

# Réseaux Locaux

*Maher SELLAMI*

# Objectifs du cours

- connaître les spécificités des réseaux locaux,
- bien assimiler les techniques d'accès à un support de transmission partagé,
- étudier l'architecture et la normalisation des réseaux locaux,
- étudier l'interconnexion au niveau 2 et l'évolution des réseaux locaux vers des réseaux commutés,
- se familiariser avec les composants matériels et le câblage des réseaux locaux
- déployer un réseau IP et configurer les services de base
- acquérir une expérience pratique à travers des TPs ciblés.

# Plan du cours (1)

## Introduction

- Motivation

- Classification des réseaux

- Caractéristiques générales d'un LAN

## Technologie des réseaux locaux

- Topologies des réseaux locaux (étoile, anneau, bus / arbre)

- Supports physiques d'interconnexion

- Le mode de transmission

- Protocoles d'accès ( jeton, anneau en tranches, aléatoire)

- Principaux paramètres d'évaluation des techniques aléatoire et à jeton

## Normalisation des réseaux locaux

- Normes IEEE 802

- Norme IEEE802.3

- Norme IEEE 802.11

# Plan du cours (2)

## Déploiement des réseaux locaux

Ethernet Wifi Plan de câblage

## Les réseaux sous TCP/IP

Architecture des protocoles

Le protocole IP

Adressage

Format d'un datagramme IP

Routage IP

Protocole ICMP

Protocole ARP

Protocoles du niveau transport (UDP, TCP)

## Interconnexion de réseaux

Répéteurs

Ponts

Routeurs et pont-routeurs

# Motivation

- Le partage de ressources communes (critère économique).
- Une meilleure fiabilité puisqu'on dispose d'un ensemble de machines et non pas d'un seul "gros" ordinateur (redondance).
- Les possibilités d'évolutions du système sont plus souples que dans le cas d'une machine unique :  
→ on peut ajouter des machines sur le réseau au fur et à mesure des besoins de l'entreprise.
- Une plus grande indépendance vis-à-vis des constructeurs si le réseau local permet l'hétérogénéité.

# Classification

- Les réseaux personnels (PAN : Personal Area Network)
  - Quelques mètres, débit faible.
  - Ex: Bluetooth et l'infra rouge, ....
- Les réseaux locaux (LAN : "Local Area Network")
  - Quelques kilomètres, site privé
  - débit important de 100 Mb/s à 1 Gb/s.
  - 2 types de LAN:
    - Réseau local d'Entreprise (RLE) : bureautique, gestion
    - Réseau Local Industriels (RLI) , connecte en plus des équipements informatiques, des robots, des machines outils, des capteurs... Les contraintes de disponibilité et de garanti de temps d'accès.
- Les réseaux métropolitains (MAN : "Metropolitan Area Network")
  - extension des réseaux locaux
  - plusieurs dizaines de kilomètres (< 100 Km)
  - Ex: Campus universitaire, Hopital, entreprise
- Les réseaux étendus (WAN : "Wide Area Network")
  - à faible et moyen débit (< 100 Kb/s) : réseaux tél.,télex, X25, ...
  - à haut débit (> 1 Mb/s) : réseaux satellites, câblo-opérateurs, RNIS ...

# Caractéristiques d'un LAN

- un étendu géographique limité ;
- le caractère privé à un organisme ou une entreprise ;
- interconnecter des équipements provenant de différents constructeurs (ordinateurs, terminaux, périphériques ...).
- un débit élevé supérieur au Mégabit par seconde ;
- un temps de réponse faible de l'ordre de la centaine de microseconde ;
- un taux d'erreur faible ( $< 10^{-9}$ ) ;
- une stabilité en pleine charge ;
- la facilité d'extension, de reconfiguration et de maintenance.

# Technologie des réseaux locaux

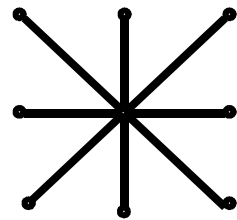
- Un réseau local se caractérise par :
  - sa topologie,
  - son support de transmission,
  - son mode de transmission et
  - sa méthode d'accès.



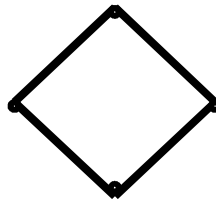
# Topologies des réseaux locaux

- décrit la configuration physique relative à l'interconnexion des nœuds entre eux au moyen d'un support de transmission.
- deux types de liaison :
  - une liaison point à point où deux nœuds sont reliés par une voie de communication,
  - une liaison multipoint (à diffusion) où plusieurs nœuds partagent la même voie de communication.

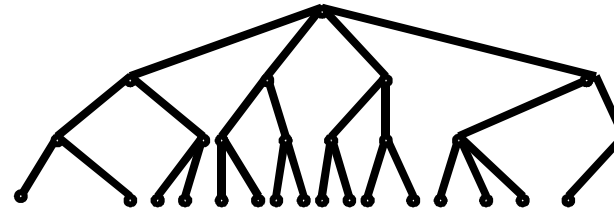
- Réseaux point à point



étoile



anneau

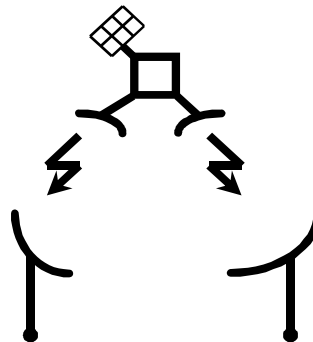


arbre

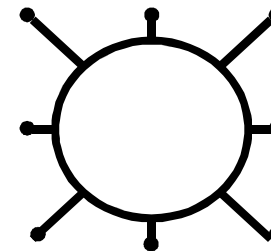
- Réseaux à diffusion



bus



satellite



anneau

# Topologie en étoile

- Un nœud de commutation central auquel sont reliés, par des liaisons point à point, tous les autres nœuds.
- Avantages :
  - facilité de maintenance ;
  - facilité d'extension dans la limite du nombre de ports ;
  - la défaillance d'un nœud, autre que le nœud central, ne paralyse pas les communications sur le réseau ;
  - possibilité de réaliser plusieurs communications en parallèle (commutation) ;
  - possibilité de construire des commutateurs rapides, à haut débit
- Inconvénients :
  - le risque de surcharge du nœud central ;
  - la défaillance du nœud central paralyse toute communication à travers le réseau ;
  - l'extensibilité du réseau est limitée ; Afin de remédier à cette limite
  - la diffusion peut nécessiter des mécanismes / opérations particulières ;
  - longueur totale du câblage importante.

# Topologie en anneau

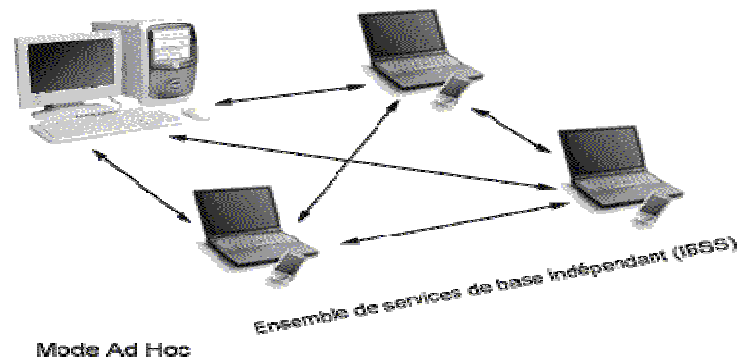
- les nœuds sont reliés entre eux par des liaisons point-à-point pour former une boucle.
- Avantages :
  - simplicité de l'acheminement des messages ;
  - le signal reste toujours de bonne qualité;
  - extension relativement facile ;
- Inconvénients :
  - la défaillance d'un nœud ou d'une liaison paralyse le réseau ;
  - l'ajout ou la suppression d'un nœud nécessite l'interruption du réseau ;
  - coûteuse : répétition du signal, synchronisation, ...

# Topologie en bus

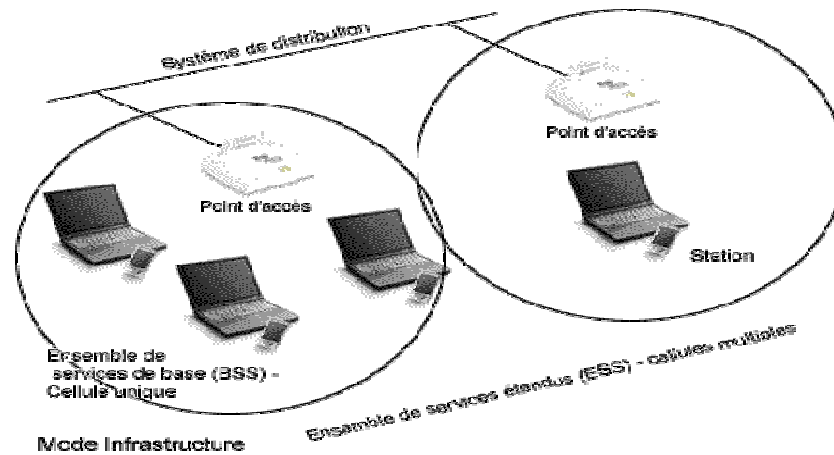
- tous les nœuds sont raccordés à une même liaison physique multipoint appelée bus.
- Avantages :
  - facilité d'ajout ou de suppression d'un nœud ;
  - la défaillance d'un nœud n'a presque pas d'incidence sur le réseau;
  - propriété de diffusion ;
  - coût relativement faible (câblage).
- Inconvénients :
  - une coupure du réseau divise le réseau en deux et rend le réseau non opérationnel ;
  - Le délai de propagation d'un signal sur le bus augmente avec la longueur
  - un seul nœud peut émettre à la fois

# Topologie des réseaux sans fils

- Mode Ad Hoc



- Mode Infrastructure



# Topologie des réseaux sans fils

- Avantages :
  - la mobilité ;
  - la facilité d'ajout ou de suppression d'un nœud ;
  - la défaillance d'un nœud, mis à part l'AP en mode infrastructure, n'a presque pas d'incidence sur le réseau ;
- Inconvénients :
  - en mode infrastructure, la défaillance d'un AP rend non opérationnelle la cellule correspondante ;
  - taux d'erreurs, sensibilité aux bruits et aux obstacles,
  - la diffusion ne permet pas de joindre forcément toutes les stations,
  - un seul nœud peut émettre à la fois (dans le cas d'un seul canal),
  - problèmes de sécurité : besoin de recourir à des techniques d'authentification et de cryptage

# Le support physique

- Paire de cuivre torsadées
- Câble coaxial
- Fibre optique








# Les paires torsadées

- Le câble est constitué d'une ou plusieurs paires de fils de cuivre en spiral (en torsade).
- Caractéristiques :
  - liaison point à point ;
  - analogique ou numérique ;
  - affaiblissement ;
  - sensible aux perturbations électromagnétiques et au problème de diaphonie.
  - simple à installer et coût relativement faible
- Utilisation :
  - Topologies : étoile et anneau ;
  - les réseaux DAN (entre le répartiteur d'étage et les nœuds de l'étage).

# Les paires torsadées: normalisation

	Cat. 3 Classe C	Cat. 5 Classe D	Cat.5E	Cat. 6 Classe E	Cat. 7 Classe F
Bande	16 MHz	100 MHz	100 MHz	200 MHz	600 MHz
Type	UTP	UTP/FTP	UTP/FTP	UTP/FTP	SSTP
Coût	0.7	1	1.2	1.5	2.2

Structure	Autre dénomination
	U / UTP
	U / FTP
	F / UTP
	SF / UTP (de Cat5e)
	ou S / FTP (de cat6 ou +)

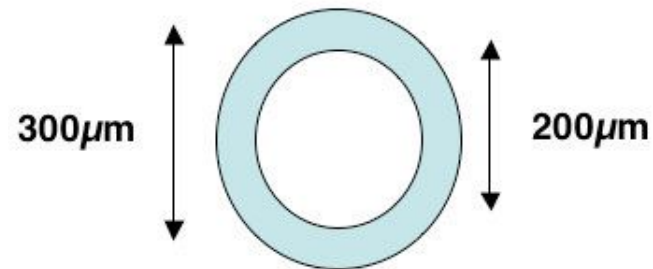
# Le câble coaxial

- câble central entouré d'un isolant et d'une tresse métallique, le tout enveloppé par une gaine protectrice.
- Caractéristiques :
  - liaison point à point ou multipoint ;
  - transmission analogique ou numérique ;
  - moins simple à installer que la paire torsadée ;
  - plus coûteux que la paire torsadée ;
  - 2 types de câbles coaxiaux : 50  $\Omega$  utilisé en bande de base, 75  $\Omega$  (ou CATV ) en large bande
  - débit : quelques Mb/s à plusieurs dizaines de Mb/s (même 1 Gb/s ) ;
- Utilisation :
  - topologies : bus, anneau, arbre ;
  - tendance à le remplacer par la paire torsadée au niveau des réseaux LAN, et par la fibre optique pour le reste du câblage.

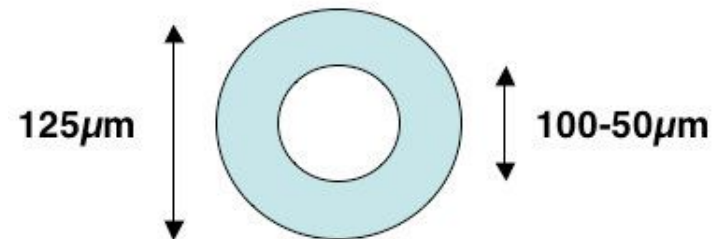
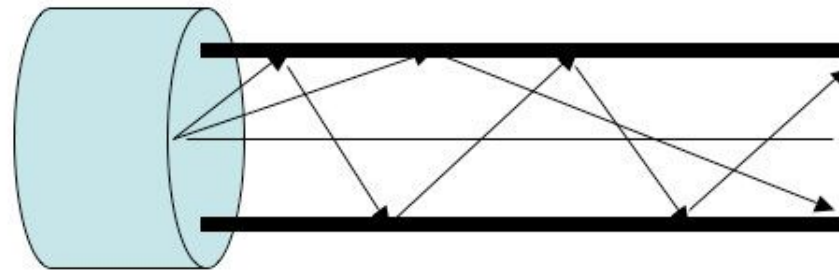
# La fibre optique

- noyau entouré d'une gaine
- Emetteur : codeur + DEL (ou DL)
- Récepteur : décodeur + photodétecteur
- 2 FO:
  - monomode : un seul angle d'incidence,  
Vitesse 0,25 millions de km/s , BP jusqu'à plusieurs milliers de Ghz/Km ;
  - multimode : plusieurs angles d'incidence, Ø quelques centaines de microns, vitesse 0,1 km/s
    - multimode à saut d'indice  
un seul indice de réfraction, BP jusqu'à 50 Mhz/Km ;
    - multimode à gradient d'indice  
un indice de réfraction qui diminue progressivement en s'éloignant de l'axe, BP jusqu'à 1 Ghz,

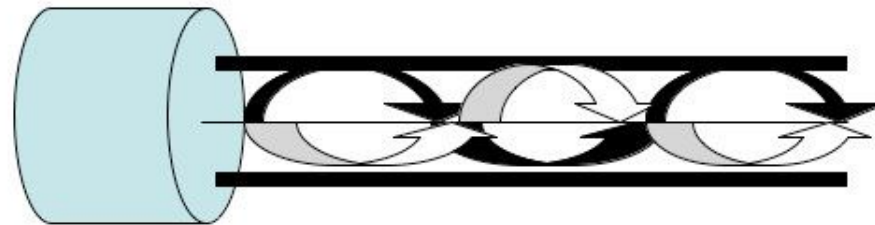
# La fibre optique (Caractéristiques)



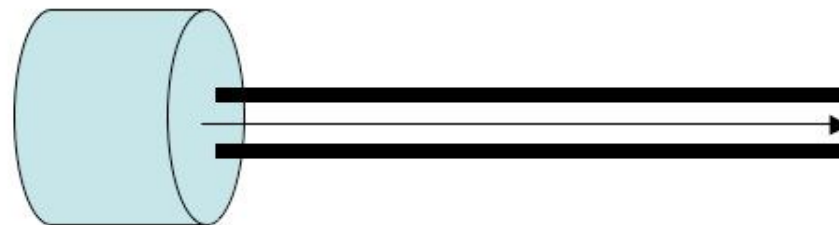
Fibre à saut d'indice



Fibre à gradient d'indice



Fibre monomode



# La fibre optique (Caractéristiques)

- s'utilise pour une liaison point à point, délicat de l'utiliser pour une liaison multipoint à cause des difficultés de dérivation ;
- le plus difficile à installer (raccordement, dérivation,...) ;
- le plus coûteux ;
- bande passante et débit important ;
- pas de diaphonie, insensible aux perturbations électromagnétiques, faible atténuation, résistance à la chaleur, au froid et à l'humidité ;
- encombrement et poids inférieurs aux autres supports (<1/10).
- Utilisation : topologies anneau, étoile
- tendance à utiliser la fibre optique multimode particulièrement dans les réseaux établissement (BAN).

# Le mode de transmission

- 2 modes:
  - bande de base: l'information est directement traduite par des changements discrets du signal et suivant un codage (Manchester, Manchester différentiel, ...)  
réseaux locaux filaires
  - large bande: le signal numérique est modulé sur une onde porteuse (variation de la fréquence, de l'amplitude et / ou de la phase)  
réseaux locaux sans fils
- Des techniques d'étalement de fréquences sont utilisées dans les réseaux WiFi :
  - FHSS: Frequency Hopping Spread Spectrum,
  - DSSS: Direct Sequence Spread Spectrum ,
  - OFDM: Orthogonal Frequency Division Multiplexing

# La transmission sans fils

- Les bandes utilisées par les WLAN sont dites sans licence :
  - La bande ISM (Industrie, Science et Médecine), 3 sous bandes :
    - Bande 900 MHz : Utilisée par le GSM en Europe
    - 2,4 GHz : Utilisée par 802.11 entre (2,4GHz et 2,4835GHz)
    - 5 GHz
  - La bande UNII , (Unlicensed National Info. Infrastructure) , 3 sous bande
    - 5,15 GHz – 5,25 GHz
    - 5,35 GHz – 5,53 GHz
    - 5,75 GHz – 5,85 GHz (Non disponible en France)

## Les lois de la Radio :

Débit plus grand = Couverture plus faible

Puissance d'émission élevée = Couverture plus grande, mais durée de vie des batteries plus faible

Fréquences radio élevées = Meilleur débit, couverture plus faible, sensibilité élevée



# FHSS *Frequency Hopping Spread Spectrum*

- Etalement du spectre par saut de fréquence
- Bande ISM (Industrial, Scientific and Medical) de 2,4 GHZ
- Divisée en 79 sous canaux de 1 MHz
- Émetteur change de fréquence d'émission de façon périodique(300 à 400 ms) suivant une séquence préétablie (interférence).
- Séquences de saut sur ces 79 sous canaux. Émetteur et Récepteur s'accordent sur cette séquence
- Les signaux sont modulés par une modulation de phase de type GFSK.
- Débit 1 à 2 Mbit/s
- technique utilisée, au départ pour des fin militaires, afin de sécuriser les transmissions. Ce n'est pas le cas pour 802.11 puisque séquences standardisées

## Avantages

- fonctionnement simultané de réseaux dans une même zone. Faible probabilité d'émission sur le même sous canal au même instant pour des couples émetteur-récepteurs
- Immunité face aux interférences. Si fréquence d'un canal perturbé. Canal inutilisé

# FHSS: Fréquences

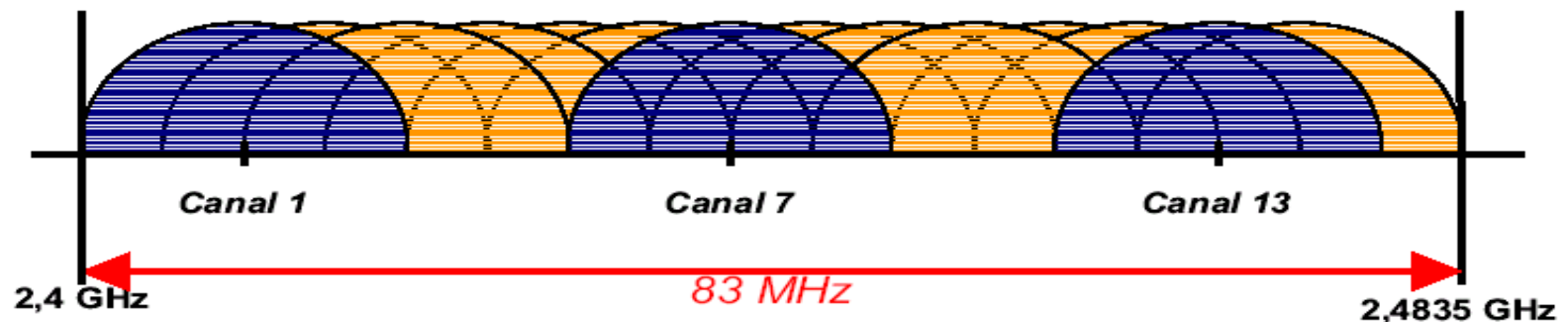
	Bandes de fréquences	Nombre de canaux
Amérique du nord	2.400-2.4835 GHz	79
Europe	2.400-2.4835 GHz	79
japon	2.471-2.497 GHz	23
France	2.4465-2.4835 GHz	35

# DSSS Direct Sequence Spread Spectrum

- étalement du spectre par séquence directe
- Divise la bande de 2,4 GHz en 14 canaux de 20MHz
- Largeur de bande ISM de 83MHz



- Impossible de placer 14 canaux adjacents.
- Les canaux se recouvrent partiellement
- seule 3 sont entièrement isolés (donc 3 réseaux)



# DSSS: Canaux

<b>Pays</b>	<b>Etats-Unis</b>	<b>Europe</b>	<b>Japon</b>	<b>France</b>
<b>sous canaux utilisés</b>	<b>1 à 11</b>	<b>1 à 13</b>	<b>14</b>	<b>10 à 13</b>

# DSSS

- DSSS permet d'augmenter le débit cependant elle est sensible aux interférences
- Utilisation de la séquence de Barker à 11 chips
  - ❖ chaque bit en une séquence de 11 bits dîtes chips.
    - ❖ 10110111000 → 1
    - ❖ 01001000111 → 0

- Modulation de phase

- ❖ BPSK (Binary Phase Shift Keying) (1 Mbits/s)

*ce type de modulation va encoder un bit à chaque changement de phase*

- ❖ QPSK (Quadrature Phase Shift Keying) (2Mbits/s)

*encoder deux bits par changement de phase*

# 802.11b

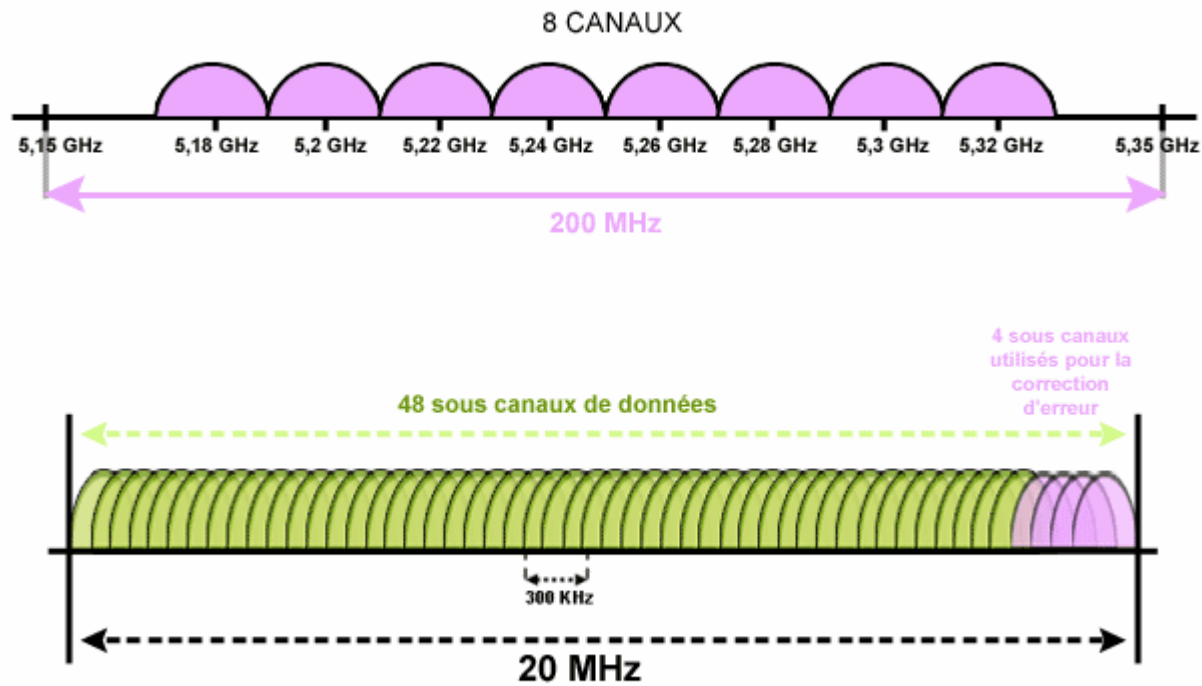
- Débit de 5.5 à 11Mbit/s
- Bande ISM
- DSSS
- Codage CCK (complementary code Keying)
- Modulation de phase QPSK

Technologie	Codage	Type de modulation	Débit
802.11b	11 bits (Barker sequence)	BPSK	1Mbps
802.11b	11 bits (Barker sequence)	QPSK	2Mbps
802.11b	CCK (4 bits)	QPSK	5.5Mbps
802.11b	CCK (8 bits)	QPSK	11Mbps

# 802.11a (Wi-Fi5 1999) OFDM *Orthogonal Frequency Division*

- fonctionne sur la bande U-NII de 5GHz
- Bande divisée en 8 canaux de 20 MHz
- contenant chacune 52 sous canaux de 300 Khz
- Pas de problème de recouvrement (atténuation du bruit)
- Co-localisation de 8 réseaux au sein d'un même espace
- Transmission en // sur plusieurs sous canaux à faible débit crée un canal à haut débit
- 802.11a offre des débits de 6 à 54 Mbits/s suivant la modulation de phase
- BPSK permet d'atteindre un débit de 6Mbits/s; 64QAM (64-level Quadrature Amplitude Modulation) permet un débit de 54 Mbit/s.

# OFDM





# Comparaison débit max / technique à la couche PHY

	802.11	802.11a	802.11b	HiperLan/2	Bluetooth
<b>Fréquence</b>	2.4 GHZ	5 GHZ	2.4 GHZ	5 GHZ	2.4 GHZ
<b>Débits max</b>	2 Mbps	54 Mbps	11 Mbps	54 Mbps	1 Mbps
<b>modulation</b>	FHSS/DSSS	OFDM	DSSS	OFDM	FHSS

# Le mode de transmission

Technologie	Principaux avantages	Principales limitations	Applications typiques
<b>FHSS</b>	<p>Technologie simple et économique</p> <p>Permet de “contourner” les interférences (possibilité de modifier la séquence des sauts en fonction des obstacles rencontrés)</p> <p>Portée relativement élevée</p> <p>Technologie avantageuse en termes de sécurité et de fiabilité</p> <p>Consommation d’énergie relativement faible</p>	<p>Efficacité spectrale peu élevée</p> <p>Débits relativement faibles</p> <p>Nécessite une synchronisation fine entre l’émetteur et le récepteur</p> <p>Sensible au nombre d’émetteurs émettant dans la même bande</p>	<p>Convient à la transmission de signaux courts, y compris en environnement perturbé</p> <p>Solution retenue notamment par Bluetooth (1 600 sauts de fréquence par seconde entre 79 fréquences dans la bande ISM 2,4 GHz)</p>
<b>DSSS</b>	<p>Systèmes de redondance par étalement peu sensible aux interférences et aux erreurs de transmission</p> <p>Bonne efficacité spectrale</p> <p>Possibilité d’obtenir des débits élevés</p> <p>Possibilité d’améliorer les performances par allongement du vecteur d’étalement</p> <p>Durée d’établissement relativement courte</p>	<p>Technologie relativement sophistiquée</p> <p>Nécessite des composants rapides</p> <p>Consommation d’énergie relativement élevée</p>	<p>Convient à la transmission de signaux relativement longs (en dessous d’un seuil de perturbations, qui est fonction du vecteur d’étalement)</p> <p>Solution retenue notamment pour ZigBee et Wi-Fi (802.11b)</p>
<b>OFDM</b>	<p>Grande efficacité spectrale</p> <p>Possibilité d’obtenir des débits très élevés (si le bilan de liaison le permet)</p> <p>Offre une grande robustesse au regard des interférences (notamment celles qui sont dues aux multitrajets)</p>	<p>Consommation d’énergie relativement élevée</p> <p>Nécessite une synchronisation très fine entre l’émetteur et le récepteur</p> <p>Efficacité limitée aux interférences sélectives</p> <p>Solution relativement difficile à mettre en œuvre avec des mobiles (effet Doppler)</p>	<p>Solution retenue pour Wi-Fi (802.11a dans la bande des 5 GHz et 802.11g dans la bande des 2,4 GHz)</p> <p>Utilisée dans l’ADSL, les courants porteurs et le WiMax</p>

# Les protocoles d'accès

- Classification 1 :
  - accès aléatoire (par contention): pas d'autorisation préalable,
  - accès déterministe : mécanisme pour désigner la station qui peut émettre.
- Classification 2 :
  - accès **statique** où l'allocation de la bande passante est définitive,
  - accès **dynamique** (adaptatif), l'allocation de la BP évolue selon les besoins.
- Classification 3 :
  - l'approche centralisée, seul un nœud primaire attribue des droits d'accès,
  - l'approche distribuée, les différents nœuds participent de la même façon aux contrôles d'accès.
- Classification 4 :
  - partage temporel (TDMA : "Time Division Multiple Access"),
  - partage fréquentiel (FDMA : "Frequency Division Multiple Access").

# Politiques d'accès dynamiques à allocation déterministes

- Allouer de la Bande Passante aux utilisateurs qui en ont besoin
- Connaître les besoins des utilisateurs
- « intelligence » centralisée ou distribuée
- **Allocation sélective ou *polling***
  - *Roll-call polling (centralisé)*
  - *Hub polling (distribué)*
- ***Allocation de Jeton***
- **anneau en tranches**

# Allocation sélective ou polling

- Consulter les compétiteurs
  - les inviter à émettre à tour de rôle
- Site maître (station centrale)
  - Interroge séquentiellement chaque station
  - Si elle a des trames à émettre
    - La trame est transmise au maître
    - Le maître interroge le destinataire (prêt à recevoir?)
- ***Roll-call polling*** (centralisé) ou ***Hub polling*** (répartie)

# Roll-call polling

- station primaire
  - interroge successivement chacune des stations secondaires
  - envoie d'une trame de poll.
- station interrogée
  - répond par une trame
    - acquittement négatif si rien à envoyer
    - données dans le cas contraire

# Hub polling

- Station primaire : démarre un cycle
  - trame de poll à la station secondaire la plus éloignée
  - Si données à envoyer au primaire
    - envoie des données à la station primaire
    - envoie une trame de poll à la station secondaire suivante
  - Dans le cas contraire
    - envoie la trame de poll à la station secondaire suivante
    - dernière station envoie une trame de poll au primaire
      - démarre un nouveau cycle.

# Allocation de Jeton

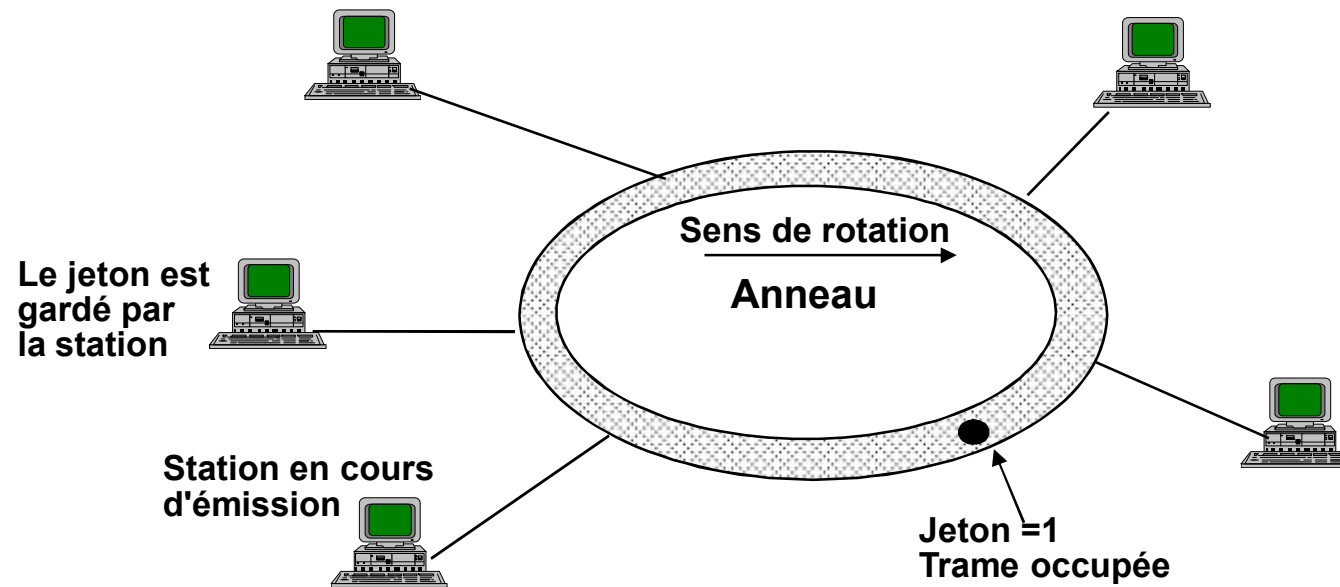
- Trame spéciale : « Jeton »
  - Faire circuler sur le réseau
- Le jeton autorise à émettre
  - Seule la station qui a le jeton peut émettre
- Jeton non adressé
- Jeton adressé



# Anneau à Jeton - 802.5

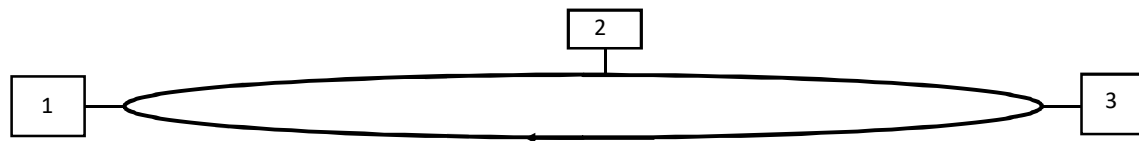
- Topologies physiques en anneau
- Un jeton circule sur l'anneau
  - État libre => donne le droit à émettre
  - État occupé
- Station veut émettre
  - Attend le jeton libre
  - Attache le message au jeton (jeton occupé)
  - Si @ source = son @ => retirer le message  
=> jeton libre

# Anneau à jeton



# Exemple de fonctionnement de la méthode d'accès du jeton sur anneau

- chaque station dispose d'un message à émettre en fonction duquel S est positionné :
- sur la station 1, S = 2
- sur la station 2, S = 4
- sur la station 3, S = 6
- notation : jeton = <état (0 : libre/1 : occupé) ; P ; R>
- le THT n'est pas pris en compte



**Station 1**

<0 ; 0 ; 0> empile 0 et P à 2  
 <1 ; 2 ; 6> empile 2 et P à 6  
 <1 ; 6 ; 4>  
 <0 ; 6 ; 4> tête(pile)< 4 et P à 4  
 <1 ; 4 ; 0>  
 <0 ; 4 ; 0> dépile 2 et P à 2  
 <0 ; 2 ; 0> dépile 0 et P à 0

**Station 2**

<1 ; 2 ; 0>  
 <0 ; 6 ; 0>  
 <1 ; 6 ; 4>  
 <0 ; 4 ; 0>  
 <1 ; 4 ; 0>  
 <0 ; 2 ; 0>  
 <0 ; 0 ; 0>

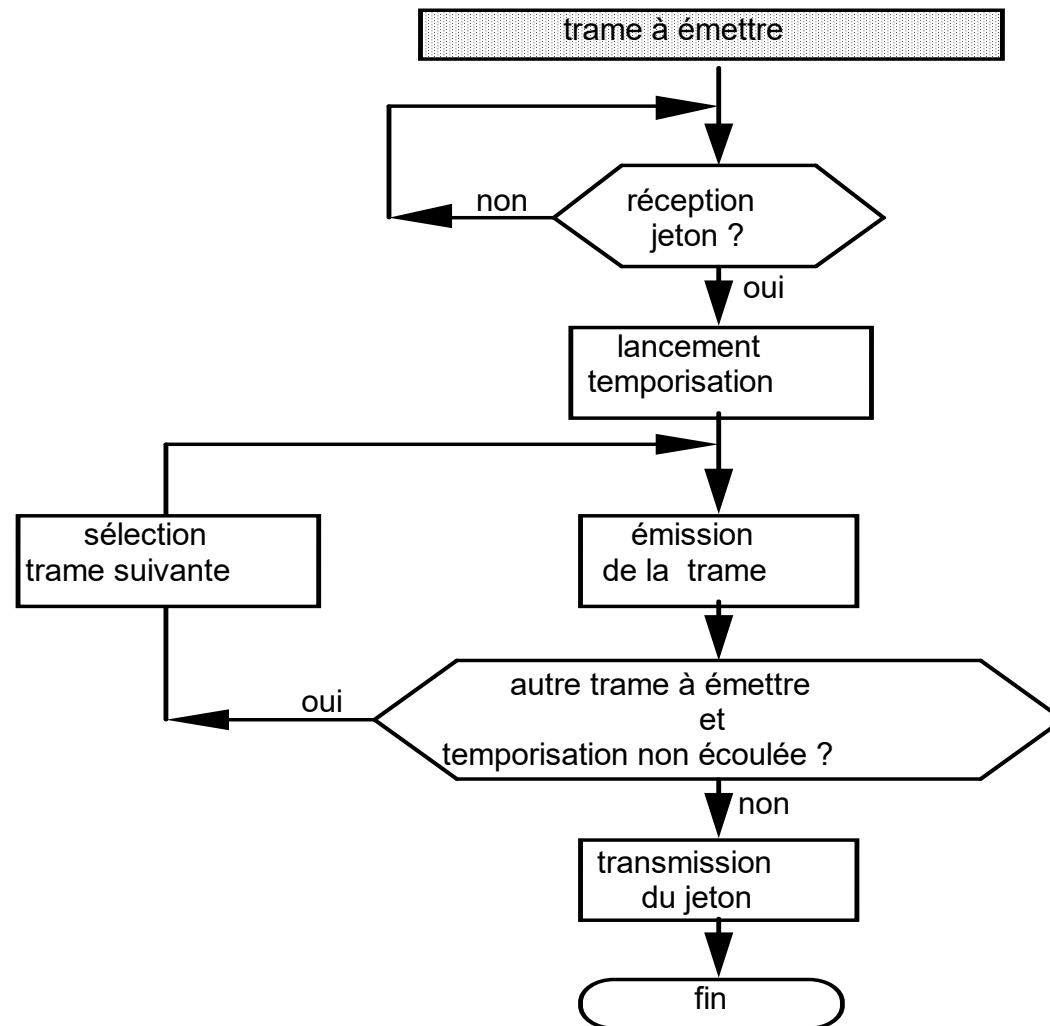
**Station 3**

<1 ; 2 ; 4>  
 <0 ; 6 ; 4>  
 <1 ; 6 ; 4>  
 <1 ; 4 ; 0>  
 <0 ; 4 ; 0>  
 <0 ; 2 ; 0>

# Bus à Jeton - 802.4

- **Topologies physiques en bus**
- **Création d'un anneau logique**
  - Insertion dans l'ordre de l'adresse
  - Chaque station connaît son successeur
- **Le jeton circule dans l'anneau logique**
- **Seul le jeton autorise à émettre**
  - Temps de transmission limité

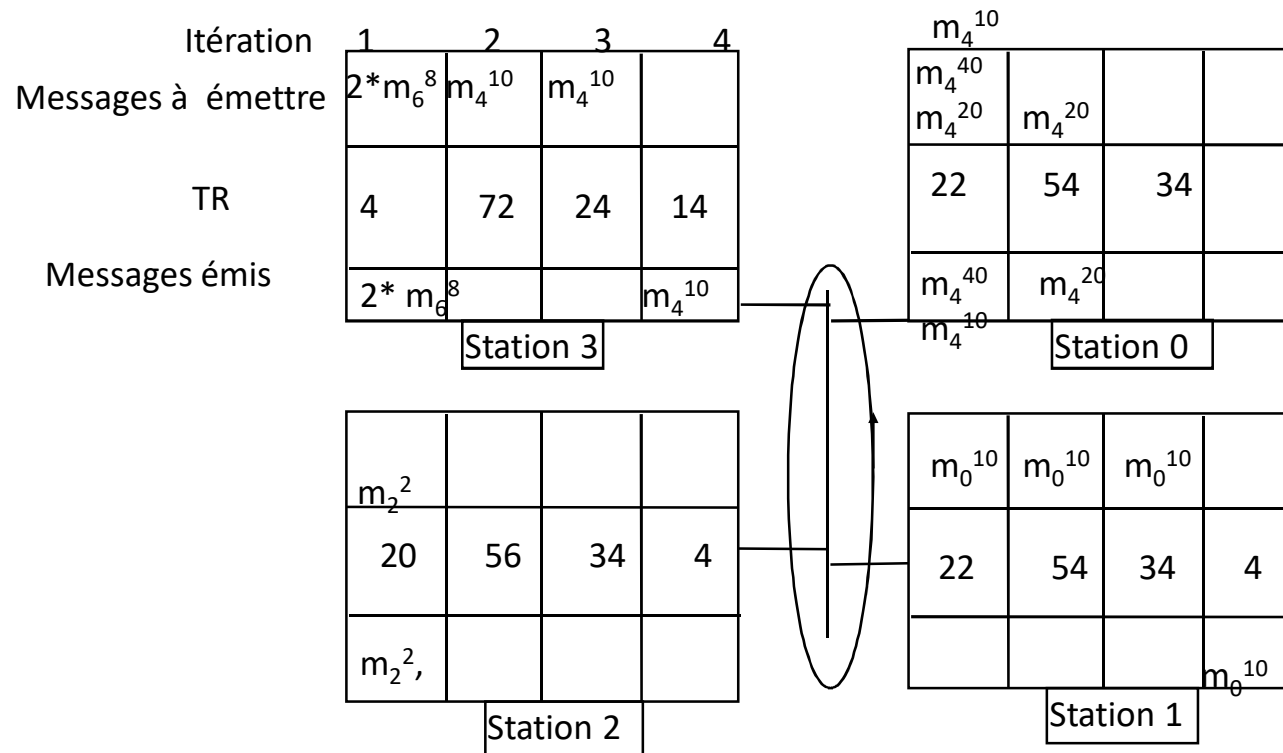
# Bus à Jeton : algorithme



# Exemple simplifié du fonctionnement de la méthode d'accès IEEE 802.4

$OTR_6 = 100$   
 $OTR_4 = 80$   
 $OTR_2 = 40$   
 $OTR_0 = 20$

- Temps de passage d'un jeton = 1
- Initialement le jeton arrive à la station 3 où  $TR=4$  ; le jeton ayant effectué un tour complet sans qu'aucun message ne soit émis
- Notation :  $m_{\text{priorité}}^{\text{durée de transmission}}$



## Technique de la tranche vide ou anneau en tranches ("empty slot" ou "slotted ring")

- l'anneau est constitué d'un ensemble de trames ayant une taille fixe (wagons) appelés tranches de temps (vides ou pleines).
- Un nœud désirant émettre un message doit attendre le passage d'un wagon libre.
- L'émetteur prélève ces données et libère le wagon (acquiescement).

