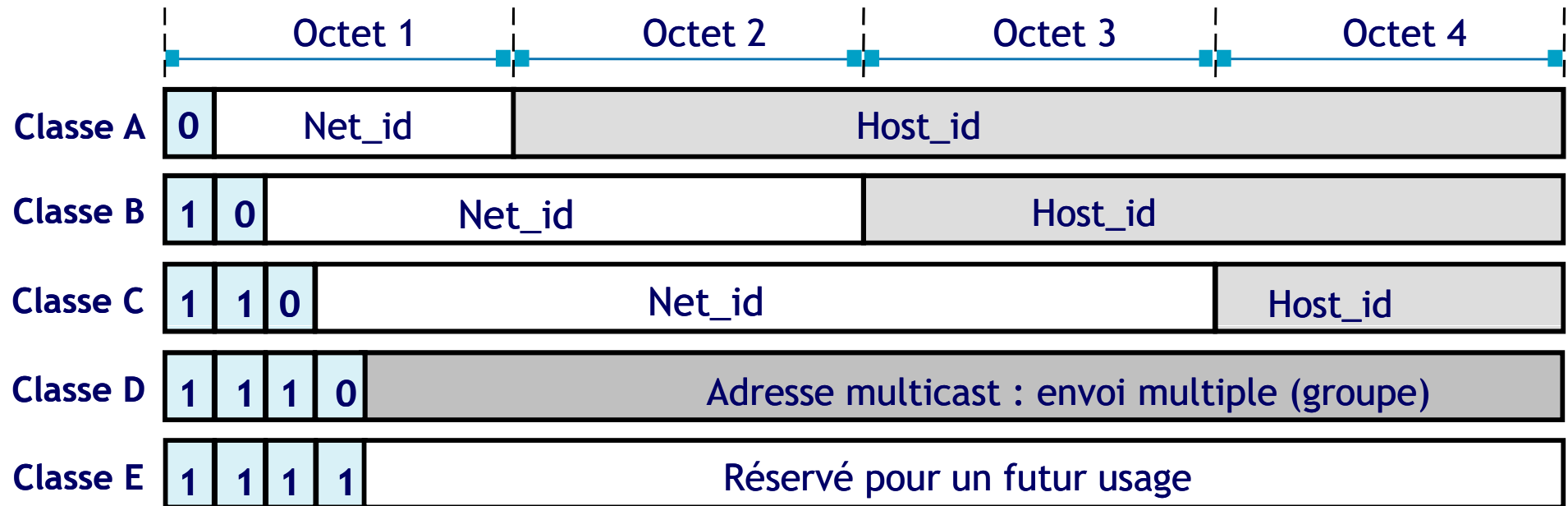


Exemple

Adresse IP :	172.	16.	1.	5
Masque en binaire :	1111 1111.11111111.	0000 0000.	0000 0000	0000
Masque en décimal :	255 .	255.	0.	0

Adressage IPv4 : Les classes d'adresses

Les classes d'adresses



Classe	Masque par défaut	1er octet compris entre
A	255.0.0.0 ou /8	0 et 127
B	255.255.0.0 ou /16	128 et 191
C	255.255.255.0 ou /24	192 et 223

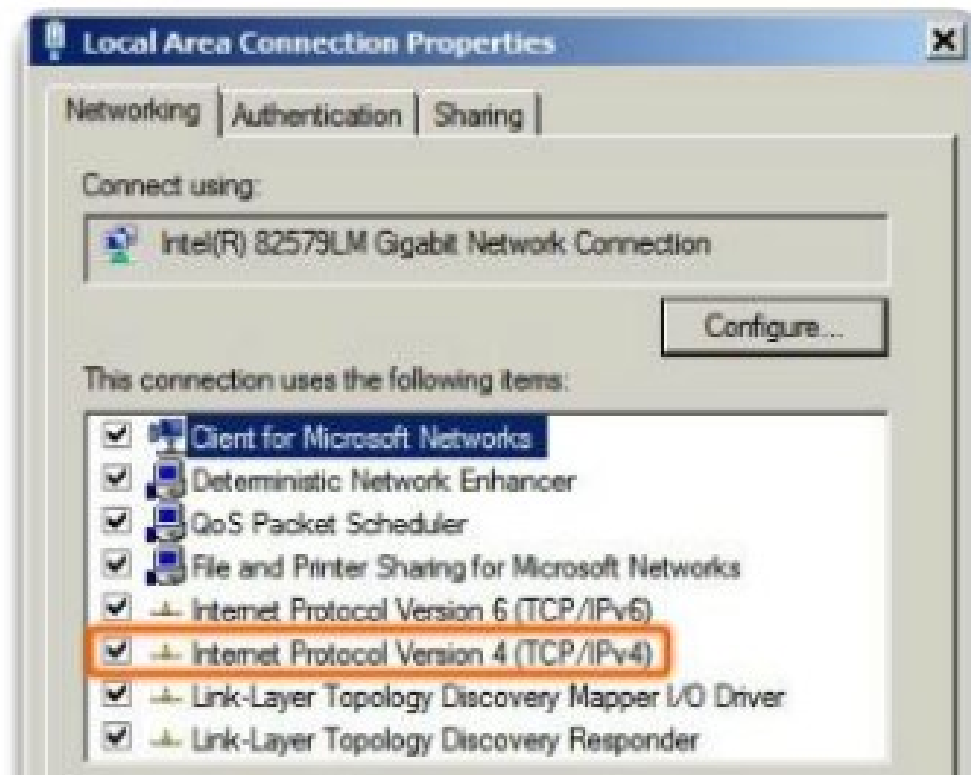
L'adressage IP: Les adresses réservées

- Les adresses entre 0.0.0.0 et 255.255.255.255 ne sont pas toutes valides pour identifier un hôte

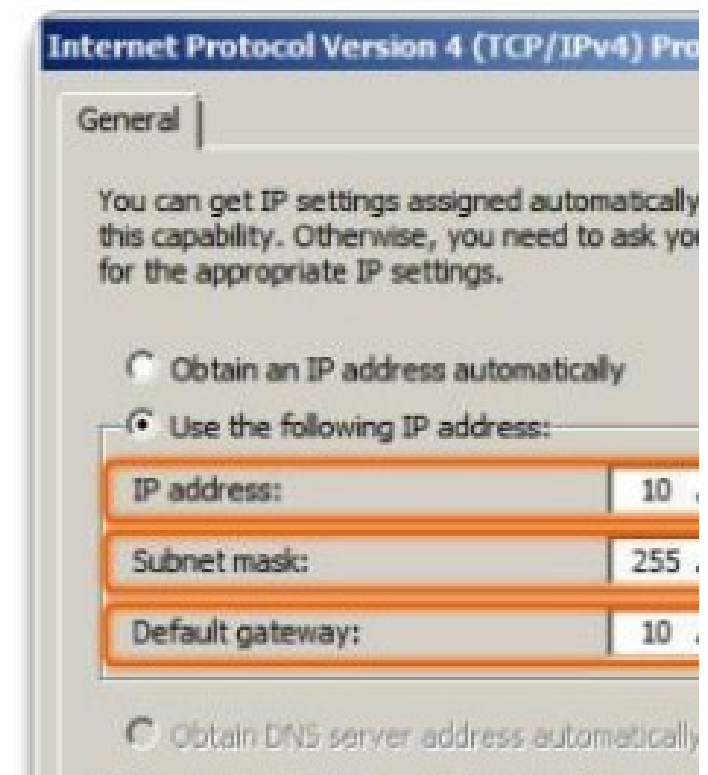
NetId	HostId	Signification
Tous '0'		Désigne la machine locale
Tous '1'		Broadcast dans chaque réseau
id_res	Tous '0'	Adresse du réseau
id_res	Tous '1'	Broadcast dans le réseau indiqué
Tous '0'	id_host	Identifie un host dans le réseau local
127	valeur quelconque	Adresse de loopback

L'adressage IP: Attribution d'une adresse statique à un hôte

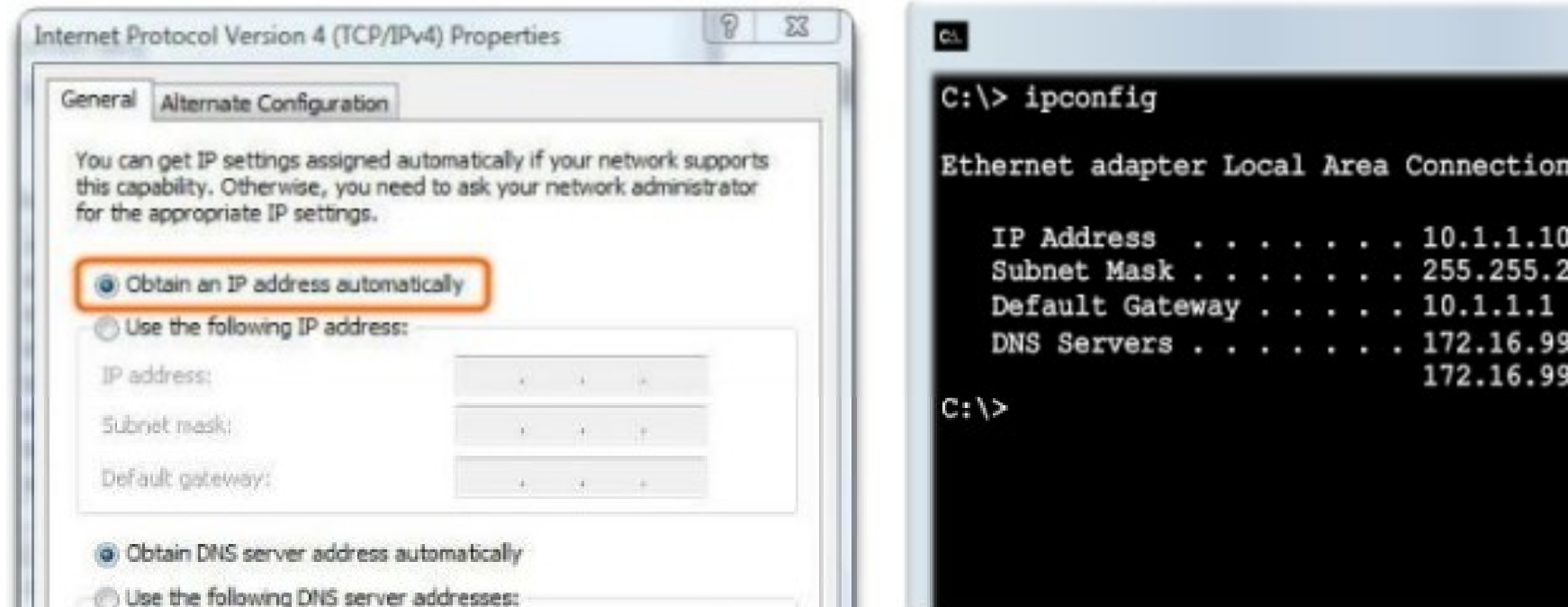
Propriétés d'interface LAN



Configuration d'une adresse



L'adressage IP: Attribution d'une adresse dynamique à un hôte



DHCP : méthode privilégiée d'attribution des adresses IPv4 aux hôtes sur les grands réseaux, car elle réduit la charge de travail de l'assistance technique et élimine presque toutes les erreurs d'entrée

Adressage IPv4 : Adressage sans classe

- Utilisation inefficace de l'espace des adresses: Réseau classe C avec 2 hosts (2/255) ou réseau classe B avec 256 hosts (256/65535)
- Prolifération des réseaux (l'Internet compte aujourd'hui des dizaines de milliers de réseaux)
- Les adresses sont presque épuisées
- Taille des tables de routage

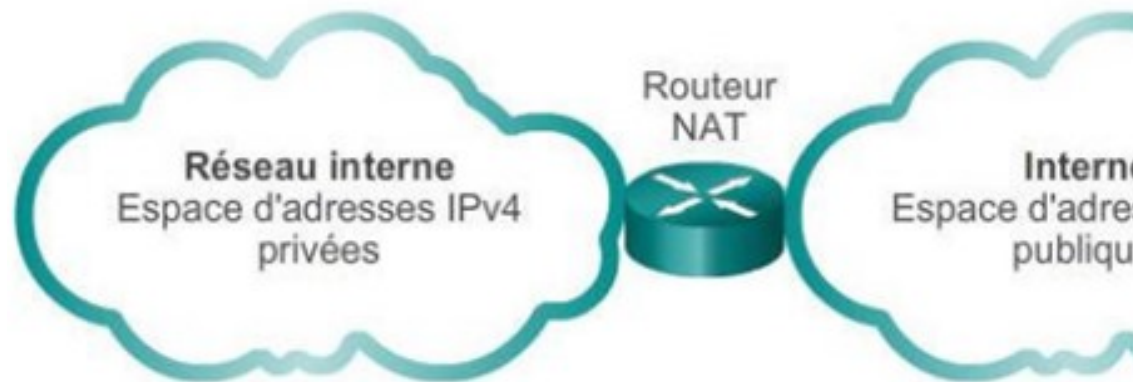
⇒ Le **CIDR** (Classless Inter-Domain Routing) permet aux fournisseurs de services d'allouer les adresses IPv4 sur n'importe quelle longueur de préfixe plutôt que seulement avec une adresse de classe A, B ou C

- /n (Préfixe) : nb. de bits réservés au «network ID » => Le nombre d'hôtes est $2^{32-n}-2$

Adressage IPv4 : Adresses privées

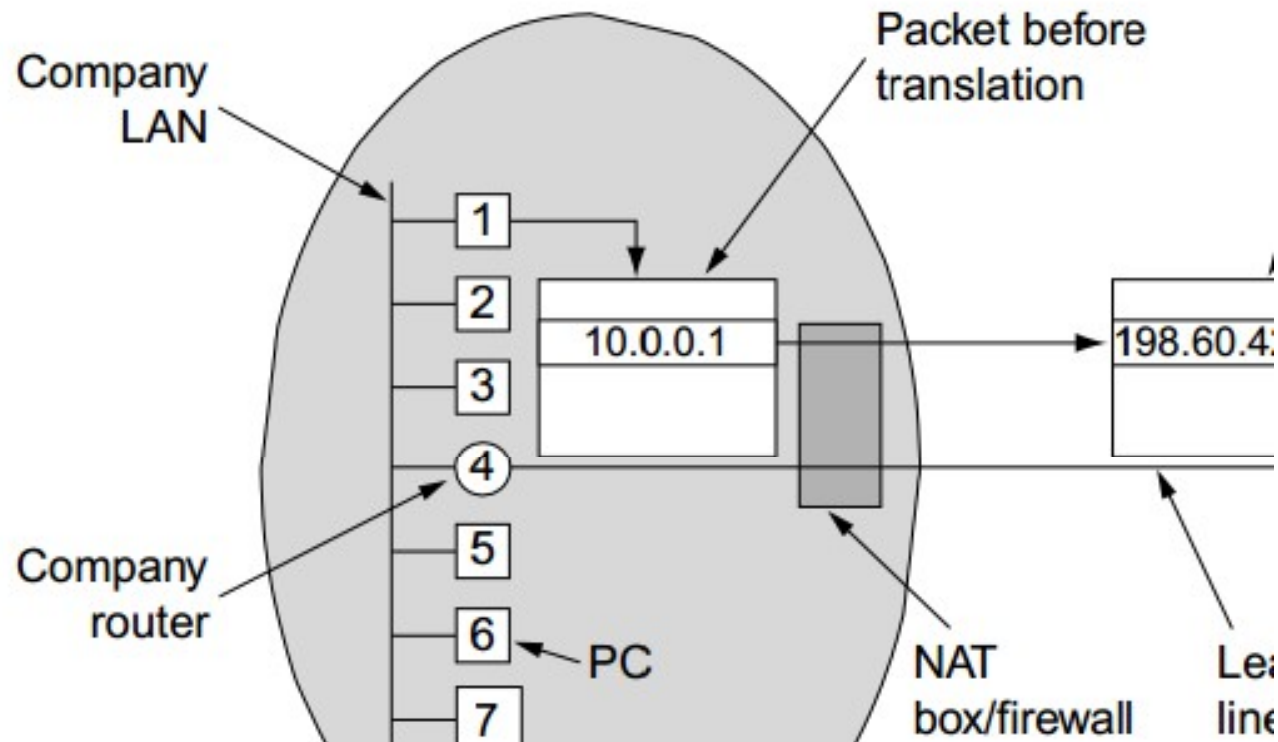
Blocs d'adresses privées :

- 10.0.0.0 à 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 à 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 à 192.168.255.255 (192.168.0.0/16)



- Les hôtes ayant des adresses privées (non routables) ne peuvent accéder à Internet que si leurs adresses soient traduites en adresse publique
=> Network Address Translation (NAT)
-

Adressage IPv4 : NAT

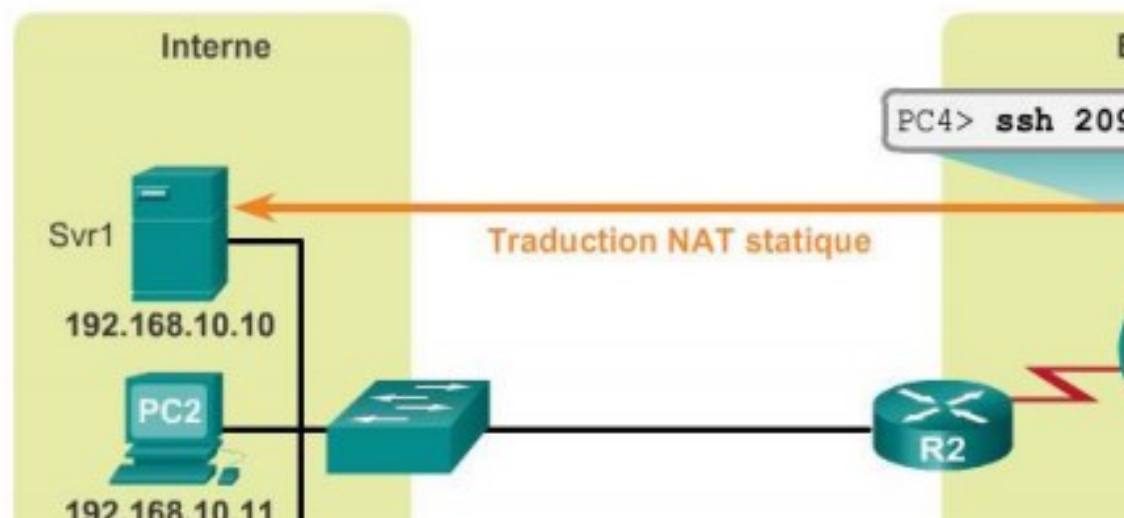


- Économiser les adresses IPv4 publiques.
- Mise en œuvre sur les périphériques réseau situés à la périphérie, tels que les pare-feu ou les routeurs.