# Politiques d'accès dynamiques à allocation aléatoires

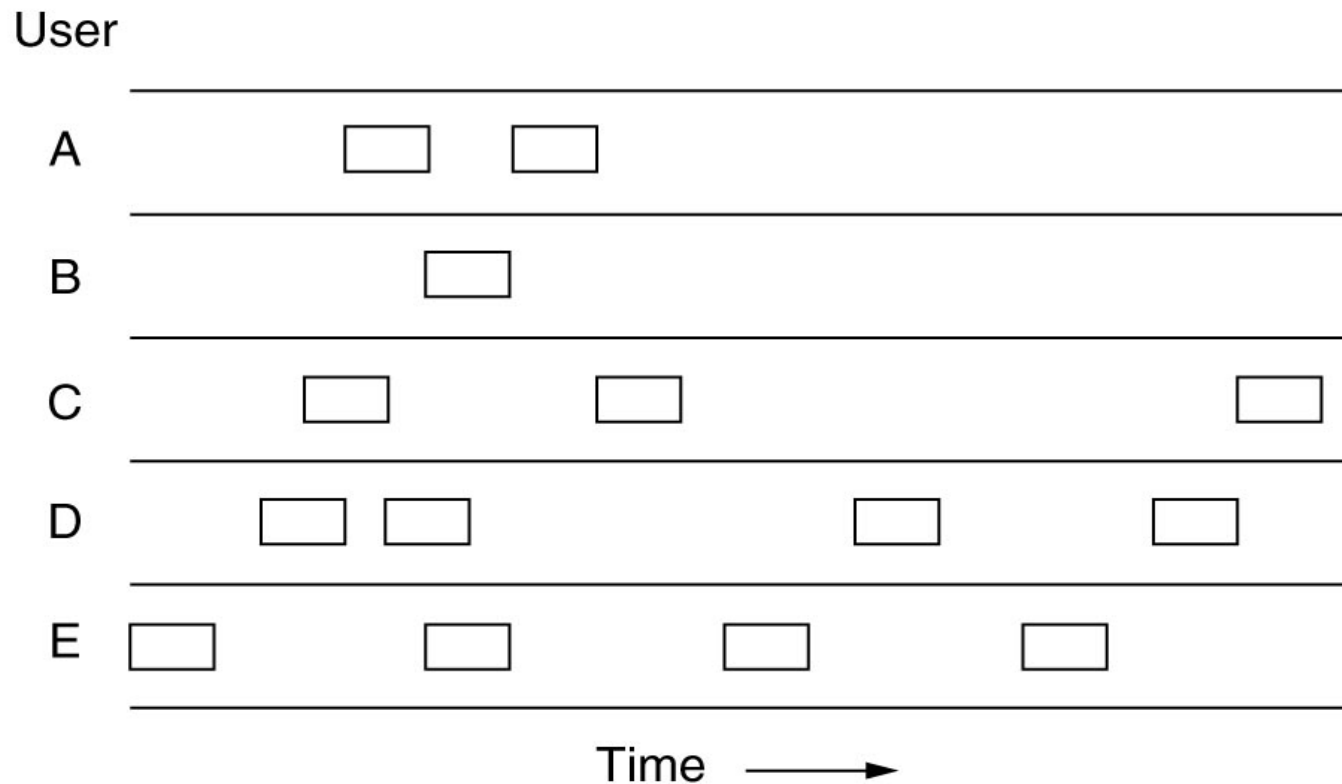
- **Ressources alloués par une station aléatoire**
  - Station ayant besoin d'émettre => **ÉMET**
- **Problème : collision**
- **Protocole ALOHA**
- **Méthode d'accès CSMA/CD**



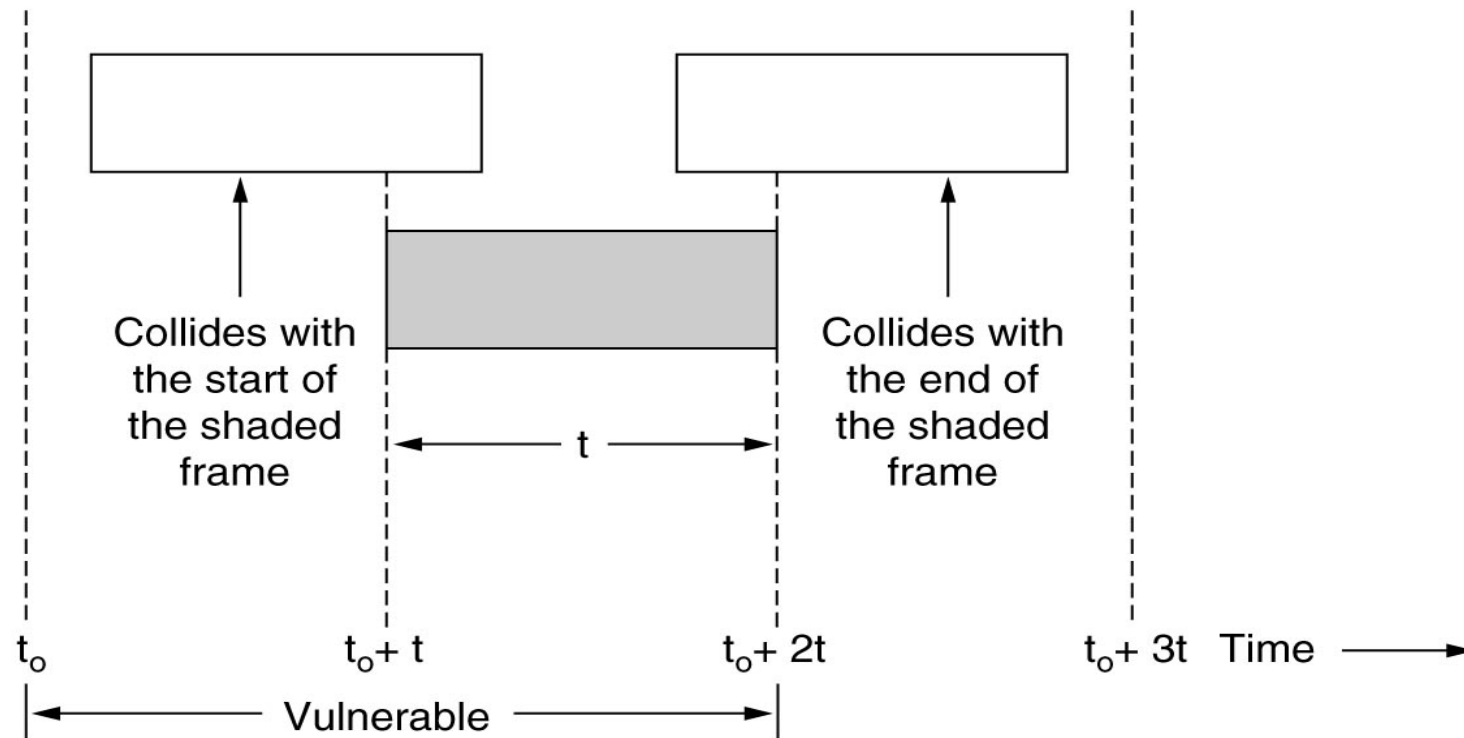
# ALOHA

- **Aloha pur: accès aléatoire sans référence temporelle**
- **Station émet quand elle a besoin**
- **Si deux trames émises en même temps**
  - **=> collision**
  - **Signal incompréhensible**
  - **Ré-émission**

# ALOHA : envoie des trames



# ALOHA : période de vulnérabilité



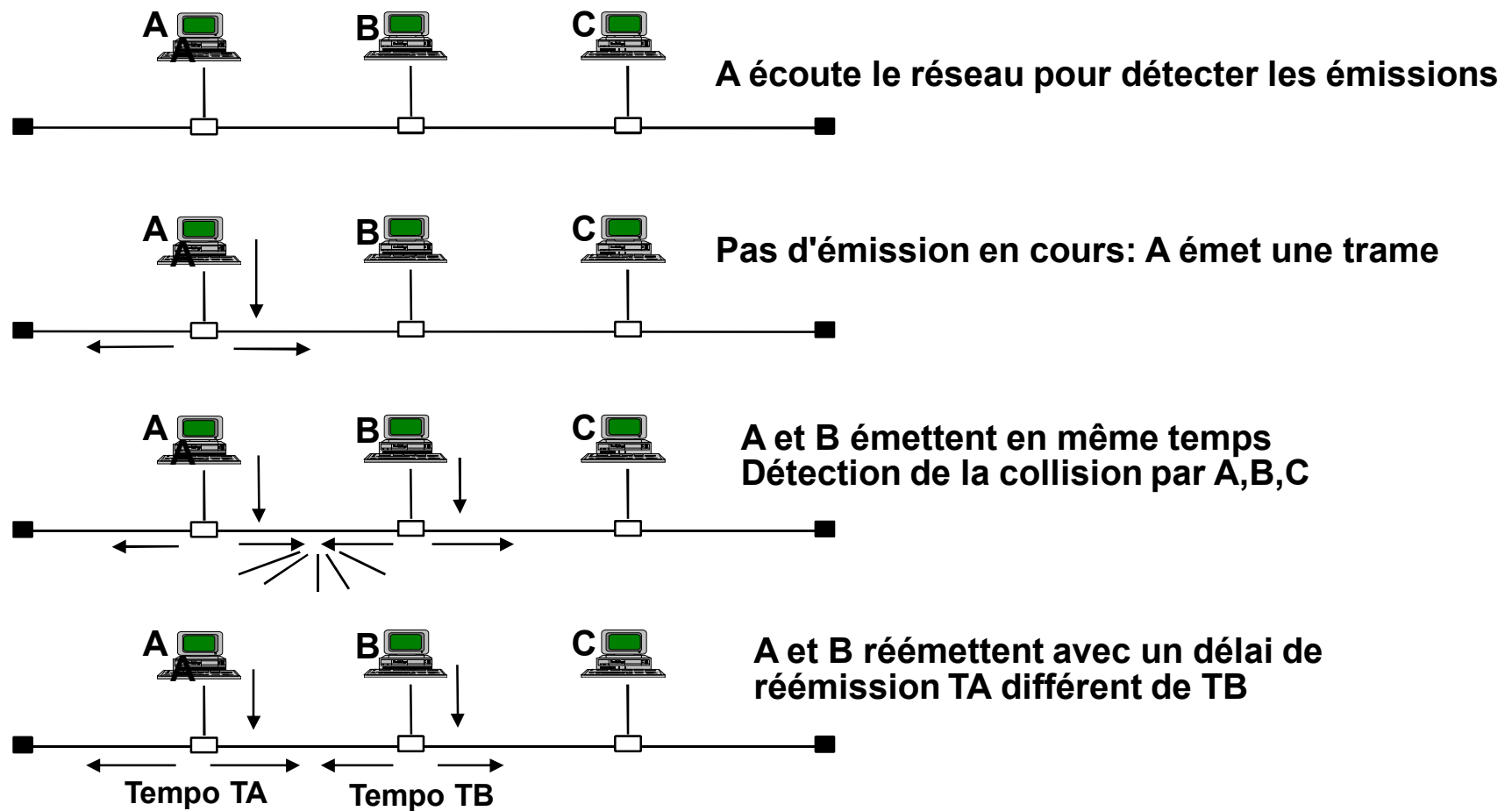
# ALOHA et compagnie

- ALOHA discrétisé (slotted)
  - Possibilité d'utiliser la totalité du débit si on est seul
  - Requier la synchronisation entre machines
- ALOHA pur (version initiale)
  - Pas de synchronisation ni de découpage en intervalle
- CSMA (Carrier Sense Multiple Access)
  - Détection de porteuse: ne pas émettre si une autre station est déjà en train d'émettre
  - Persistant : attente après collision et émission dès que libre
  - Non-persistant : écoute, attente, écoute... jusqu'à libre
  - P-persistant : Emission avec une probabilité  $p$ , diffère l'émission avec une prob  $(1-p)$
- CSMA/CD (Collision Detection)
  - Interrompre l'émission dès qu'une collision est détectée

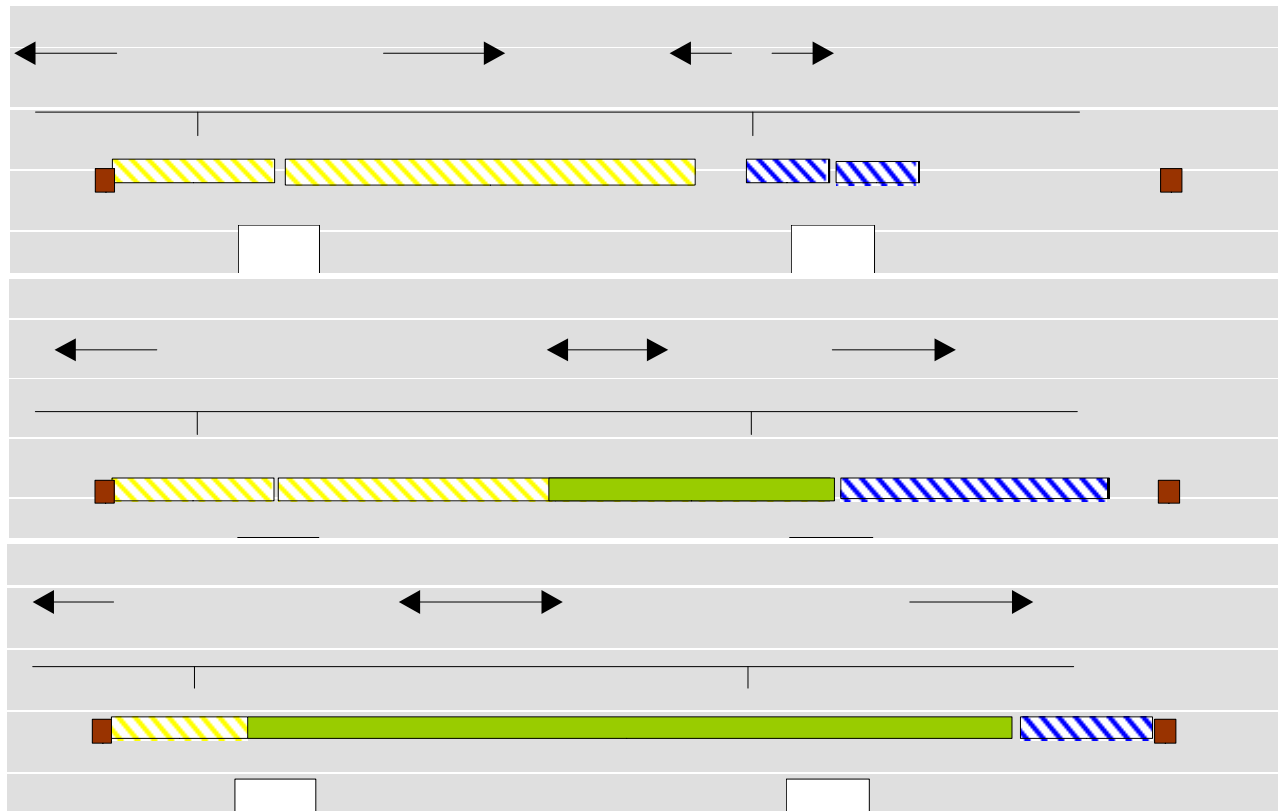
# CSMA/CD -802.3 : Ethernet

- ***Carrier Sense Multiple Access with Collision Detection*** (*Protocole d'accès multiple avec surveillance de porteuse et détection de collision*)
- **Toute machine est autorisé à émettre**
- **« écoute » le support avant d'émettre**
- **Détection de collision => fin d'émission**
  - Attendre un délai aléatoire avant de réémettre
- **Technique la plus répandue**

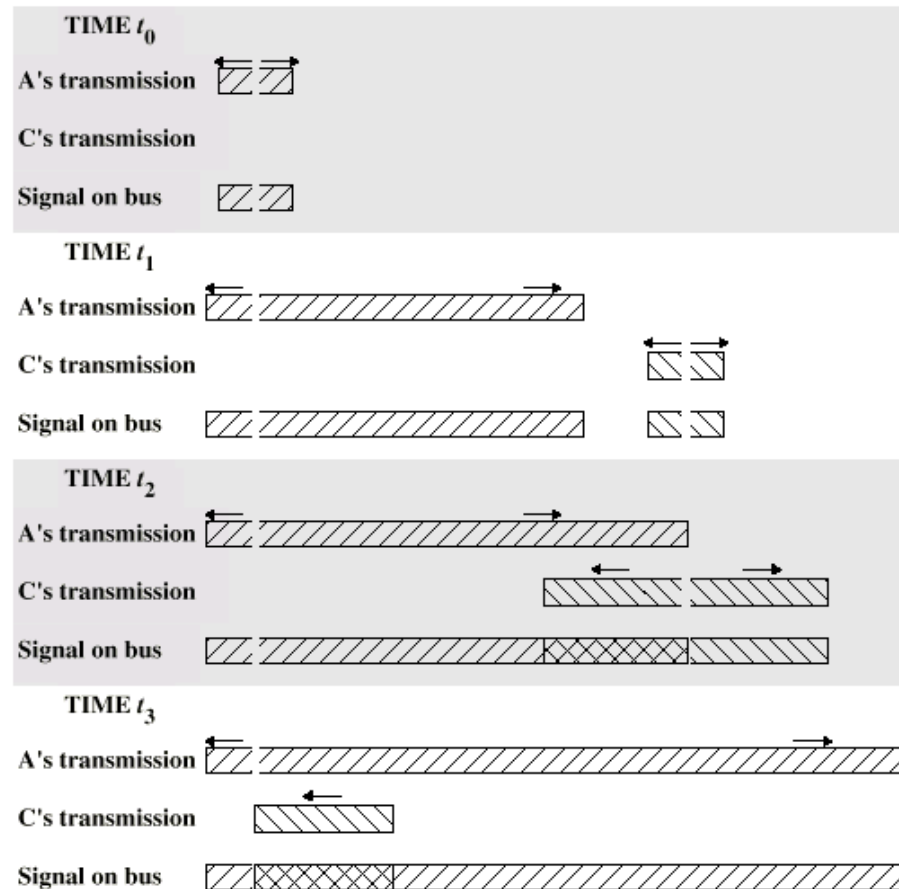
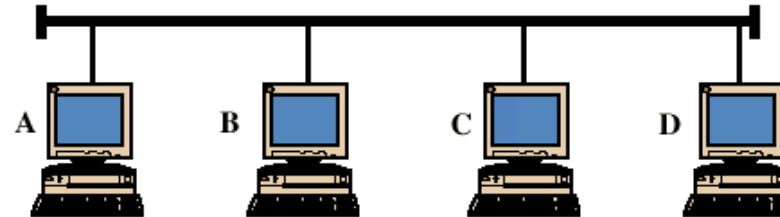
# CSMA/CD



# CSMA/CD : collision

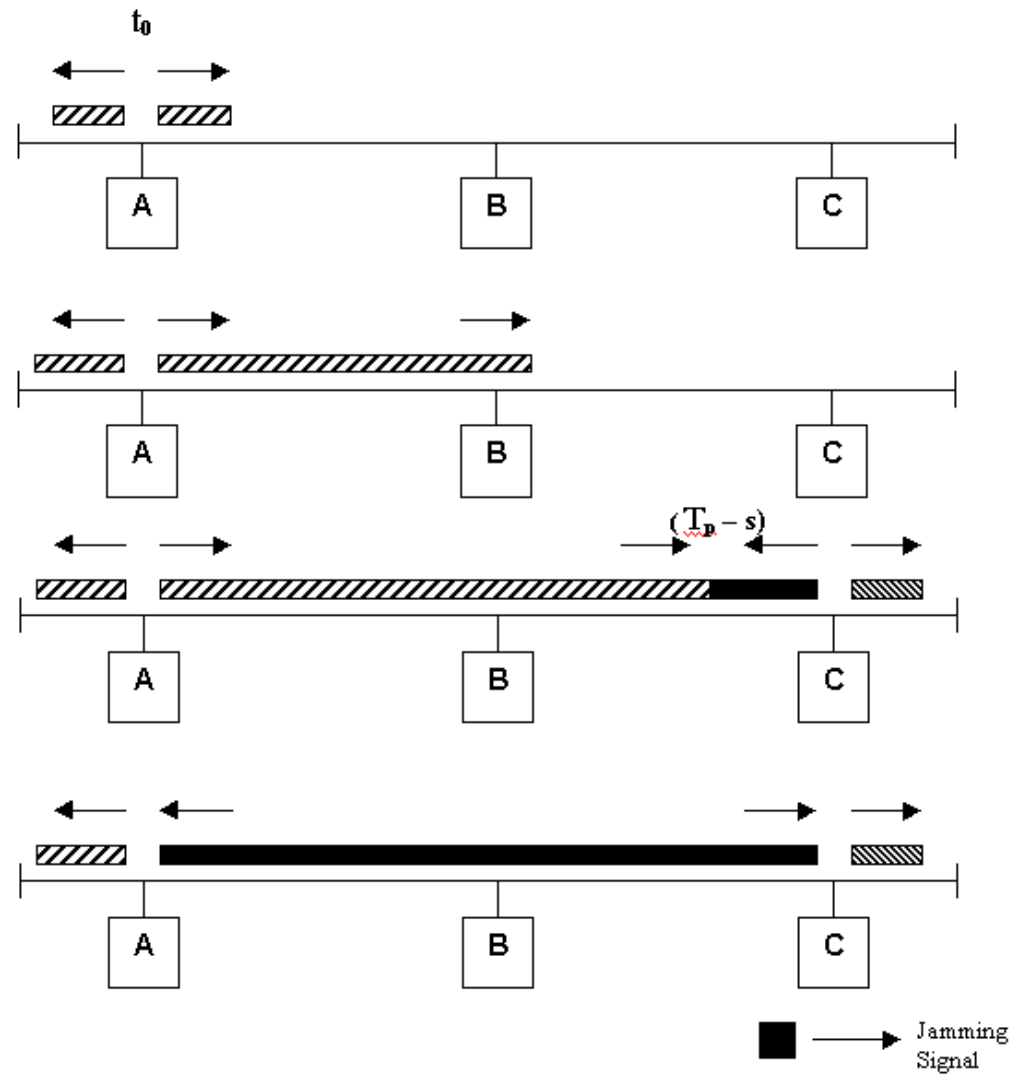


# CSMA/CD : collision



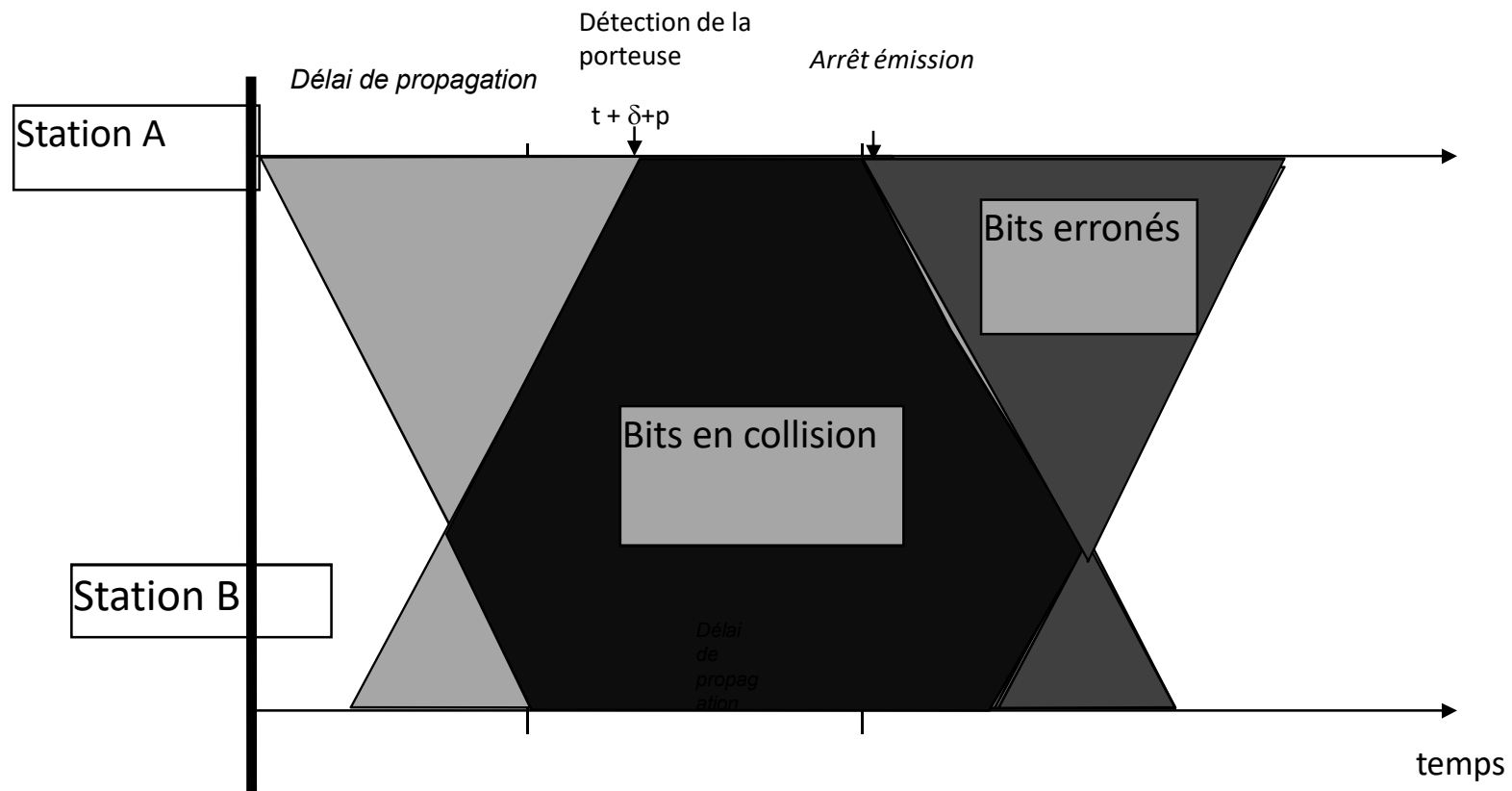


# CSMA/CD : collision

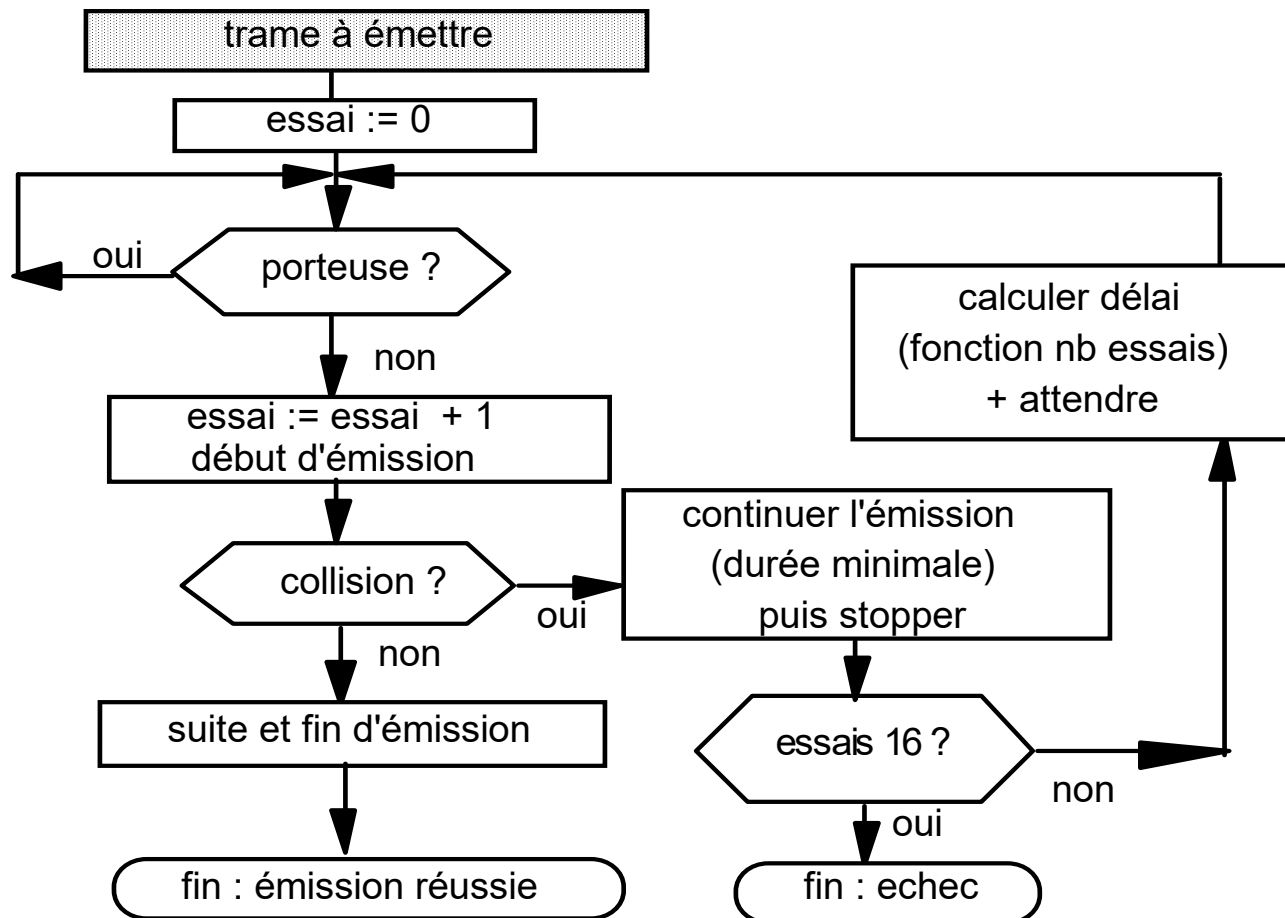


# CSMA/CD

collision entre deux émissions



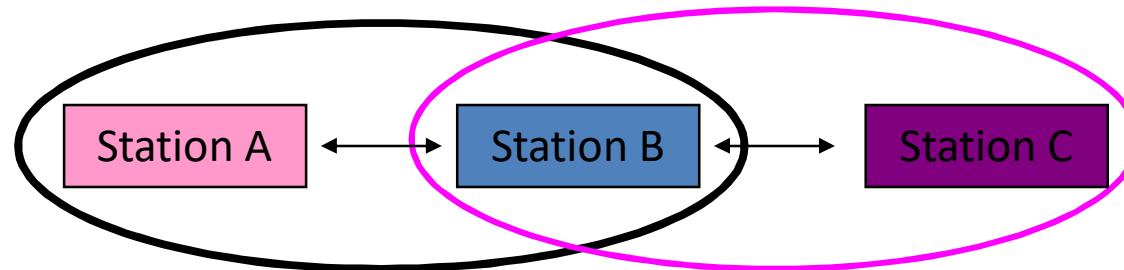
# CSMA/CD : algorithme



# CSMA/CA

- des mécanismes d'écoute du support
- l'algorithme de *back-off* pour la gestion d'accès au support,
- un mécanisme optionnel de réservation, dont le rôle est de limiter le nombre de collision en s'assurant que le support est libre (RTS/CTS)
- des trames d'acquittement positif (ACK).

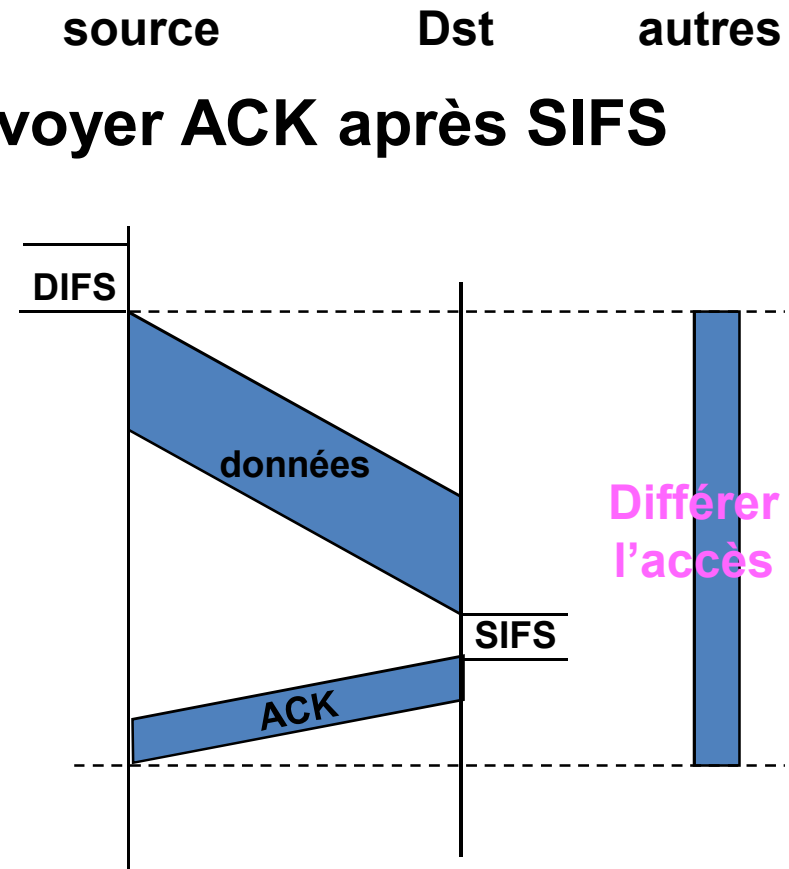
# PB station cachée



- ☐ A envoie à B, C ne peut pas recevoir A
- ☐ C veut envoyer à B, C croit le support libre
- ☐ collision à B, A n'entends pas la collision
- ☐ A est "caché" pour C

# DCF *Distributed Coordination Function*

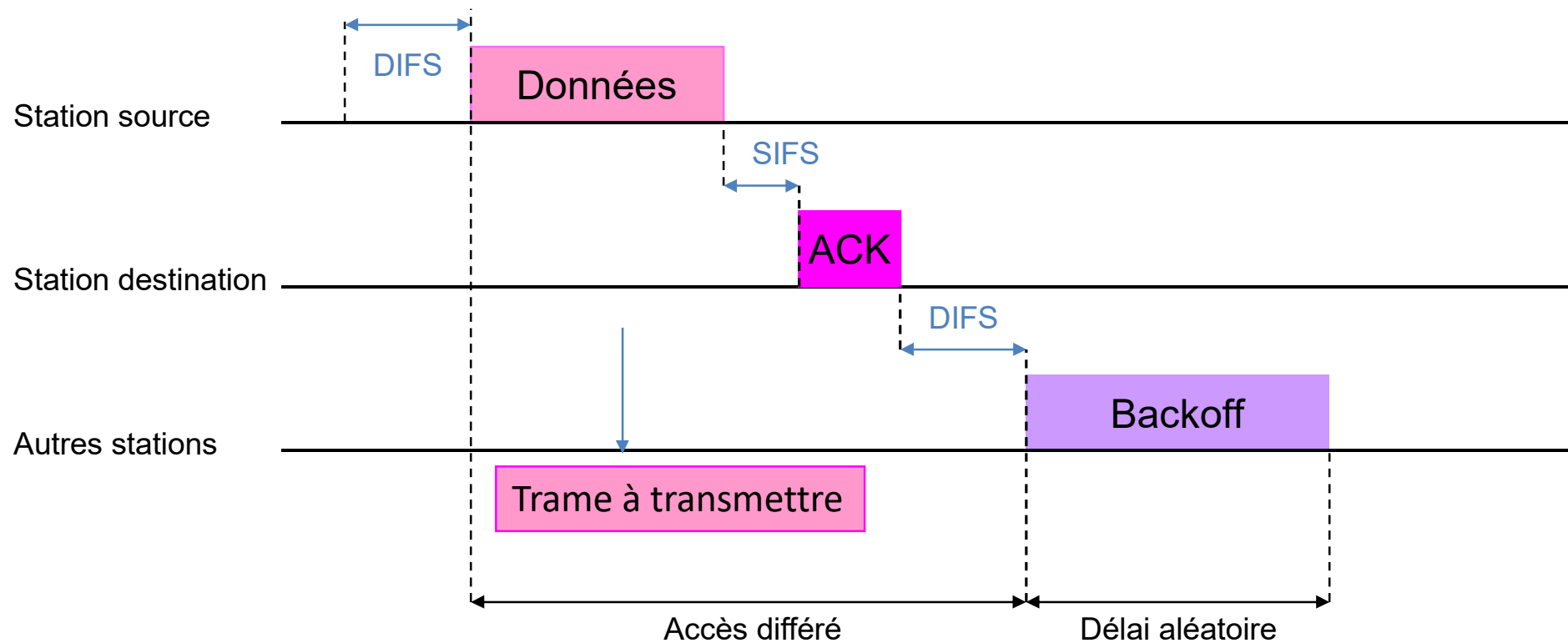
- **CSMA source**
  - Si le canal est libre pour DIFS secondes alors transmettre toute la trame (pas de CD)
  - Si le canal est occupé alors backoff
- **CSMA recepateur**
  - Si reception = OK alors envoyer ACK après SIFS



# DCF (2)

- IFS Inter **F**rame **S**pace
  - 4 types d'IFS
    - *Short Inter-Frame Spacing* (SIFS)  
séparer les différentes trames transmises au sein d'un même dialogue
    - *DCF Inter-Frame Spacing* (DIFS)  
Temps avant d'émettre un paquet en mode DCF
    - *PCF Inter-Frame Spacing* (PIFS)  
Temps avant d'émettre un paquet en mode PCF. (<DIFS)
    - *Extended Inter-Frame Spacing* (EIFS)  
Temps attendu lorsque une station reçoit une trame erronée
- SIFS<PIFS<DIFS

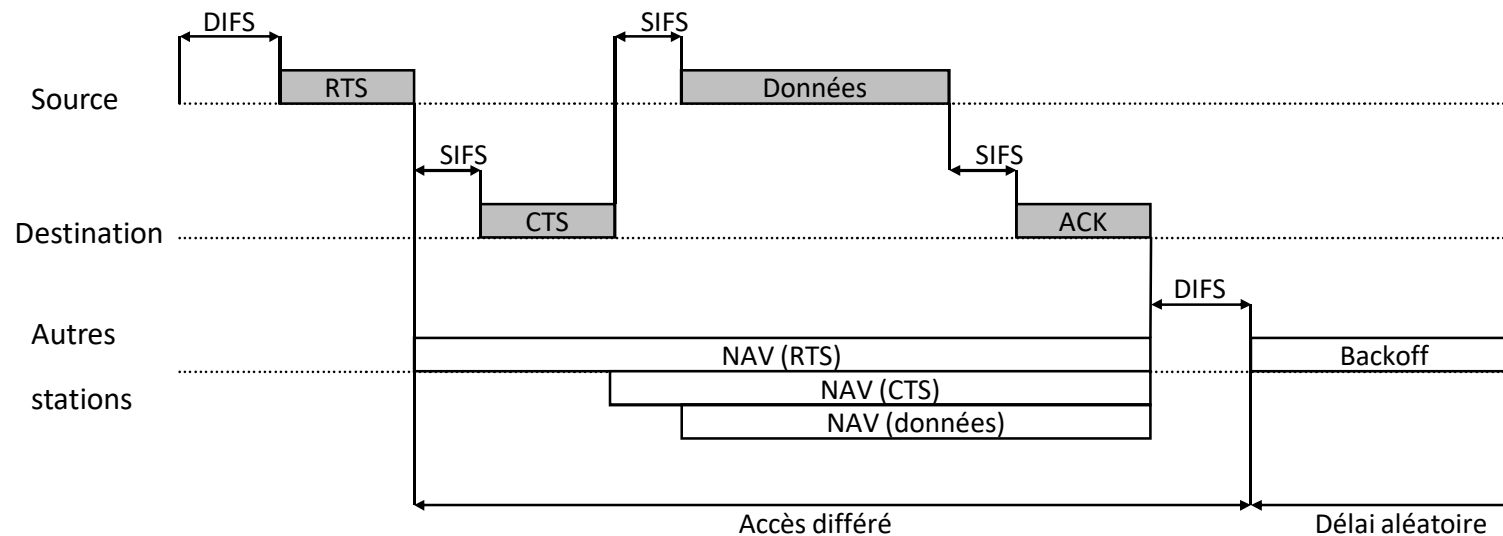
# DCF (3)





# DCF (4)

- transmission CSMA/CA & "Virtual Carrier Sensing"



- Slot = 50μs

- SIFS : « Short Inter Frames Space » = 28μs, valeur minimale pour qu'une station puisse changer du mode émission vers le mode réception (dans le cadre d'un même dialogue, le récepteur gagne le droit d'accès).

- DIFS « Distributed Inter Frame Space » = SIFS + 2 \* Slot = PIFS + Slot = 128μs, utilisé lorsqu'une station veut commencer une nouvelle transmission

# Normalisation des réseaux locaux

# Les normes IEEE 802

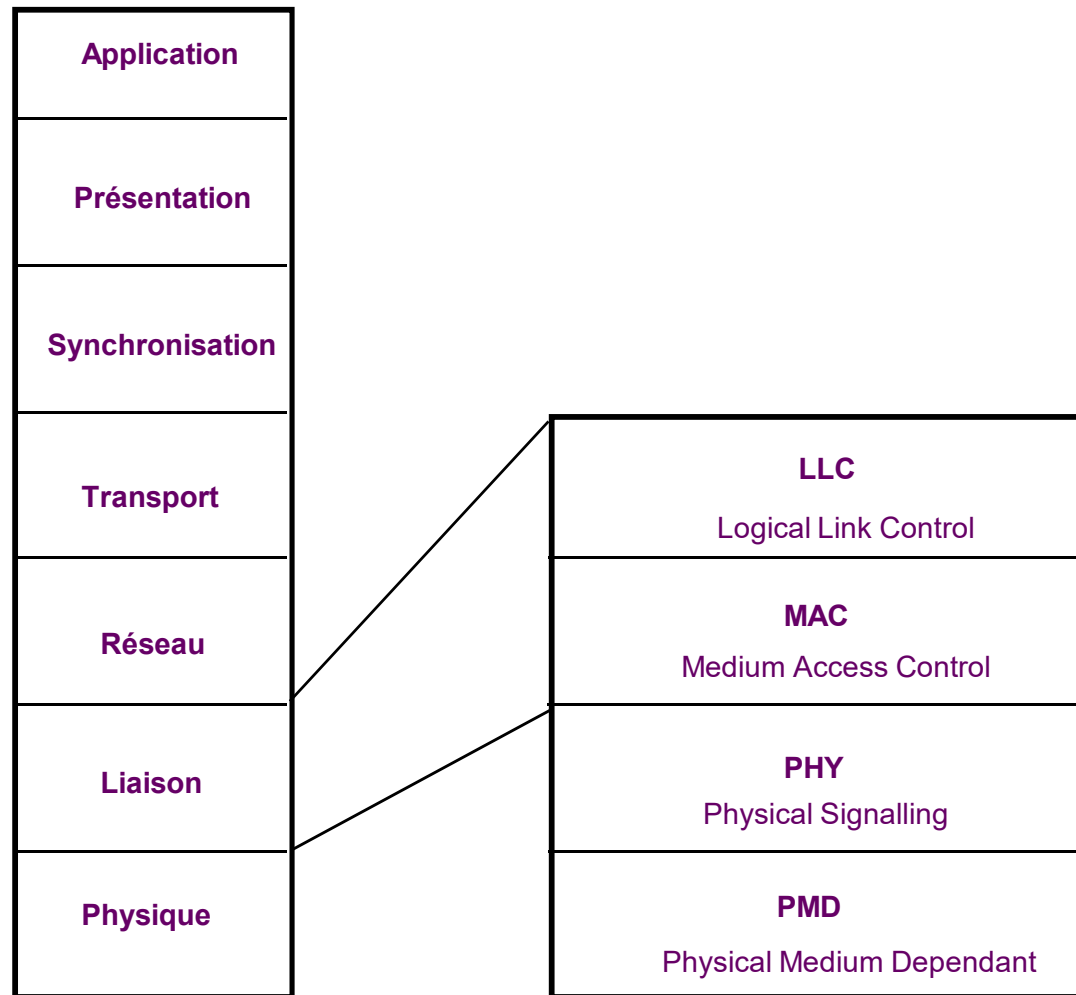
- Particularité des LAN :
  - ✓ réseau de diffusion: toutes les stations ont la possibilité d'émettre et de recevoir sur le même canal
  - ✓ Pas de nœuds intermédiaire
- Nécessité de contrôler l'accès au support pour mettre de l'ordre
  - ✓ Fonctions non définies dans le modèle OSI
  - ✓ Nouvelles définitions des niveaux physiques et liaisons de données

# La norme 802.1

- PMD : support, connecteur, mode de transmission, raccordement actif / passif,...
- PHY : conversion parallèle/série, contrôle d'erreur , codage en ligne ...
- MAC : «*Medium Access Control* » contrôle d'accès
- LLC : « Logical Link Control » contrôle de liaison

# La norme 802.1

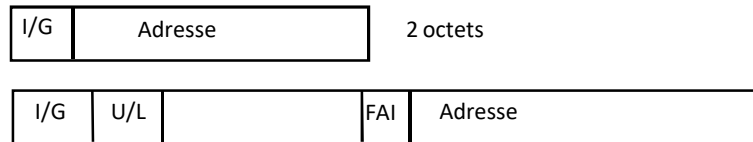
- Modèle



# Les normes 802

- IEEE 802.3 : CSMA/CD sur bus, elle concerne les réseaux Ethernet.
- IEEE 802.4 : jeton sur bus (dissous),
- IEEE 802.5 : jeton sur anneau (Token-Ring).
- IEEE 802.6 (MAN, dissous) remplacée par le Gigabit Ethernet utilisé dans de nombreux MAN.
- IEEE 802.11 : WLAN (Wifi)  
plusieurs normes de transmission:  
fréquence, débit , portée du signal radio.
- IEEE 802.15 : WPAN (Bluetooth)

# Adressage MAC



formats d'adresses

- Exemple d'adresses universelles

IBM 08:00:5A:XX:XX:XX

SUN 08:00:20:XX:XX:XX

3COM 02:60:8C:XX:XX:XX

CISCO 00:00:0C:XX:XX:XX

- Adresse Particulières

FF:FF:FF:FF:FF:FF

Adresse [broadcast](#)

01:00:0C:CC:CC:CC

[Cisco Discovery Protocol](#)

01:80:C2:00:00:00

[Spanning Tree Protocol](#)

33:33:xx:xx:xx:xx

Adresses multicast [IPv6](#)

01:00:5E:xx:xx:xx

Adresses multicast IPv4

00:00:0c:07:ac:xx

Adresses [HSRP](#)

00:00:5E:00:01:XX

Adresses [VRRP](#)

# La norme IEEE 802.2

- LLC 1 : sans connexion, non fiable,
- LLC 2 : avec connexion, fiable,
- LLC 3 : sans connexion, la récupération des erreurs est décidée par l'émetteur.

Une trame LLC, ou LPDU

DSAP	SSAP	Contrôle	Données
------	------	----------	---------

I-Frame (information)	0	N (S)							P/F	N (R)
S-Frame (supervisory)	1	0	S	S	X	X	X	X	P/F	N (R)
(Receive ready) RR	1	0	0	0	0	0	0	0	P/F	N (R)
(Reject) REJ	1	0	0	1	0	0	0	0	P/F	N (R)
(Receive not ready) RNR	1	0	1	0	0	0	0	0	P/F	N (R)
U-Frame (unnumbered)	1	1	M	M	P/F	M	M	M		
	1	1	1	1	P	1	1	0		SABME command (set ABM mode extended)
	1	1	0	0	P	0	1	0		DISC command (disconnect)
	1	1	1	0	F	0	0	0		UA response (unnumbered acknowledge)
	1	1	1	0	F	0	0	0		DM response (disconnect mode)
	1	1	1	0	F	0	0	0		FRMR response (frame reject)
	1	1	0	0	P	0	0	0		UI command (unnumbered information)
	1	1	0	0	P/F	1	1	1		TEST cmd/rsp (test)
	1	1	1	0	P/F	0	0	0		XID cmd/rsp (exchange identification)
	1	1	1	0	P/F	0	0	0		AC0 cmd/rsp (information/acknowledge sequence 0)
	1	1	1	0	P/F	0	0	0		AC1 cmd/rsp (information/acknowledge sequence 1)

*le champ contrôle*



# Trames LLC2 (HDLC)

- **Trames de données : I**

Ces trames transportent des données fournies par les entités de la *couche réseau*.

- **Trames de supervision : S**

transportent des **commandes** ou des **réponses** liées au contrôle d'erreurs, et au contrôle de flux.

**RR** = *Receive Ready* [ 1 0 0 0 P/F Nr ] : le récepteur est prêt à recevoir

**RNR** = *Receive Not Ready* [ 1 0 1 0 P/F Nr ] : le récepteur ou la couche réseau est débordé

**REJ** = *Reject* [ 1 0 0 1 P/F Nr ] : demande de retransmission des trames  $\geq$  Nr

**SREJ** = *Selective Reject* [ 1 0 1 1 P/F Nr ] : demande de retransmission de la trame numéro Nr

- **Trames non numérotées : U**

transportent des **commandes** ou des **réponses** de la gestion de la liaison (établissement, rupture, choix d'un mode de réponse...).

## Commandes

**SABM** = *Set Asynchronous Balanced Mode* [ 1 1 1 1 P/F 1 1 0 ] : demande de connexion

**SABME** = Identique à SABM, mais mode étendu (numéroté en modulo 128).

**DISC** = *Disconnect* [ 1 1 1 1 P/F 0 1 0 ] : libération de connexion

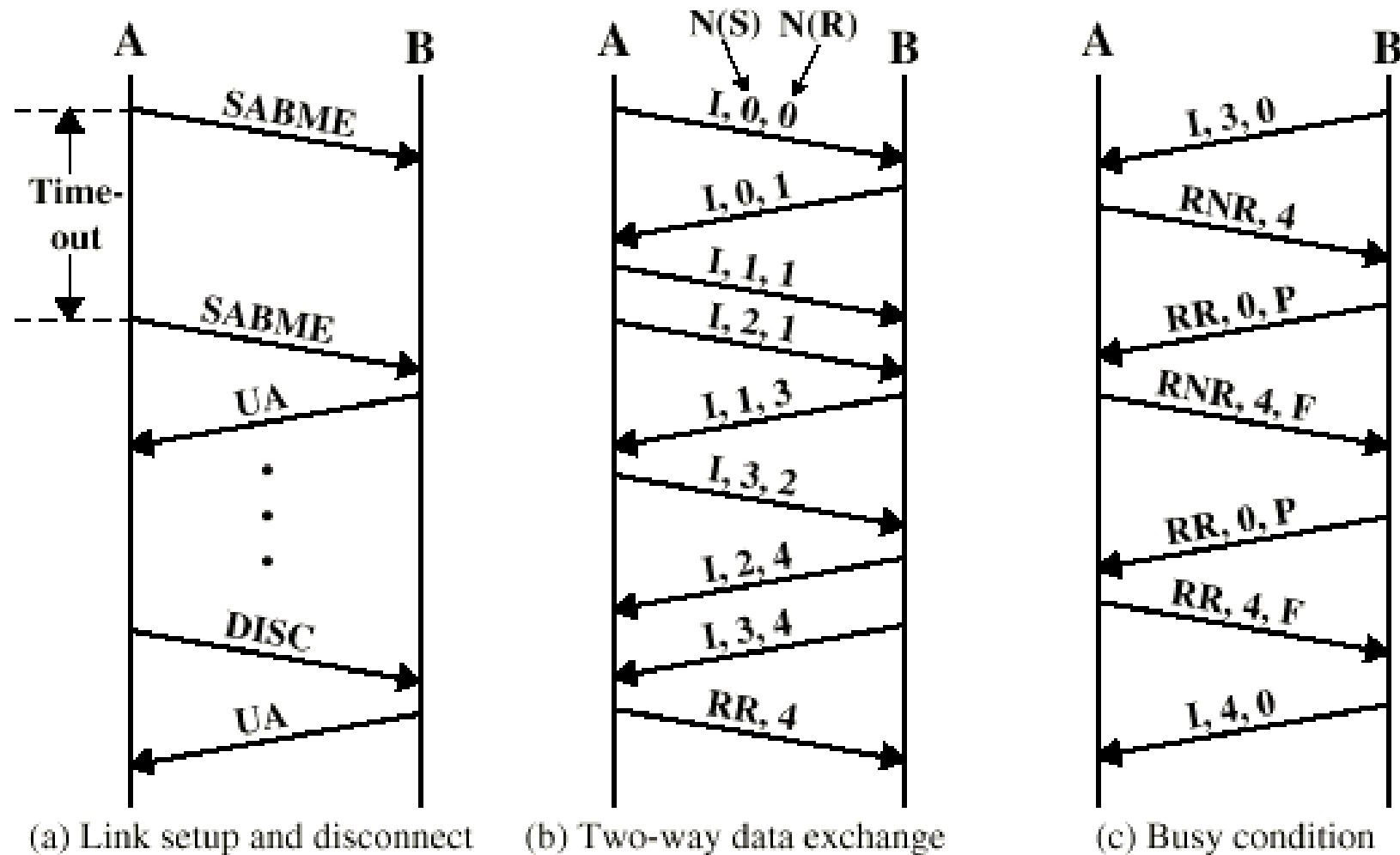
## Réponses

**UA** = *Unnumbered Acknowledgement* [ 1 1 0 0 P/F 1 1 0 ] : acquittement de trame non-numérotée

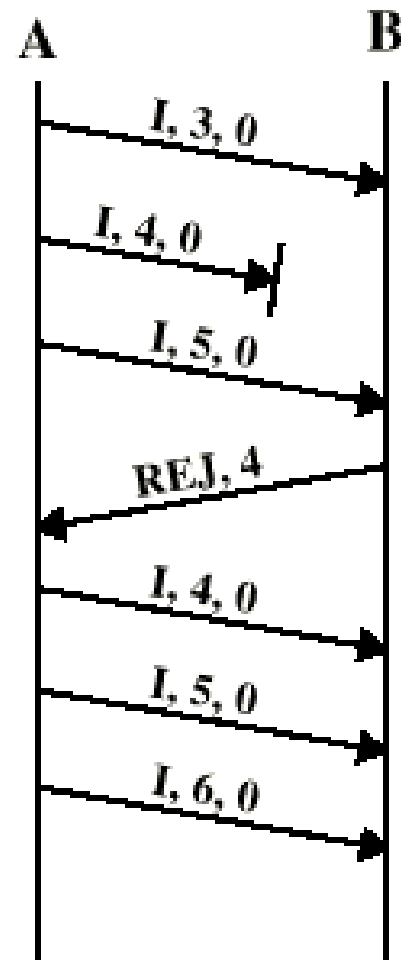
**FRMR** = *FRaMe Reject* [ 1 1 1 1 P/F 0 1 1 ] : rejet de trame

**DM** = *Disconnect Mode* [ 1 1 1 1 P/F 0 0 0 ] : le terminal est déconnecté

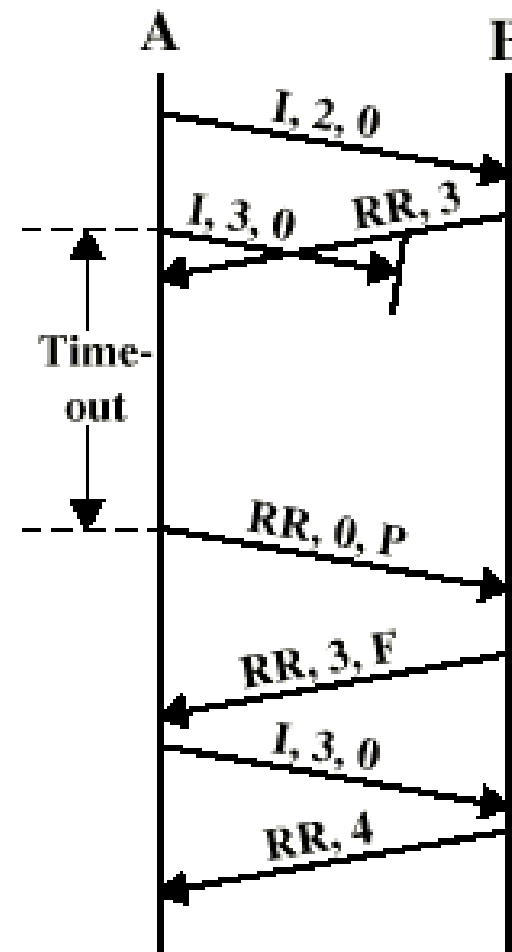
# Examples of Operation (1)



# Examples of Operation (2)

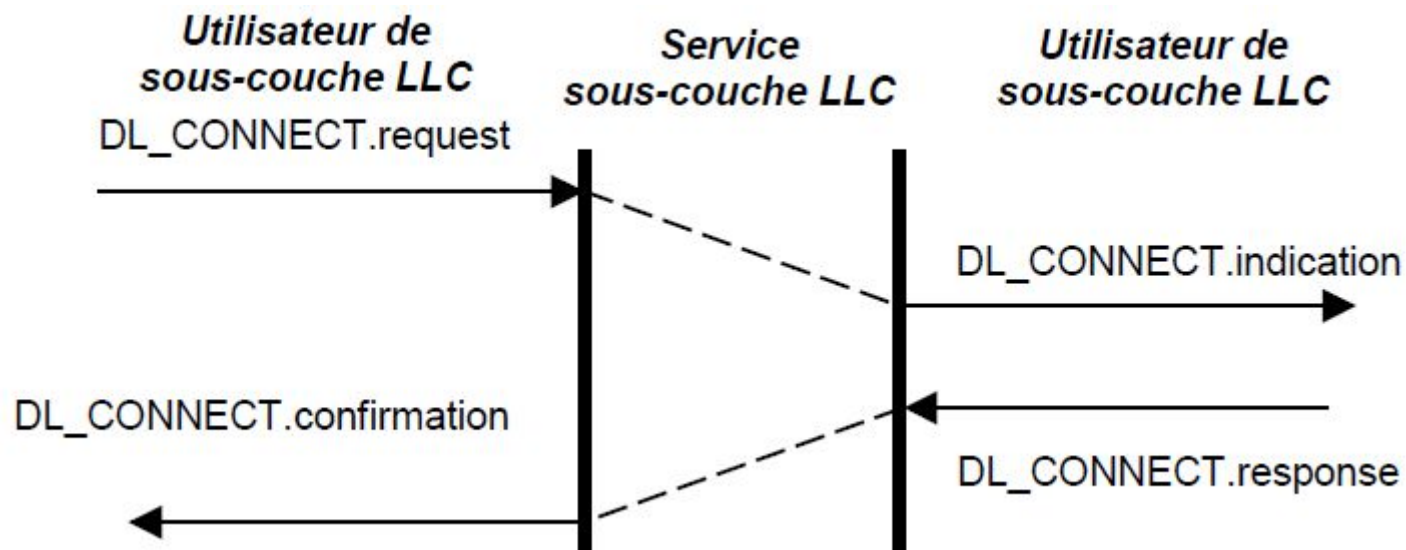
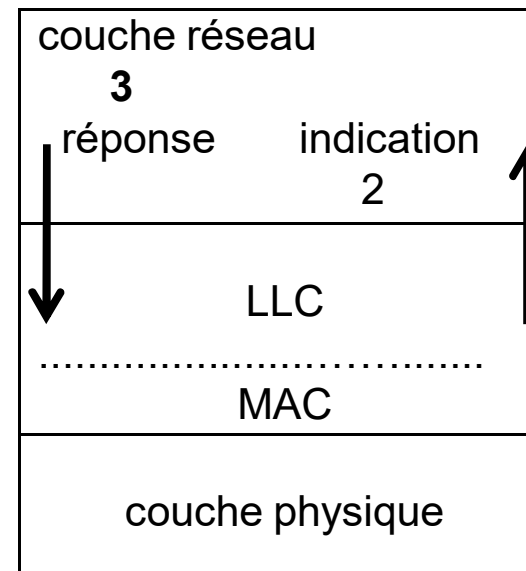
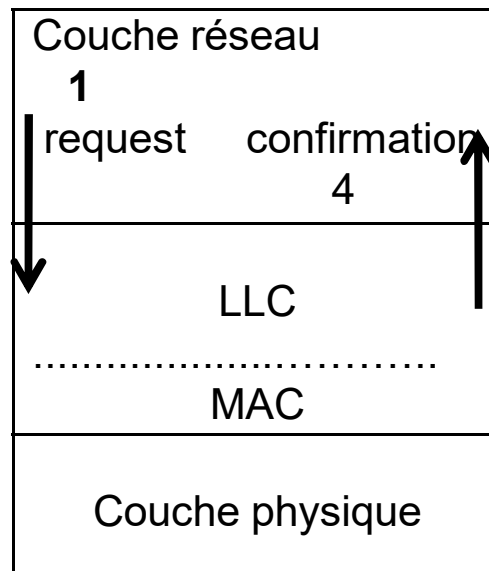


(d) Reject recovery



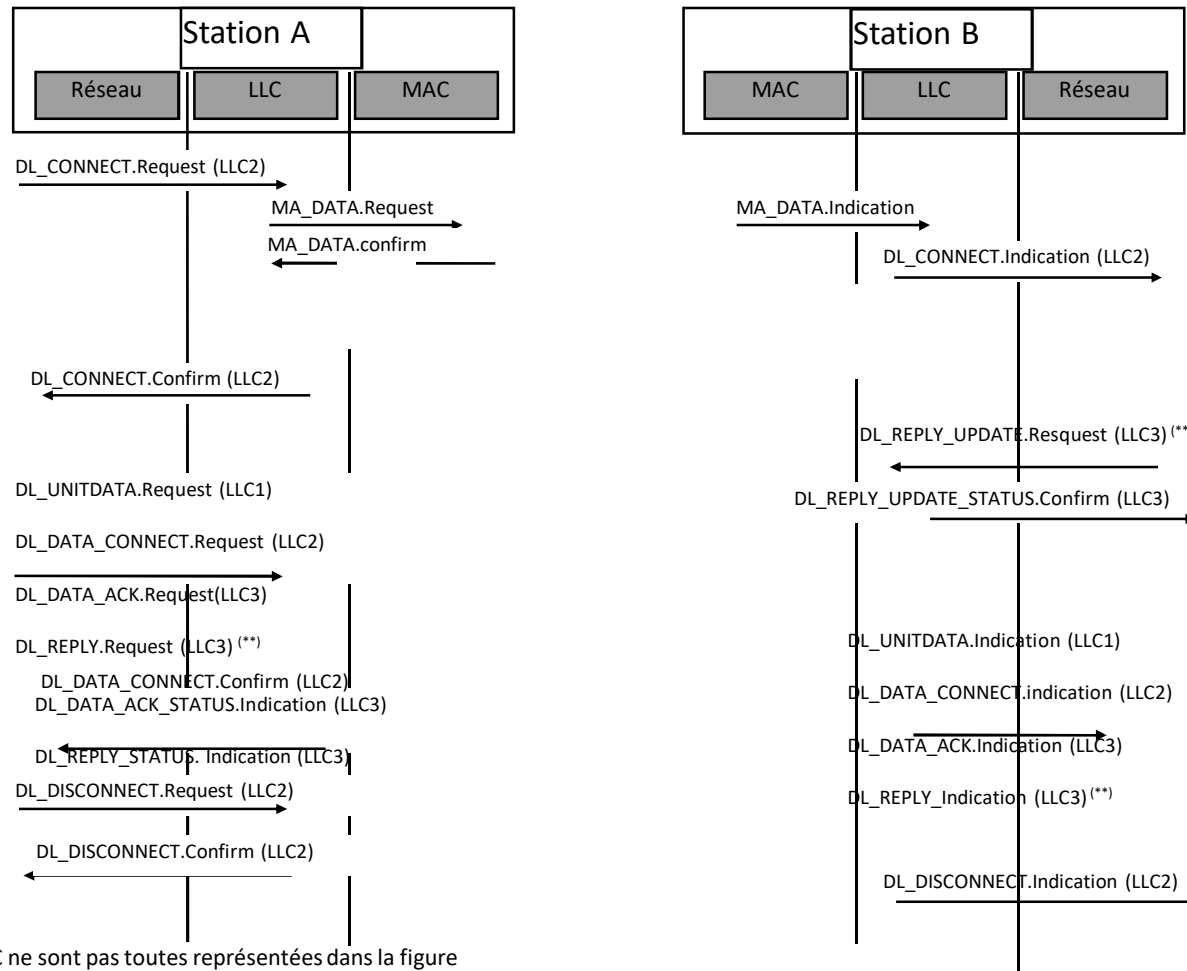
(e) Timeout recovery

# Primitives LLC



**Primitives d'appel de service avec connexion**

# Exemple d'échange de primitives LLC



N.B : -Les primitives MAC ne sont pas toutes représentées dans la figure

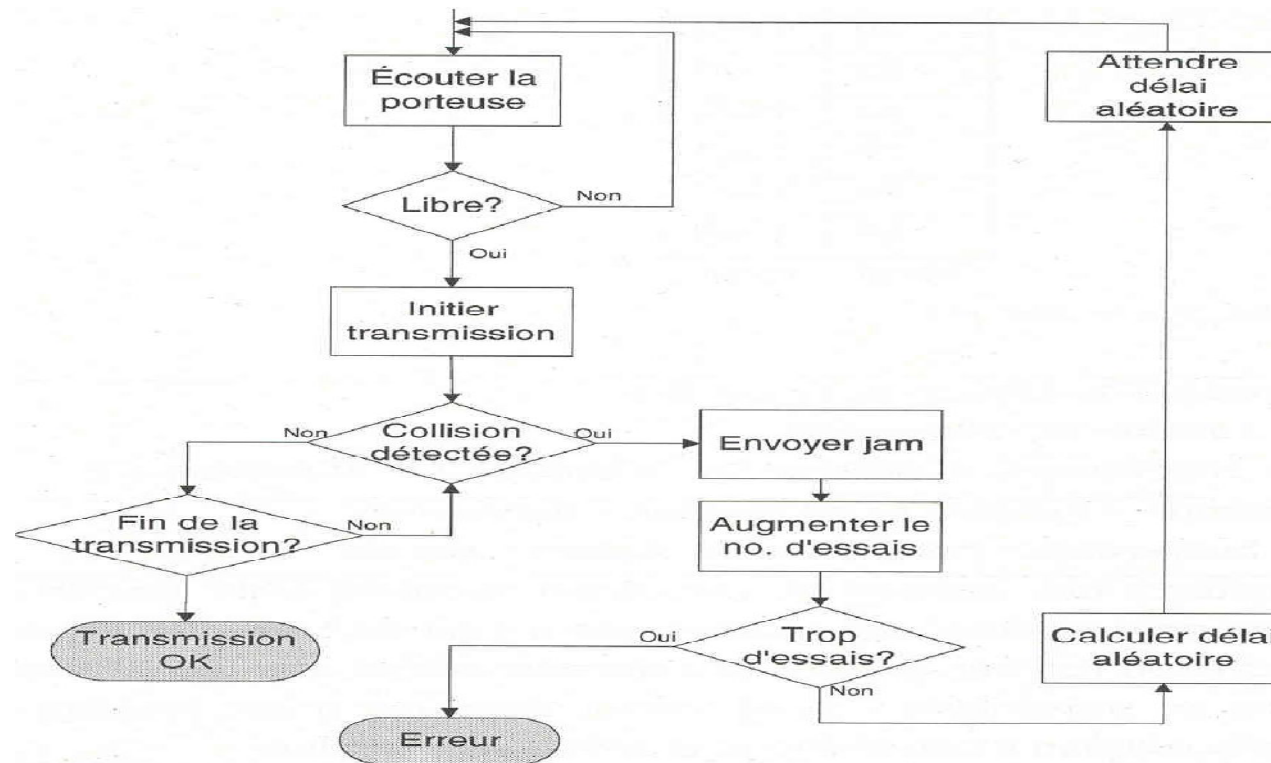
-Les primitives DL\_REPLY\_X permettent au récepteur de renvoyer des données en réponse, en même temps que l'ack.

- Les primitives LLC2 pour le contrôle de flux ne sont pas représentées

- Les primitives STATUS sont équivalentes à une confirmation

# Les normes IEEE 802.3

- Méthode d'accès CSMA/CD

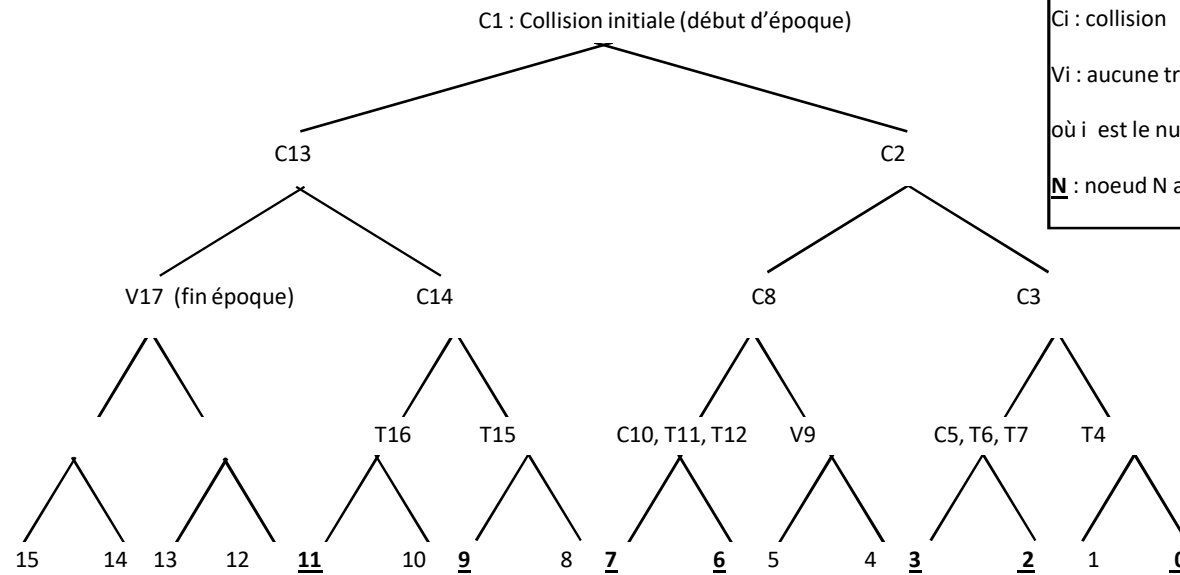


- algorithme de reprise, BEB ("Binary Exponential Backoff"):  
à la N ième collision ( $N \leq 16$ ); une nouvelle tentative sera effectuée après  $V * 51,2 \mu s$  ( $V * \text{Time\_Slot}$ )  $V \in [0..2^{\min(N,10)}]$

# La norme 802.3D

- un autre algorithme de reprise déterministe (DCR : « Deterministic Collision Resolution »)
  - assure un délai maximum de transmission.
  - basé sur le principe de résolution en arbre binaire
  - chaque station possède un index unique. Avec chaque index un message peut être transmis au sein d'une époque.
  - une époque : temps qui s'écoule entre une collision initiale et la fin de la résolution de celle-ci. Elle débute après la première collision.

# La norme 802.3D

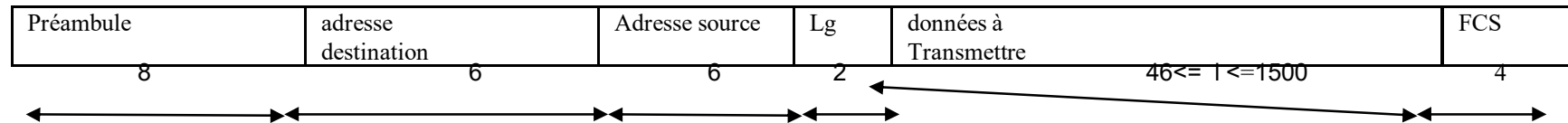


Ti : transmission d'un message  
 Ci : collision  
 Vi : aucune transmission (tranche vide)  
 où i est le numéro de tranche  
N : noeud N ayant un message à transmettre

Borne d'une époque =  $N * T + (N-1) * TC$  où N : nombre de noeuds ; T : temps de transmission d'une trame ; TC : tranche canal



# Trame 802.3



## •Primitives de service

- MA\_UNITDATA.Request (*adresse\_destination*, *adresse\_source*, *MA\_SDU*) ;
- MA\_UNITDATA-STATUS.indication(état (transmission\_OK, collisions\_excessives))
- MA\_UNITDATA.Indication (*adresse\_destination*, *adresse\_source*, *MA\_SDU*, état (Reception\_OK, longueur\_incorrecte, erreur\_FCS, erreur\_alignement))

## •Evolution de la norme

Supplement	Year	Description
802.3a	1985	10 BASE-2 thin Ethernet
802.3c	1985	10 Mbps repeater specification
802.3d	1987	Fiber Optic Inter Repeater Link
802.3i	1990	10 BASE-T twisted pair
802.3j	1993	10 BASE-F fiber optic
802.3u	1995	100 BASE-T Fast Ethernet and auto negotiation
802.3x	1997	Full duplex standard
802.3z	1998	1000 BASE-X Gigabit Ethernet – SX, LX, CX
802.3ab	1999	1000 BASE-T Gigabit Ethernet over twisted pair
802.3ac	1998	Frame size extension to 1522 bytes for VLAN tag
802.3ad	2000	Link aggregation for parallel links

# Fast Ethernet : Principes (1)

- Fast Ethernet = Ethernet 10 Mb/s en 10 fois plus rapide avec le soucis principal de **ménager l'existant**
  - 802.3u  $\Leftrightarrow$  extension de 802.3
  - Câblage structuré existant **pérennisé** (pour fibres et paires torsadées)
  - Par contre **disparition du coaxial** (non liée aux performances)
    - Mais pour confidentialité et protection contre erreur utilisateur
- Évolution du CSMA/CD à 100 Mb/s
  - Reste simple, efficace, mais non déterministe
  - Gestion des collisions, format et longueur de trames **identiques**
  - RTD à 5.12  $\mu$ s et Inter-trames 0.96  $\mu$ s (96 temps bit)
  - Full-Duplex : **Plus de contrainte du CSMA/CD** (Pont, switch)

# Fast Ethernet : Principes (2)

- Les supports normalisés
  - Paire torsadée
    - 100 Base TX câble de catégorie 5 avec 2 paires
    - 100 Base T4 câble de catégorie 3,4 et 5 avec 4 paires
  - Fibre optique
    - 100 Base FX => 2 fibres multimodes 62.5/125
- Codage 4B/5B pour 100 Base X
- Codage 8B/6T pour 100 Base T4

# Gigabit Ethernet : Buts en 1996

- Permettre les connexions half et full-duplex
- Utilisation du même format de trame Ethernet 802.3
- Utilisation de la méthode d'accès CSMA/CD avec 1 seul répéteur par domaine de collision
- Assurer compatibilité avec les technologies 10/100 base
- 3 objectifs spécifiques au niveau des liens :
  - Fibre multimode avec un maximum de 550 mètres
  - Fibre monomode avec un maximum de 3 kms (extensible à 5 kms)
  - Câble cuivre allant au moins à 25 mètres.
- Ratification des standards Gigabit Ethernet
  - IEEE 802.3z : 1000 base-X (lx,sx,cx), Juin 1998
  - IEEE 802.3ab : 1000 base-T (min. UTP), 26 Juin 1999
  - IEEE 802.3ae : 10 Gigabit Ethernet en 2002
  - IEEE 802.3ba : 40 et 100 Gigabit Ethernet en 2010

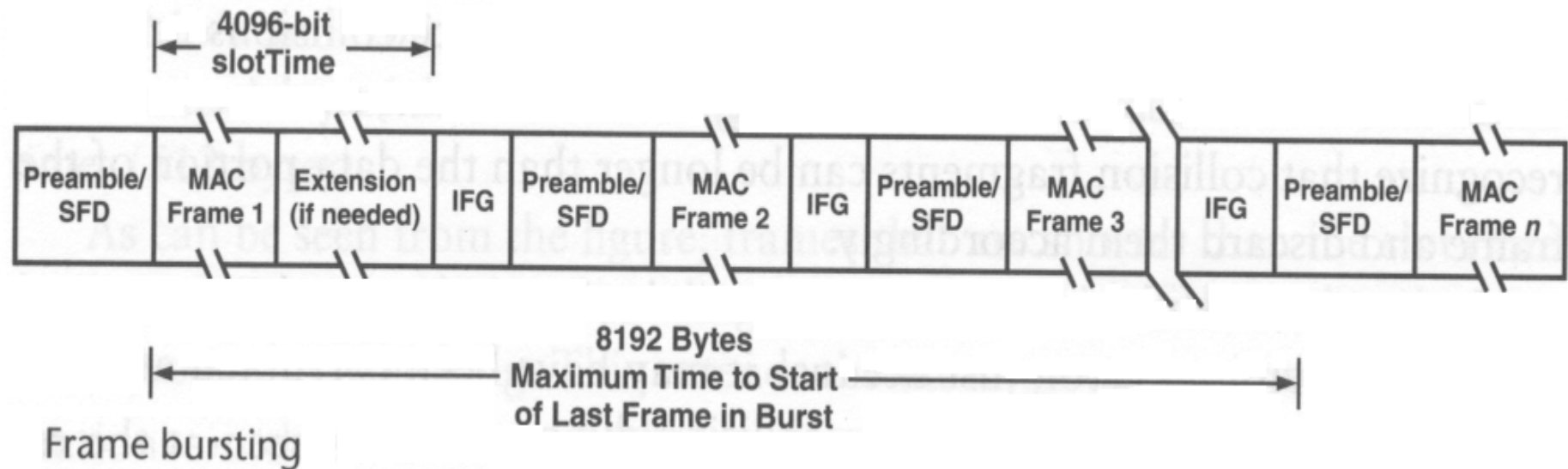
# Gigabit Ethernet

- Trame IEEE 802.3 : Rappel
  - Half duplex : méthode d'accès CSMA/CD
  - Full duplex : pas de collision
  - Taille des trames : 64 octets à 1500 octets
  - Délai inter-trame : 96 bits
  - RTD est divisé par 100, par 10 pour Ethernet 100
  - Slot Time : 512 bits (64 octets)
- débit ↗ ⇨ diamètre du domaine de collision ↘
  - 10Mbps ⇨ 2500m
  - 100Mbps ⇨ 250m
  - 1000Mbps ⇨ 25m : aucun intérêt

# Gigabit Ethernet : CSMA/CD

- Pour conserver un  $\emptyset$  de domaine de collision à 200m (comme le 100 Base ...), on augmente le slot time (temps d'acquisition du canal)
  - Taille du Slot Time passe de 64 à 512 octets
    - Taille minimale trame reste à 64 octets
    - Extra carrier extension si taille inférieure à 512 octets.
    - Trames de taille > 512 octets non affectées
    - Packet bursting : agrégation des petites trames pour optimiser la bande passante.
- Mêmes adresses que IEEE 802.3

# Gigabit Ethernet : Frame bursting (2)



# Gigabit Ethernet : CSMA/CD (3)

- Développement de matériel proche du répéteur appelé "**buffered distributor**" pour éliminer les contraintes du CSMA/CD
- Le "buffered distributor" est un répéteur **full-duplex** sans adresse MAC (comme répéteur) avec 2 ports ou plus (multi-répéteur),
- Il répète les trames sur tous les ports, sauf d'ou elles viennent
- Différence avec le répéteur : possibilité de mémoriser (tampons) une ou plusieurs trames avant de les envoyer sur le lien
- Appelé "CSMA/CD in a box."



# LES NORMES IEEE 802.11

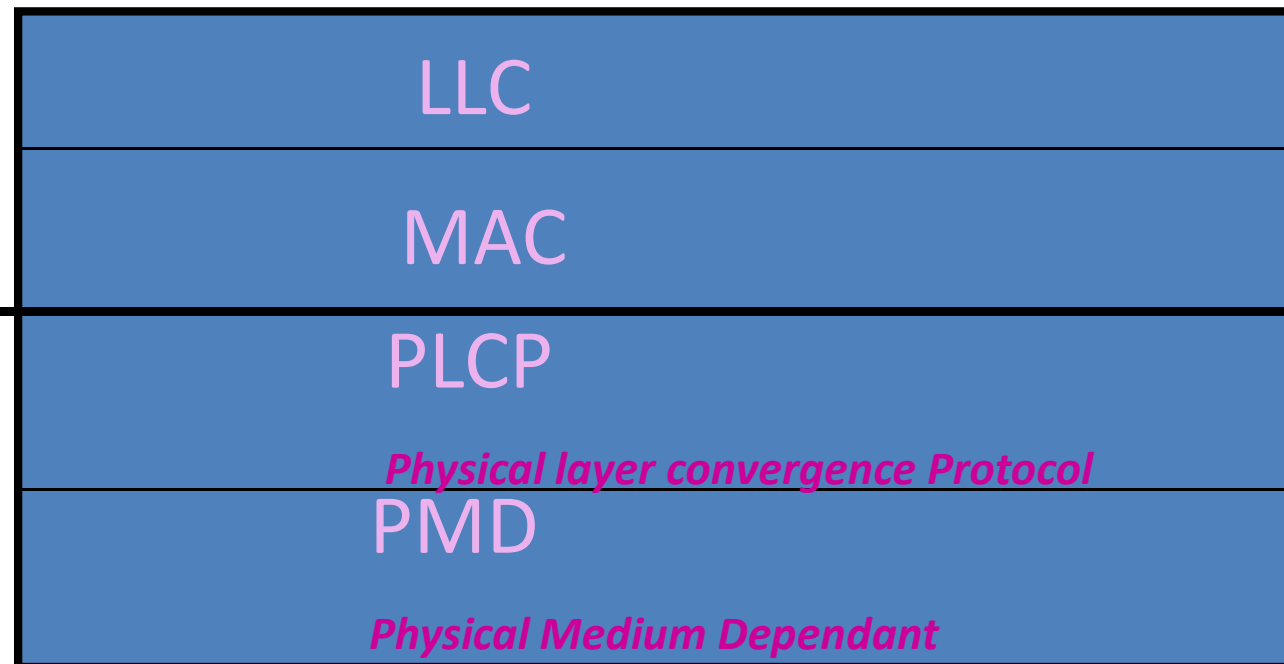
<b>802.11 a</b>	utilisation de la technologie OFDM au niveau physique pour atteindre des débits de 54 Mbps dans la bande U-NII de 5 GHz
<b>802.11 b</b>	Couche physique jusqu'à 11Mbit/s dans la bande ISM des 2,4 GHz
<b>802.11 d</b>	permet aux points d'accès de communiquer l'information sur les canaux radio disponibles et les niveaux de puissances acceptables selon les restrictions des différents pays.
<b>802.11 e</b>	qualité de service (QoS) pour applications multimédia. S'applique à la norme 802.11 a, b et g.
<b>802.11 f</b>	Interopérabilité entre les points d'accès. Protocole Inter Access Point Protocol
<b>802.11 g</b>	54 Mbit/s dans la bande de 2.4 GHz. Utilise la modulation OFDM (Orthogonal Frequency Division Multiplexing). Compatible avec la norme IEEE 802.11b.
<b>802.11 i</b>	Amélioration de la sécurité S'applique aux standards 802.11 a, b et g.

# Les normes IEEE 802.11

- Couche Physique

*liaison*

*Physique*



*PLCP* écoute le support et fournit à la couche Mac un Clear channel assesment

*PMD* encodage des données et modulation

# Les normes IEEE 802.11

- Méthodes d'accès (MAC)

- ❖ **DCF** Distributed Coordination Fonction

- **CSMA/CA Carrier Sense Multiple Access/Collision Avoidance**

**impossible d'émettre et d'écouter en même temps**

- **algorithme du back-off**

- ❖ **PCF** Point Coordination Fonction

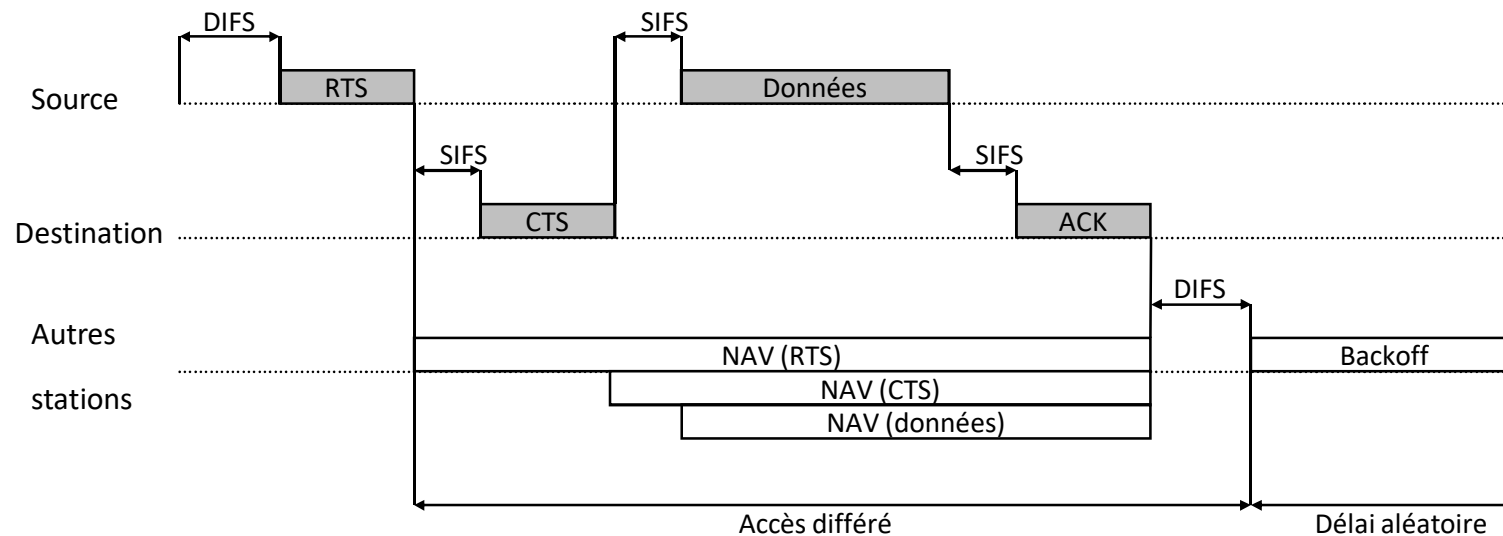
- Point Coordination Fonction (PCF)
  - Les stations de base ont la charge de la gestion de l'accès au canal dans leur zone de couverture pour les mobiles qui leur sont rattachés adapté pour les applications temps réels.

# Méthode d'accès/Topologie

- Mode ad-hoc
  - Uniquement DCF
- Mode infrastructure (avec points d'accès)
  - DCF et PCF

# DCF (rappel)

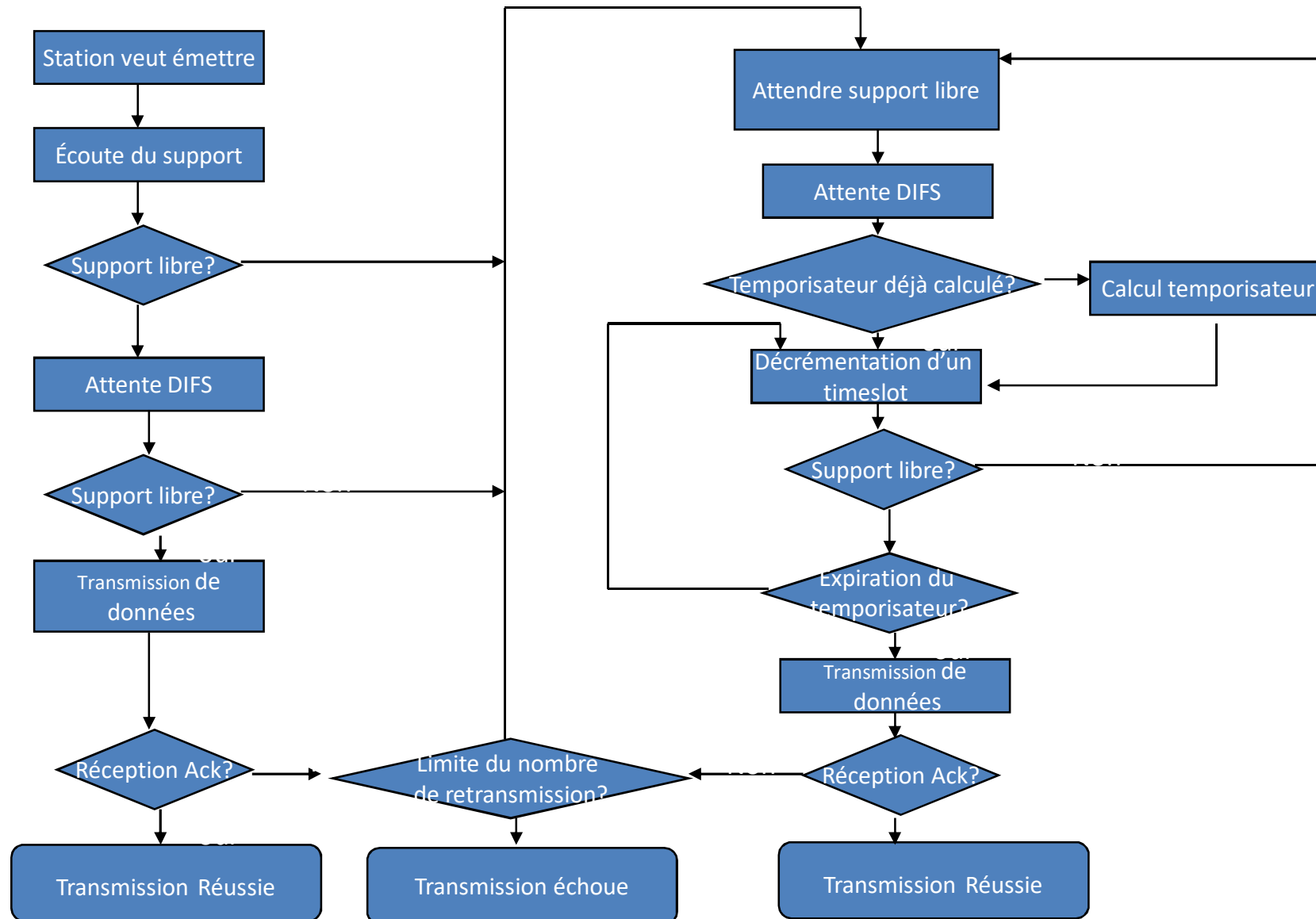
- transmission CSMA/CA & "Virtual Carrier Sensing"



- Slot = 50μs

- SIFS : « Short Inter Frames Space » = 28μs, valeur minimale pour qu'une station puisse changer du mode émission vers le mode réception (dans le cadre d'un même dialogue, le récepteur gagne le droit d'accès).