Adressage IPv4 : NAT

NAT statique

Table NAT statique	
Adresse locale interne	Adresse globale interne - accessible via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



Adressage IPv4 : Notion de sous réseau

Au lieu d'avoir tous les hôtes connectés à un seul vaste réseau global, il s'avère plus pratique et gérable de les grouper en réseaux spécifiques

- Amélioration des performances :

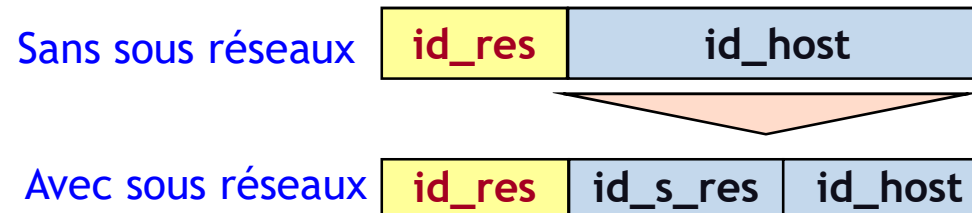
- trafic lié à la gestion du réseau augmente avec le nombre d'hôtes
- division en des domaines de diffusion limite les diffusions à un seul sous réseau.

- Amélioration de la sécurité

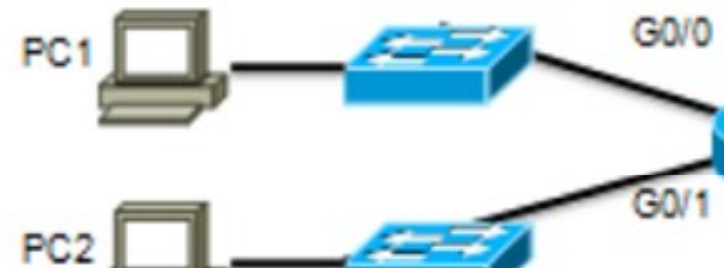
- Meilleure gestion des adresses :

- Si chaque hôte connait l'@ de tout autre => charge de traitement
- les hôtes ont besoin de connaître uniquement l'@ de la passerelle

Adressage IPv4 : Notion de sous réseau



Exemple : Adresse de classe C 192.168.2.0
avec id sous-réseau sur 1 bit:



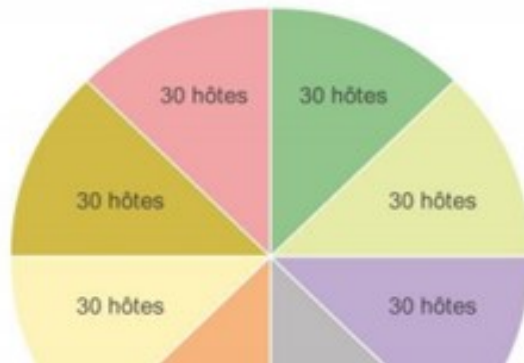
- 4^{ème} octet
- | | |
|---|---------|
| 0 | 0000000 |
| 1 | 0000000 |
- Sous réseau 1 : 192.168.2.0/25
 - Sous réseau 2 : 192.168.2.128/25
 - Masque : 255.255.255.128

Nb. sous-réseaux= 2^M (M : nb. bits utilisés pour identifier le sous réseau)
Nb. hôtes par sous-réseaux= 2^U-2 (U: nb. bits restant pour identifier l'hôte)

Adressage IPv4 : VLSM

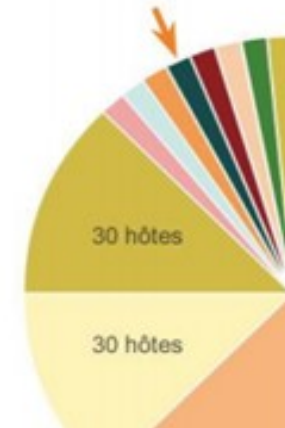
- ◆ Segmentation traditionnelle : le même nombre d'adresses est attribué à chaque sous-réseau.
- ◆ Les sous-réseaux qui n'ont pas besoin de la totalité ont des adresses inutilisées (les liaisons WAN n'ont besoin que de 2 adresses)
- ◆ La technique VLSM permet de décomposer un espace réseau en parties inégales
- ◆ Le masque varie alors selon les besoins de chaque sous-réseau

La segmentation en sous-réseaux traditionnelle crée des sous-réseaux de taille égale

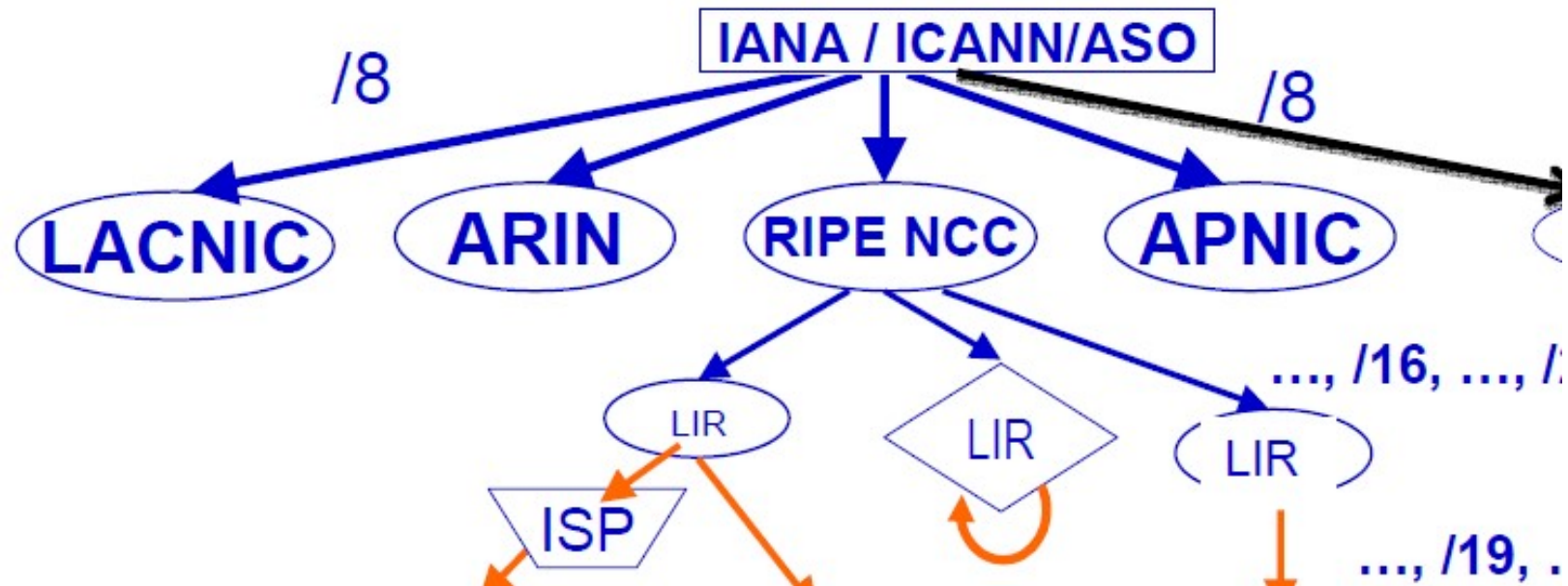


Sous-réseaux de

Un sous-réseau a été à nouveau divisé pour créer 8 sous-réseaux plus petits de 4 hôtes chacun



Adressage IPv4 : Allocation des adresses IP



ASO Address Supporting Organisation

IANA Internet Assigned Numbers Authority

ICANN Internet Corporation for Assigned Names and Numbers

LIR Local Internet Registry (opérateur réseau, ISP ou une grande org.)