- DIFS « Distributed Inter Frame Space » = SIFS + 2 \* Slot = PIFS + Slot = 128μs, utilisé lorsqu'une station veut commencer une nouvelle transmission



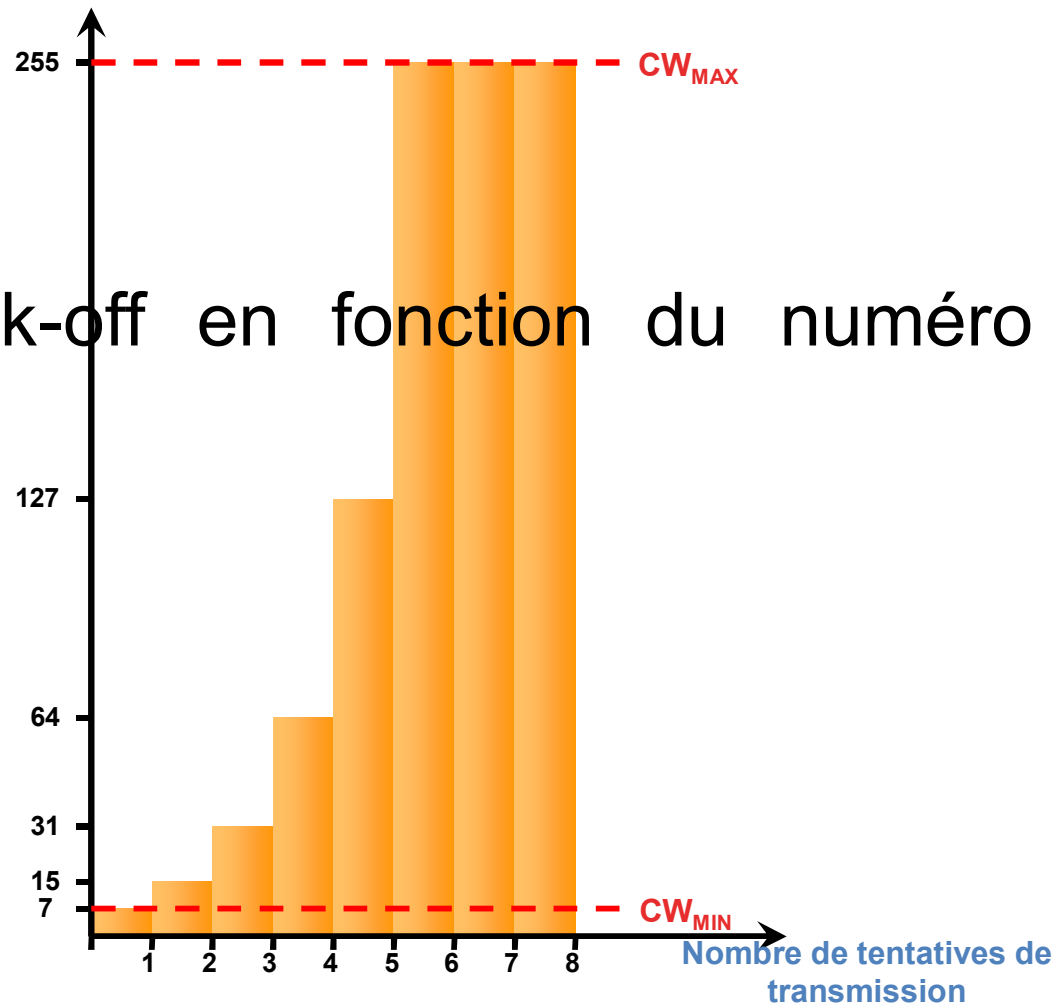
# Backoff

- Temps découpé en slotTime
- Fenêtre de contention : CW ( $CW_{min} \leq CW \leq CW_{max}$ )  
( $CW_{min}$  et  $CW_{max}$  prédéfinis dans la norme)
- Une station écoute le support avant tout essai de transmission
  - Si le support est libre après un DIFS : transmission
  - Sinon elle calcule un temporisateur  
 $BO = \text{random}(0, CW) \times \text{slotTime}$
  - CW initialisé à  $CW_{min}$
  - CW doublée entre 2 tentatives de transmission en échec
- A chaque collision, la taille de la fenêtre de contention (CW) double jusqu'à la valeur  $CW_{max}$

# Intervalles de back-off / du n° tentative

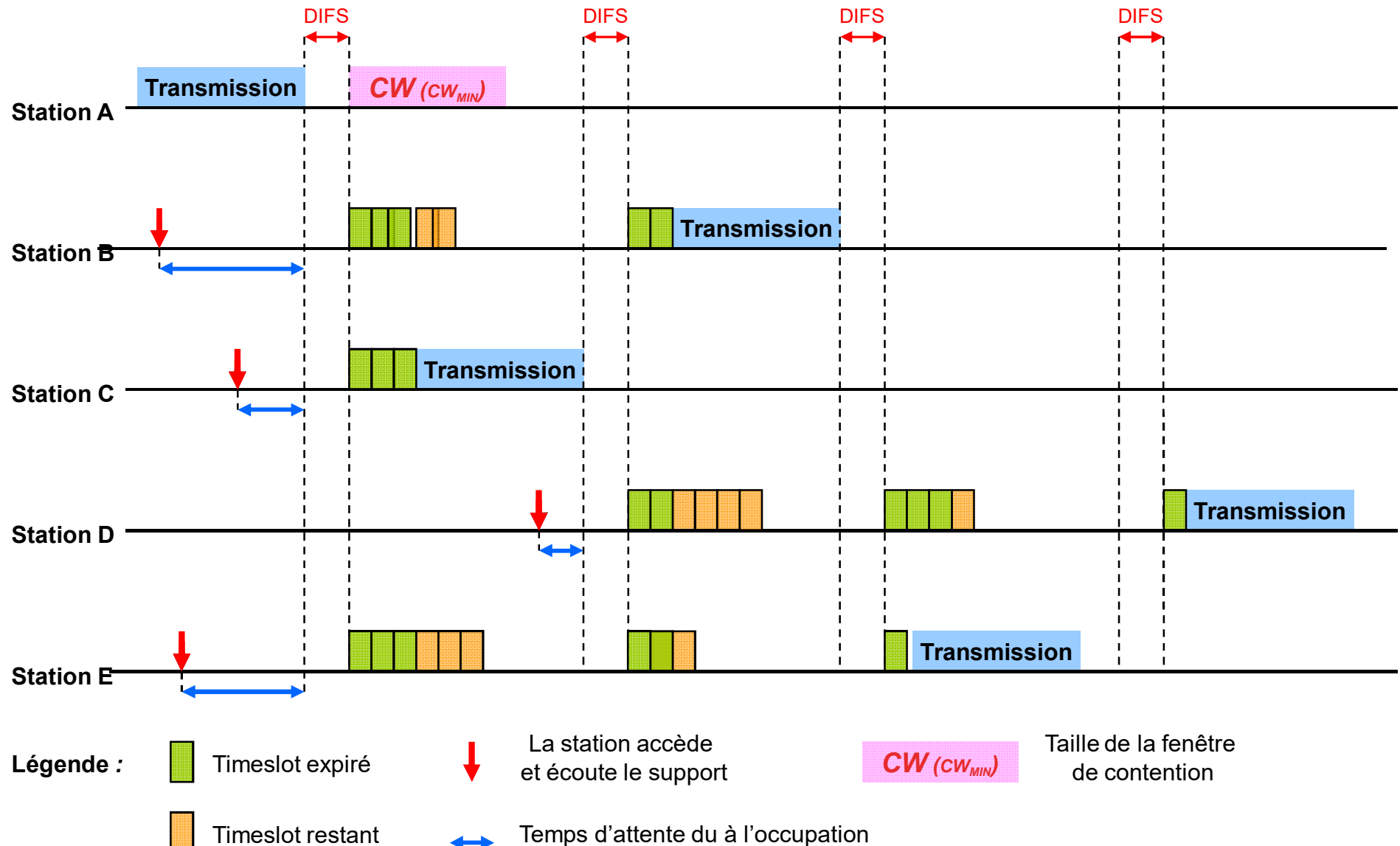
Intervalles de back-off en fonction du numéro de tentative

Taille de la fenêtre  
de contention

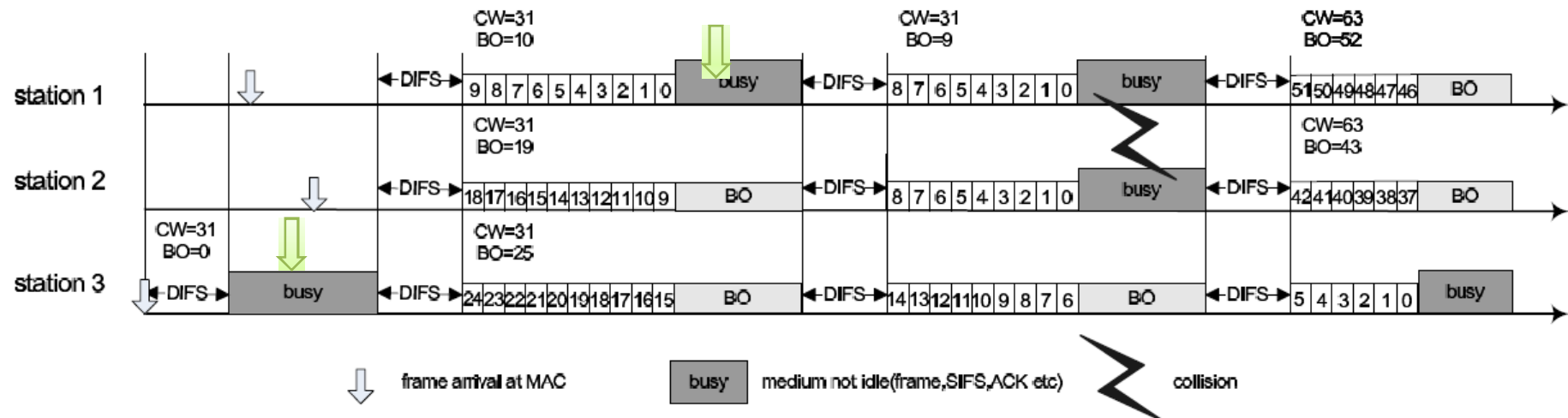




# Backoff (Exemple)



# Backoff (Exemple)



# Couche liaison : autres fonctions

- Accès au réseau
- authentification et sécurité
- Fragmentation – réassemblage
- Handover
- Économie d'énergie
- Performances
- Trames 802.11

# Connexion au réseau et association

- Allumer station → **phase de découverte**
  - Découvrir l'AP et/ou les autres stations
- Présence détectée → **rejoindre le réseau**
  - Service Set Id (SSID) : nom du réseau de connexion
  - Synchronisation
  - Récupération des paramètres de PHY
- Négocier la connexion
  - Authentification & Association

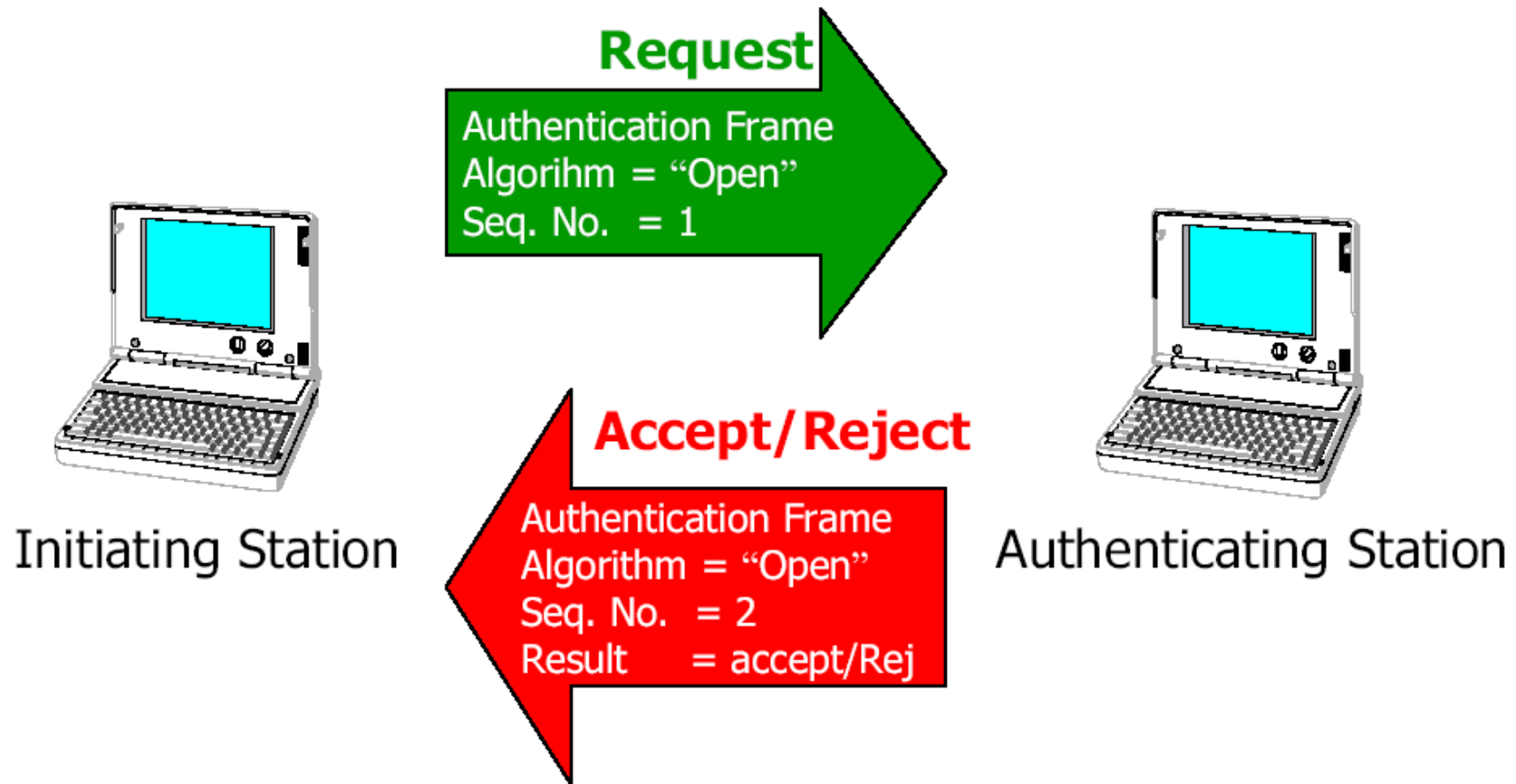
# Phase de découverte du réseaux

- Phase d'écoute
  - écoute passive / écoute active
- Écoute **passive**
  - La station **attend de recevoir** une trame balise (Beacon)
  - A la réception de Beacon prendre les paramètres (SSID & autres)
- Écoute **active**
  - La station **envoie directement** une requête d'association (Probe Request Frame)
  - **Attendre** la réponse de l'AP ou des autres stations

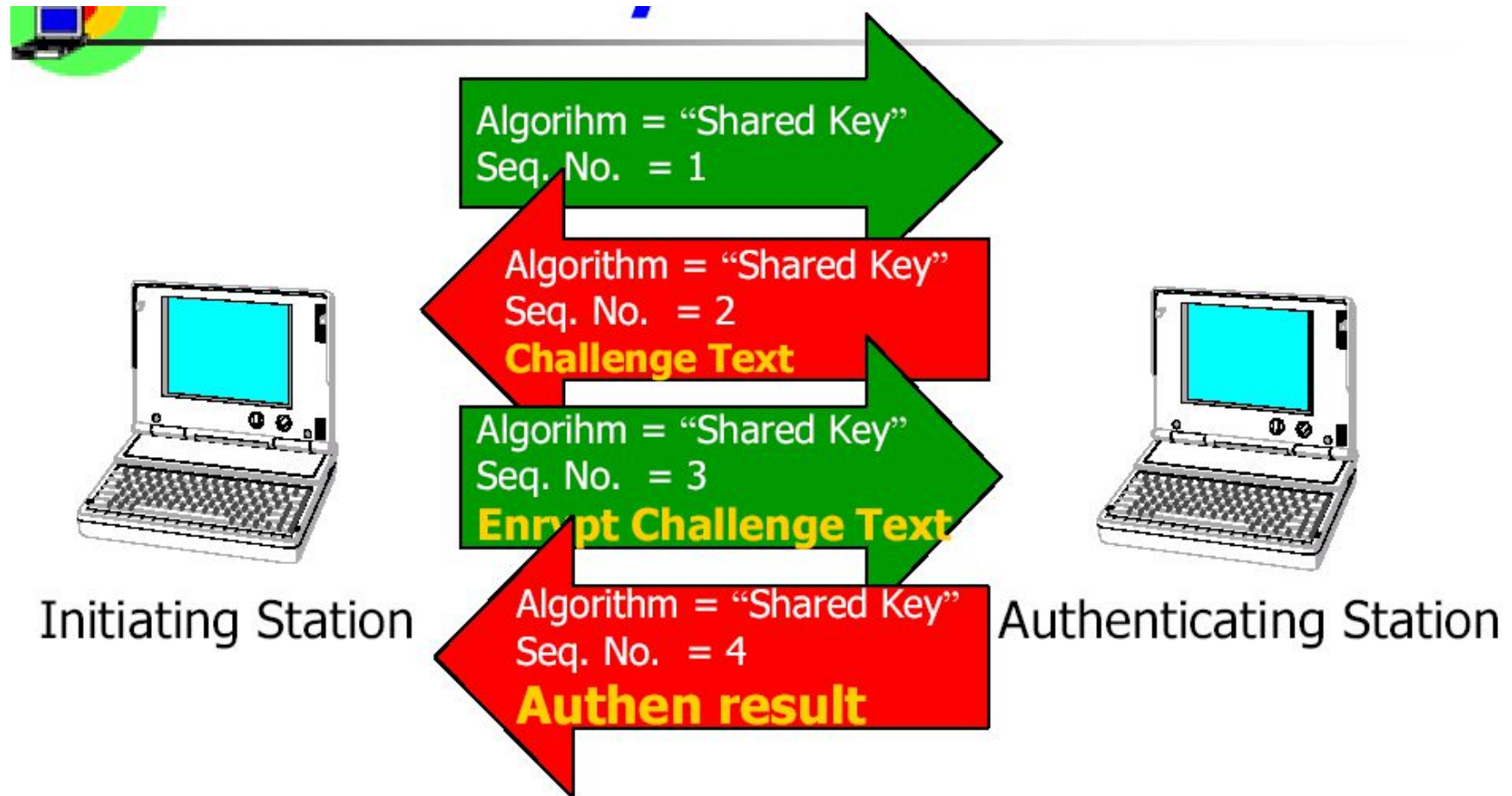
# Authentification-Sécurité

- Se protéger contre les accès non autorisés
- Open system authentication
  - Mode par défaut
- Shared key authentication
  - Plus haut degré de sécurité
  - Echange de trame plus rigoureux
  - Utilise le mécanisme WEP (Wired Equivalent Privacy)

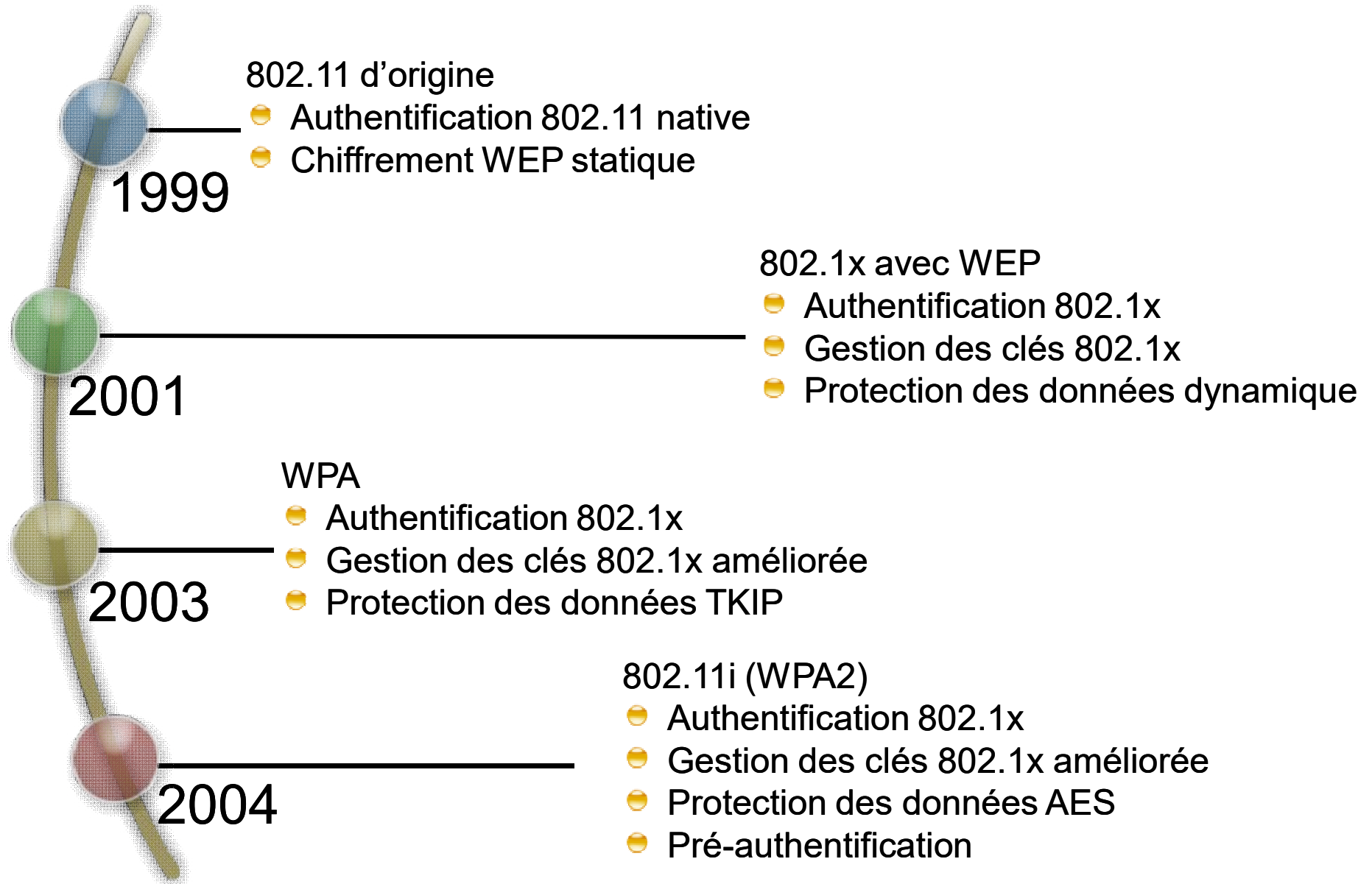
# Open System Authentication



# Shared Key



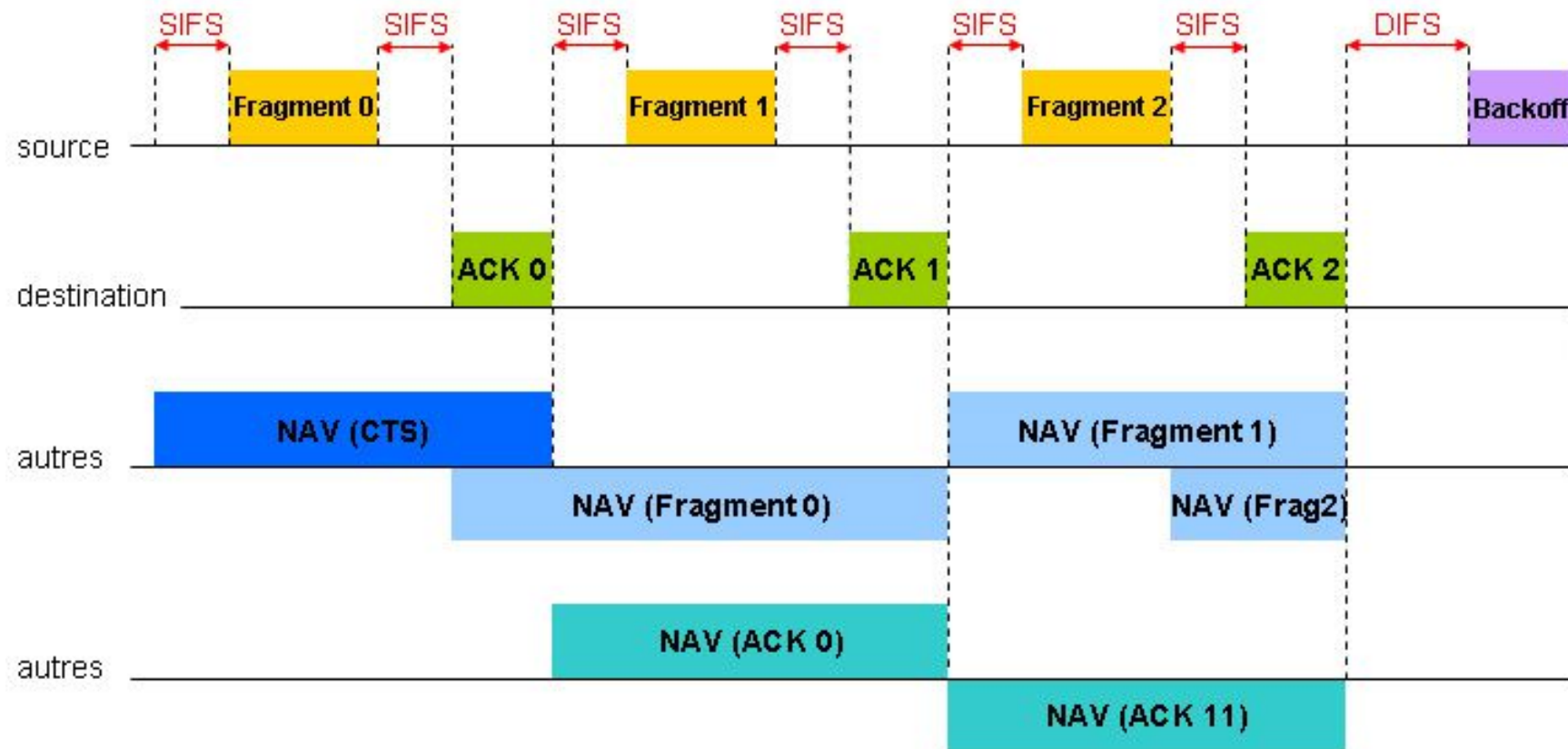




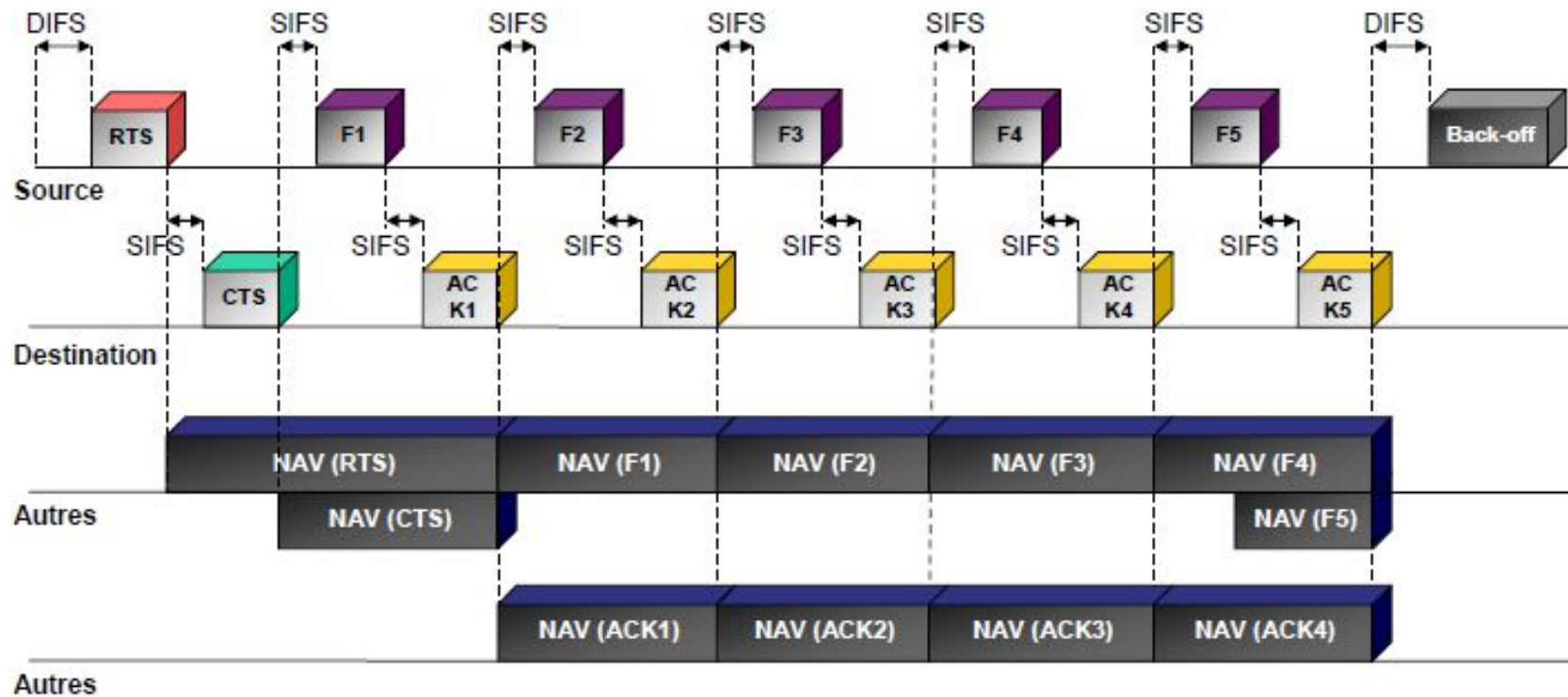
# Fragmentation - réassemblage

- Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil, appelée `Fragmentation_Threshold`
- Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle
  - Le support n'est libéré qu'une fois tous les fragments transmis avec succès
  - Si un ACK n'est pas correctement reçu, la station arrête de transmettre et essaie d'accéder de nouveau au support et commence à transmettre à partir du dernier fragment non acquitté
  - Si les stations utilisent le mécanisme RTS / CTS, seul le premier fragment envoyé utilise les trames RTS / CTS

# Fragmentation - réassemblage



# Fragmentation - réassemblage



# Handover

- passage d'une cellule à une autre sans interruption de la communication
  - Le standard **ne définit pas** de **handover** de **roaming** dans les réseaux 802.11 (coupures de quelques secondes)
  - 802.11f retirée en février 2006 (roaming lent, non finalisée, désintéressement des acteurs).
  - 802.11r (coupures de tout au plus 50 ms)
- Le standard définit **quelques règles** à respecter
  - Synchronisation
  - Écoute active et passive
  - Mécanismes d'association et de réassociation, qui permettent aux stations de choisir l'AP auquel elles veulent s'associer
- **Sécurité renforcée** pour éviter :
  - qu'un client ne prenne la place d'un autre
  - Qu'il n'écoute les communications d'autres utilisateurs

# Économie d'énergie

- **Problème principal** des terminaux mobiles: faible autonomie de la batterie
  - Mode d'économie d'énergie prévu par le standard
- 2 modes de travail pour le terminal
  - **Continuous Aware Mode**
    - Fonctionnement par défaut
    - La station est tout le temps allumée et écoute constamment le support
  - **Power Save Polling Mode**

# Power Save Polling

- Permet une économie d'énergie
- **Géré** par le point d'accès
  - L'AP tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie
  - Stocke toutes les données qui leur sont adressées
  - Les stations en veille s'activent périodiquement pour recevoir une trame **TIM** (Traffic Information Map), envoyée par l'AP
    - Si l'AP possède des données destinées à la station, celle-ci envoie une requête à l'AP : Polling Request Frame
- Entre les trames **TIM**, les terminaux retournent en **mode veille**

# Format de Trame

Préambule	En-tête PLCP	Données MAC	CRC
-----------	-----------------	-------------	-----

## Préambule

- Synch : 80 bits alternant 0 et 1, utilisée pour sélectionner l'antenne appropriée, et pour corriger l'offset de fréquence et de synchronisation.
- SFD : Le Start Frame Delimiter (16 bits) 0000 1100 1011 1 101,

## En-tête PCLP (Trame 802.11)

transmis à 1 Mbps et contient des informations logiques utilisées par la couche physique pour décoder la trame :

- Longueur de mot du PLCP\_PDU : nombre d'octets du paquet  
→ utile à la couche physique pour détecter correctement la fin du paquet.
- Fanion de signalisation PLCP : information de taux, encodé à 0,5 Mbps, incrémenté de 1 Mbps à 4,5 Mbps
- Champ d'en-tête du contrôle d'erreur : détection d'erreur CRC 16 bits.



# Données MAC

1	2	3	4	5	6	7	8
FC		Durée/ID		Adresse 1			
(Adresse 1)		Adresse 2					
Adresse 3						SC	
Adresse 4							
Corps de la Trame							
				CRC			

# Frame Control

- **Version** : 2 bits permettant de connaître la version 802.11
- **Type/sous-type** : 6 bits qui définissent le type de trames :
  - 00 Gestion : échange d'info de gestion tel que requête/réponse de (ré)association, Balise, ATIM, Authentification....
  - 01 Contrôle : pour le contrôle d'accès au support (RTS, CTS, ACK, PS
  - 10 données : transfert des données avec ou sans ACK
- **To (From) DS** : mis à 1 quand une trame est adressée à (provient de) l'AP
- **More Fragment** : mis à 1 quand 1 fragment est suivie d'un autre fragment
- **Retry** : Mis à 1 si la trame a déjà été transmise (le récepteur peut savoir si un ACK s'est perdu)
- **Power Management (gestion d'énergie)** : la station ayant envoyé ce fragment entre en mode de gestion d'énergie (à 1).
- **More Data (gestion d'énergie)** : permet à l'AP de spécifier à une station que des trames supplémentaires sont stockées en attente.
- **WEP** : ce bit indique que l'algorithme de chiffrement WEP a été utilisé pour chiffrer le corps de la trame.
- **Order (ordre)** : indique que la trame a été envoyée en utilisant la classe de service strictement ordonnée (*Strictly-Ordered service class*). Cette classe est définie pour les utilisateurs qui ne peuvent accepter de changement d'ordre entre les trames unicast et multicast.

# Les adresses

- **Adresse 1** est toujours l'adresse du récepteur (ie. la station de la cellule qui est le récepteur du paquet). Si To DS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station.
- **Adresse 2** est toujours l'adresse de l'émetteur (ie. celui qui, physiquement, transmet le paquet). Si From DS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice.
- **Adresse 3** est l'adresse de l'émetteur original quand le champ From DS est à 1. Sinon, et si To DS est à 1, Adresse 3 est l'adresse destination.
- **Adresse 4** est utilisé dans un cas spécial, quand le système de distribution sans fil (*Wireless Distribution System*) est utilisé et qu'une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, To DS et From DS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire.

# Les adresses

Scénario	Vers DS	De DS	Adresse 1	Adresse2	Adresse 3	Adresse 4
Mode ad -hoc	0	0	DA	SA	BSSID	-
Mode infrastructure De l'AP	0	1	DA	BSSID	SA	-
Mode infrastructure Vers l'AP	1	0	BSSID	SA	DA	-
Mode infrastructure À travers un DS	1	1	RA	TA	DA	SA

**DS:** Distribution System    **AP:** Access Point    **DA:** Destination Address  
**SA:** Source Address    **BSSID:** Basic Service Set Identifier  
**RA:** Receiver Address    **TA:** Transmitter Address

# Autres champs

- **Durée/ID**

Ce champ à deux sens, dépendant du type de trame :

- pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station
- dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

- **SC Contrôle de séquence**

- numéro de fragment
- numéro de séquence

# Trame RTS

<b>FC</b> <b>2 octets</b>	<b>Durée</b> <b>2 octets</b>	<b>RA</b> <b>6 octets</b>	<b>TA</b> <b>6 octets</b>	<b>CRC</b> <b>4 octets</b>
------------------------------	---------------------------------	------------------------------	------------------------------	-------------------------------

- **RA est l'adresse du récepteur de la prochaine trame de données ou de gestion.**
- **TA est l'adresse de la station qui transmet la trame RTS.**
- **Durée est le temps, en microsecondes:**
  - transmission de la trame de gestion ou de données suivante, +
  - trame CTS + trame ACK + 3 SIFS.

# Trame CTS

<b>FC</b> 2 octets	<b>Durée</b> 2 octets	<b>RA</b> 6 octets	<b>CRC</b> 4 octets
-----------------------	--------------------------	-----------------------	------------------------

- **RA est l'adresse du récepteur de la trame CTS**
- **Durée est le temps, en microsecondes:**
  - **trame RTS - trame CTS + SIFS.**

# Plan du cours

Introduction

Technologie des réseaux locaux

Normalisation des réseaux locaux

**Déploiement des réseaux locaux**

Les réseaux sous TCP/IP

Interconnexion de réseaux



# Déploiement des réseaux locaux

- Ethernet
- WiFi
- Plan de câblage

# Composants d'un réseau Ethernet (1)

- **média et connectique**

- 10 Base 5 : Câble coaxial blindé jaune

- 10 Base 2: Cheapernet, câble coaxial non blindé, thin Ethernet

- 1 Base 5 : Starlan 1 Mbits/s, Câblage téléphonique

- 10 Base T : 10 Mbits/s , Twisted-Pair (paires de fils torsadées)

- 10Base F, Fiber Optic

- 10 Base FL, Fibre Link

- 10 Base FB, Fibre Backbone

- 10 Base FP, Fibre Passive (hub passive)

- 100 base T, Twisted Pair ou encore FastEthernet (100 Mbits/s, CSMA/CD)

- 100 Base TX

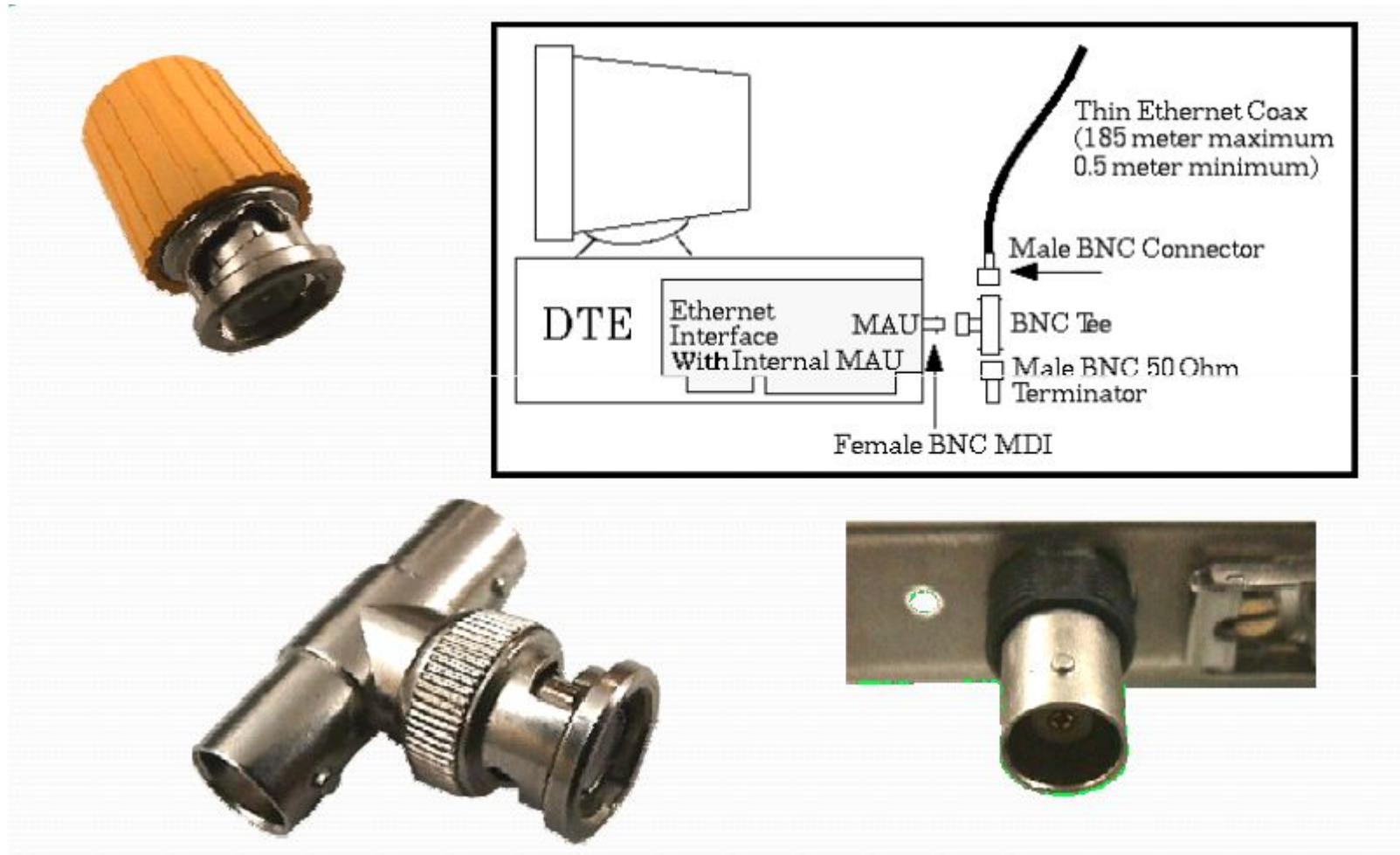
- 100 Base T4

- 100Base FX,

- 1000 Base CX, 1000 Base LX, 1000 Base T, 1000 Base SX

- **Transceiver** : l'émission et de la réception des signaux sur le support
- **Répéteur** : relier deux segments. ( max., selon la norme utilisée).
- **Câble de transceiver** (AUI) relie le transceiver au coupleur
- **Fan out** ou multiplicateur d'accès : connecter plusieurs nœuds à un même transceiver via des câbles AUI (10 BASE 5).

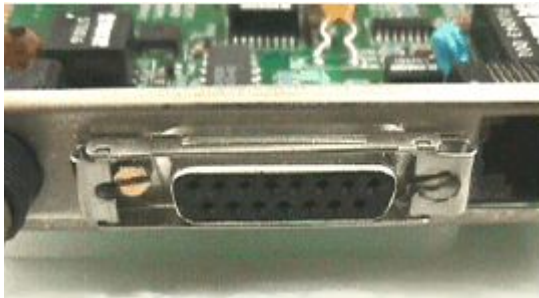
# 10 base 2



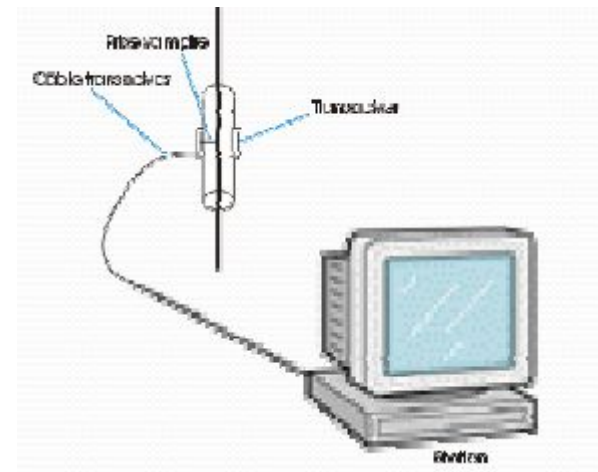
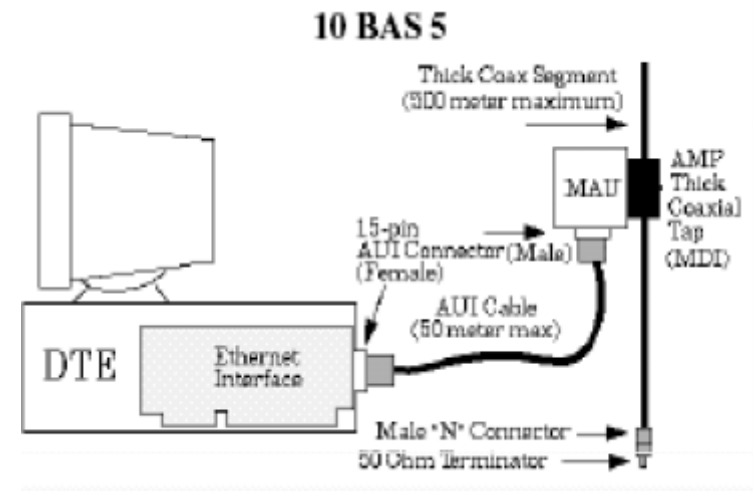
# 10 base 5



Tranceiver



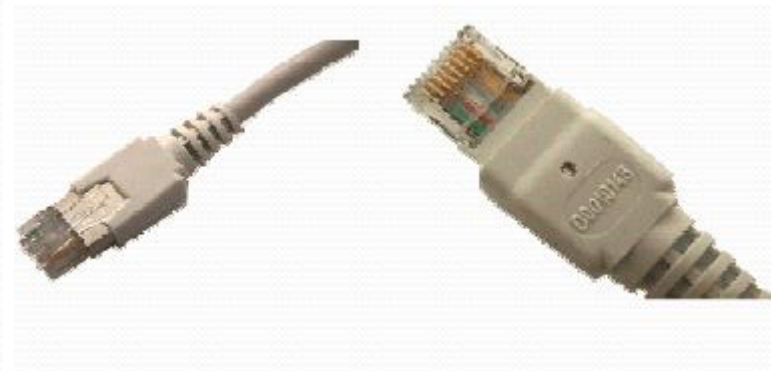
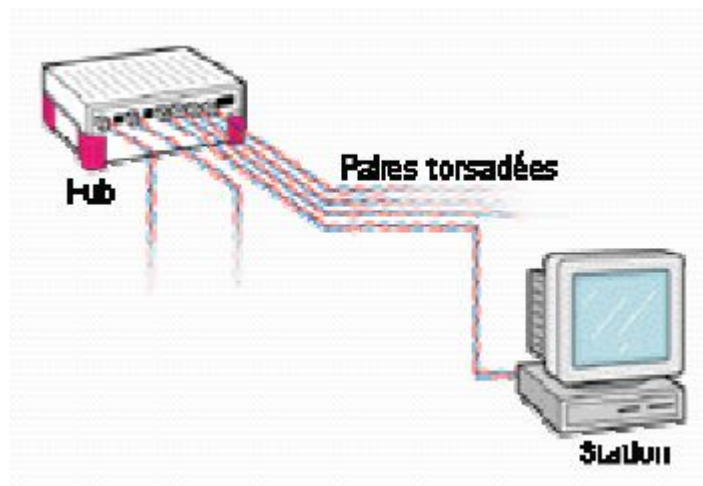
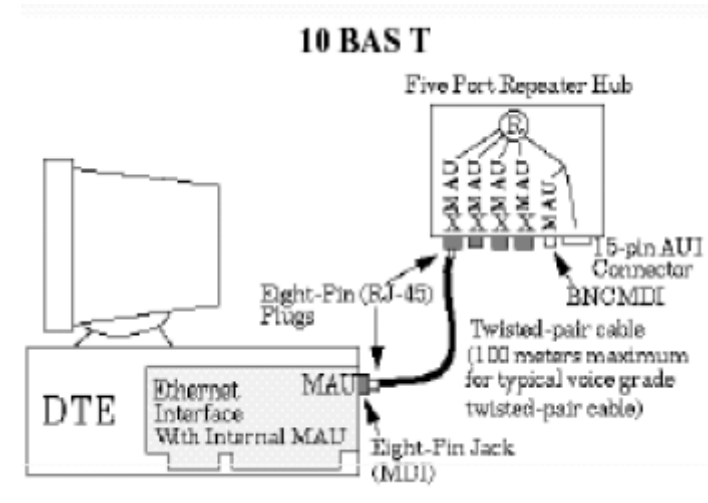
Connecteur AUI



# 10 base T

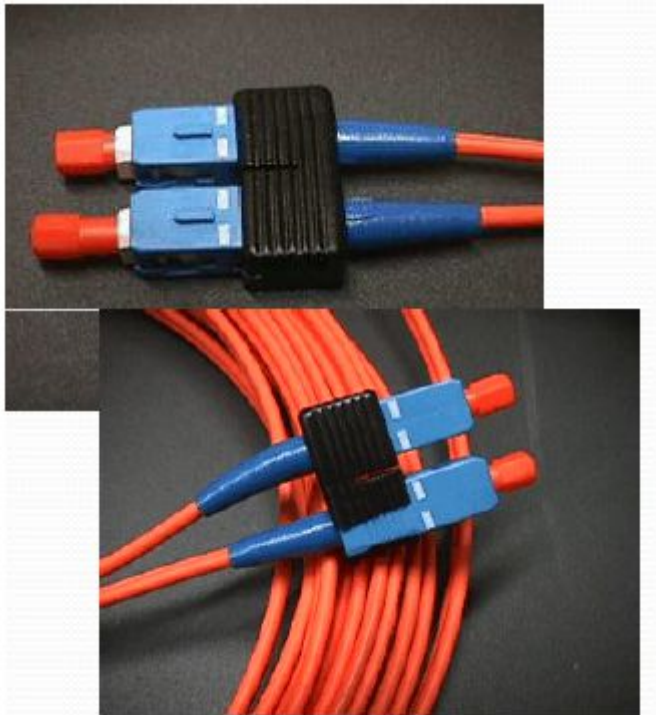


HUBs

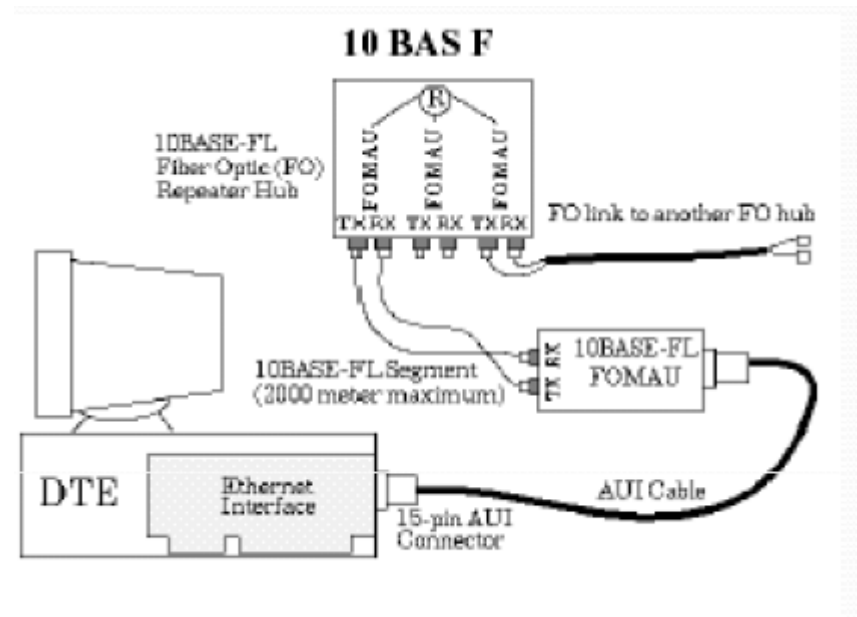


RJ45

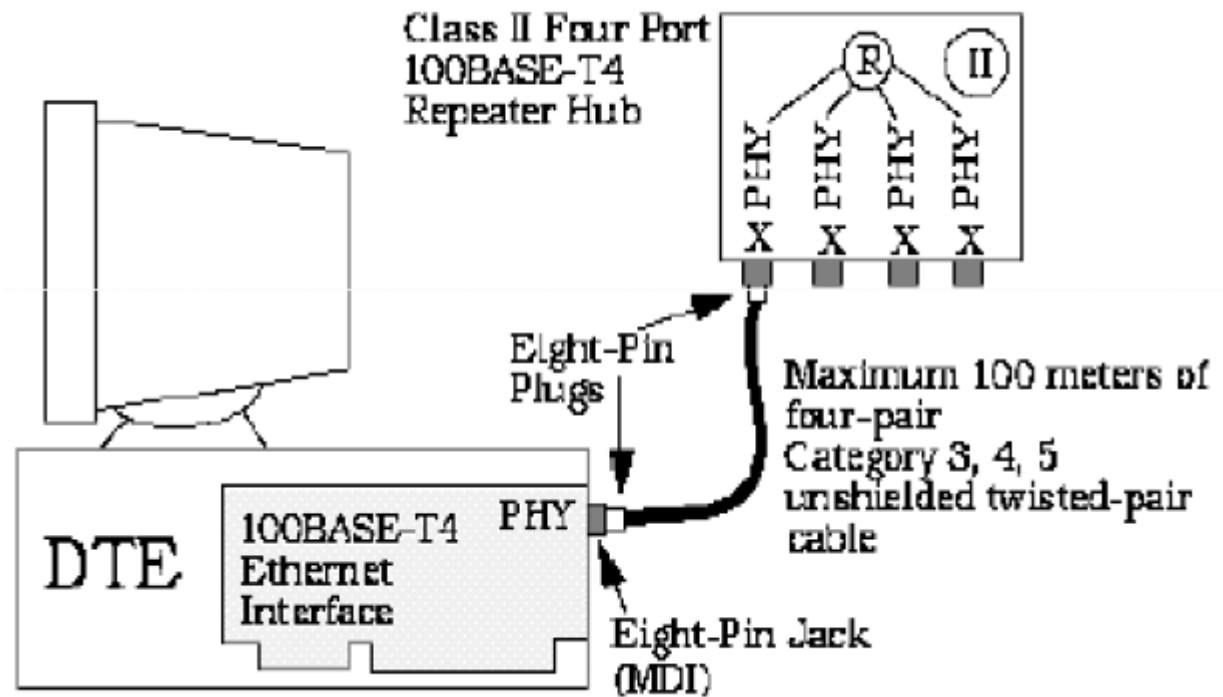
# 10 base F



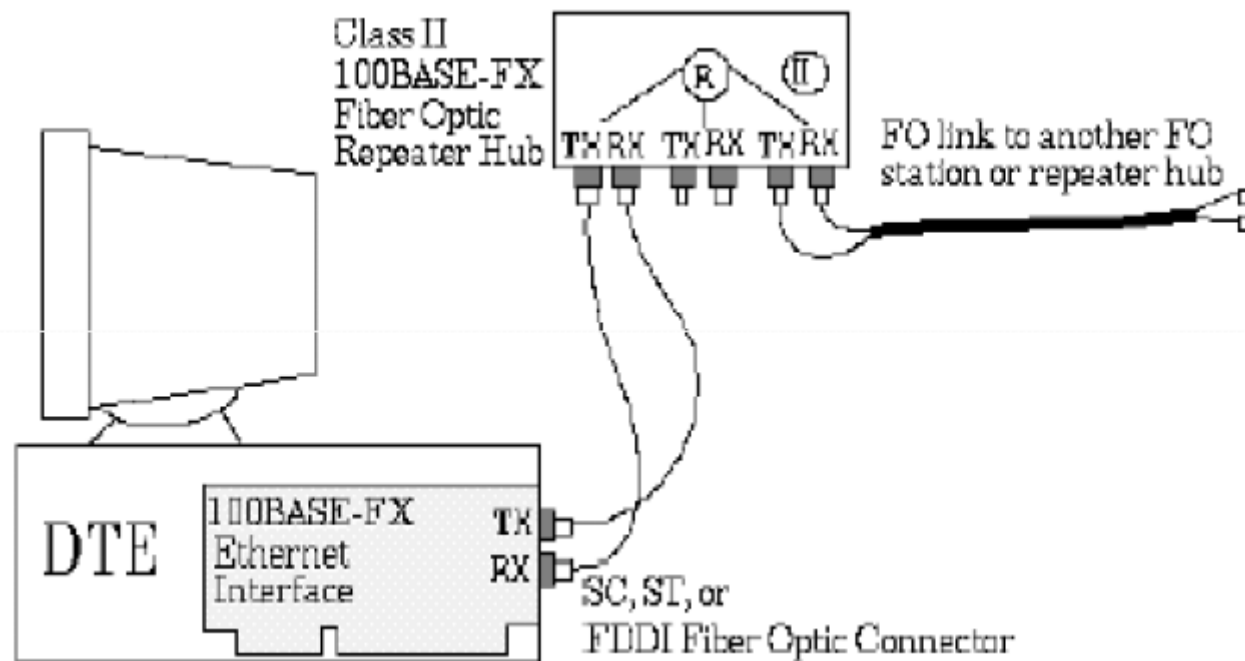
Connecteur Fibre Optique



# Fast Ethernet: 100 base T4



# Fast Ethernet: 100 base FX





# Composants d'un réseau Ethernet (2)

- **Carte coupleur** (NIC : « Network Interface Card ») : chargé de contrôler les communications (fonctions de la couche I et II )

## Emission

- construction de la trame,
- attente de la libération du canal
- Surveillance du canal, en appliquant la méthode d'accès CSMA/CD.

## Réception

- détection de l'arrivée d'une trame,
- réception bit par bit jusqu'au repos du signal,
- vérification que la taille de la trame n'est pas courte ("runt"),
- comparaison des adresses du nœud et de destination, s'ils sont égaux la trame est retenue pour être délivrée à la couche supérieure,
- vérification de l'alignement et du FCS,
- vérification que la taille de la trame n'est pas longue ("jabber"),
- mise à jour du mot d'état indiquant la validité de la transmission.

# Composants d'un réseau Ethernet (2)

- Répéteur (2 ports)
  - Régénération
  - Duplication du signal
    - Augmente la distance entre 2 stations en reliant 2 segments Ethernet
    - Augmente le nombre de machines connectable au réseau
  - **Partitionnement** en cas de collisions excessives (30 à la suite)
  - Ne regarde pas le contenu de la trame
  - N'a **pas d'adresse Ethernet**

Avantages : **sans aucune d'administration**

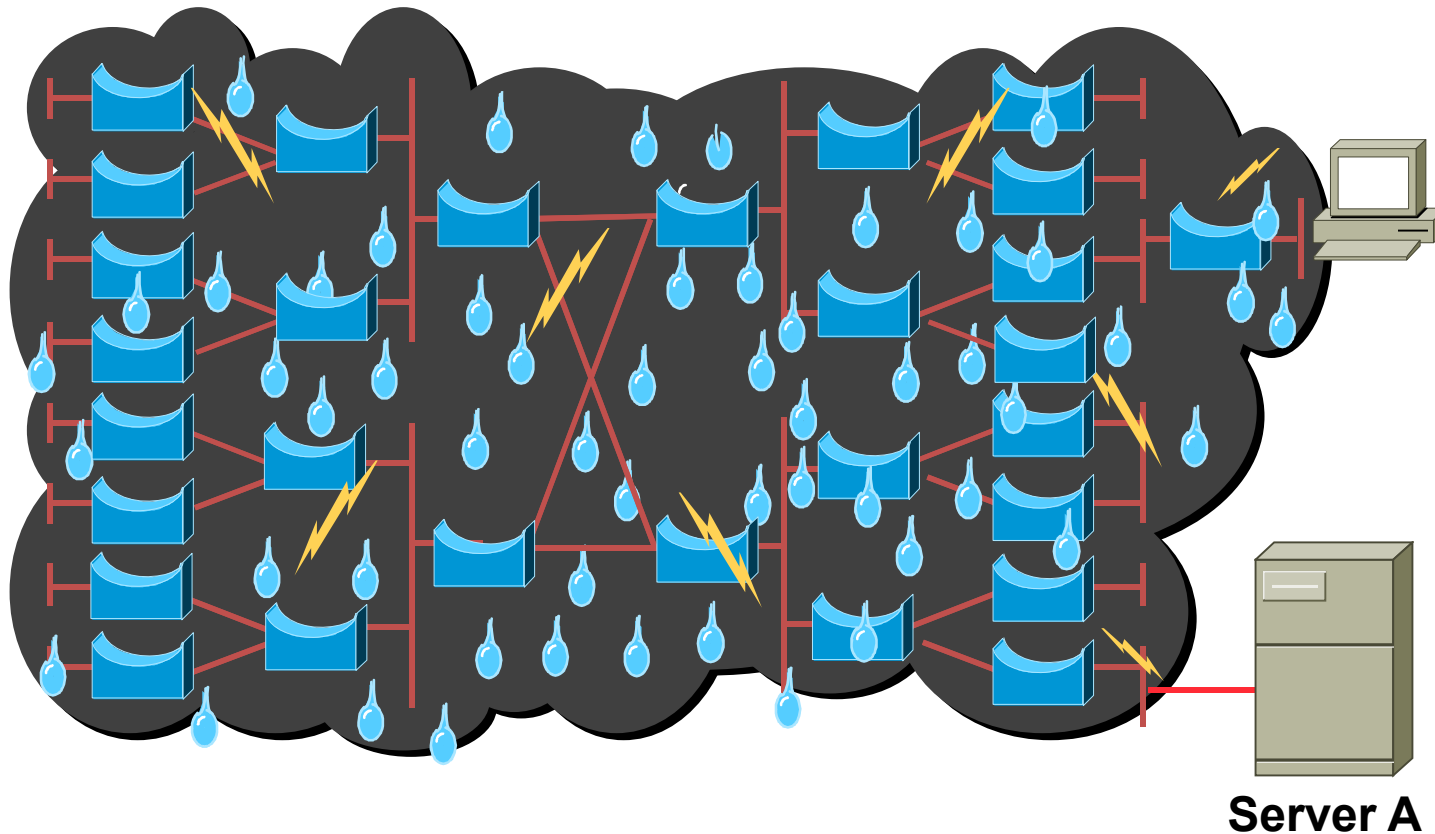
Désavantages : **ne diminue pas la charge et ne filtre pas les collisions (Domaine de Collision)**

- Concentrateur  $\approx$  répéteur moderne (appelé aussi **hub**, multi-répéteur ):
  - Fonction de répéteur avec une **structure en étoile**
  - Les multi-répéteurs n'ont **pas d'adresse Ethernet**
  - **Permet de changer de média**,
    - Avec **éléments modulables** ou non
    - Avec un **type de carte par média**
  - Fonction de **partitionnement pour chacun des ports**
    - Segment en faute automatiquement coupé

## Composants d'un réseau Ethernet (3)

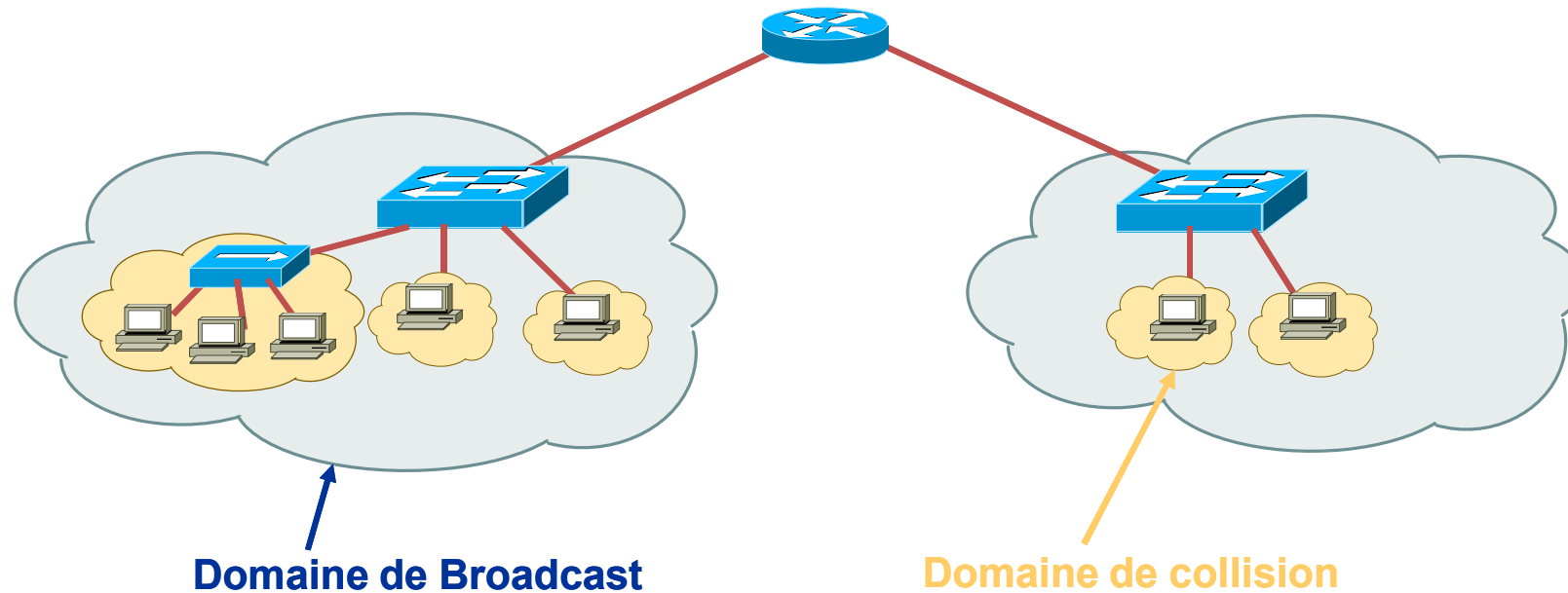
- Commutateurs : Justification
  - Accroissement important des besoins en débits
    - Augmentation du parc informatique (micro puissants)
    - Évolution des applications (bande passante), nouveaux serveurs internet
  - Problèmes à résoudre sur les LANs
    - Charge croissante (multimédia)
    - Collisions, broadcast et multicast

# Commutateurs : Justification



- Les Broadcasts peuvent consommer toute la bande passante !
- Tous les équipements doivent décoder les trames broadcast.

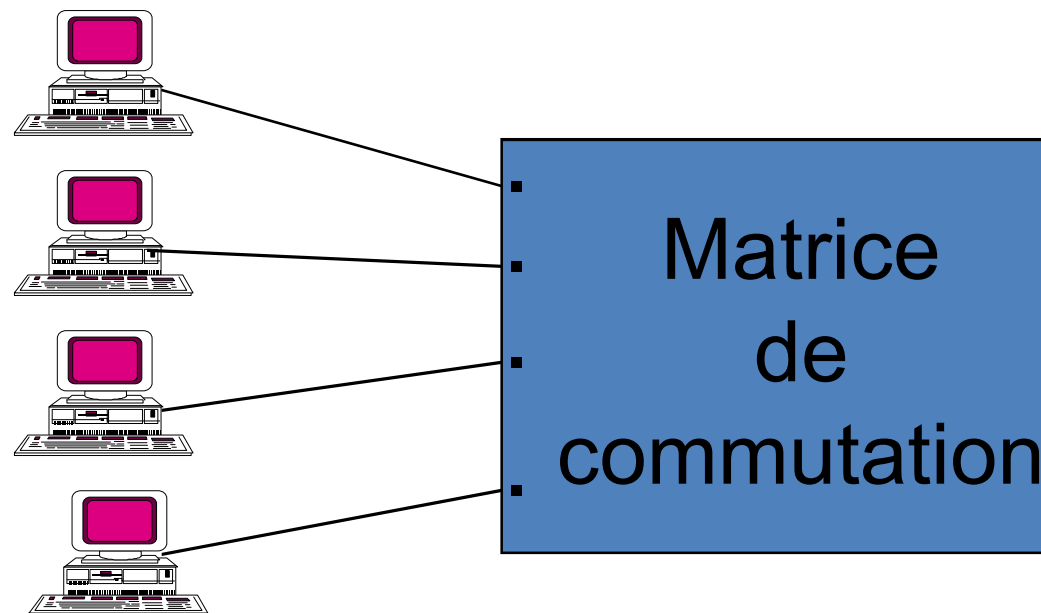
# Commutateurs : Justification



- Les **répéteurs** ne séparent pas les domaines de collision. Les **Ponts, les commutateurs** et les **routeurs** oui.
- Les **répéteurs, ponts et commutateurs** ne séparent pas les domaines de broadcast. Les **Routeurs OUI !**

# Commutateurs : Principes

- Fonctionnement **type "multi-ponts"**
- Processeurs spécialisés (Commutation niveau Circuits Intégrés)
- Ports avec **bande passante "dédiée"** et non partagée



# Méthodes de commutations (1)

- La commutation "**On the fly**" ou "**Cut through**"
  - Lecture des premiers octets de la trame ethernet
    - principalement de **l'adresse de destination**
  - Commute la trame vers le ou les port(s) de sortie
- Avantages : **temps de latence très faible**
  - Inférieur à 20µs, et indépendant de la longueur de la trame
- Inconvénients : Retransmission des erreurs
  - **Inutilisable** avec commutateur de **≠ protocoles**
    - Ethernet 10 avec ports haut débit (uplink) ATM ou FDDI
    - ...



# Méthodes de commutations (2)

- La commutation "Store & Forward"
  - Lecture complète de la trame et stockage
  - Commutation vers le port de sortie
- Avantages
  - Adaptée aux commutateurs de  $\neq$  protocoles
  - Traitement des erreurs
- Inconvénients
  - Plus lent que la commutation "on the fly"
  - Temps de latence = fonction(longueur de trame)

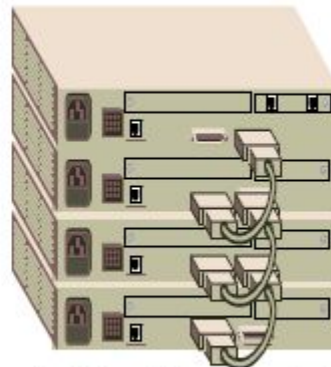
# Méthodes de commutations (3)

- Méthode "**adaptive**"
  - Démarrage en mode "**cut through**"
  - Passage en "**store & forward**" à partir d'un certain **seuil** du taux d'erreurs (paramétrable ou non)
  - Retour mode "**cut through**" en dessous du seuil
  - Fixé par commande de l'administrateur
- Méthode "**fragment-free**"
  - "cut through", mais sans les "runts" (< 64 octets)

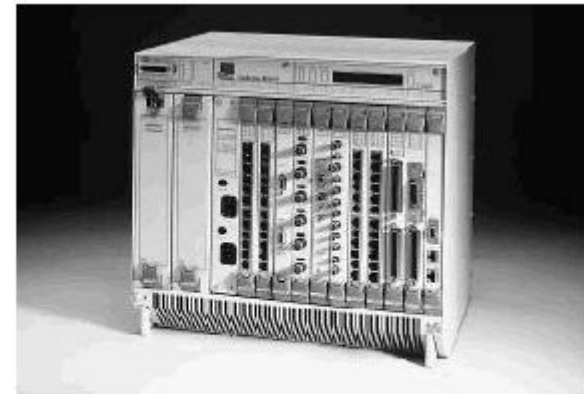
# Format d'équipement hub/Commutateur



"Stand alone"



Empilable "Stackable"



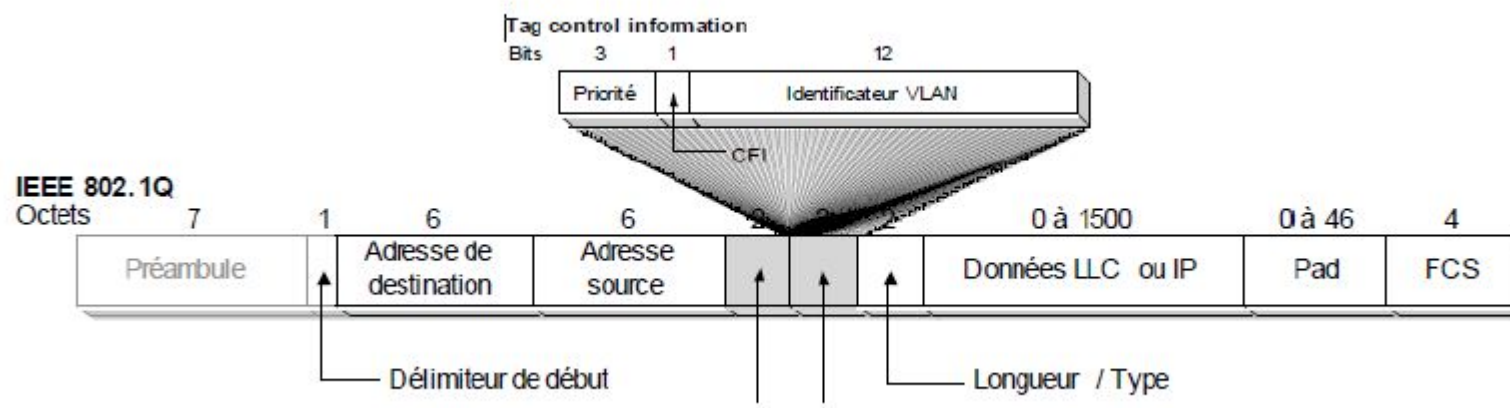
Châssis

# Commutateurs : VLAN (1)

- Les commutateurs peuvent (en option) permettre de définir des réseaux locaux virtuels (VLAN )
- VLANs: sous-réseaux logiques définis sur un même réseau physique.
- délimiter les diffusions qui sollicitent les couches supérieures pour une meilleure gestion du trafic,
- séparer les ressources selon des critères d'appartenance, de partage ou de sécurité (protection du backbone).

# Commutateurs : VLAN (2)

- Tagging

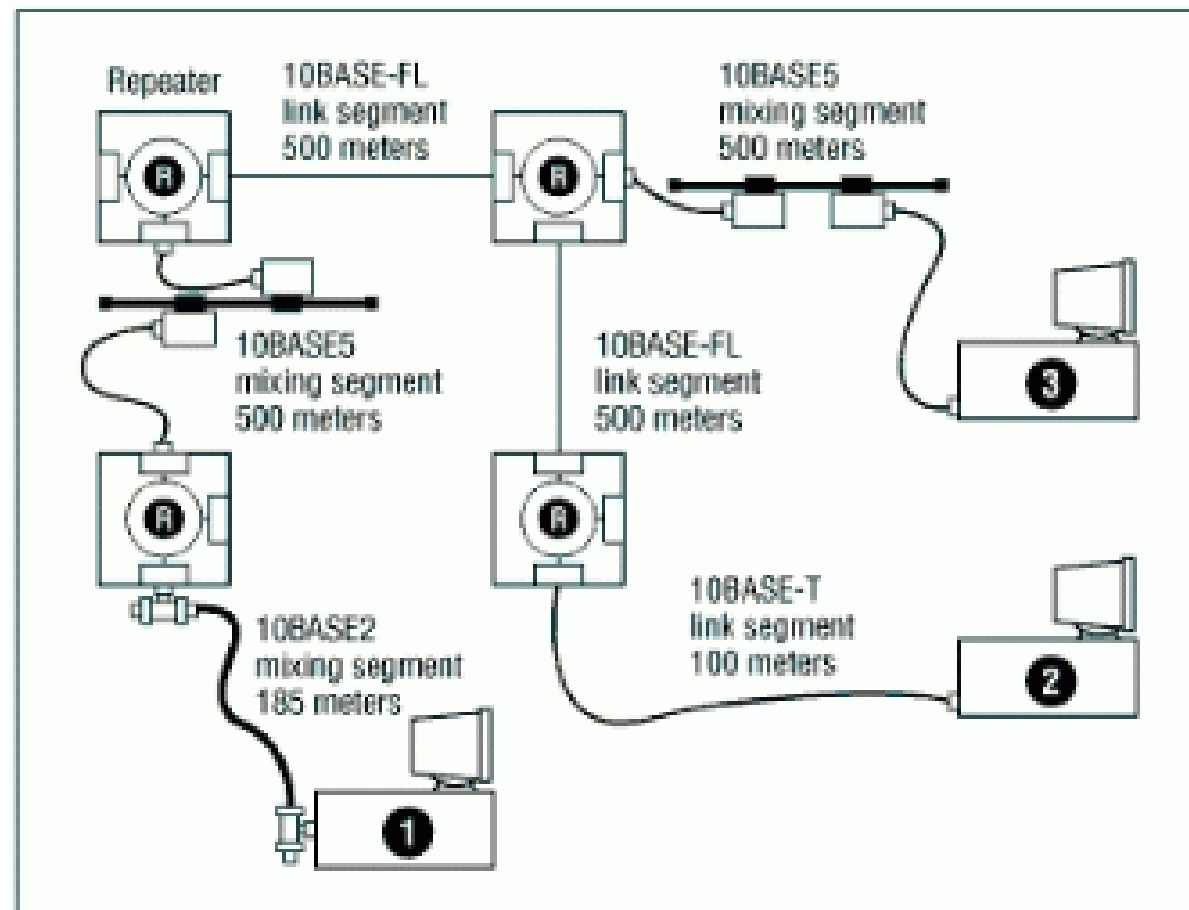


# Composition d'un Ethernet multi-segments

- **Modèle 1 : Règles de configuration**

- les interconnexions sont réalisées moyennant des répéteurs
- un chemin entre deux stations peut comporter cinq segments tout au plus et donc quatre répéteurs.
- Les câbles AUI ne dépassent pas 25m (10Base-FP, 10Base-FL)
- Si un chemin de transmission comporte cinq segments, deux de ces segments au moins doivent être de liaison,
- Si un chemin comporte cinq segments, tout segment FOIRL, 10Base-FB ou 10Base-FL ne peut dépasser 500 m alors qu'un segment 10 BASE FP ne peut dépasser 300 m.
- Si un chemin de transmission comporte quatre segments, tout segment FOIRL, 10Base-FB ou 10Base-FL ne peut dépasser 1000 m alors qu'un segment 10Base-FP ne peut dépasser 700 m

- Exemple conforme au modèle 1



# Composition d'un Ethernet multi-segments

- **Modèle 2 du délai d'un chemin**
  - toute station émettrice doit être notifiée d'une éventuelle collision durant les 512 premiers bits de l'émission
  - $RTD \leq 512$  temps bit quels que soient les médias utilisés dans la configuration.

Type de segment	long. Max	Segment Gauche		Segment interm.		Segment droit		Délai / mètre
		Base	Max	Base	Max	Base	Max	
10Base5	500	11.75	55.05	46.5	89.8	169.5	212.8	0.0866
10Base2	185	11.75	30.73	46.5	65.48	169.5	188.48	0.1026
FOIRL	1000	7.75	107.75	29	129	152	252	0.1
10BaseT	100	15.25	26.55	42	53.3	165	176.3	0.113
10BaseFP	1000	11.25	111.25	61	161	183.5	284	0.1
10BaseFB	2000	-	-	24	224	-	-	0.1
10BaseFL	2000	12.25	212.25	33.5	233.5	156.5	356.5	0.1
Excès AUI	48	0	4.88	0	4.88	0	4.88	0.1026



# Composition d'un Ethernet multi-segments

- $RTD = \sum SDV$  « délais de segments » composant le chemin.  
 $SDV = \text{Base} + (\text{longueur du segment} * RTD / \text{mètre})$
- Si les segments gauche et droit sont de différents types, effectuer le calcul à nouveau en inversant la gauche et la droite et retenir le délai le plus long,
- Si les câbles AUI > 2 m, rajouter le délai en excès,
- Ajouter une marge de 5 temps bit,
- Si  $RTD \leq 575$  temps bit, le chemin est valide.
- Effectuer cette procédure entre toutes les extrémités du réseau.

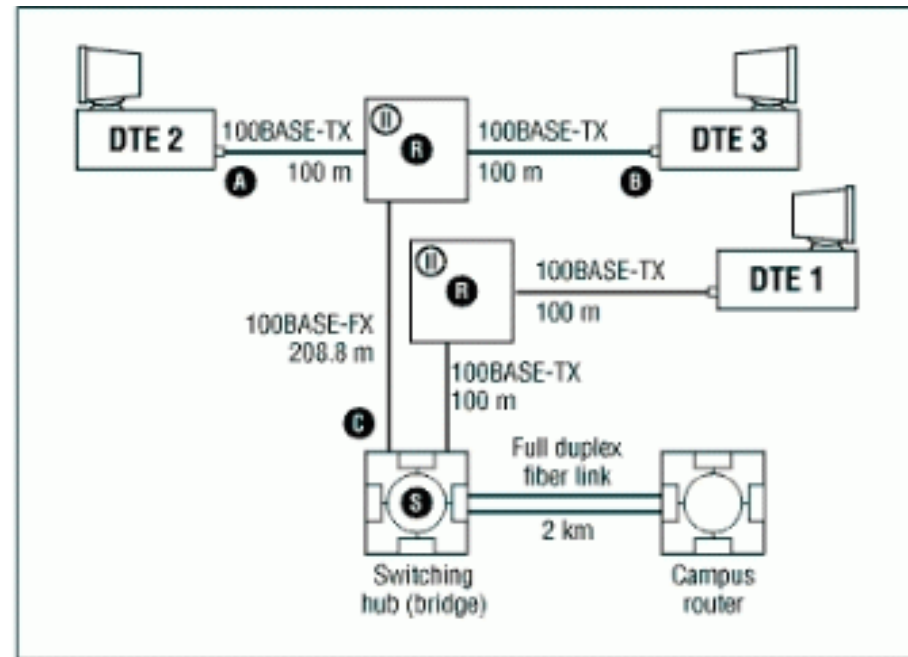
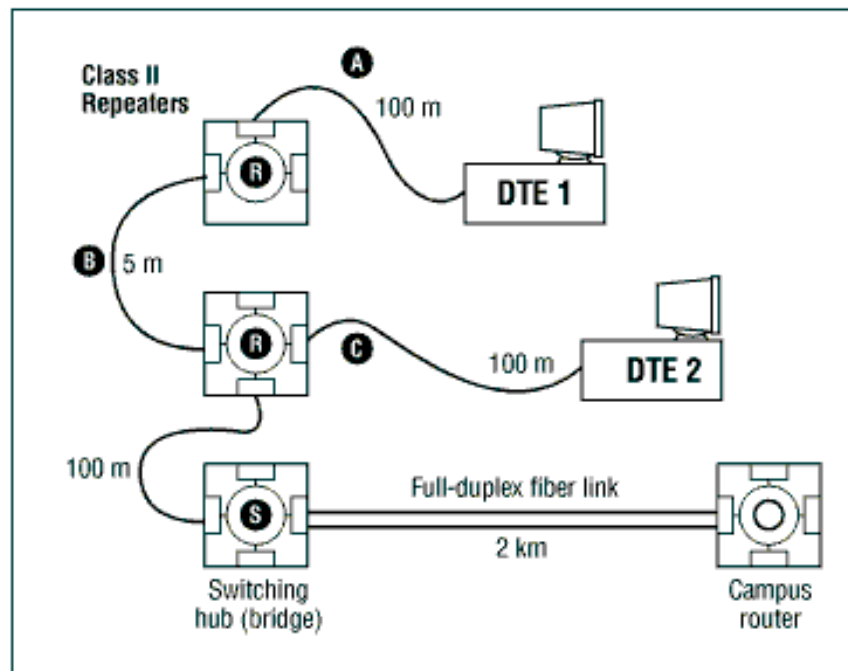
# Composition d'un réseau Ethernet multi-segments (Fast Ethernet)

- Fast Ethernet est limité à deux répéteurs et n'utilise que des segments de liaison.
- Le domaine de collision est limité à 205 m avec du câble UTP.

	<b>T</b>	<b>FX</b>	<b>T et FX</b>
<b>1 segment</b>	100 m	412 m	
<b>2 segments (1 répéteur Class I)</b>	200 m	272 m	100+160,8 m
<b>2 segments (1 répéteur Class II)</b>	200 m	320 m	100+208 m
<b>3 segments (2 répéteurs Class II)</b>	205 m	228 m	105+111.2 m

# Composition d'un réseau Ethernet multi-segments (Fast Ethernet)

- deux exemples de configuration Fast Ethernet



# Composition d'un réseau Ethernet multi-segments (Fast Ethernet)

- Autre modèle basé sur le calcul du RTD pour la validation de configurations

Component	RTD / mètre (temps-bit)	RTD Maximum
Deux DTEs TX/FX		100
Deux DTEs T4		138
Un DTE T4 et un DTE TX/FX		127
Catégorie 3 /4	1.14	114 (100 m)
Catégorie 5	1.112	111.2 (100 m)
STP	1.112	111.2 (100 m)
Fibre Optique	1.0	412 (412 m)
Répéteur Classe I		140
Répéteur Classe II tous les ports TX/FX		92
Répéteur classe II avec des ports T4		67

# Composition d'un réseau Ethernet multi-segments (Gigabit)

- Gigabit : un répéteurs et la longueur d'un segment  $\leq 316$  mètres.