- En février 2011, la réserve de blocs libres d'adresses publiques IPv4 de l'IANA est arrivée à épuisement

Adressage IPv4 : Allocation des adresses IP

- Des blocs d'adresses IP sont distribués aux registres internet régionaux (RIR) par l'IANA
- Les RIR distribuent des blocs d'adresses aux opérateurs et aux ISPs
- 5 Regional Internet Registries (RIR) :
 - AfriNIC (Africa Network Information Center)
 - APNIC (Asia Pacific Network Information Center)
 - ARIN (American Registry for Internet Numbers)
 - LACNIC (Latin-American and Caribbean Network Information Center)
 - RIPE NCC (Réseaux IP Européens - Network Coordination Center)



Plan

1- Introduction

2- L'adressage

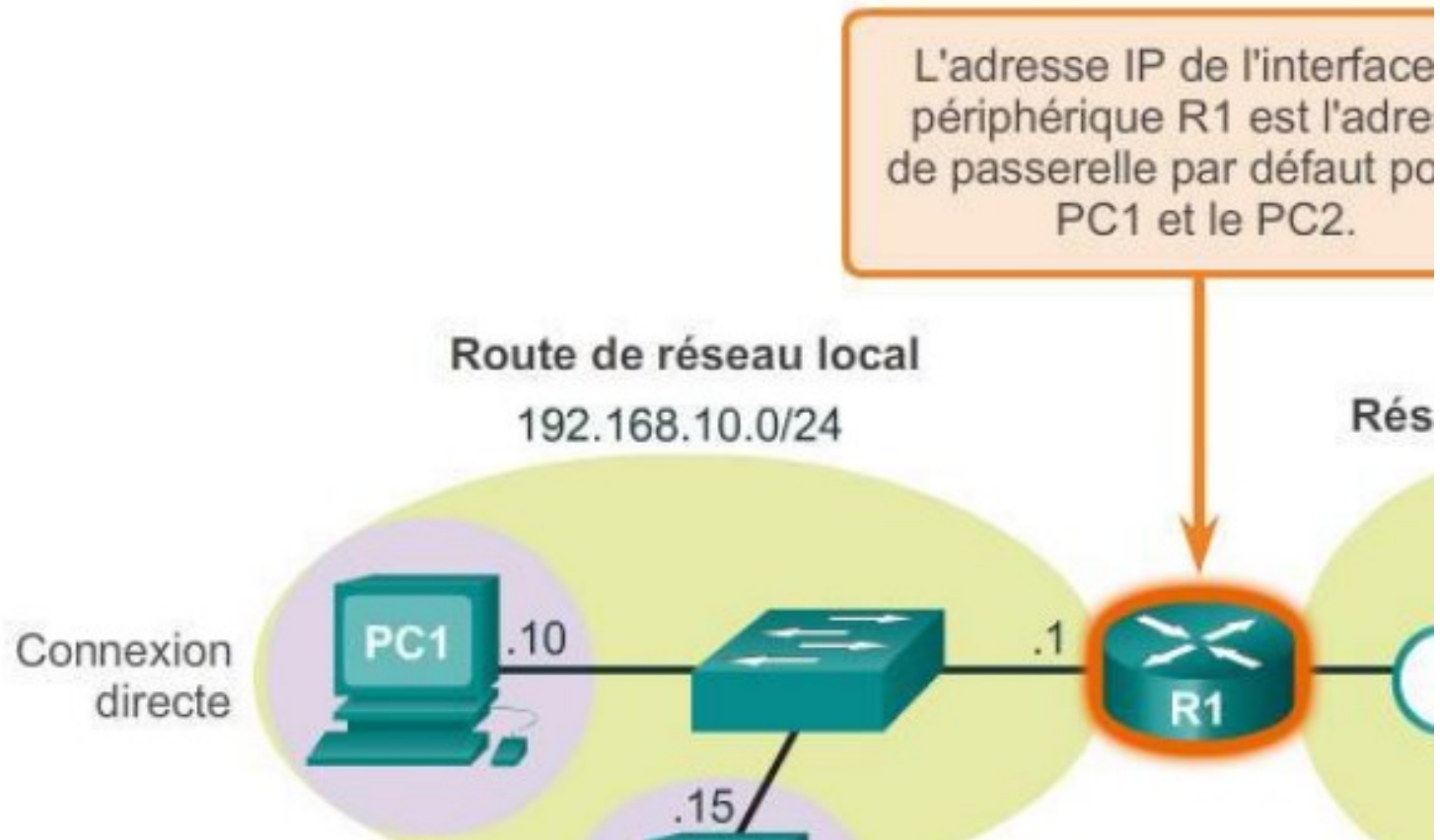
3- Le routage

4- Exemple : le protocole IPv4

Le routage

- Au niveau d'un routeur se pose le problème de la décision du chemin à emprunter par les différents paquets
- Cette décision est appelée décision de routage et est prise à l'aide d'un **algorithme de routage**
- Les algorithmes de routage se basent sur des **tables de routage** qui précisent, pour chaque nœud destination du paquet, le prochain nœud à visiter ou la ligne à emprunter
- Le routeur connecté au segment d'un réseau LAN est dit **passerelle par défaut**

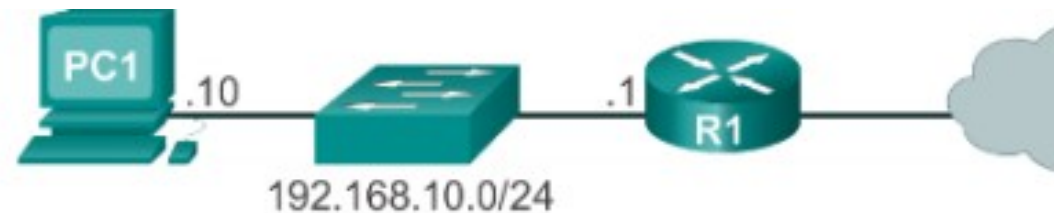
Le routage



Le routage : La table de routage d'un hôte

- Les hôtes ont également besoin d'une table de routage locale pour diriger correctement les paquets vers le réseau de destination correspondant.
- La table locale de l'hôte contient généralement :
 - Connexion directe (route vers l'interface de bouclage)
 - Route de réseau local
 - Route par défaut locale (utile pour router les paquets destinés aux réseaux distants)

Le routage : La table de routage d'un hôte



```
C:\Users\PC1>netstat -r
```

```
<Output omitted>
```

```
IPv4 Route Table
```

```
=====
```

```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.1
	127.0.0.0	255.0.0.0	On-link	127.0.0.1
	127.0.0.1	255.255.255.255	On-link	127.0.0.1
	127.255.255.255	255.255.255.255	On-link	127.0.0.1
	192.168.10.0	255.255.255.0	On-link	192.168.10.1
	192.168.10.10	255.255.255.255	On-link	192.168.10.1
	192.168.10.255	255.255.255.255	On-link	192.168.10.1
	224.0.0.0	240.0.0.0	On-link	127.0.0.1
	224.0.0.0	240.0.0.0	On-link	192.168.10.1

Le routage : La table de routage d'un hôte



```
C:\Users\PC1> netstat -r
```

```
<Output omitted>
```

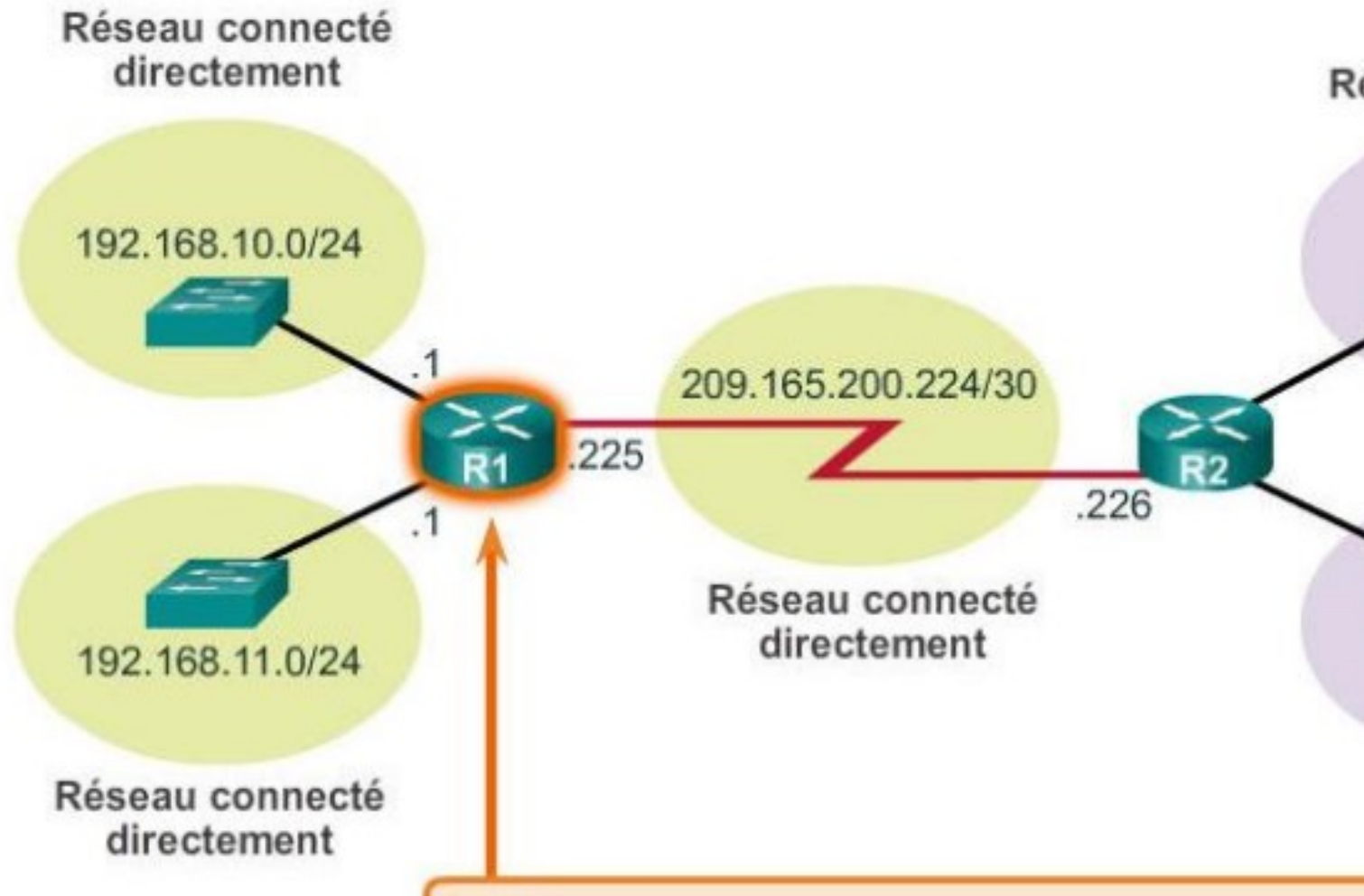
```
IPv4 Route Table
```

```
=====
```

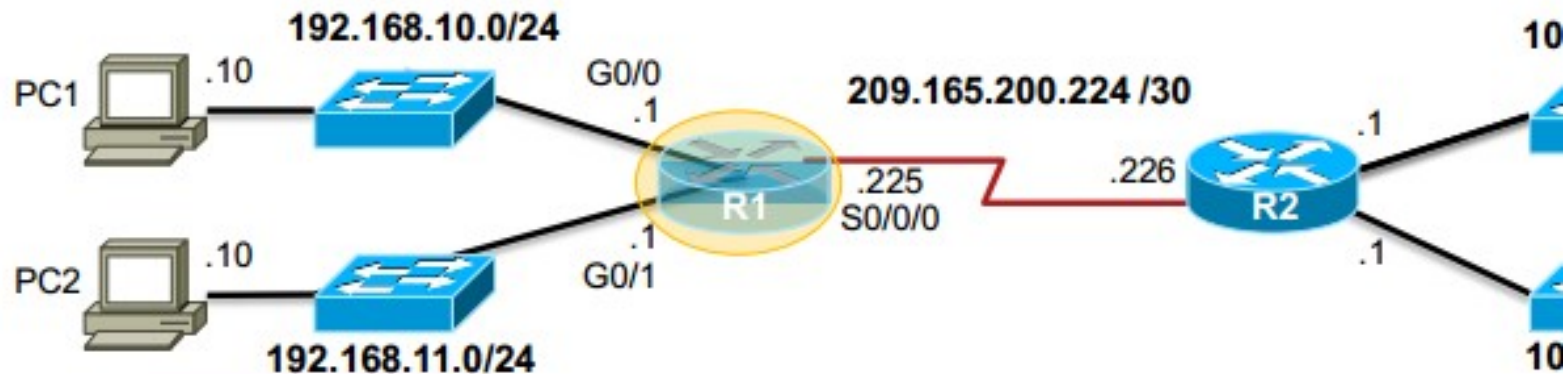
```
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.1
	127.0.0.0	255.0.0.0	On-link	127.0.0.1
	127.0.0.1	255.255.255.255	On-link	127.0.0.1
	127.255.255.255	255.255.255.255	On-link	127.0.0.1
	192.168.10.0	255.255.255.0	On-link	192.168.10.1
	192.168.10.10	255.255.255.255	On-link	192.168.10.1
	192.168.10.255	255.255.255.255	On-link	192.168.10.1
	224.0.0.0	240.0.0.0	On-link	127.0.0.1
	224.0.0.0	240.0.0.0	On-link	192.168.10.1

Le routage : La table de routage d'un routeur



Le routage : La table de routage d'un routeur



```
R1#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D    10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D    10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
```

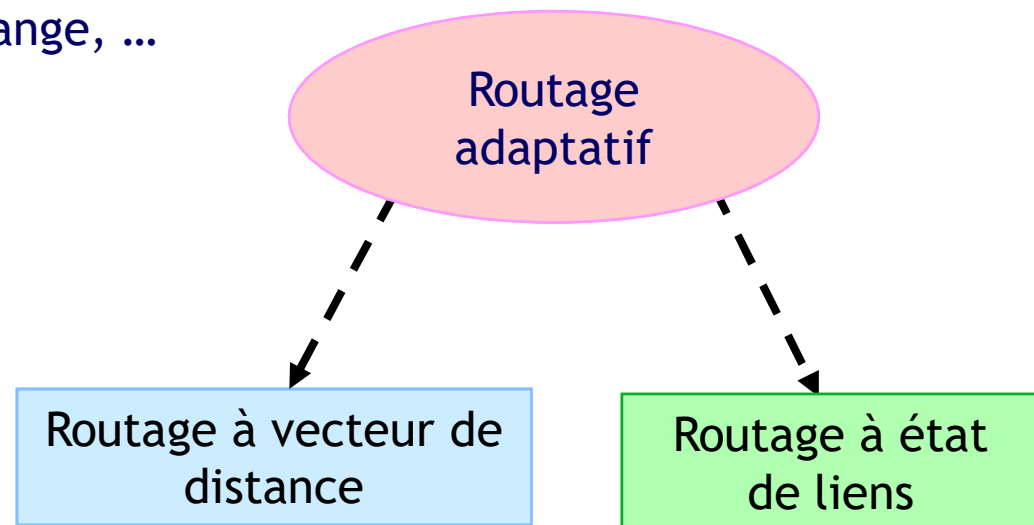
Les algorithmes de routage

- Si les tables de routages sont fixes (constantes) : les algorithmes de routage sont dit **non adaptatifs (ou statiques)**
- Si les tables de routages sont mises à jour (par les algorithmes de routage) en fonction de l'état du réseau : les algorithmes sont dits **adaptatifs (ou dynamiques)**

Les algorithmes de routage : Algorithmes adaptatifs

Ces algorithmes adaptatifs diffèrent selon :

- l'endroit où ils se procurent l'information
- la métrique utilisée (l'information qu'ils reçoivent)
- l'instant où ils changent leurs décisions
 - toutes les n secondes
 - lorsque la topologie change, ...



Algorithmes adaptatifs : Routage à vecteur de distance

- Utilisé par le protocole **RIP** (Routing Information Protocol)
- Chaque routeur dispose d'une table de routage précisant pour chaque destination la **meilleure distance** connue et par quelle ligne l'atteindre
- Les informations (vecteurs) de distance sont échangées régulièrement entre routeurs voisins
- Un élément du vecteur de distance est associé à une destination possible (donc un routeur)
- Cet élément représente l'estimation de la distance pour atteindre le routeur
- **Vecteur de distance = table de routage sans les indications des lignes à emprunter**

Algorithmes adaptatifs : Routage à vecteur de distance

Algorithme

- Hypothèse: chaque routeur connaît la distance avec ses voisins
- Mise à jour des tables de routage
 - Elle se fait de façon périodique: toutes les t ms par exemple
 - Chaque routeur
 - envoie son vecteur de distance à ses voisins
 - reçoit un vecteur de distance de ses voisins
 - effectue les mises à jour de son vecteur de distance à partir de ceux qu'il a reçu

Router

A B C D

E F G H

I J K L

**Vectors received from
J's for neighbors**

Line	
8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	-
6	K
15	K

Table for J

Algorithmes adaptatifs : Routage à état de liens

- Utilisé par le protocole **OSPF** (Open Shortest Path First) utilisé dans Internet
- Principe : tout routeur doit :
 - ❶ Découvrir ses voisins (apprendre leurs adresses)
 - ❷ Mesurer la distance vers chacun des voisins
 - ❸ Construire un paquet spécial indiquant tout ce qu'il vient d'apprendre
 - ❹ Envoyer ce paquet spécial à tous les routeurs
 - ❺ Calculer le plus court chemin vers tous les autres routeurs à partir des paquets reçus

Algorithmes adaptatifs : Routage à état de liens

Description

❶ Découvrir ses voisins

- envoyer sur chaque ligne de sortie un paquet spécial d'interrogation (HELLO)
- récupérer les infos (nom, adresse IP, ...) de la réponse

❷ Mesurer la distance avec les voisins

- envoyer sur chaque ligne de sortie un paquet spécial (ECHO)
- mesurer le temps pris pour récupérer la réponse

❸ Construire un paquet d'information d'état de lien : ce paquet comprend

- * L'identité du routeur source
- * Un numéro de séquence
- * L'âge du paquet
- * La liste des voisins accompagnée du temps d'acheminement