	Cat 5 UTP	CX	SX/LX	Cat 5 et F.O	CX et SX/LX
<b>1 segment</b>	100	25	316		
<b>1 répéteur</b>	200	50	220	210	220

- full-duplex (FO), longueurs plus importantes

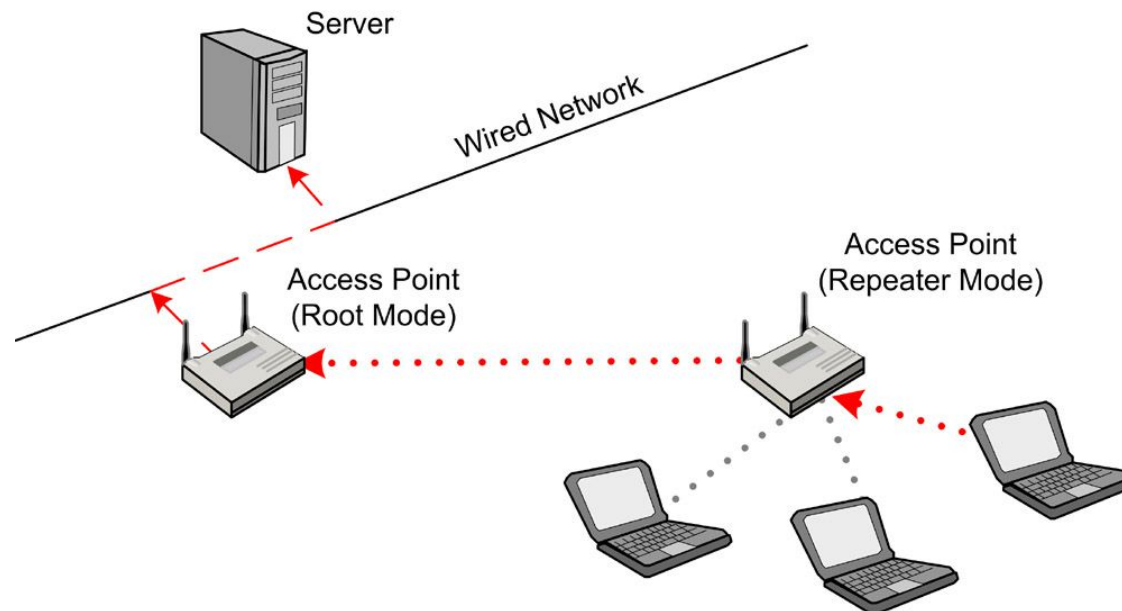
Nom	Type	Longueur max segment	Remarques
<b>1000Base-SX</b>	2 fibres optiques	220-550m	<u>Multimode</u>
<b>1000Base-LX</b>	2 fibres optiques	550-5000m	<u>Multimode</u> - Monomode

# Composants d'un réseau WiFi

- **Carte Wifi, existe en PCI / PCMCIA/ USB**  
même rôle que les cartes réseaux traditionnelle
- **Antenne**
  - **omnidirectionnelle** rayonne dans toute les directions
  - **Directionnelle** peuvent capter un signal à plus grande distance qu'une antenne omnidirectionnelle, mais dans une zone très restreinte.
- **Point d'Accès (AP) ou bornes sans fil** (mode infrastructure)
  - assure la communication entre les stations WiFi (hub)
  - est raccordé à un réseau filaire (DS), Ethernet par exemple

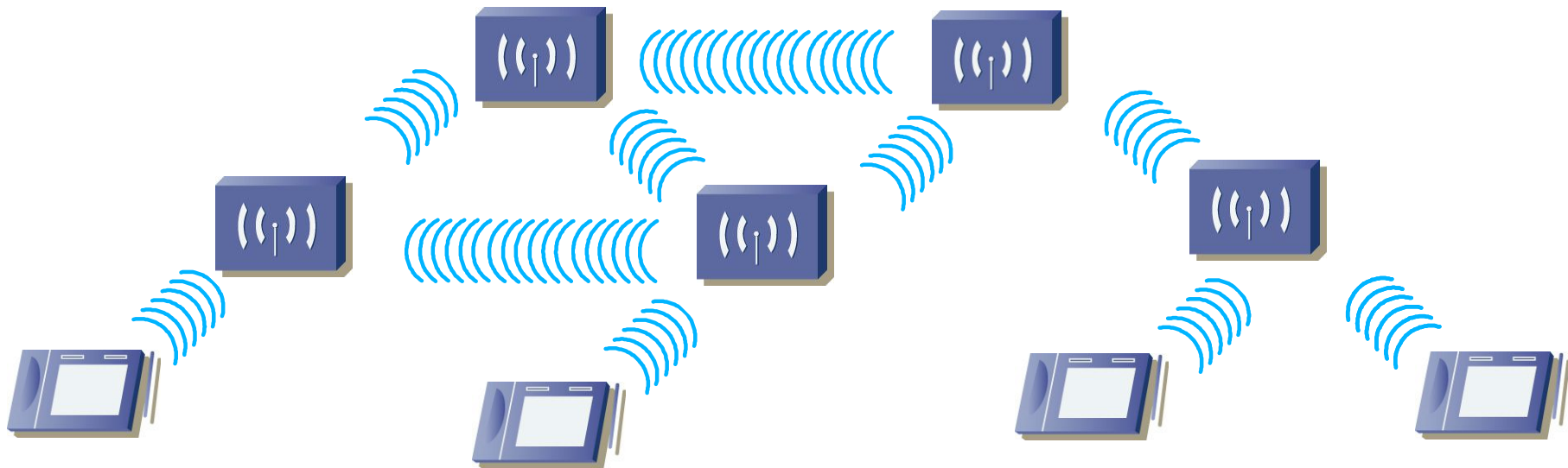
# Composants d'un réseau WiFi

- **2 modes :**
  - Pont « wireless bridge », 2 LAN (niveau 2 différents ) connectés par un lien sans fil en point à point.
  - répéteur, ou « Wireless repeater » ou encore « range expander », étendre la portée d'un premier AP (« root mode ») par un second AP (« repeater mode »).



# WiFi: Wireless Distribution System

- créer un réseau fortement maillé à l'aide de point d'accès.





# WDS, « Wireless Distribution System »

- 3 types d'AP:
  - « Main Base Station » (ou AP principal), connexion à un réseau filaire ;
  - « Remote Base Station » (ou AP secondaire) prise en charge les clients WiFi
  - « Relay Base Station » (ou AP relais) relayer



# WDS, « Wireless Distribution System »

- Les « Base Stations » doivent utiliser le même canal et la même méthode/clé de cryptage.
- La bande passante est divisée par 2.
- WDS prévoit deux modes de connectivité :
  - « Bridging » où l'AP ne communique qu'avec d'autres APs,;
  - « Repeating » où l'AP communique en plus avec les clients WiFi.
- WDS peut être incompatible d'un produit à un autre (non certifié par la WiFi Alliance).

# WDS, « Wireless Distribution System »

3 types de point d'accès :

- **principal ou maître** : c'est un point d'accès qui effectue le pont entre le réseau sans fil et le réseau câblé.
- **secondaires** : ce sont les équipements qui retransmettent les données des stations ou des points d'accès relais vers le point d'accès maître.
- **relais** : ils jouent le rôle de simple répéteur en transmettant les données des stations vers les points d'accès secondaires.

# Wifi : Couverture et débit

## • 802.11 b

à l'intérieur		à l'extérieur	
Débit	Distance	Débit	Distance
11 Mbits/s	50 m	11 Mbits/s	200 m
5,5 Mbits/s	75 m	5,5 Mbits/s	300 m
2 Mbits/s	100 m	2 Mbits/s	400 m
1 Mbits/s	150 m	1 Mbits/s	500 m

## • 802.11 a

Débit	Distance
54 Mbits/s	10 m
48 Mbits/s	17 m
36 Mbits/s	25 m
24 Mbits/s	30 m
12 Mbits/s	50 m
6 Mbits/s	70 m

# Wifi : Couverture et débit

- 802.11a,b,g,n

Protocol Version	Typical Data Rate	Net. Data Rate	Distance à l'intérieur	Distance à l'extérieur
802.11a	27 Mbit/s	54 Mbit/s	~50 ft/15 m	~100 ft/30 m
802.11b	~5 Mbit/s	11 Mbit/s	~150 ft/45 m	~300 ft/90 m
802.11g	~22 Mbit/s	54 Mbit/s	~150 ft/45 m	~300 ft/90 m
802.11n	50-144 Mbit/s	600 Mbit/s	300 ft/91 m	600 ft/182 m

# Plan de câblage

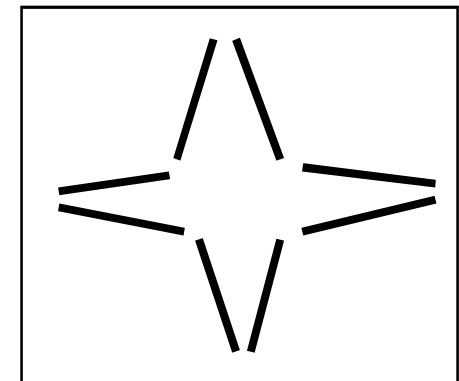
- Principes de base
- Câblage horizontal
- Répartiteur
- Câblage vertical
- Le brassage
- Validation de câblage

# Principes (1)

- Pré ou Post Câblage = Recherche d'économie financière (mélange téléphonie et informatique) et de facilité d'exploitation
  - Optimisation des coûts d'installation et d'exploitation
    - À terme, le pré-câblage est + économique
  - Souplesse d'exploitation et sécurité
    - Pas d'intervention sur la partie fixe du câblage
  - Conformité aux normes internationales,
    - Offres supérieures aux normes dues à la forte évolution de la demande
  - Câbler pour l'avenir (10 à 15 ans).

# Principes (2)

- Topologie de distribution en étoile à la base
  - C'est la plus ouverte
  - Totalelement adaptée à la téléphonie
- Indépendance par rapport à l'architecture réseau
  - ✓ Par un jeu de brassage, on peut recréer une **topologie logique en Bus ou en anneau**.
  - ✓ Attention aux distances et à l'affaiblissement





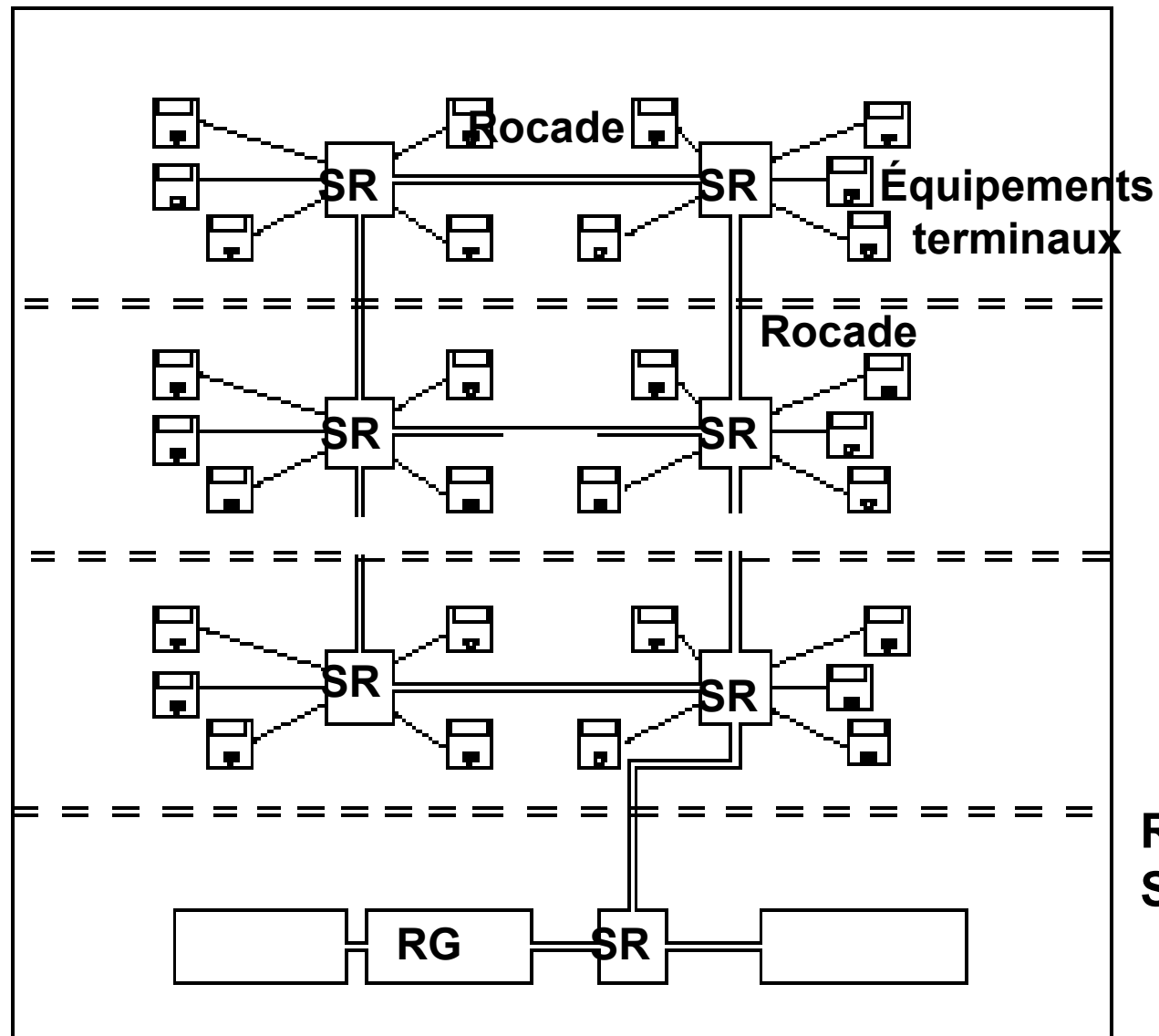
# Principes (3)

- Banalisation de la connectique (RJ45 pour câble cuivre)
  - Adaptateurs possibles fonction du matériel à brancher
- Banalisation des câbles eux mêmes
  - 4 paires torsadées 100Ω normalisé (ou 120Ω)(pas de mélange)
- Ajout de la fibre optique pour
  - Les longues distances,
  - Les liaisons inter bâtiments ou autres passages difficiles,
  - Pour les dorsales grâce à leurs bandes passantes élevées pour assurer la pérennité dans le temps.

# Principes (4)

- Respect des règles de conception et d'installation,
- Répondre à l'ensemble des besoins des utilisateurs
  - Diversités des flux (numérique, analogique)
  - Diversités des protocoles (fréquences variables)
  - Évolutivité (clé de la durée de vie du câblage)
  - Performances (surdimensionnement des besoins en débit)
  - Mobilité (surdimensionnement des besoins en prise)

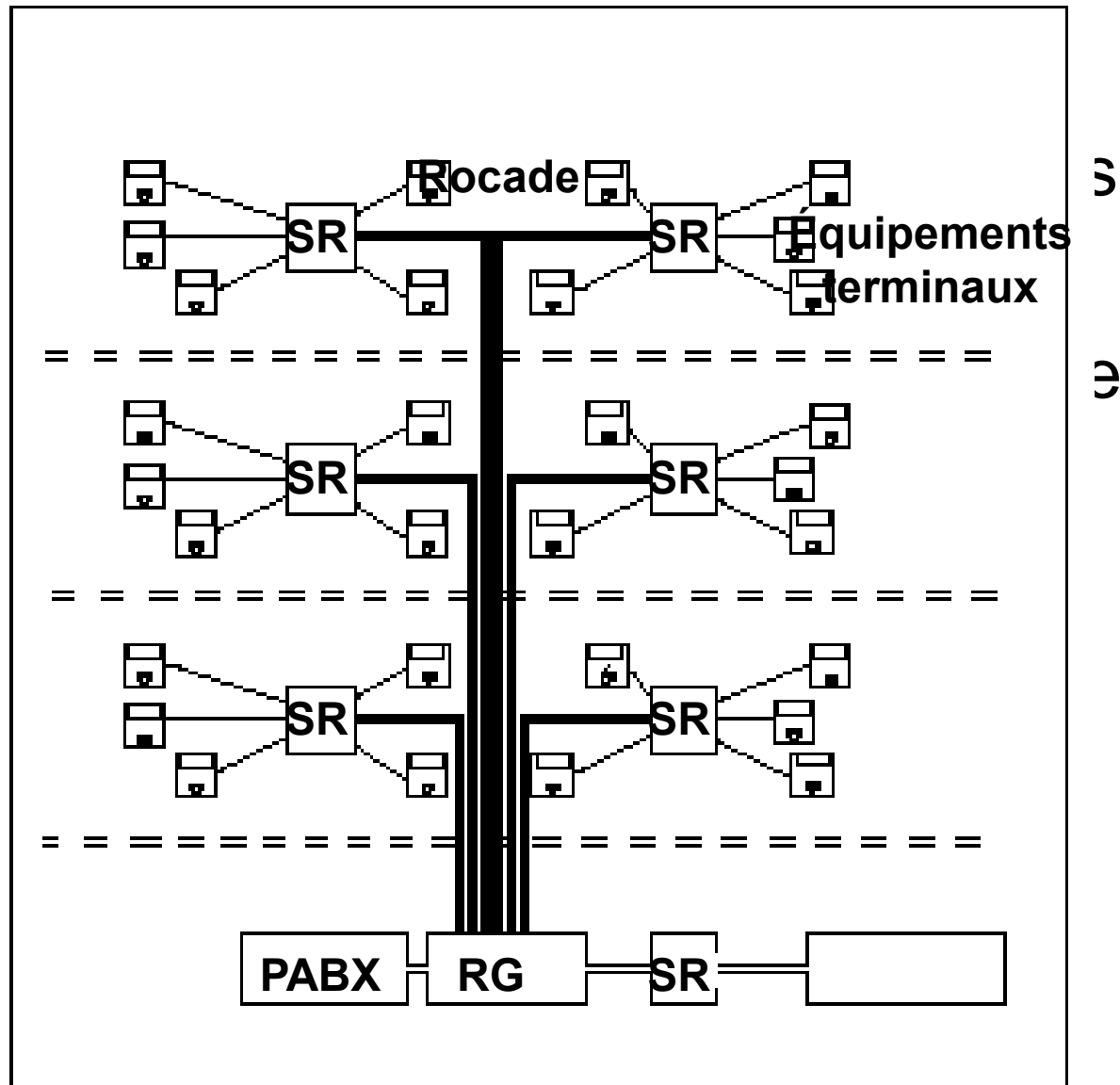
# Principes (5)



Maillé  
Réseau de  
données

**RG** : Répartiteur Général  
**SR** : Sous répartiteur

# Principes (6)



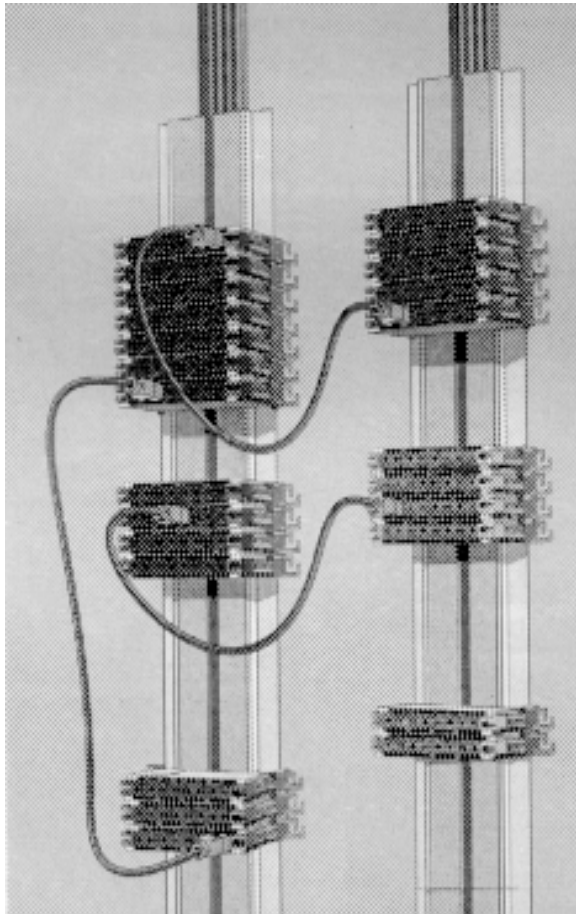
**RG** : Répartiteur Général  
**SR** : Sous répartiteur

# Principes (7)

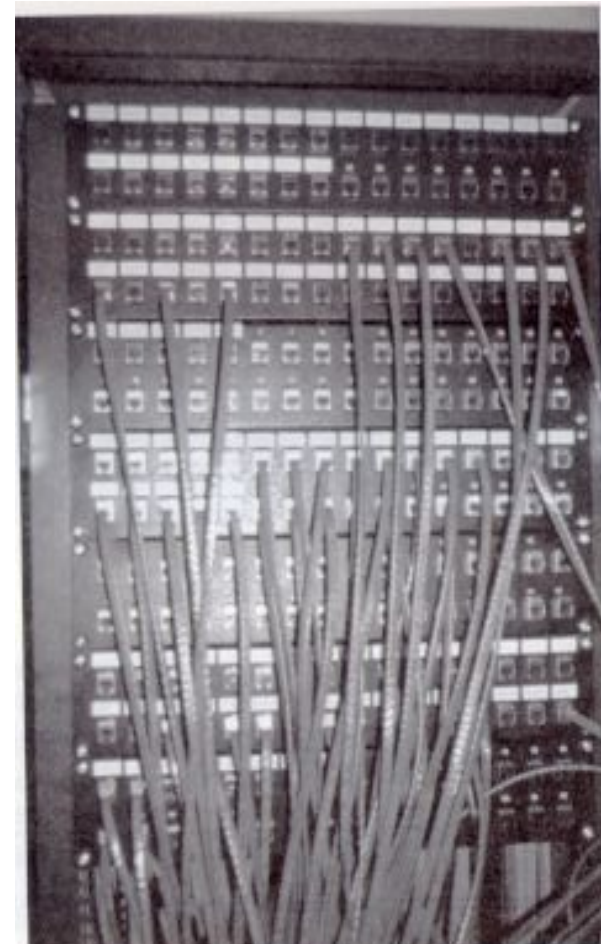
Les composants principaux sont :

- Les répartiteurs (général ou sous répartiteur d'étage)
  - Concentration capillaire du câblage
- L'ensemble du câblage est constitué de 2 sous parties :
  - Le câblage départemental ou horizontal (liaison d'étage)
    - Liaison Sous Répartiteur d'étage - Équipement terminal
  - Le câblage d'établissement ou vertical (liaison inter-étage) (dorsale)
    - Liaison Répartiteur Général - Sous Répartiteur d'étage

# Brassage: Exemples de Répartiteurs



**Ferme de brassage  
Informatique ou téléphonique**



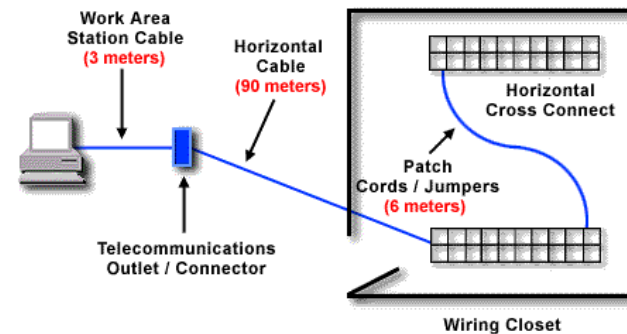
**Panneau de brassage  
Bandeau de RJ 45**

# Câblage horizontal

- C'est l'ensemble des câbles reliant le sous-répartiteur d'étage et les prises informatiques ou téléphoniques des utilisateurs.
  - constitués généralement de câbles 4 paires.
- Le rattachement des câbles sur les répartiteurs :
  - Permet de créer une topologie hiérarchisée en étoile
  - Autorise l'indépendance de chaque prise des points de travail
  - Permet de d'effectuer facilement la gestion et l'administration du réseau de câblage par un brassage à la demande.
- Les câbles quatre paires forment les branches de l'étoile

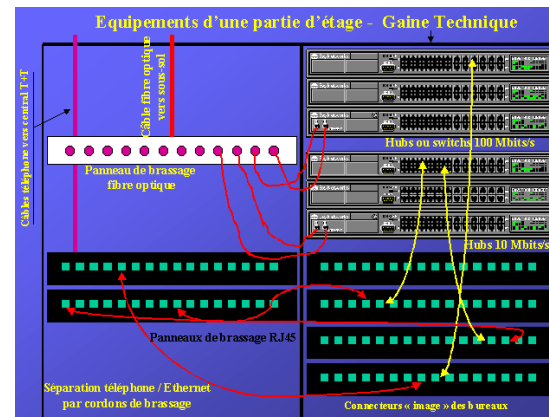
# Câblage départemental (horizontal)

- Distances maximales autorisés



EIA/TIA-568A maximum recommended distances for horizontal cabling.

- Répartiteur ou Gaine technique





# Câblage d'établissement (vertical)

C'est le câblage qui réunit les Répartiteurs entre eux.

- Il est de 2 types :
  - Les Colonnes pour la partie téléphonie
  - Les Rocades pour la partie informatique

# Câblage d'établissement (vertical)

- Les Rocades (partie informatique) sont des câbles de regroupement de forte capacité reliant les répartiteurs entre eux.
  - Chaque répartiteur est relié à un ou plusieurs répartiteurs si on désire une topologie maillée.
  - Le maillage permet l'accès de tous les nœuds de brassage par le chemin le plus court
    - la possibilité de séparer le cheminement des flux informatiques (saturation de certaines rocales)
    - procurer un chemin d'accès de secours.

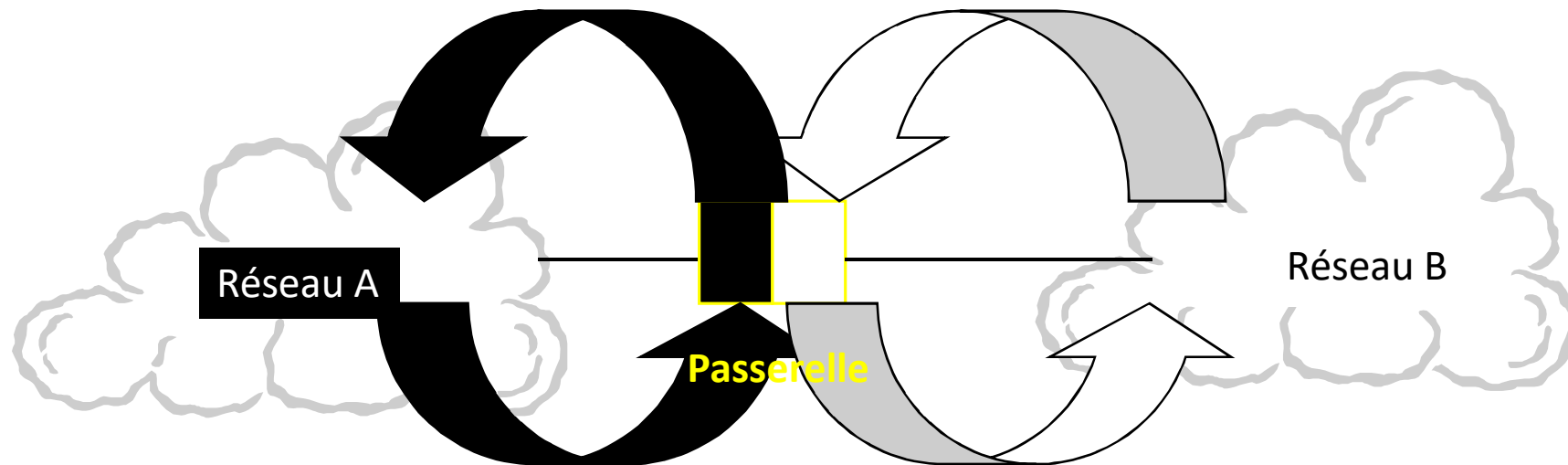
# Câblage vertical : Rocades

- Les Rocades forment la dorsale du réseau informatique du bâtiment.
  - En général, les rocales sont constituées par de la fibre optique :
    - Un média universel à forte bande passante (évolutivité, pérennité)
    - De type **gradient d'indice** ou **monomode** en fonction des distances et des protocoles (attention aux coûts des matériels actifs si monomode)
    - Immunité aux perturbations électromagnétiques
    - Immunité aux problèmes d'équipotentialité des terres électriques inter bâtiments

# Validation du câblage

- examen visuel : nombre, emplacement et type des prises installées ; dans les locaux techniques : ventilation, revêtement, alimentation, terre, différenciation des raccordements (ex. code couleur, étiquetage),...
- tests statiques :
  - mesurer les temps de monter de descente d'un signal : oscilloscope
  - mesurer sur un brin les points de variation de l'impédance càd la continuité des conducteurs, réflectomètre (échomètre)...
- tests dynamiques : tests au niveau MAC (comptage des trames, des collisions, des trames en erreurs, ... ) grâce à des valises de test et / ou des analyseurs de réseaux

# Interconnexion des réseaux

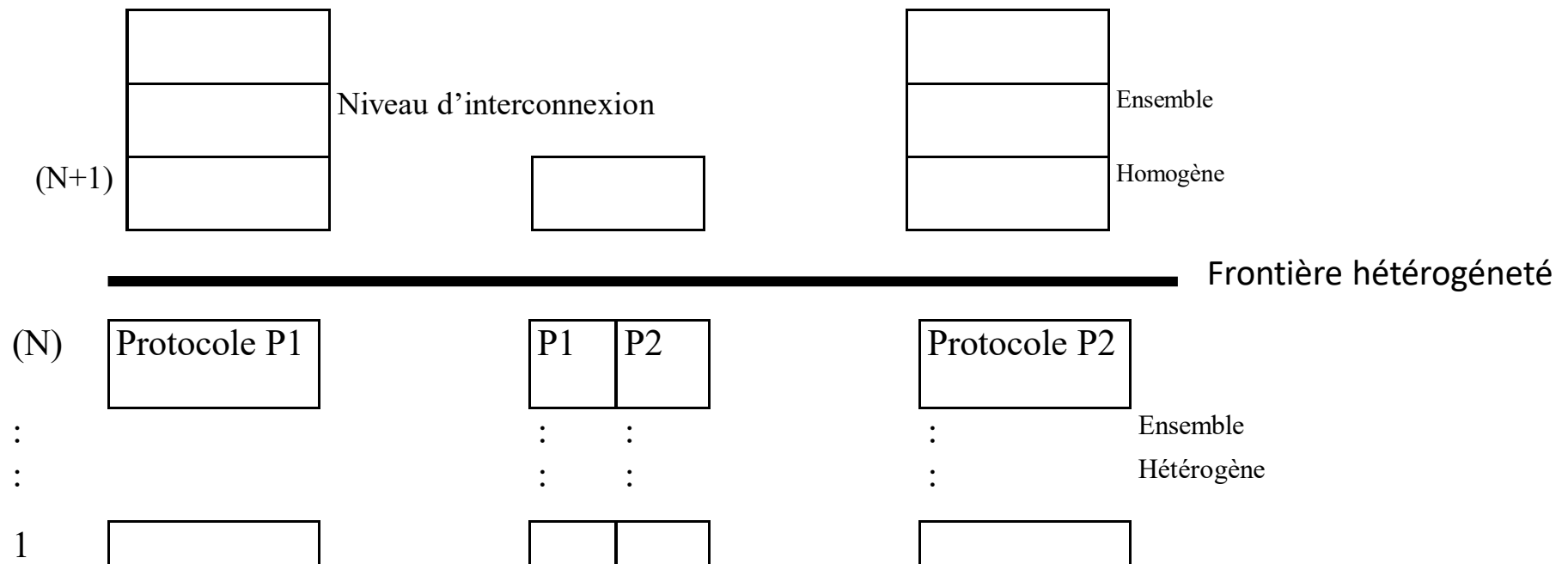


- Une passerelle est un équipement connecté à chacun des réseaux et qui sait acheminer les paquets d'un réseau à un autre.
- Sur le réseau A, la passerelle accepte les paquets destinés à B
- Sur le réseau B, la passerelle accepte les paquets destinés à A

# Principes

- Accéder à des ressources extérieures au RL
- Dialogue entre deux architectures différentes (support et protocoles)
  - Comparer les architectures (OSI) des réseaux à interconnecter
  - Identifier les différences de services, de protocoles
  - Déterminer le niveau de compatibilité des architectures. À ce niveau l'interconnexion se réalise.
- Différentes techniques d'interconnexion donc différents équipements mettant en œuvre ces techniques
- Interconnexion locale : les réseaux sont sur le même site. Un équipement suffit à réaliser l'interconnexion
- Interconnexion distante : les réseaux sont éloignés. Utilisation d'une liaison télécoms, avec un équipement placé à chaque extrémité

# Principes d'interconnexion



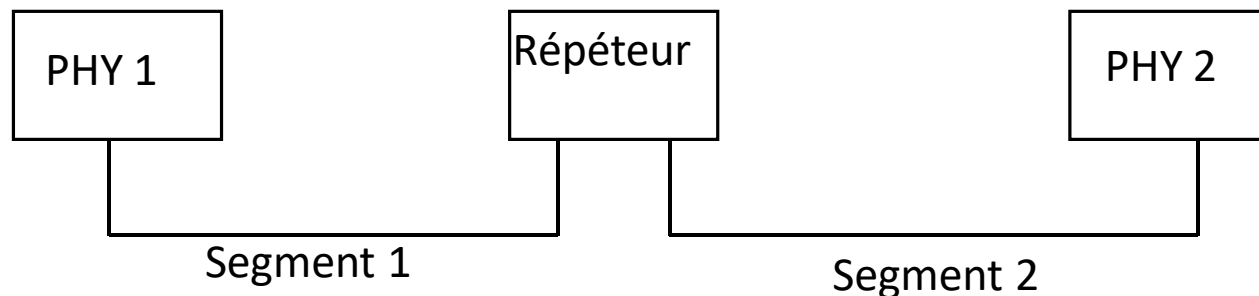
# Techniques d'interconnexion

- La conversion de services ou la concaténation de services.
  - La **conversion**, lorsque les niveaux inférieurs des sous-réseaux sont différents mais compatibles (par exemple, deux couches MAC).
    - traduit les primitives de services d'un sous-réseau en primitives utilisables sur l'autre.
  - La **concaténation**, lorsque les protocoles du niveau d'interconnexion sont identiques mais utilisées dans des contextes différents et avec des valeurs de paramètres différents.
    - fait appel à des mécanismes de contrôle de congestion (débits différents) et de fragmentation (longueurs PDU différentes).
- La conversion de protocoles travaille directement sur les PDU plus complexes que la conversion de services.
- L'encapsulation consiste, en émission, à envelopper chaque unité de données
  - + généralité, à tous les cas de figures.
  - introduction d'un niveau de protocole supplémentaire.



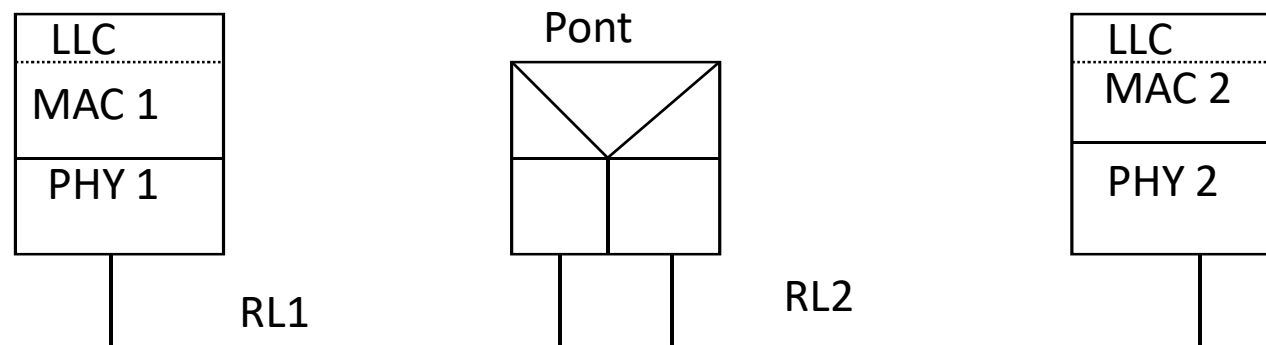
# Le répéteur

- Il relie deux segments d'un même réseau,  
➤ ne fait que prolonger le support physique.
- Niveau 1 de l'OSI
  - Répétition des bits d'un segment à l'autre, avec régénération
  - Changement de support physique, même débit
  - Pas d'isolation des segments



# Les ponts

- C'est un équipement de couches 2 (MAC)
- Interconnexion de 2 réseaux ayant des couches PHY et MAC différentes; même LLC
- Fonctions
  - mémoriser les informations reçues avant de les retransmettre
  - Convertir les formats de trames (MAC) et les router



# Types de pont

- Le pont simple : route la trame en fonction de l'adresse, soit par diffusion, soit par table de routage statique chargée à l'initialisation
- Pont intelligent : établit par apprentissage sa table de routage et filtre les trames en fonction de leur adresse. Garantir l'unicité d'un chemin entre 2 stations, STA: Spanning Tree Algorithm
- Pont à routage : spécifie dans TR. Le chemin que doit suivre la trame est indiqué dans le champ RI, positionné par la source (Source routing)
  - Station A émet une trame pour B, sur un autre anneau
  - La trame lui revient, sans modification du champ FS
  - A diffuse une trame, dupliquée par tous les ponts, transmise sur tous les anneaux donc passant par tous les chemins
  - B reçoit X trames (égale au nombre de chemins possibles entre A et B)
  - A retient le chemin qui lui convient le mieux
- Pont distant : interconnexion de RL éloignés via une liaison grande distance et deux demi-pont.

# Spanning Tree

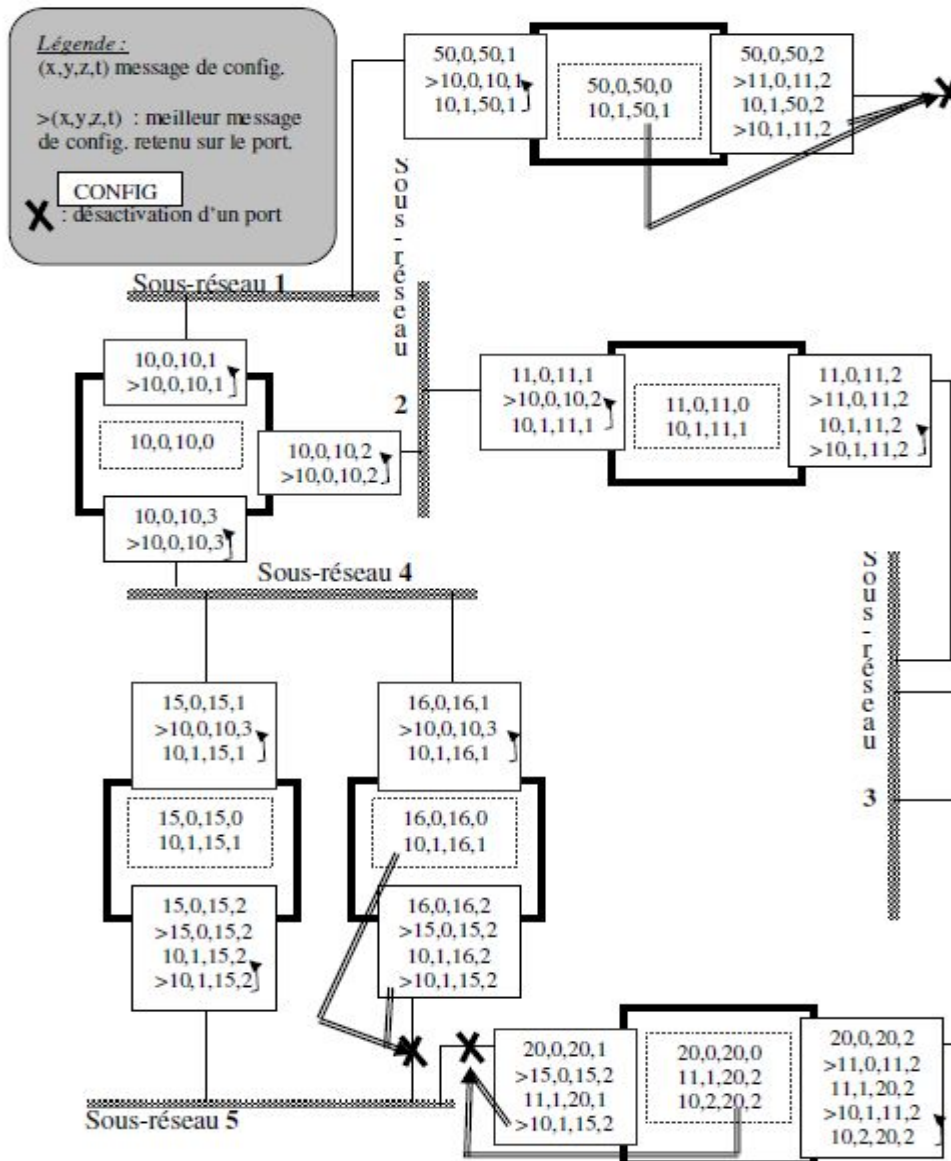
- Une solution au problème posé par les boucles est de déterminer un arbre recouvrant
- Les noeuds de l'arbre représentent les ponts et les arêtes représentent les sous-réseaux. Les ponts ne peuvent ainsi router qu'à travers les arêtes de l'arbre.
- Construction de l'arbre :
  - L'algorithme est distribué, il s'exécute sur les  $\neq$  ponts du réseau.
  - A chaque pont est attribué un identificateur
  - Le pont, ayant la plus petite identification, est élu racine de l'arbre. Initialement chaque pont se considère comme étant la racine de l'arbre.
  - Chaque port (interface) d'un pont sera identifié par un numéro
  - Le coût d'une route est comptabilisé en nombre en nombre de sauts et/ou dépendant du débit des ports

# Spanning Tree

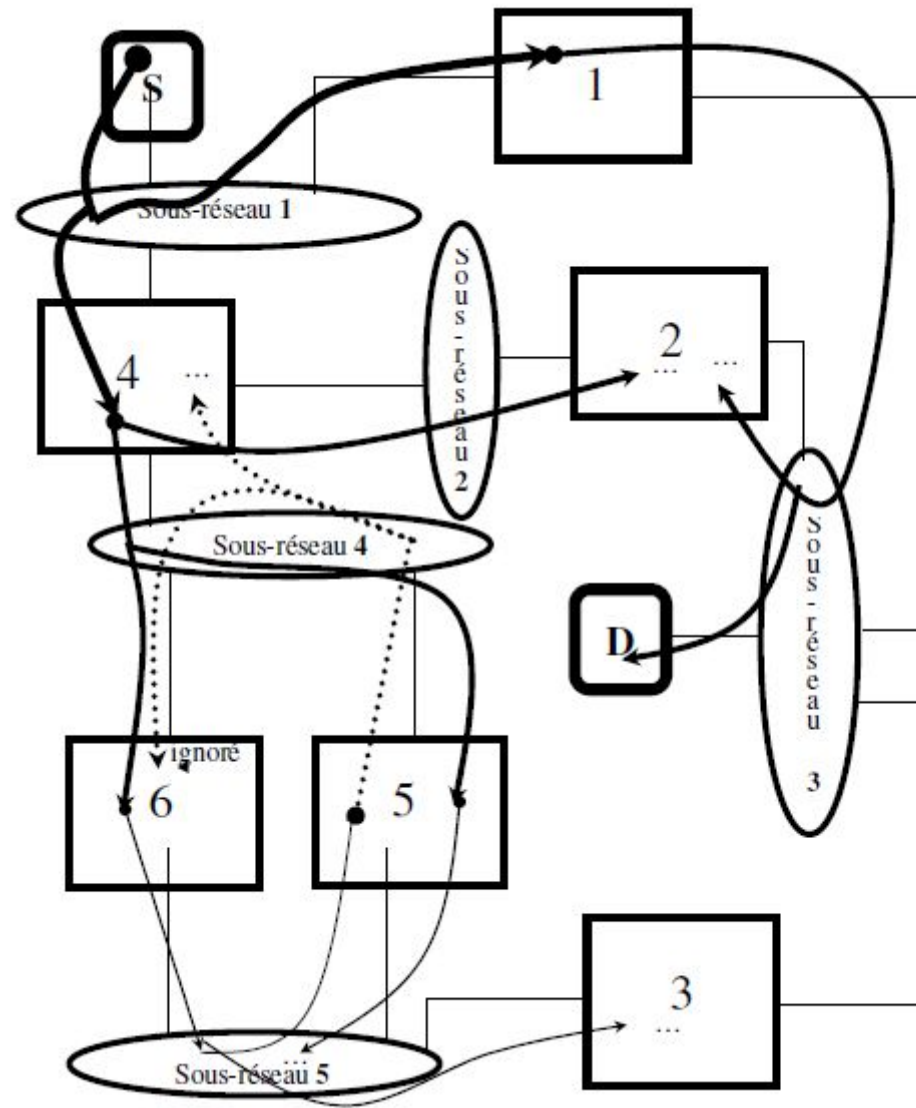
- Déroulement de l'algorithme
  - Les ponts échangent entre eux des messages de configuration.
    - l'identité supposée de la racine,
    - le coût de la route vers la racine,
    - l'identité du pont ayant émis le message,
    - le numéro du port à travers lequel le message est émis.
  - Chaque pont maintient la meilleure configuration trouvée (CONFIG).
    - identité supposée de la racine,
    - coût de la route vers cette racine,
    - identité du pont local,
    - numéro du port vers la racine
  - A chaque port est associée un meilleur message de configuration observé sur ce port.
  - Un port, mis à part celui menant vers la racine, ayant une meilleure Configuration que CONFIG est désactivé

# Spanning Tree

exemple de  
déroulement de  
l'algorithme «  
spanning tree »