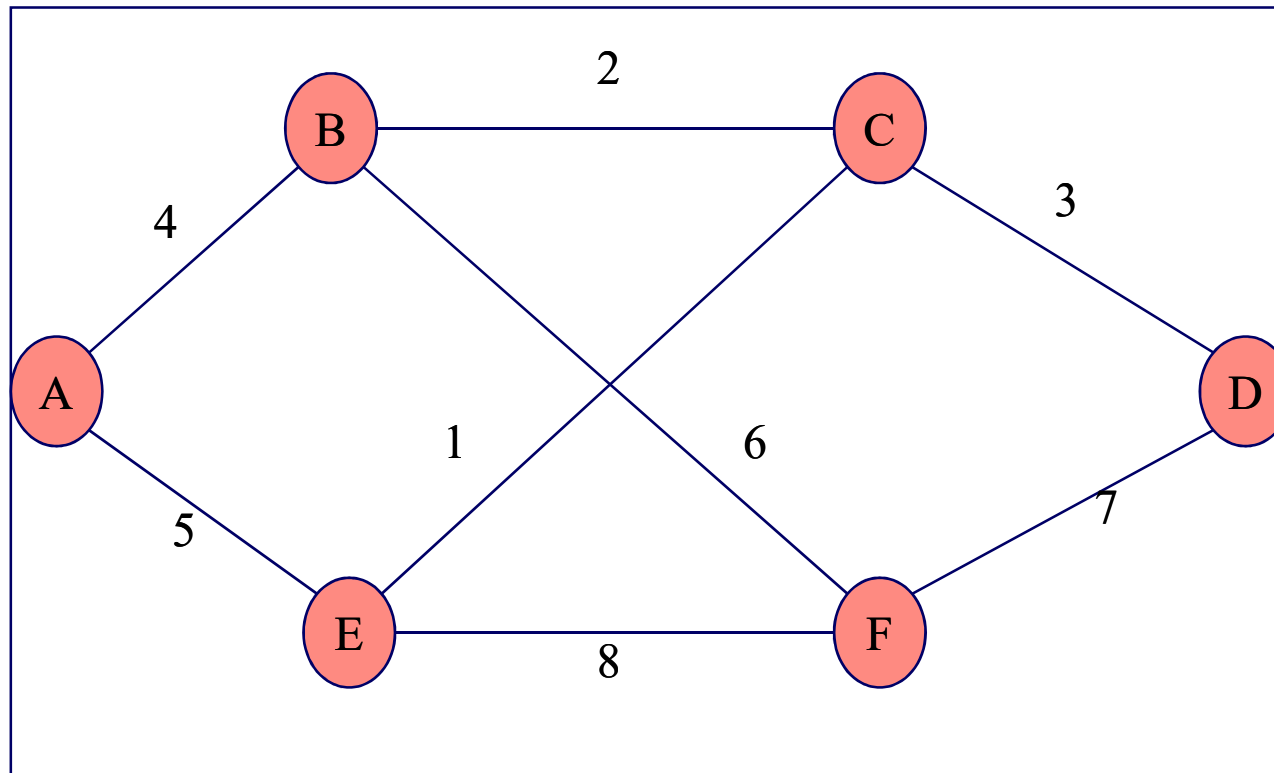
Algorithmes adaptatifs : Routage à état de liens

Description

- ④ Envoyer les paquets d'information d'état de lien
 - Utiliser l'inondation
 - Contrôler l'inondation
 - * Chaque routeur contient une trace de toutes les paires (routeur source, numéro de séquence) reçues
 - * Si un paquet déjà arrivé revient, il sera détruit
- ⑤ Calculer la nouvelle table de routage
 - L'algorithme de Dijkstra peut être utilisé au niveau de chaque routeur

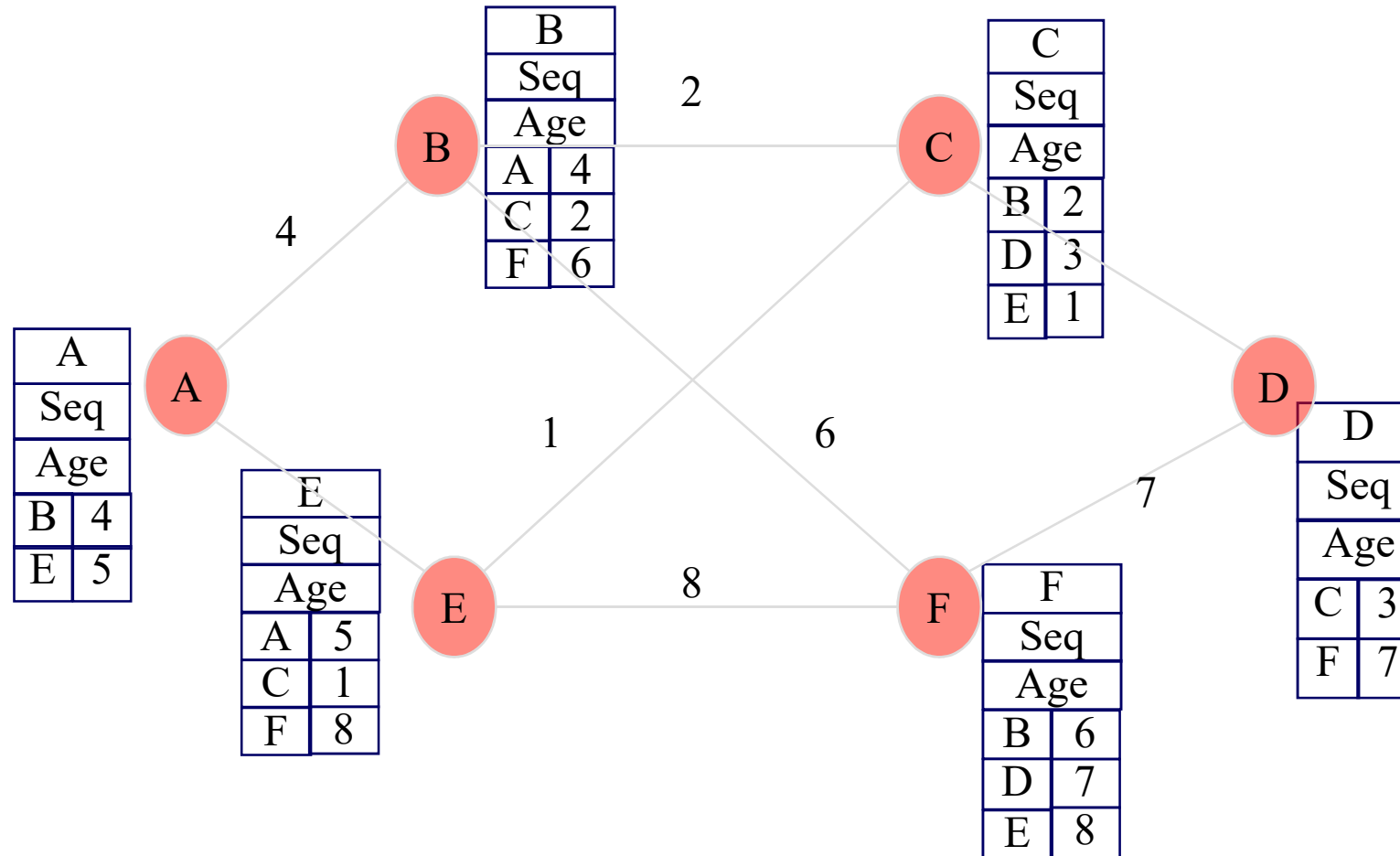
Algorithmes adaptatifs : Routage à état de liens

Exemple



Algorithmes adaptatifs : Routage à état de liens

Les paquets d'information d'états de lien construits par les routeurs :



Plan

1- Introduction

2- L'adressage

3- Le routage

4- Exemple : le protocole IP v4

Le protocole IP: Présentation

- IP offre un service **best effort**, c.à d. faire le mieux possible pour transmettre le paquet de la source à la destination
- Le service est aussi **non fiable**, car la remise ne présente aucune garantie. Un paquet peut être perdu, dupliqué ou remis hors séquence, sans que la couche réseau ne détecte rien ou n'en informe l'émetteur ou le récepteur
- IP offre un service **sans connexion**
- L'unité de donnée est le paquet IP appelé aussi **datagramme IP**

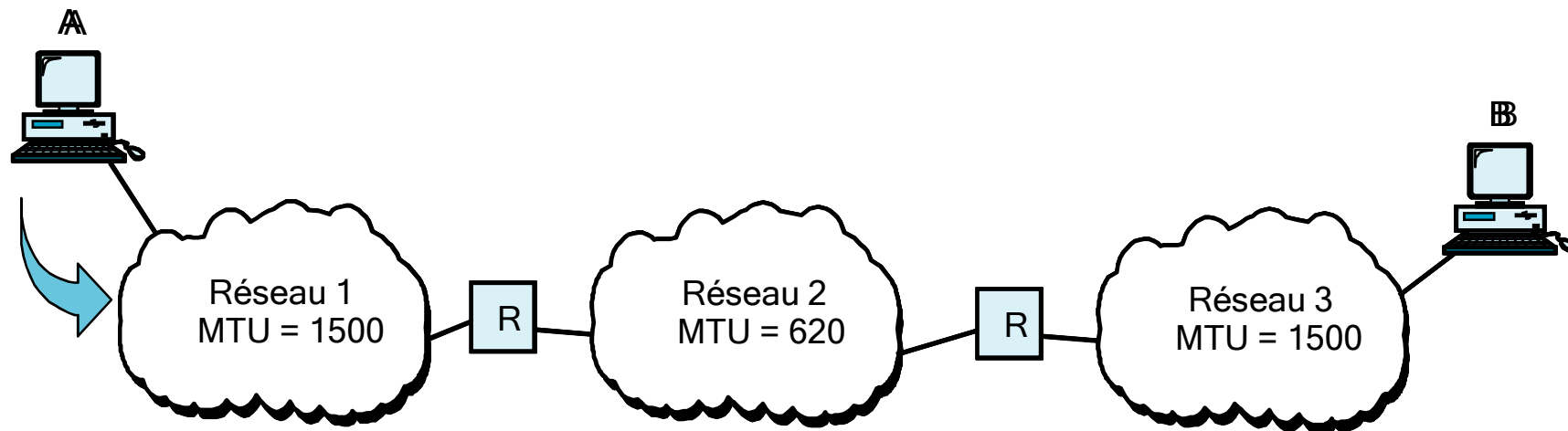
Le protocole IP: Fragmentation des datagrammes

- Les datagrammes transitent d'un routeur en routeur => ils peuvent être fractionnés pour s'adapter à la structure de la trame sous jacente : **Fragmentation**
- Les fragments sont transmis indépendamment les uns des autres jusqu'à leur destination, où ils seront ré-assemblés
- Si l'un des fragments est perdu, le reste des fragments du datagramme doivent être détruits

Le protocole IP: Fragmentation des datagrammes

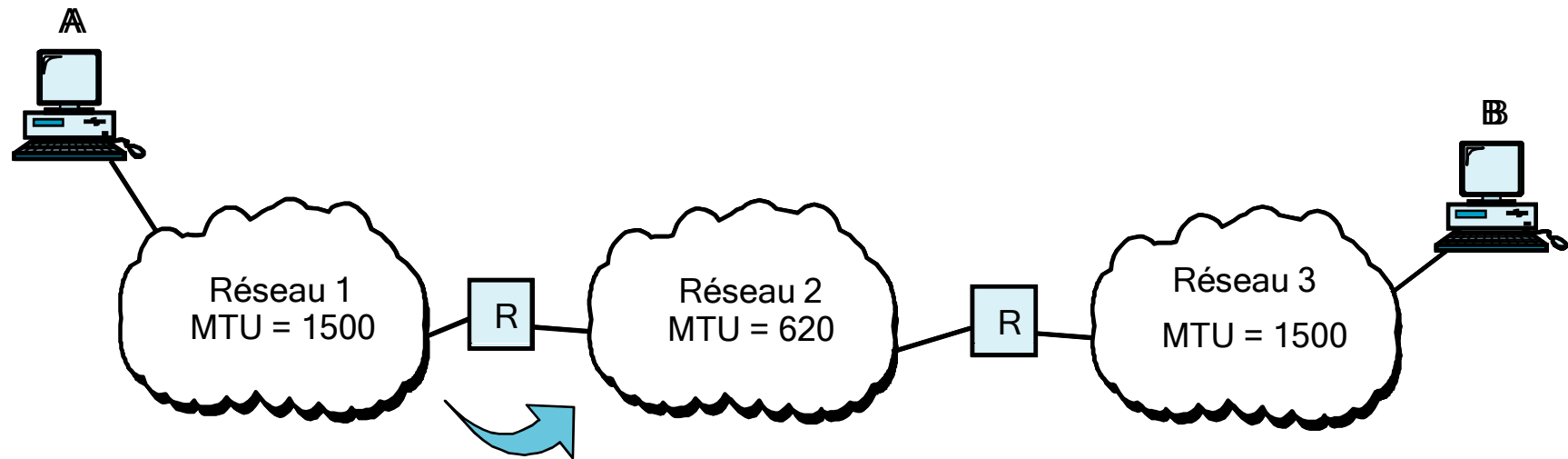
Exemple

Envoi de A à B d'un datagramme de taille 1420 octets



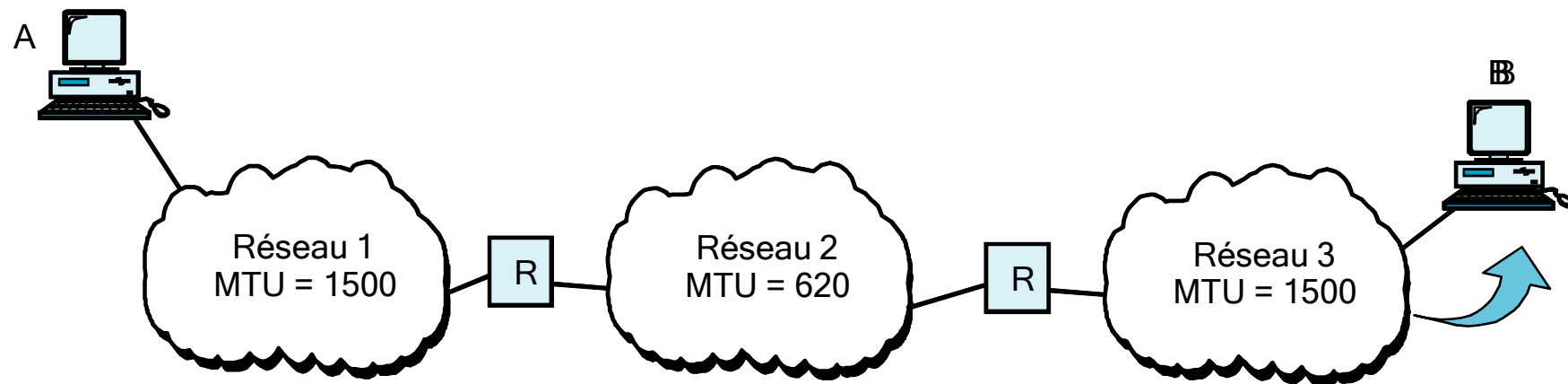
Longueur Totale 1420	Identificateur 44	DF=0 MF=0	Données 1400 bytes
-------------------------	----------------------	--------------	-----------------------

Le protocole IP: Fragmentation des datagrammes



Longueur Totale 1420	Identificateur 44	DF=0 MF=0	Données 1400 bytes	
Longueur Totale 620	Identificateur 44	DF=0 MF=1	Offset 0 (0)	Données 1 600 bytes
Longueur Totale 620	Identificateur 44	DF=0 MF=1	Offset 75 (600)	Données 2 600 bytes
Longueur Totale 220	Identificateur 44	DF=0 MF=0	Offset 150 (1200)	Données 3 200 bytes

Le protocole IP: Fragmentation des datagrammes



Longueur Totale 620	Identificateur 44	DF=0 MF=1	Offset 0 (0)	Données 1 600 bytes
------------------------	----------------------	--------------	-----------------	------------------------

Longueur Totale 620	Identificateur 44	DF=0 MF=1	Offset 75 (600)	Données 2 600 bytes
------------------------	----------------------	--------------	--------------------	------------------------

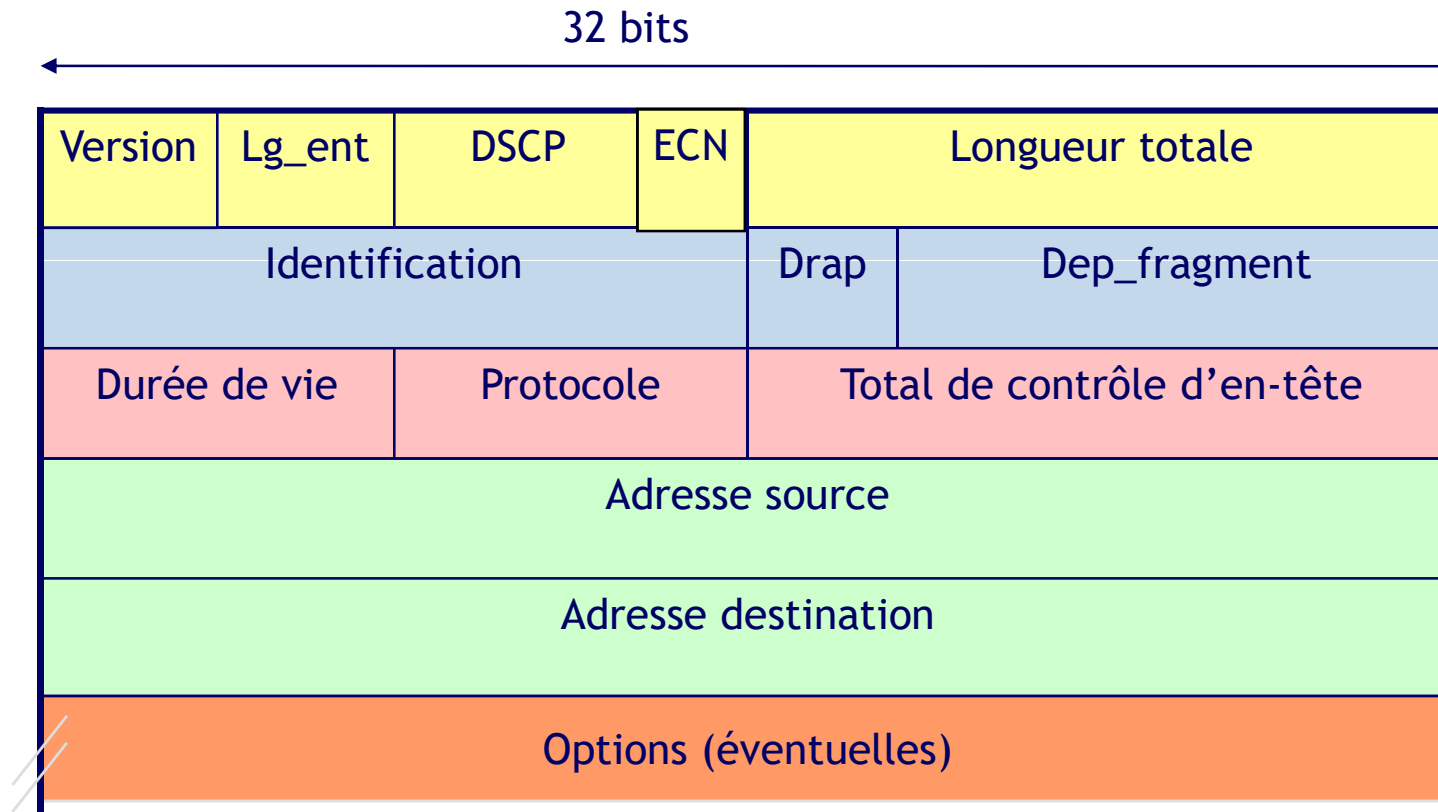
Longueur Totale 220	Identificateur 44	DF=0 MF=0	Offset 150 (1200)	Données 3 200 bytes
------------------------	----------------------	--------------	----------------------	------------------------