# Source Routing



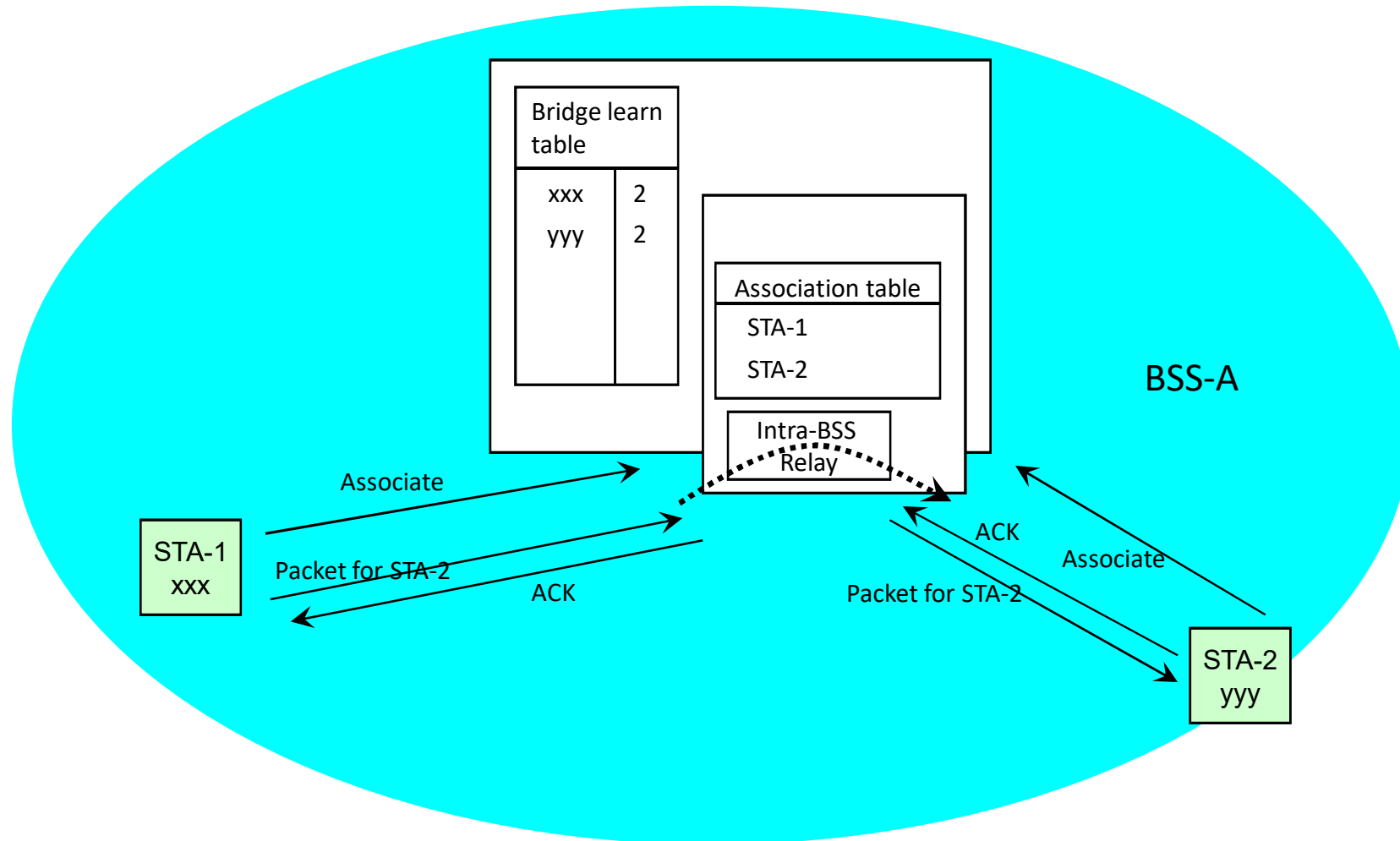
# Relayage des trames à travers les points d'accès

- Lors de l'association, un AP maintient la table des associations ainsi la table des correspondances adresses MAC/ port (1=Ethernet, 2=PC card/Slot-A, 3=PC card/Slot-B, 4-15=WDS ports)

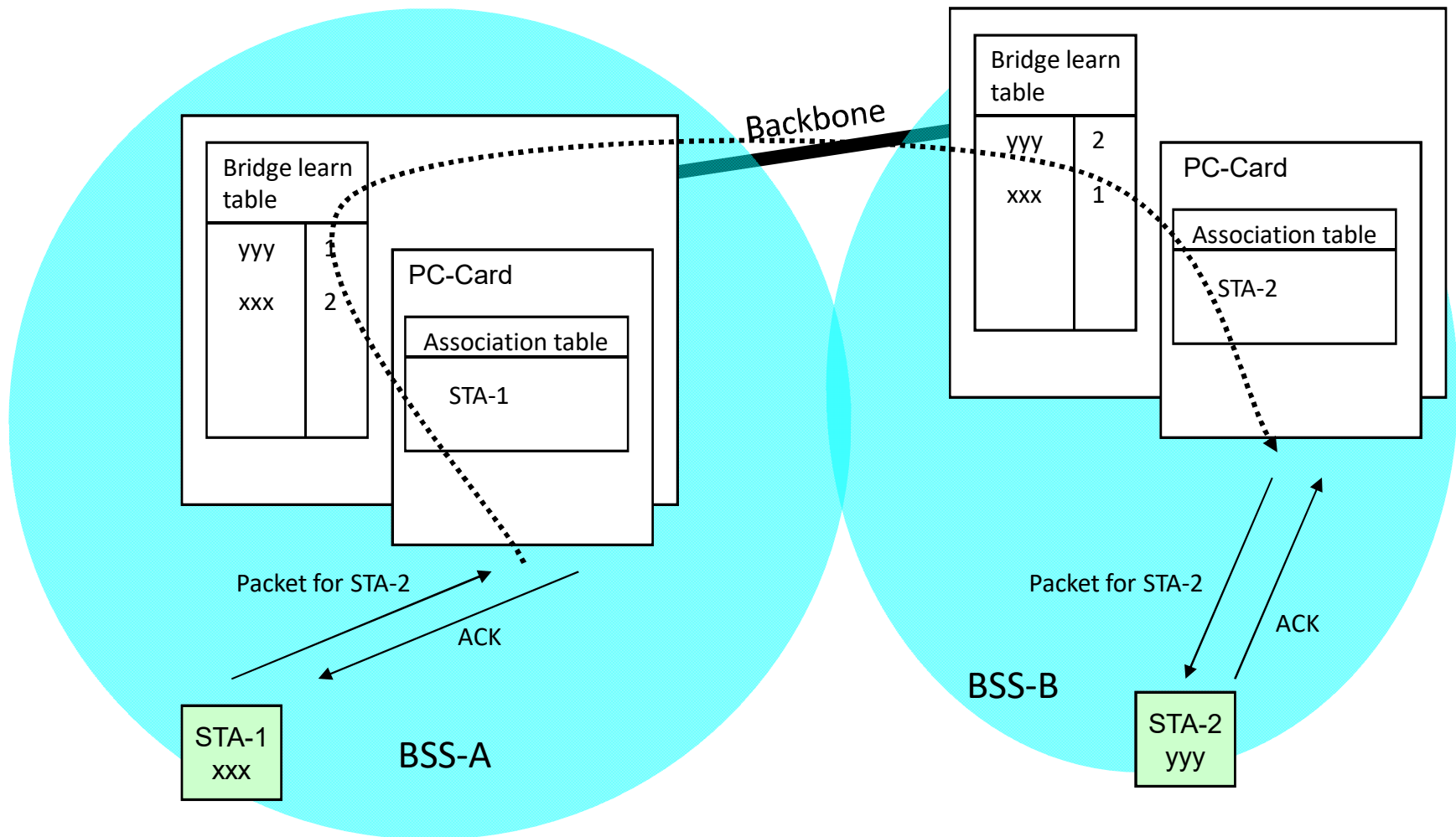
Bridge learn table	
Mac Addr	Port#



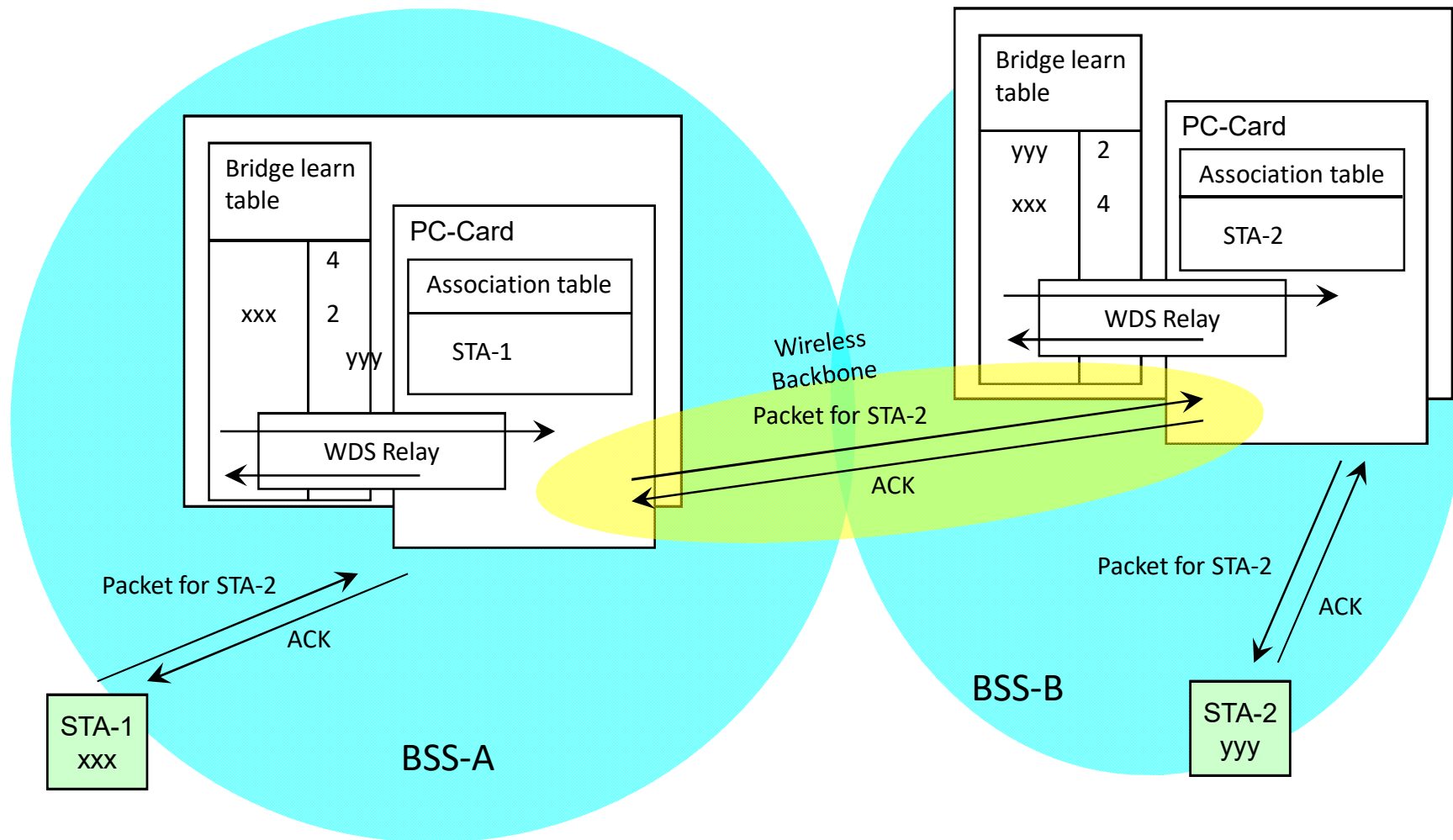
# Cas d'un BSS



# Cas d'un ESS



# Cas d'un WDS

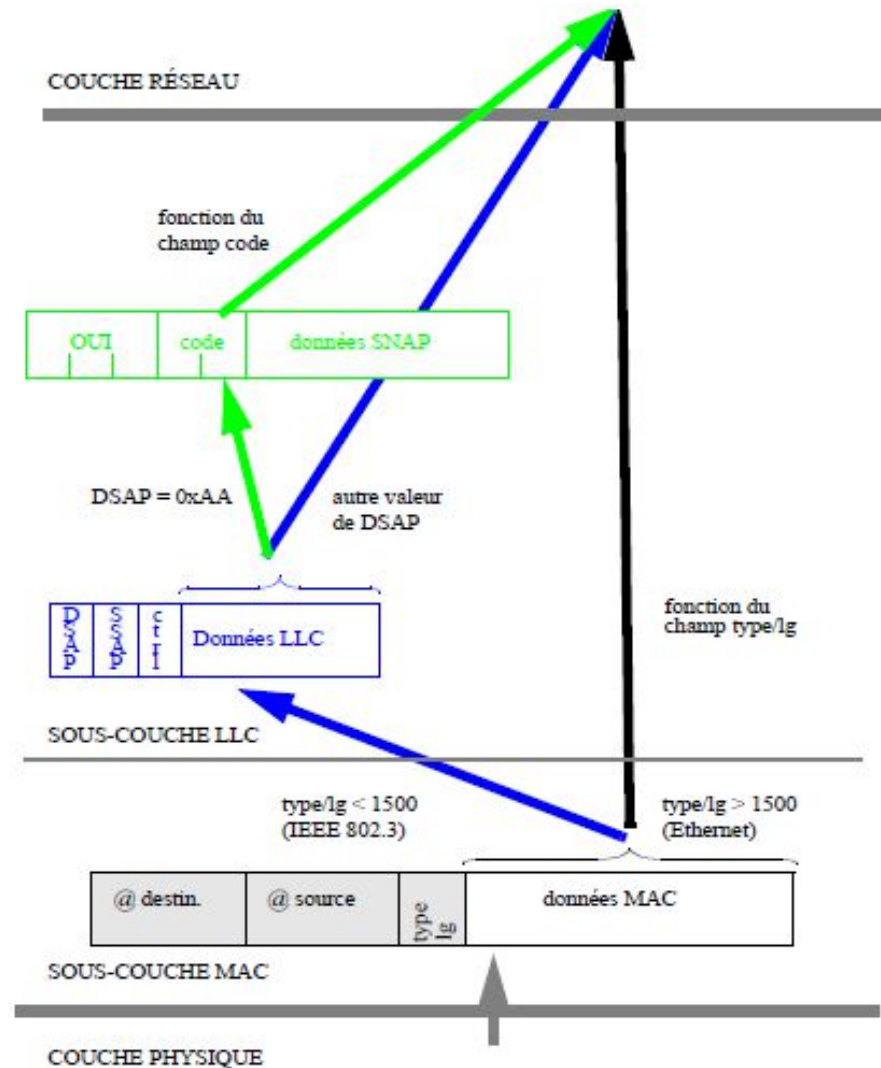


# Sous Couche SNAP

- SNAP (Sub-Network Access Protocol ) propose une encapsulation supplémentaire au dessus de LLC En-tête : 5 octets
  - 3 octets : Organizational Unit Identifier (OUI), généralement à 0
  - 2 octets : Code du protocole de niveau 3
- Permet de combler les lacunes de LLC :
  - Adresse sur un nombre impair de bits : peu performant,
  - Espace de valeurs des SAP limités,
  - Compatibilité avec l'adressage d'Ethernet.
  - En-tête LLC + SNAP = 8 octets => résoud pb alignement
- Valeur du SAP : 0xAA
- SNAP ne met pas en oeuvre de protocole supplémentaire
- Permet au protocole de niveau 3 de travailler avec X25, FDDI, ATM, Frame Relay ...

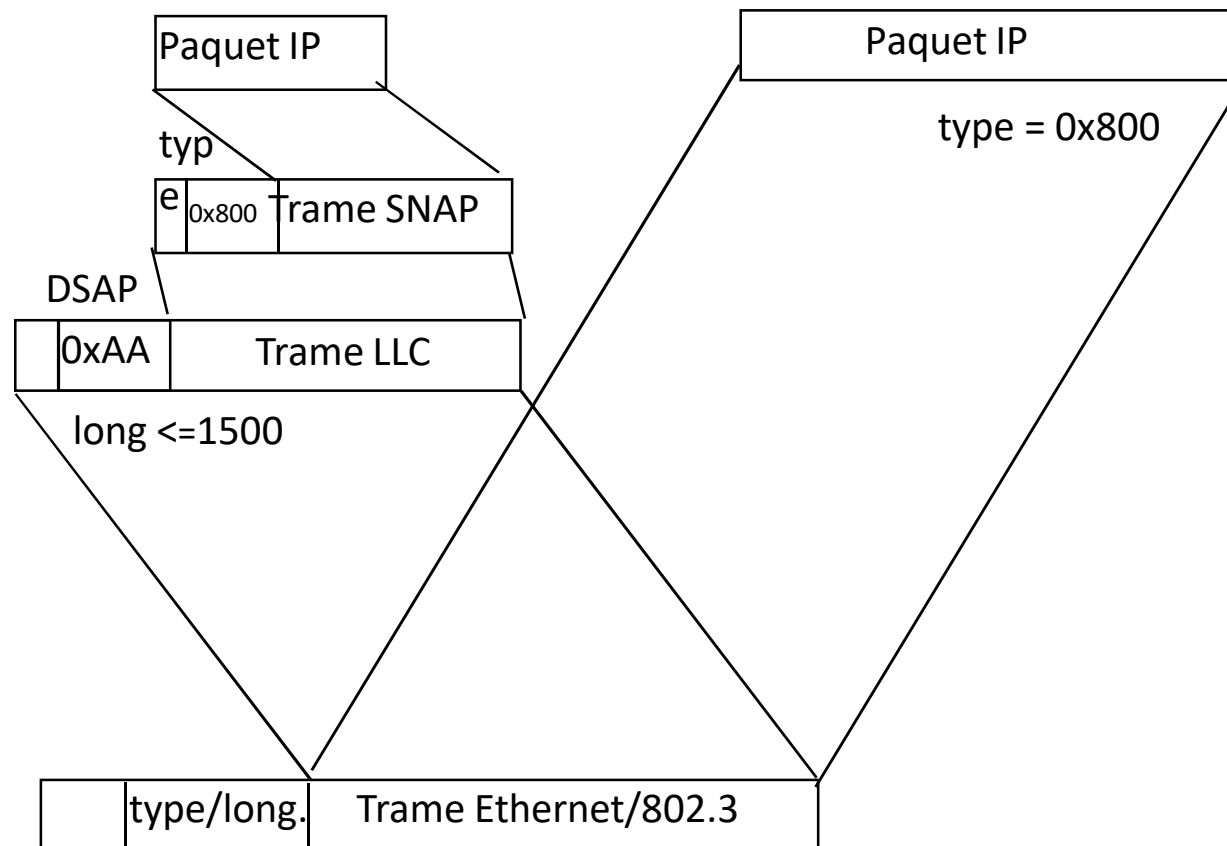
# Sous Couche SNAP

- Ethernet II et LLC/SN



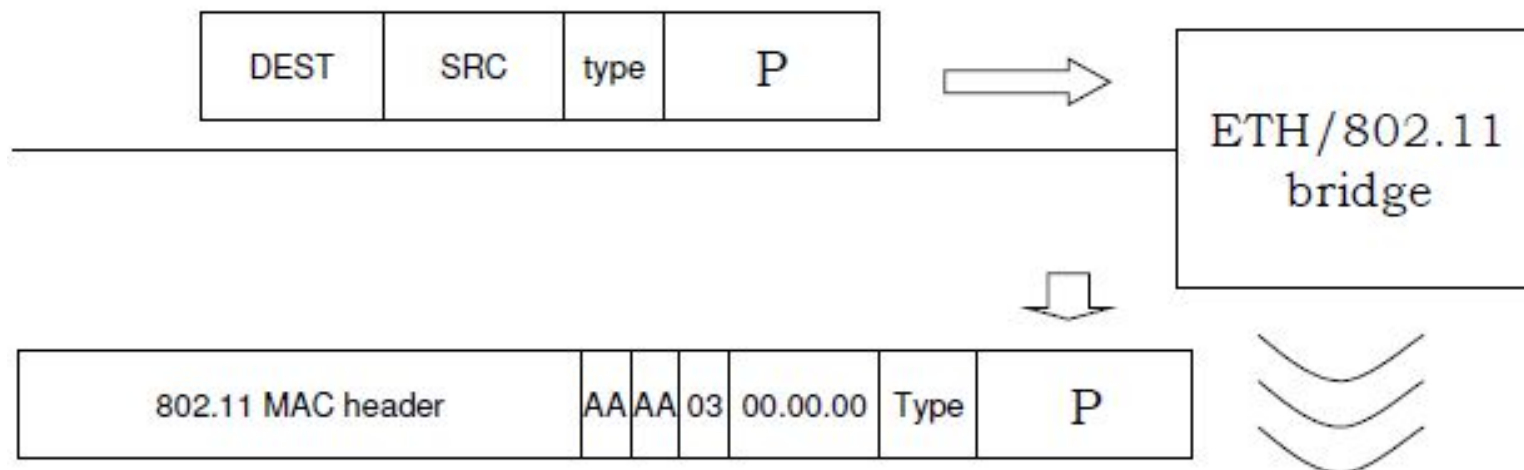
# Sous Couche SNAP

- Encapsulation d'un paquet IP



# Translation des trames

- Ethernet vers Wifi , trois cas :
  - Si trame Ethernet 802.3, les entêtes LLC/SNAP restent intacts.
  - Si trame Ethernet 2 et type  $\neq 0x80F3$  (ARP) et type  $\neq 0x8137$  (IPX), AP convertit la trame en une trame IEEE 802.11 et rajoute les entêtes LLC/SNAP (RFC 1042)



# Translation des trames

- Si trame Ethernet 2 et type = 0x80F3 (ARP) ou type = 0x8137 (IPX), AP convertit la trame en IEEE 802.11 et rajoute les entêtes LLC/SNAP (conformément au protocole (BTEP) « Bridge Tunnel Encapsulation Protocol »)





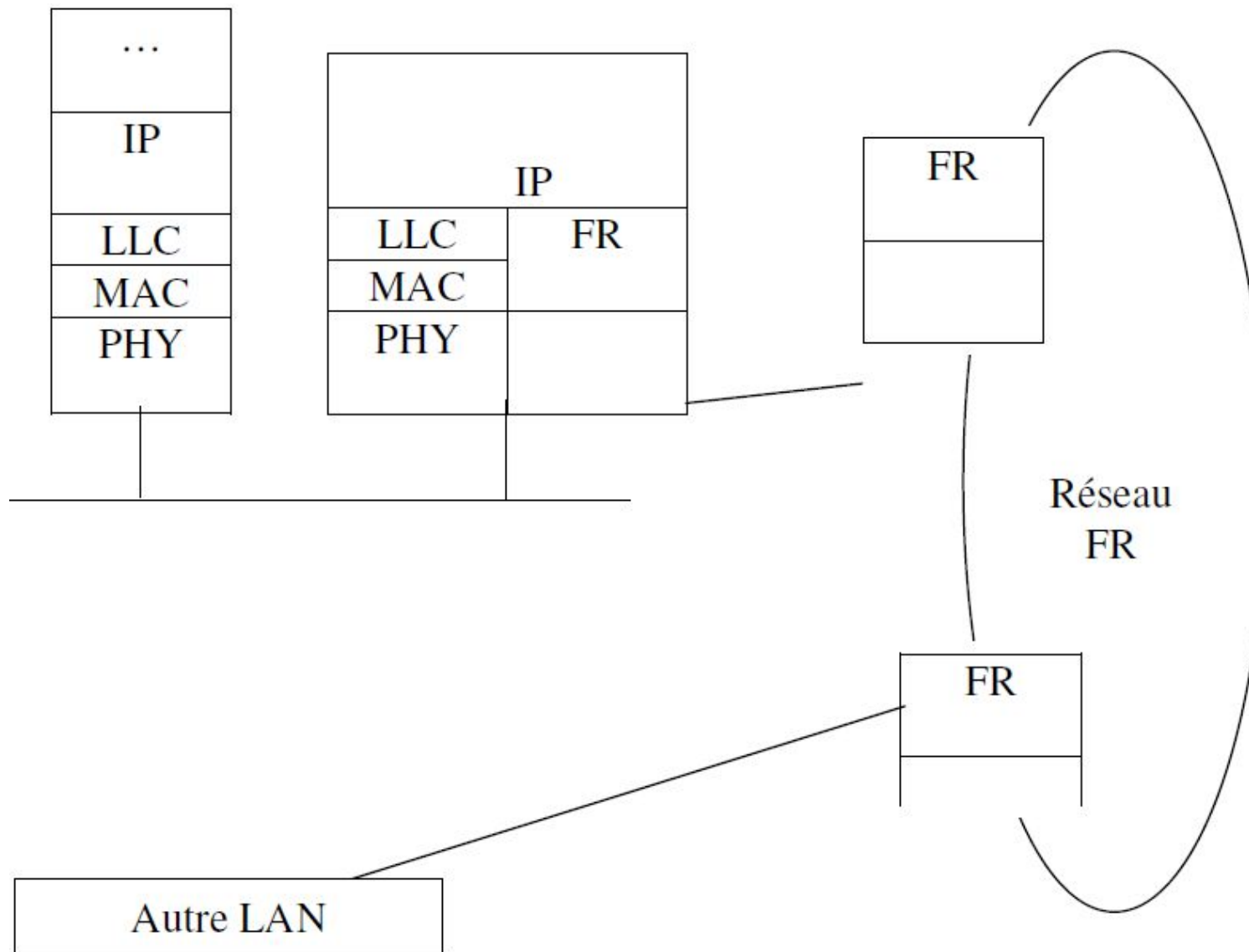
# Translation des trames: Wifi vers Ethernet

- Si trame avec entête SNAP/BTEP (commençant par 0xAA-AA-03-00-00-F8), elle est décapsulée en une trame Ethernet II dont le champ type est repris des 2 derniers octets de l'entête SNAP.
- si la trame avec entête SNAP/RFC 1042 (commençant par 0xAA-AA-03-00-00-00) et si les 2 derniers octets de l'entête SNAP ne sont pas dans la table STT, la trame est décapsulée en une trame Ethernet II dont le champ type est repris de l'entête SNAP.
- si la trame avec entête SNAP/RFC 1042 (commençant par 0xAA-AA-03-00-00-00) et si les 2 derniers octets de l'entête SNAP sont dans la table STT, la trame n'est pas décapsulée elle reste conforme au format IEEE 802.3 et les entêtes LLC/SNAP restent intacts.
- Tout autre trame (IEEE 802.3) passe intacte dans le réseau Ethernet.

# Les routeurs

- Opèrent au niveau de la couche 3 (réseau)
- Couches PHY et LD différentes, mais même couche réseau
- Effectuent le routage à travers l'ensemble des réseaux interconnectés
- Différence avec un pont
  - Plus chers
  - Moins performant, consomme plus de CPU
  - Séparation logique des sous-réseaux (liés à l'architecture des protocoles)
  - Ne reçoivent que les paquets qui leur sont destinés
  - Recherchent la meilleure route
- Utilisent une table de routage

# Interconnexion d'un LAN à travers un réseau FR



exemple d'interconnexion d'un réseau local à un réseau FR « Frame Relay ».

# Les passerelles

- Assurent une compatibilité au niveau des protocoles de couche hautes entre Réseaux hétérogènes
- Permettent à des applications sur des RL de communiquer avec d'autres applications situées sur un ordinateur avec une architecture propriétaire

# TCP/IP - Protocoles de base

- INTRODUCTION
- CONCEPTS DE L'INTERCONNEXION
- LE MODELE TCP/IP
- LE PROTOCOLE INTERNET
- L'ADRESSAGE INTERNET
- LE PROTOCOLE ICMP
- ARP : PROTOCOLE DE RESOLUTION D'ADRESSE
- LE PROTOCOLE UDP
- LE PROTOCOLE TCP

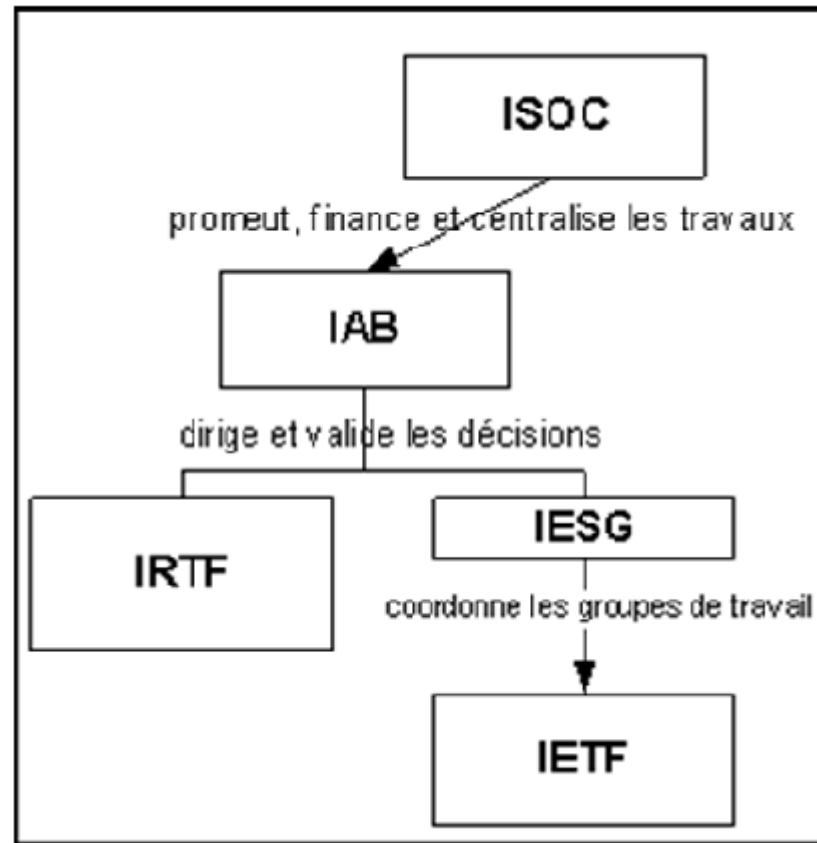
# Introduction

- but : interconnexion de réseaux sur une base planétaire
- Technologie issue des années 1970, de projets DARPA
- Aujourd'hui : 100000 réseaux interconnectés, +millions de machines, +dizaines de millions d'utilisateurs de "l'Internet".
- Interconnecte divers réseaux : Ethernet, TR, X25, FR, FDDI, ...
- La technologie est constituée de protocoles de base (suite TCP/IP) qui offrent les services de base :
  - transport de datagrammes : service élémentaire de commutation de paquets.
  - transport de messages sécurisés : service orienté connexion  
→ acheminer des données en garantissant leur intégrité
- Adaptation de la technologie TCP / IP à la plupart des interfaces matérielles.
- Ces services de base sont indépendants du support de transmission

# Organisation de l'internet

- *L'IAB ( succède ICCB en 84) se charge, en particulier, de l'étude des choix stratégiques pour le développement du réseau Internet et de la définition de l'Internet, crée 2 structures*
- *IRTF (Internet Research Task Force), coordination des efforts de recherche à travers le monde (expérimentation)*
- *IETF (Internet Engineering Task Force) , Normalisation*

# Organisation de l'internet





# RFC « Request For Comment »

- rapports techniques produisant les propositions d'ajout, de modification, ou de normalisation
- RFC :célèbres:
  - RFC 791 : IP
  - RFC 792 ICMP
  - RFC 959 FTP
- maintenues par le NIC "Network Information Center".
- caractérisée par un niveau de maturité ou "state" qui traduit la position dans le chemin de standardisation :
  - Standard : "Proposed", "Draft" (test), "Standard"
  - Non standards : "Experimental" (échec d'un test), "Informational", "Historic«
- Les proportions des protocoles selon le state et le status sont décrites comme suit:

# RFC « Request For Comment »

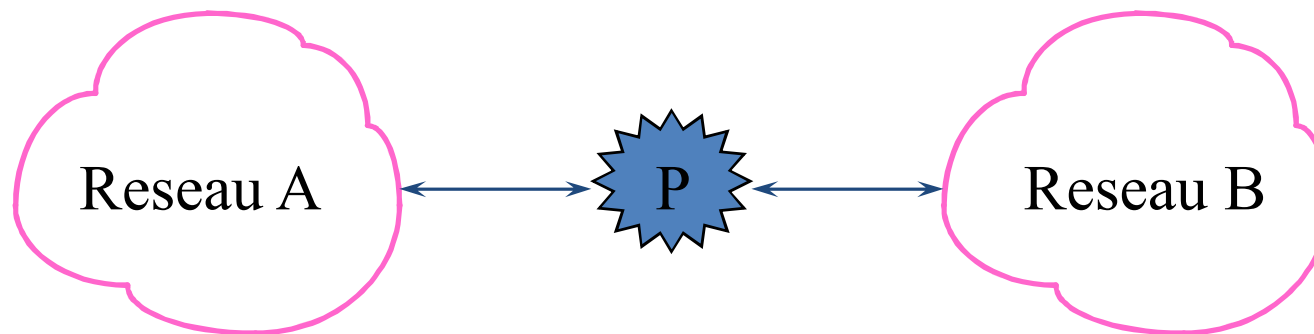
<b><i>STATUS/ STATE</i></b>	<b>Req</b>	<b>Rec</b>	<b>Ele</b>	<b>Lim</b>	<b>Not</b>	
<b>Std</b>	X	XXX	XXX			
<b>Draft</b>	X	X	XXX			
<b>Prop</b>		X	XXX			
<b>Info</b>						
<b>Expr</b>				XXX		
<b>Hist</b>					XXX	

# Concepts de l'interconnexion

- mise en oeuvre d'une couche réseau masquant les détails de la communication physique du réseau et détachant les applications des problèmes de routage.
- faire transiter des informations depuis un réseau vers un autre réseau par des noeuds spécialisés appelés passerelles (*gateway*) ou routeurs (*router*)

# Concepts de l'interconnexion (suite)

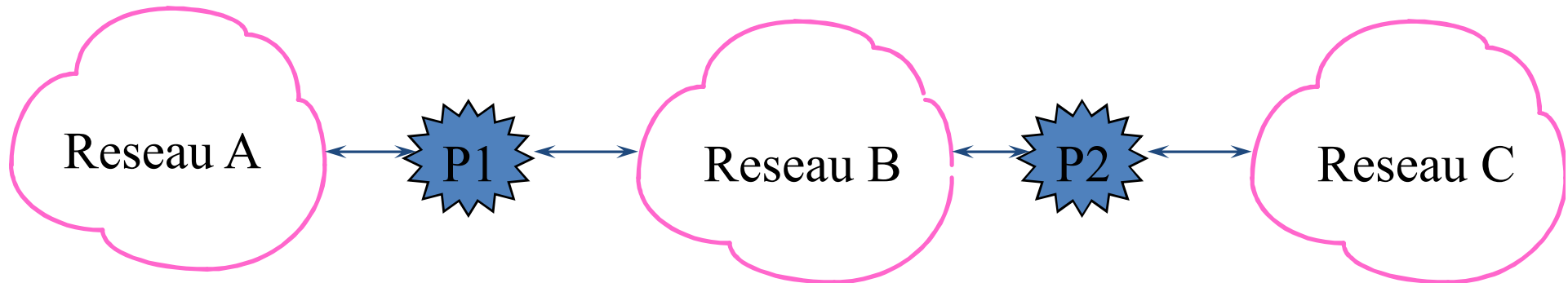
- Les routeurs possèdent une connexion sur chacun des réseaux:



*La passerelle P interconnecte les réseaux A et B.*

- Le rôle de la passerelle P est de transférer sur le réseau B, les paquets circulant sur le réseau A et destinés au réseau B et inversement.

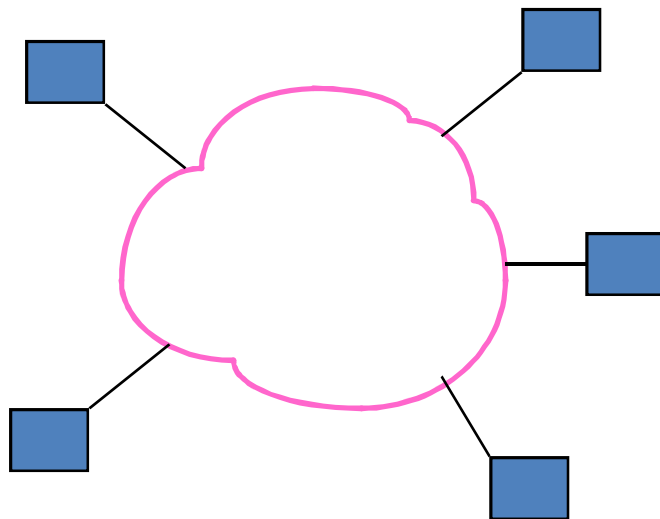
# Concepts de l'interconnexion (suite)



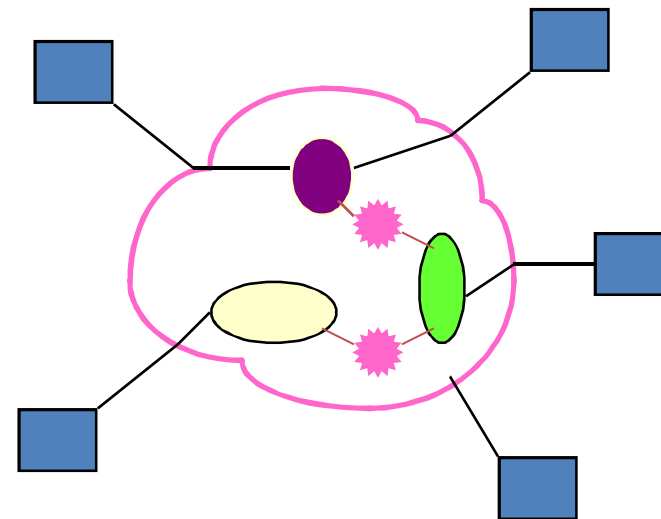
- P1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés aux réseaux B et C
- P1 doit avoir connaissance de la topologie du réseau; à savoir que C est accessible depuis le réseau B.
- Le routage n'est pas effectué sur la base de la machine destinataire mais sur la base du réseau destinataire

# Concepts de l'interconnexion (suite)

- A l'intérieur de chaque réseau, les noeuds utilisent la technologie spécifique de leur réseau (Ethernet, X25, etc)
- Le logiciel d'interconnexion (couche réseau) encapsule ces spécificités et offre un service commun à tous les applicatifs, faisant apparaître l'ensemble de ces réseaux disparates comme un seul et unique réseau.



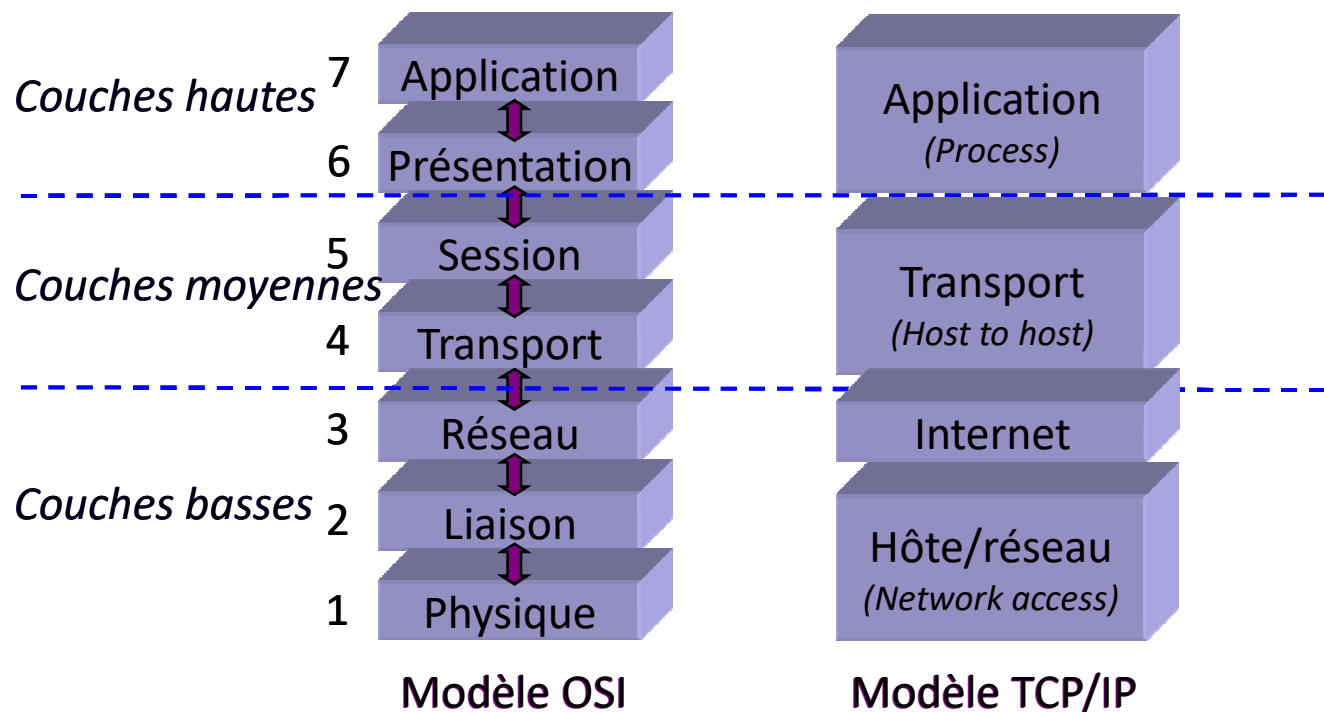
Vue utilisateur



Vue réelle du réseau

# Le modèle TCP/IP

- Il s'agit du modèle de référence du réseau ARPANET et de son successeur Internet.
- Il est ainsi nommé en raison de ses deux principaux protocoles : TCP (*Transmission Control Protocol*) et IP (*Internet Protocol*).
- Le modèle TCP/IP propose une architecture en 4 couches.



# Les principaux protocoles du modèle TCP/IP

*(Processus)*

Application

Telnet FTP SMTP  
POP3 IMAP HTTP

DNS SNMP TFTP  
NFS

*(Host to Host)*

Transport

TCP

UDP

*(Internet)*

Réseau

IP ICMP RIP OSPF ARP RARP

*(Network Access)*

Hôte/Réseau

*Token Ring, Ethernet, WiFi, FDDI, ARPANET, PPP, PPTP, ATM, SONET/SDH...*



# Les principaux protocoles du modèle TCP/IP

- Telnet : Emulation d'une connexion de terminal à un hôte distant
- FTP et TFTP : Transfert de fichier
- SMTP : Envoi de courrier
- POP3 et IMAP : Réception de courrier
- HTTP : Consultation de page web
- DNS : Résolution du nom de domaine en @IP
- SNMP : Gestion du réseau
- NFS : Export de systèmes de fichiers
- IP : Routage des paquets
- ICMP : Messages d'alerte et de diagnostic
- RIP / OSPF : Construction dynamique des tables de routage
- ARP : Résolution d'@IP en @MAC
- RARP : Résolution d'@MAC en @IP

# IP : Internet Protocol

- Interface unique masquant les spécificités de la topologie de l'internet et des réseaux traversés
- Assure :
  - ✓ le transfert des données en mode datagramme
  - ✓ le routage
  - ✓ la ségmentation
  - ✓ un contrôle de flux rudimentaire
- ☞ Le service offert par le protocole IP est dit non fiable :
  - remise de paquets non garantie,
  - sans connexion (paquets traités indépendamment les uns des autres),
  - pour le mieux (*best effort*, les paquets ne sont pas éliminés sans raison).

# IP : Internet Protocol (le datagramme)

## ● Le datagramme IP

– unité de transfert de base dans un réseau internet

0		4		8		16		19		24		31	
VERS		HLEN		Type de service				Longueur totale					
Identification						Flags		Offset fragment					
Durée de vie				Protocole				Somme de contrôle Header					
Adresse IP Source													
Adresse IP Destination													
Options IP (eventuellement)										Padding			
Données													
										...			