Longueur Totale 1420	Identificateur 44	DF=0 MF=0	Données 1400 bytes	
-------------------------	----------------------	--------------	-----------------------	--

Le protocole IP: Format d'un paquet IPv4

Un paquet IP est composé de :

- En-tête : partie fixe (20 octets) + partie optionnelle variable
- Données : charge utile du datagramme



Le protocole IP: Format d'un paquet IPv4

Les champs de l'entête :

- **Version**: numéro de la version du protocole (4 bits)
 - **Lg_ent**: longueur de l'en-tête exprimée en mots de 32 bits (4 bits)
 - **DSCP**: code de différenciation de service (6 bits) (l'ancien champ TOS)
 - **ECN**: notification explicite de congestion (2 bits)
 - **Longueur totale** : en octets (16 bits)
 - **Identification** : permet au destinataire de savoir à quel datagramme appartient un fragment (16 bits)
 - **Drapeau** (3 bits): DF “ Don't fragment ”, MF « More fragments » et 1bit inutilisé
 - **Dep_fragment**: localisation du déplacement du fragment dans le datagramme(13bits)
 - **Durée de vie (TTL)**: compteur utilisé pour limiter la durée de vie des datagrammes (8 bits) : décrémenté à chaque saut et détruit quand passe à 0
 - **Protocole**: indique à quel protocole confier le contenu du paquet(TCP ou UDP)(8bits)
 - **Total de contrôle d'en-tête** : vérifie la validité de l'en-tête, doit être recalculé à chaque saut (16 bits)
 - **Adresse source** (32 bits) et **Adresse destination** (32 bits)
-

Le protocole IP: Format d'un paquet IPv4

Exemple de paquet IP

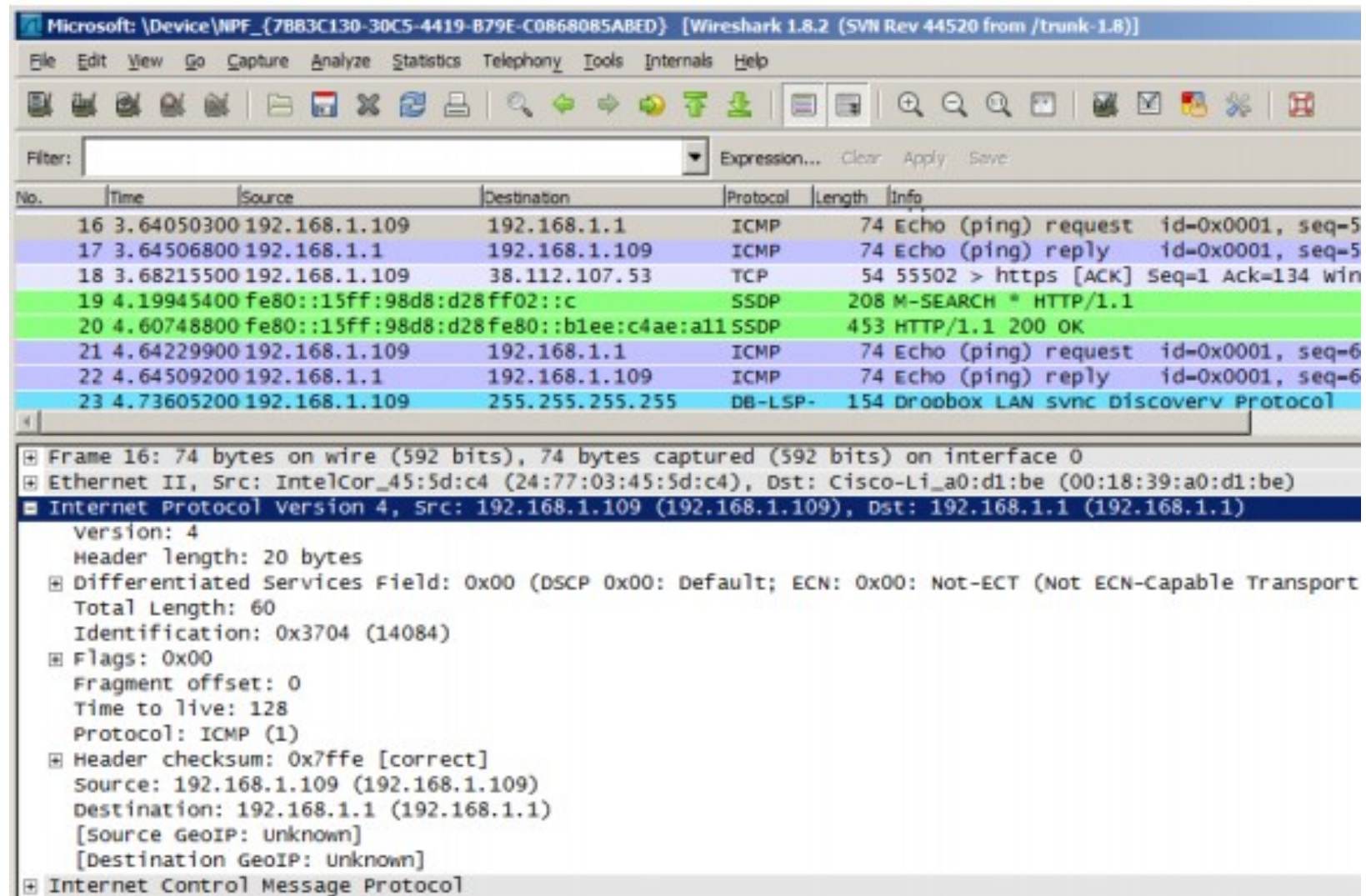
```
45 00 00 34 b8 71 00 00 3c 11 ab 50 c0 2c 4d 51 c0 2c 4d 4d
02 05 0e 23 00 20 00 00 03 00 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 6e 74 00 00 00 69 00 00
```

Le protocole IP: Format d'un paquet IPv4

Exemple de paquet IP

45 00 00 34 b8 71 00 00 3c 11 ab 50 c0 2c 4d 51 c0 2c 4d 4d
02 05 0e 23 00 20 00 00 03 00 00 00 00 00 00 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 6e 74 00 00 00 69 00 00

Le protocole IP: Exemple d'en-tête IPv4 (Wireshark)



Microsoft: \Device\NPF_{78B3C130-30C5-4419-B79E-C0B68085ABED} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
16	3.64050300	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=5
17	3.64506800	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=5
18	3.68215500	192.168.1.109	38.112.107.53	TCP	54	55502 > https [ACK] Seq=1 Ack=134 win
19	4.19945400	fe80::15ff:98d8:d28ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
20	4.60748800	fe80::15ff:98d8:d28ff02::c	fe80::b1ee:c4ae:a11	SSDP	453	HTTP/1.1 200 OK
21	4.64229900	192.168.1.109	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=6
22	4.64509200	192.168.1.1	192.168.1.109	ICMP	74	Echo (ping) reply id=0x0001, seq=6
23	4.73605200	192.168.1.109	255.255.255.255	DB-LSP-	154	Droobox LAN svnc Discoverv Protocol

Frame 16: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: IntelCor_45:5d:c4 (24:77:03:45:5d:c4), Dst: Cisco-Li_a0:d1:be (00:18:39:a0:d1:be)

Internet Protocol Version 4, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)

- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport
- Total Length: 60
- Identification: 0x3704 (14084)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: ICMP (1)
- Header checksum: 0x7ffe [correct]
- Source: 192.168.1.109 (192.168.1.109)
- Destination: 192.168.1.1 (192.168.1.1)
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Internet Control Message Protocol