# L'adressage Internet

- But
  - Fournir un service de communication universelle
  - Pour communiquer avec une autre machine de 'interconnexion
- Solution
  - Identification d'une machine : (1 nom, 1 adresse, 1 route)
    - Protocoles de haut niveau tel que DNS
      - Nom = mnémotechnique pour les utilisateurs
      - Adressage "à plat" par opposition à un adressage hiérarchisé
    - Protocoles de bas niveau tel que ARP
      - Adresse = identificateur universel de la machine
      - Adresse binaire dite "Internet address" ou "IP address »
    - Protocoles de niveau réseau tel que RIP

# L'adressage Internet: IP address

- Assure un routage codée sur 32 bits : couple (netid, hostid)
  - netid identifie le réseau
  - hostid identifie la machine sur ce réseau
- (netid, hostid) structurée de manière à définir cinq classes d'adresse

# L'adressage Internet (suite)

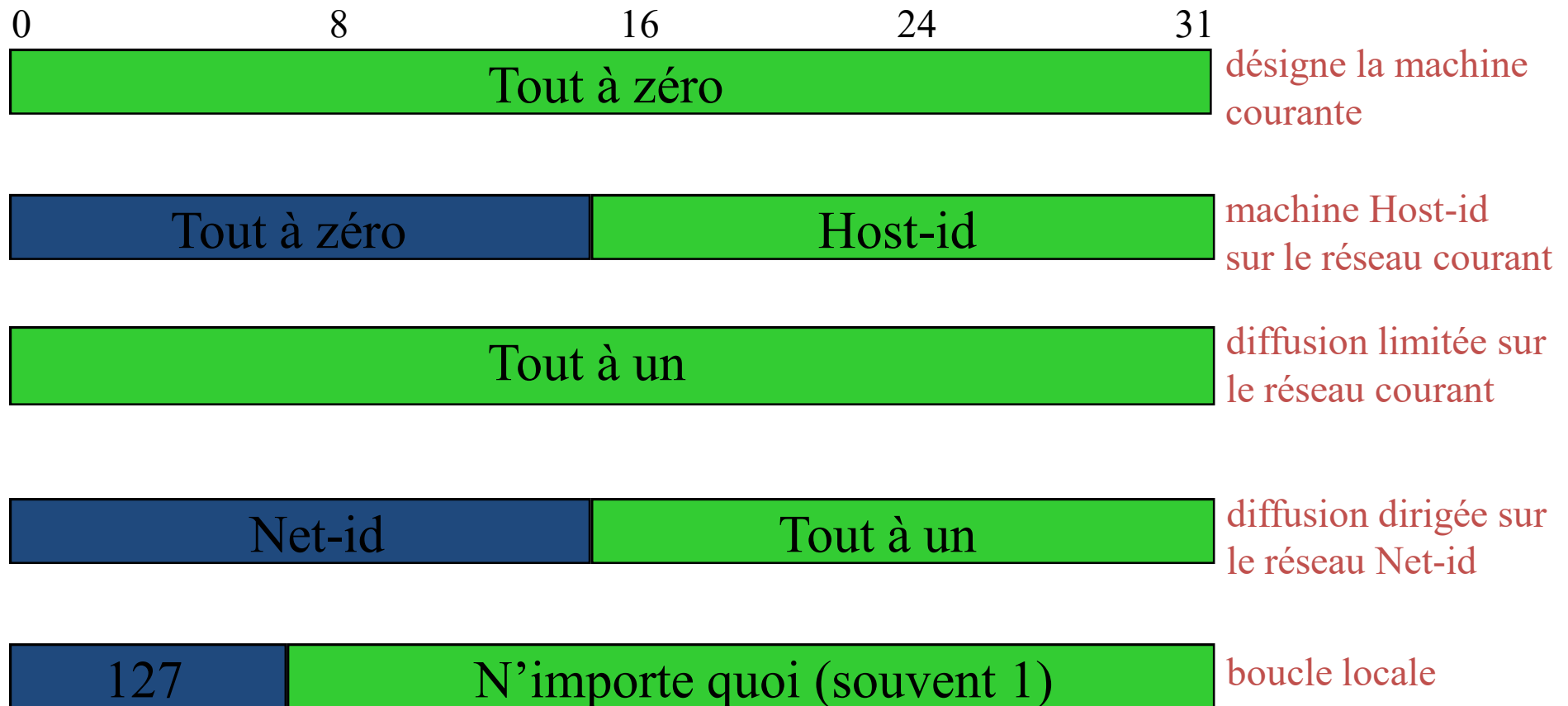


# L'adressage Internet (suite)

- Notation décimale des adresses IP
  - Notation de 4 entiers décimaux séparés par un point
    - 1 entier représente un octet de l'adresse IP
    - Ex : 10000000 00001010 00000010 00011110 s'écrit 128.10.2.30
- Adresses particulières
  - Adresse de boucle locale : 127.0.0.0
  - Réservée pour désigner la machine locale
    - communication intra-machine
    - netid =127 ne doit jamais être véhiculée sur un réseau et un routeur
  - Adresse de diffusion limitée : netid ne contient que des 1
    - Concerne uniquement le réseau physique associé
  - Adresse de diffusion dirigée : hostid ne contient que des 1
    - Concerne toutes les machines du réseau netid
    - Ne peut être attribuée à une machine réelle
    - Ex: 193.95.17.255 désigne toutes les machines du réseau 193.95.17.0

# L'adressage Internet (suite)

- Résumé





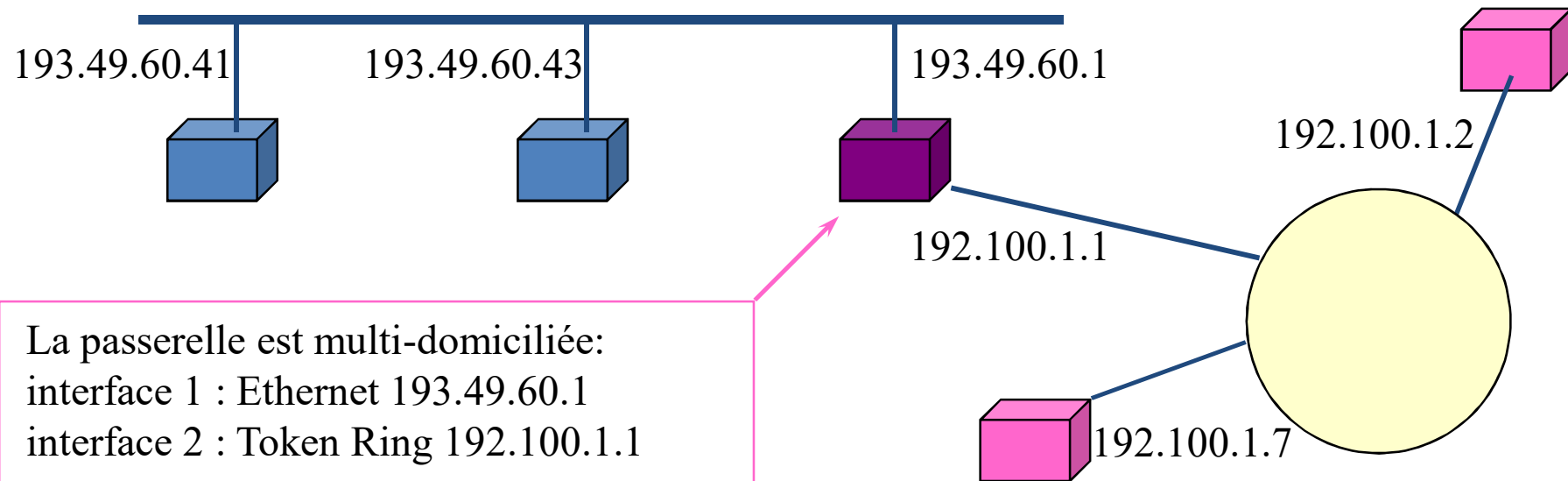
# L'adressage Internet (suite)

## ● Adresses et connexions

Une adresse IP => une interface physique  
=> une connexion réseau.

- S'applique particulièrement aux routeurs qui possèdent par définition plusieurs connexions à des réseaux différents
- A une machine, est associé un certain nombre  $N$  d'adresses IP. Si  $N > 0$  la machine (ou passerelle) est multi-domiciliée.

# L'adressage Internet (suite)

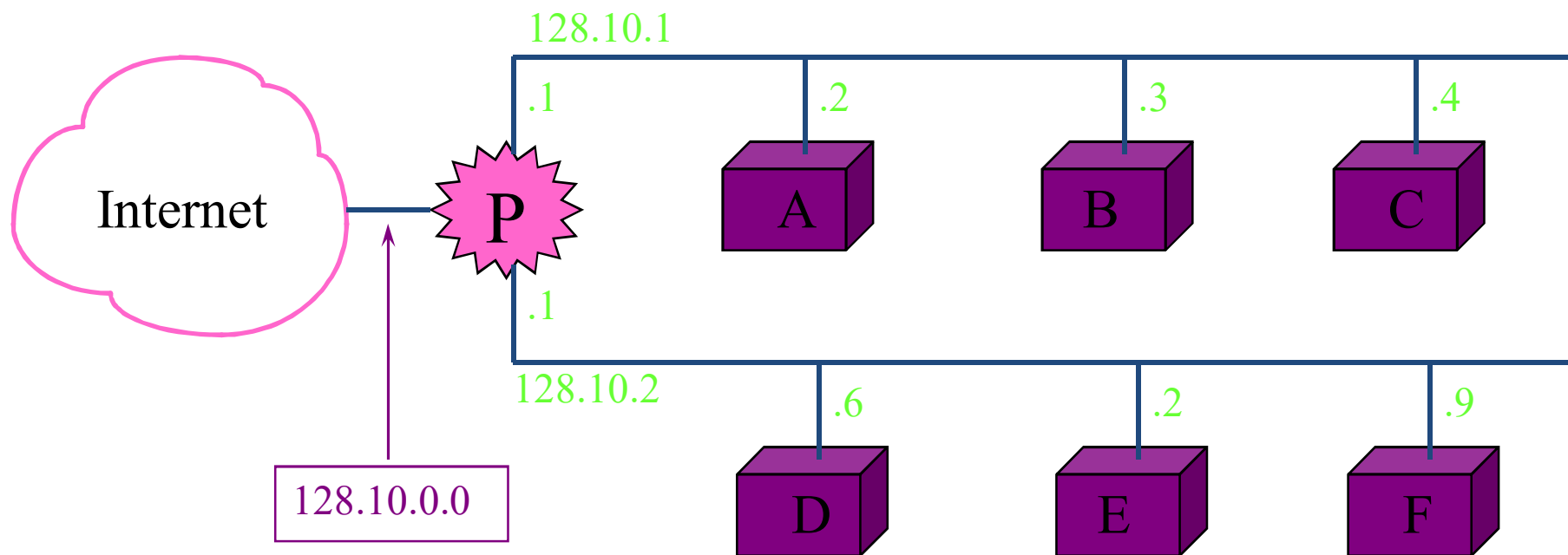


# Le sous-adressage

- Croissance du nombre de réseaux de l'Internet,
- limiter la consommation d'adresses IP:
  - la gestion administrative des adresses IP,
  - la taille des tables de routage des passerelles,
  - la taille des informations de routage,
  - le traitement effectué au niveau des passerelles.
- Principes
  - A l'intérieur d'une entité associée à une adresse IP de classe A, B ou C, plusieurs réseaux physiques partagent cette adresse IP.
  - On dit alors que ces réseaux physiques sont des sous-réseaux (subnet) du réseau d'adresse IP.

# Le sous-adressage (suite)

Les sous-réseaux 128.10.1.0 et 128.10.2.0 sont notés seulement avec le **NetId**, les machines seulement avec le **Hostid** ; exemple IP(F) = 128.10.2.9



Un site avec deux réseaux physiques utilisant le sous-adressage de manière à ce que ses deux sous-réseaux soient couverts par une seule adresse IP de classe B.  
La passerelle P accepte tout le trafic destiné au réseau 128.10.0.0 et sélectionne le sous-réseau en fonction du troisième octet de l'adresse destination.

# Le sous-adressage (suite)

- Le choix du découpage dépend des perspectives d'évolution du site:
  - Exemple Classe B :
    - 8 bits pour les parties réseau et machine :  
256 sous-réseaux et 254 machines par sous-réseau
    - 3 bits pour la partie réseau et 13 bits pour le champ machine:  
8 réseaux de 8190 machines par sous-réseau.
  - Exemple Classe C :
    - 4 bits pour la partie réseau et 4 bits pour le champ machine:  
16 réseaux de 14 machines par sous-réseau.
- toutes les machines du réseau doivent s'y conformer sous peine de dysfonctionnement du routage ==> configuration rigoureuse.

# Le sous-adressage (suite)

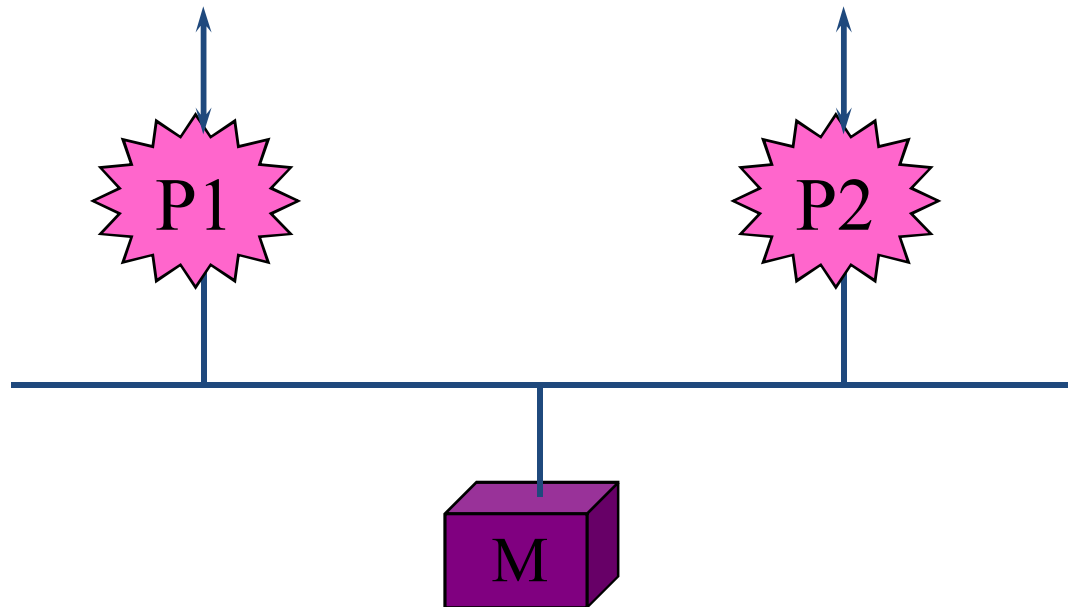
- Utilisation de masques
- Le sous-adressage ==> masque de 32 bits associé au sous-réseau.
- Bits du masque de sous-réseau (subnet mask) :
  - positionnés à 1 : partie réseau,
  - positionnés à 0 : partie machine
- 11111111 11111111 11111111 00000000  
==> 3 octets pour le champ réseau, 1 octet pour le champ machine
- Les notations suivantes sont utilisées :
  - décimale pointée; exemple : 255.255.255.0
  - triplet : { <ident. réseau> , <ident. sous-réseau> <ident. machine> } ; cette notation renseigne les valeurs mais pas les champs de bits;  
exemple { -1, -1, 0 } , { 128.10, 27, -1 }.
  - adresse réseau/masque : 193.49.60.0/27 (27=# bits contigus du masque)

# Routage des datagrammes

- permet à un datagramme d'être acheminé vers le destinataire
- Le chemin parcouru est le résultat du processus de routage qui effectue les choix nécessaires afin d'acheminer le datagramme.
- Les routeurs forment une structure coopérative  
un datagramme transite de passerelle en passerelle jusqu'à ce que l'une d'entre elles le délivre à son destinataire.
- Machines et routeurs participent au routage :
  - les machines doivent déterminer si le datagramme doit être:
    - délivré sur le réseau physique sur lequel elles sont connectées (routage direct)
    - acheminé vers une passerelle; dans ce cas (routage indirect), elle doit identifier la passerelle appropriée.
  - les routeurs effectuent le choix de routage vers d'autres passerelles afin d'acheminer le datagramme vers sa destination finale.

# Routage des datagrammes (suite)

- Le routage indirect repose sur une table de routage IP, présente sur toute machine et passerelle, indiquant la manière d'atteindre un ensemble de destinations.



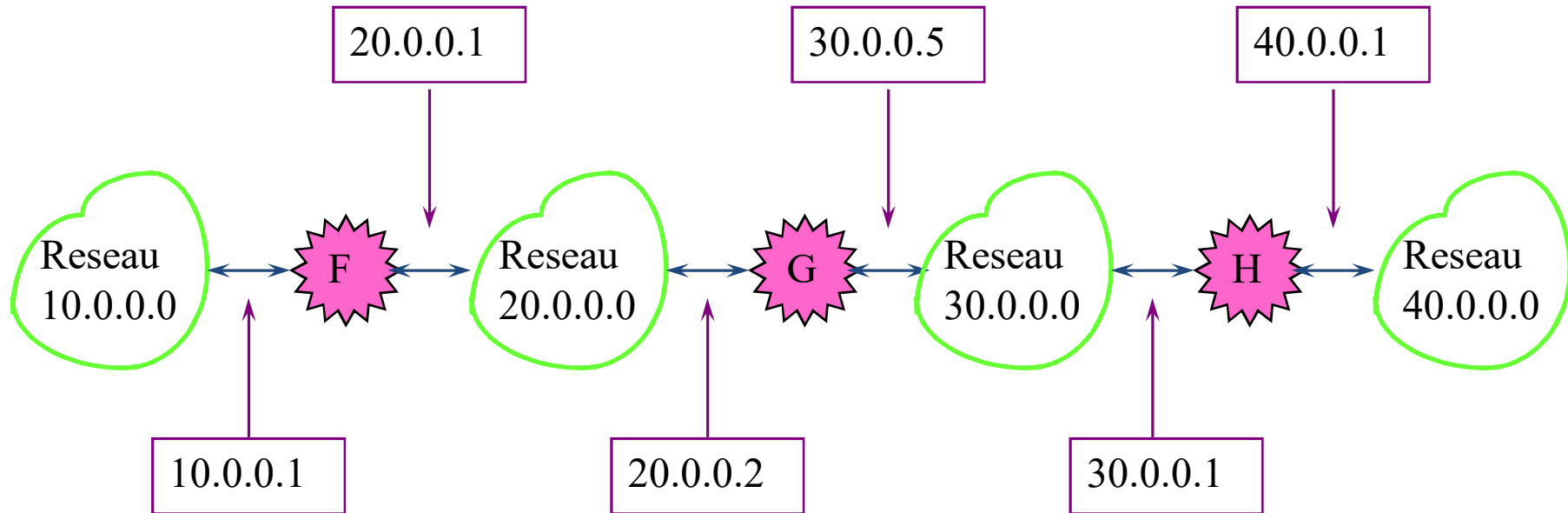
M est mono-domiciliée et doit acheminer les datagrammes vers une des passerelles P1 ou P2; elle effectue donc le premier routage. Dans cette situation, aucune solution n'offre un meilleur choix.



# Routage des datagrammes (suite)

- Les tables de routage IP, pour des raisons évidentes d'encombrement, renseignent seulement les adresses réseaux
- une table de routage contient des couples (R, P)
  - R est l'adresse IP d'un réseau destination
  - P est l'adresse IP de la passerelle correspondant au prochain saut dans le cheminement vers le réseau destinataire.
- La passerelle ne connaît pas le chemin complet pour atteindre la destination.
- une table de routage d'une machine M contenant des couples (R, P) ; P et M sont connectés sur le même réseau

# Routage des datagrammes (suite)



<i>Pour atteindre les machines du réseau</i>	10.0.0.0	20.0.0.0	30.0.0.0	40.0.0.0
<i>Router vers</i>	20.0.0.1	direct	direct	30.0.0.1

Table de routage de G

# Routage des datagrammes (suite)

- Mise à jour de la table de routage :
  - Manuelle = Routage statique
    - commandes "route" des station unix
    - langage de commande des routeurs (ip route ...)
  - Automatique = Routage dynamique
    - Processus sur les stations et les routeurs
    - Echanges d'informations de routage : protocoles de routage: RIP
  - Mixte : Routage statique et dynamique

# Routage Dynamique

- Deux types de protocoles de routage
  - Interne : Interior Protocol
    - au sein d'un même Autonomous System
    - ex.: RIP, OSPF, IGRP ...
    - Détermine dynamiquement la meilleure route vers chaque réseau ou sous-réseau.
  - Externe : Exterior Protocol
    - Utilisé pour interconnecter les grands réseaux entre 2 Autonomous Systems (ou plus)
    - ex.: EGP, BGP ...
    - "Interdomain routing protocols"
- On peut utiliser n'importe quel protocole, mais ...

# Le Protocole ICMP

- Envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles.
- ICMP rapporte les messages d'erreur à l'émetteur
  - machine destination déconnectée,
  - durée de vie du datagramme expirée,
  - congestion de passerelles intermédiaires ...
- Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial.
- Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP (routés comme un datagramme IP)
- un message ICMP ne peut donner naissance à un autre message ICMP (évite l'effet cumulatif).

# ICMP : format des messages

TYPE                      8 bits; type de message  
CODE                      8 bits; informations complément.  
CHECKSUM    16 bits; champ de contrôle  
HEAD-DATA    en-tête datagramme + 64 premiers  
bits des données.

<u>TYPE</u>	<u>Message ICMP</u>	<u>TYPE</u>	<u>Message ICMP</u>
0	Echo Reply	13	Timestamp Request
3	Destination Unreachable	14	Timestamp Reply
4	Source Quench	15	Information Request (obsolete)
5	Redirect (change a route)	16	Information Reply (obsoletè)
8	Echo Request	17	Address Mask Reques
11	Time Exceeded (TTL)	18	Address Mask Reply
12	Parameter Problem with a Datagram		

# ICMP (types)

Type	Code	Description	Type	Code	Description
<a href="#">0</a>	0	Réponse à une demande d'écho	<a href="#">10</a>	0	Sollicitation routeur
<a href="#">3</a>	0	Réseau inaccessible	<a href="#">11</a>	0	Durée de vie écoulée avant d'arrivée à destination
<a href="#">3</a>	1	Hôte inaccessible	<a href="#">11</a>	1	Temps limite de réassemblage du fragment dépassé
<a href="#">3</a>	2	Protocole inaccessible	<a href="#">12</a>	0	En-tête IP invalide
<a href="#">3</a>	3	Port inaccessible	<a href="#">12</a>	1	Manque d'une option obligatoire
<a href="#">3</a>	4	Fragmentation nécessaire mais interdite	<a href="#">12</a>	2	Mauvaise longueur
<a href="#">3</a>	5	Echec de routage par la source	<a href="#">13</a>	0	Requête pour un marqueur temporel
<a href="#">3</a>	6	Réseau de destination inconnu	<a href="#">14</a>	0	Réponse pour un marqueur temporel
<a href="#">3</a>	7	Hôte de destination inconnue	<a href="#">15</a>	0	Demande d'adresse réseau
<a href="#">3</a>	8	Machine source isolée	<a href="#">16</a>	0	Réponse d'adresse réseau
<a href="#">3</a>	9	Réseau de destination interdit administrativement	<a href="#">17</a>	0	Demande de masque de sous réseau
<a href="#">3</a>	10	Hôte de destination interdite administrativement	<a href="#">18</a>	0	Réponse de masque de sous réseau
<a href="#">3</a>	11	Réseau inaccessible pour ce type de service			
<a href="#">3</a>	12	Hôte inaccessible pour ce type de service			
<a href="#">3</a>	13	Communication interdite par un filtre			
<a href="#">3</a>	14	Host Precedence Violation			
<a href="#">3</a>	15	Precedence cutoff in effect			
<a href="#">4</a>	0	Volume de donnée trop importante			
<a href="#">5</a>	0	Redirection pour un hôte			
<a href="#">5</a>	1	Redirection pour un hôte et pour un service donné			
<a href="#">5</a>	2	Redirection pour un réseau			
<a href="#">5</a>	3	Redirection pour un réseau et pour un service donné			
<a href="#">8</a>	0	Demande d'écho			
<a href="#">9</a>	0	Avertissement routeur			

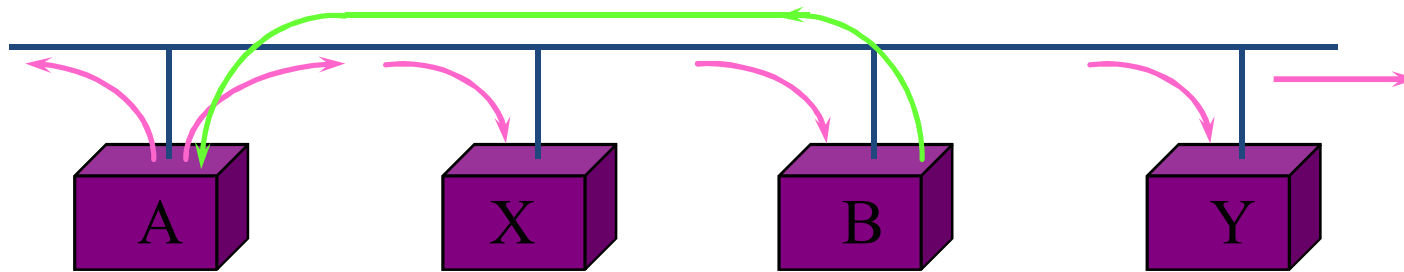
# ARP: Address Resolution Protocol

- Le besoin
  - La communication entre machines ne peut s'effectuer qu'à travers l'interface physique
  - Les applicatifs ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique?
- La solution : ARP
  - Mise en place dans TCP/IP d'un protocole de bas niveau appelé Address Resolution Protocol (ARP)
  - Rôle de ARP : fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP de la machine destinatrice
- La technique :
  - Diffusion d'adresse sur le réseau physique
  - La machine d'adresse IP émet un message contenant son adresse physique
  - Les machines non concernées ne répondent pas
  - Gestion cache pour ne pas effectuer de requête ARP à chaque émission



# ARP: Address Resolution Protocol

- L'association **adresse physique - adresse IP** de l'émetteur est incluse dans la requête ARP de manière à ce que les récepteurs enregistrent l'association dans leur propre mémoire cache



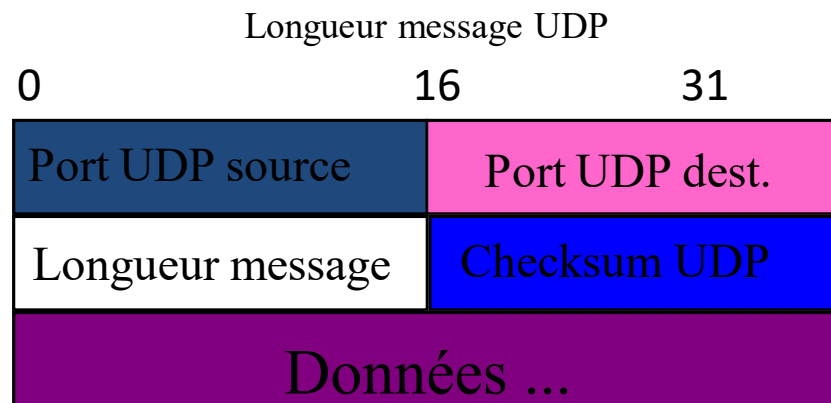
- Pour connaître l'adresse physique de B, PB, à partir de son adresse IP IB, la machine A **diffuse une requête ARP** qui contient l'adresse IB vers toutes les machines; la machine B **répond avec un message ARP** qui contient la paire (IB, PB).

# UDP : User Datagram Protocol

- UDP : protocole de transport sans connexion de service applicatif:
  - émission de messages applicatifs : sans établissement de connexion au préalable
  - l'arrivée des messages et l'ordonnancement non garantis.
- Identification du service : les ports
  - les adresses IP désignent les machines
  - Un processus désire entrer en communication avec un autre, doit adresser le processus s'exécutant sur cette machine.
  - L'adressage de ce processus est effectué selon un concept abstrait indépendant du système d'exploitation des machines
  - Ces destinations abstraites permettant d'adresser un service applicatif s'appellent des **ports** de protocole.
  - L'émission d'un message se fait sur la base d'un port source et un port destinataire.

# UDP : format des messages

- également appelés des datagrammes UDP.
- contiennent deux parties : « en-tête UDP » + « données UDP »



Format des messages UDP

- ✓ Les ports sont utilisés par UDP pour démultiplexer les datagrammes destinés aux processus.
- ✓ Le port source est facultatif (égal à zéro si non utilisé).
- ✓ La longueur du message est exprimée en octets (8 au minimum) (en-tête + données), le champ de contrôle est optionnel (0 si non utilisé).

# UDP : les ports standards

- Les ports sont numérotés
- Certains ports sont réservés (*well-known port assignments*) :

<u>No port</u>	<u>Mot-clé</u>	<u>Description</u>
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
37	TIME	Time
42	NAMESERVER	Host Name Server
53	DOMAIN	Domain Name Server
67	BOOTPS	Boot protocol server
68	BOOTPC	Boot protocol client
69	TFTP	Trivial File transfert protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management prot.

- D'autres ports (non réservés) peuvent être assignés dynamiquement aux applications.

# TCP : Transmission Control Protocol

- transport fiable de la technologie TCP/IP.
  - fiabilité = illusion assurée par le service
  - transferts tamponés : découpage en segments
  - connexions bidirectionnelles et simultanées
- service en mode connecté
- garantie de non perte de messages ainsi que de l'ordonnancement

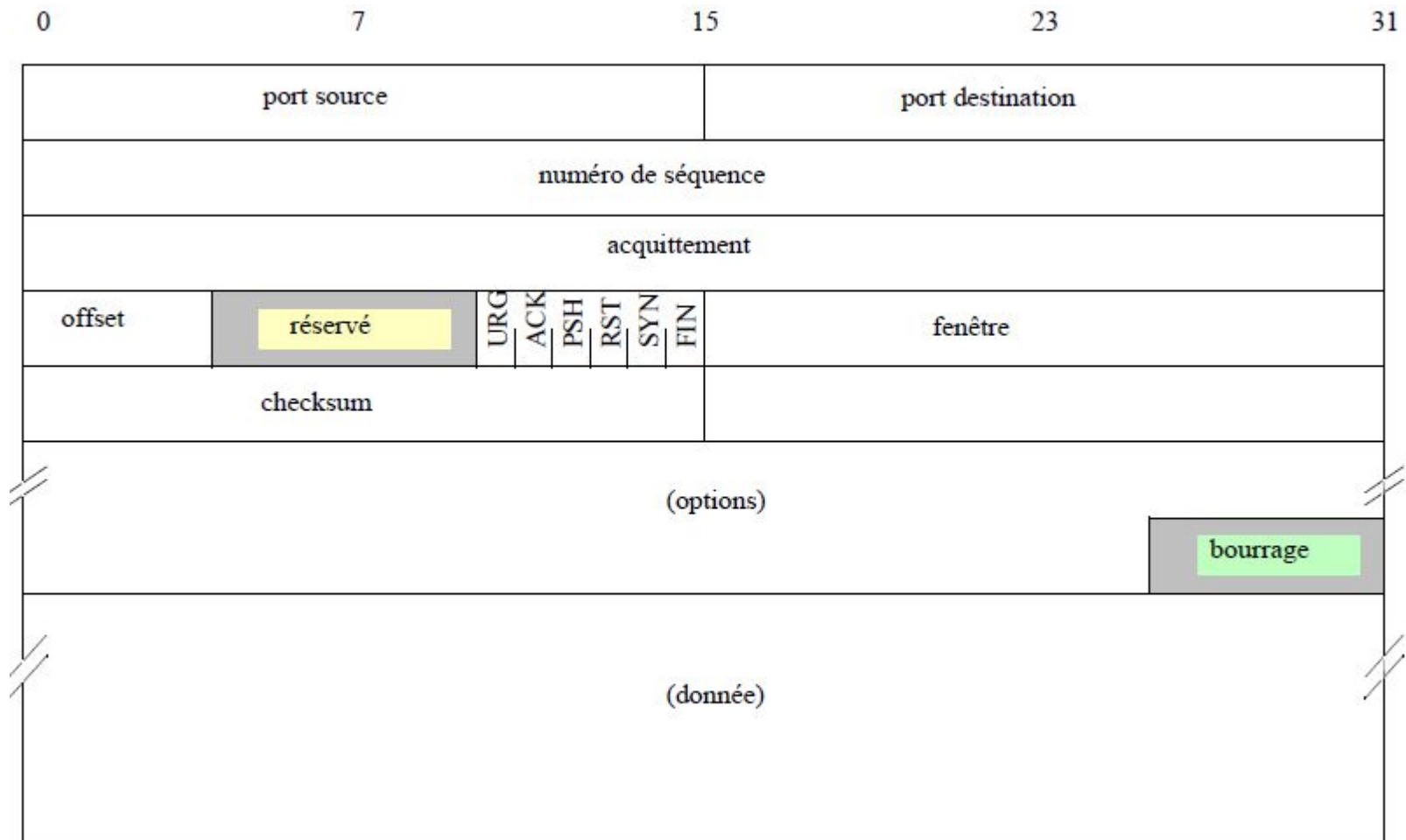
# TCP : La connexion

- une connexion de type circuit virtuel est établie avant que les données ne soient échangées : appel + négociation + transferts
- Une connexion = une paire d'extrémités de connexion
- Une extrémité de connexion = couple (adresse IP, port)
- Exemple de connexion : ((124.32.12.1, 1034), (19.24.67.2, 21))
- Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciation)
- La mise en oeuvre de la connexion se fait en deux étapes :
  - une application (extrémité) effectue une ouverture passive en indiquant qu'elle accepte une connexion entrante,
  - une autre application (extrémité) effectue une ouverture active pour demander l'établissement de la connexion.

# TCP : ports standards

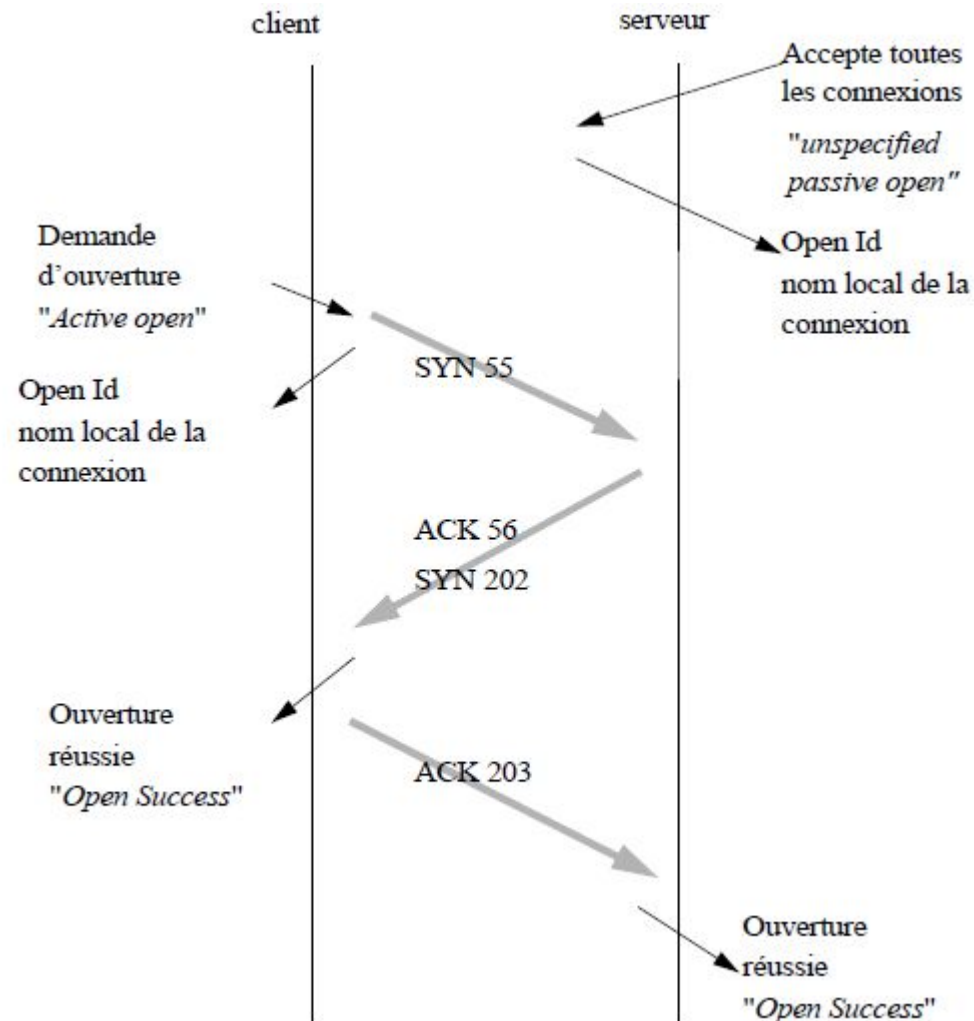
<u>No port</u>	<u>Mot-clé</u>	<u>Description</u>
20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
79	FINGER	Finger
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3
111	SUNRPC	SUN Remote Procedure Call

# TCP: Format des Messages

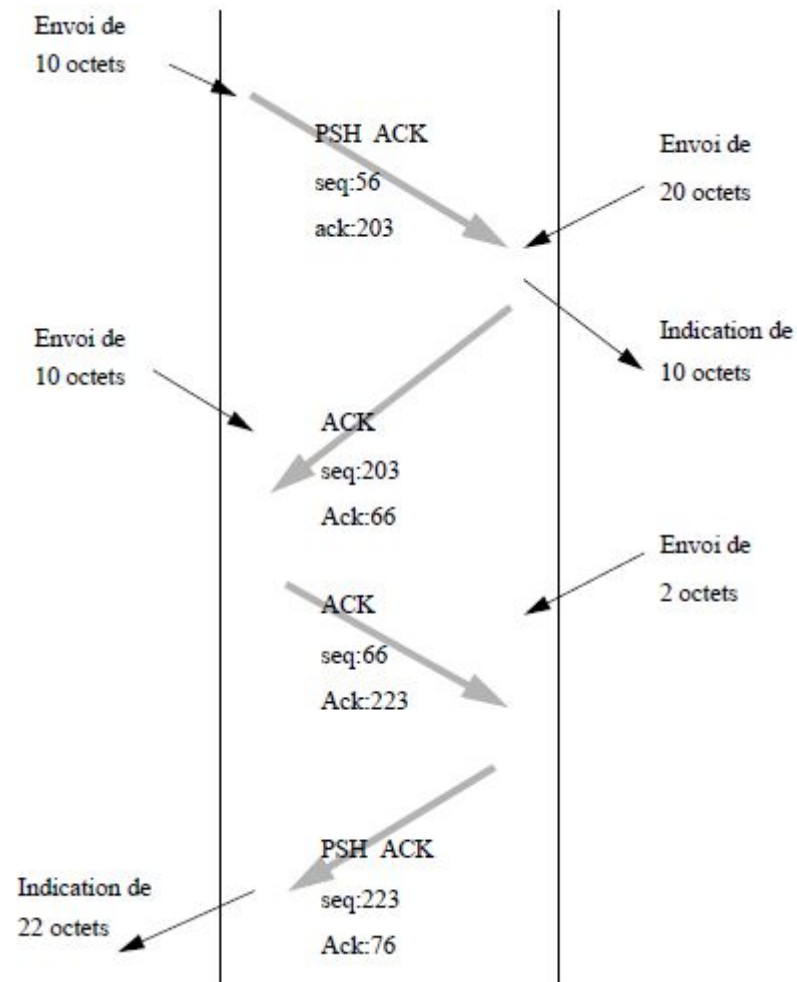




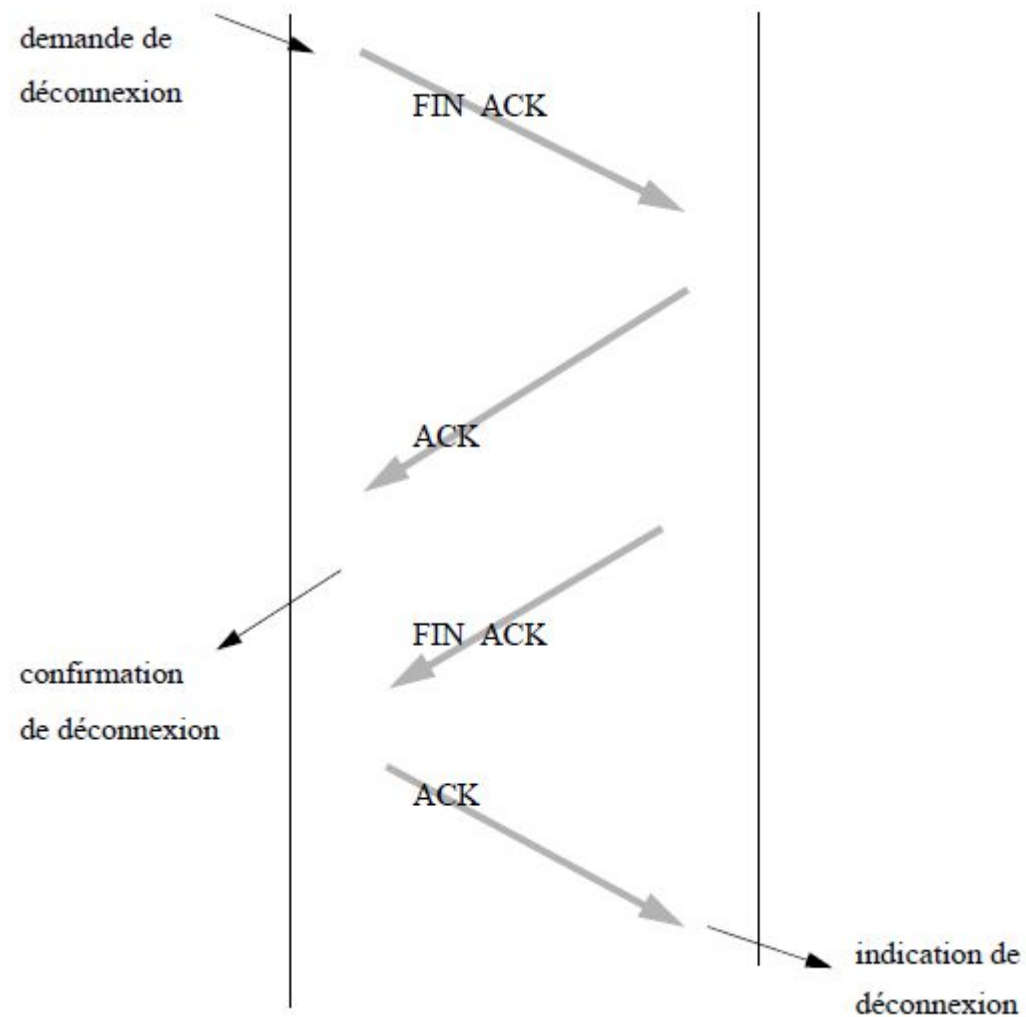
# TCP: Ouverture de la connexion



# TCP: Transfert de données



# TCP: Fermeture de connexion



# TCP: ADAPTATION À L'ENVIRONNEMENT

- Gestion dynamique des valeurs temporisation
- RTT : *Round Trip Time*. Temps mesuré pour un aller et retour.
- L'estimation du RTT va déterminer le temporisateur de *Retransmission Time Out (RTO)*.
- Ne pas prendre en compte le RTT lors de retransmissions (algorithme de Karn)

On a :

$erreur = mesure - moyenne$

$moyenne = moyenne - \alpha \times erreur$

$deviation = deviation + \beta \times (|erreur| - deviation)$

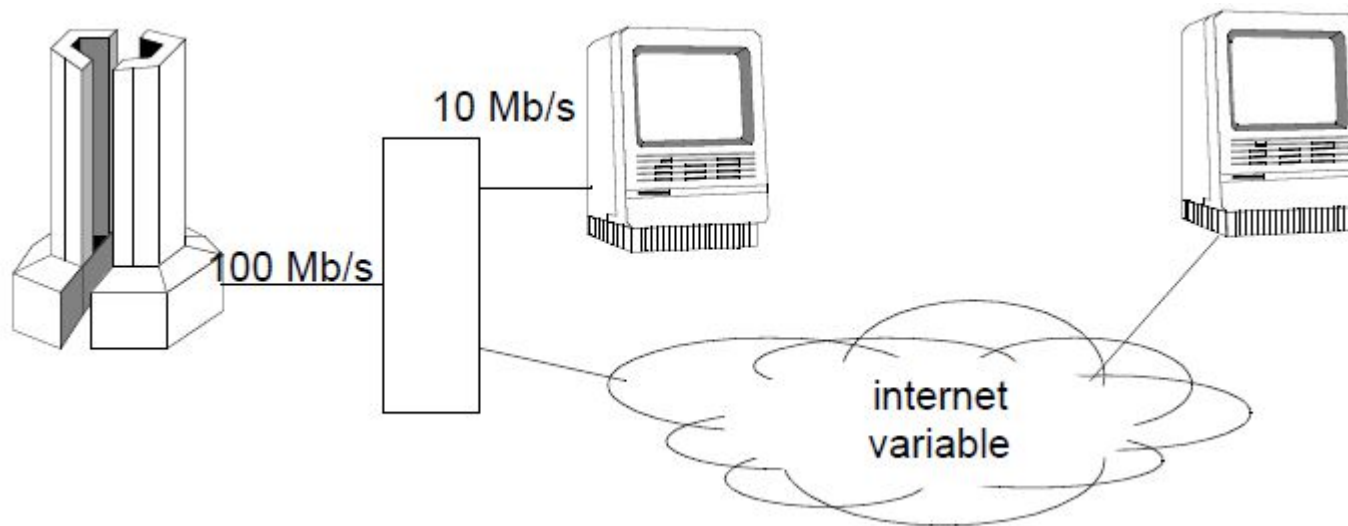
et

$RTO = moyenne + 4 \times deviation$

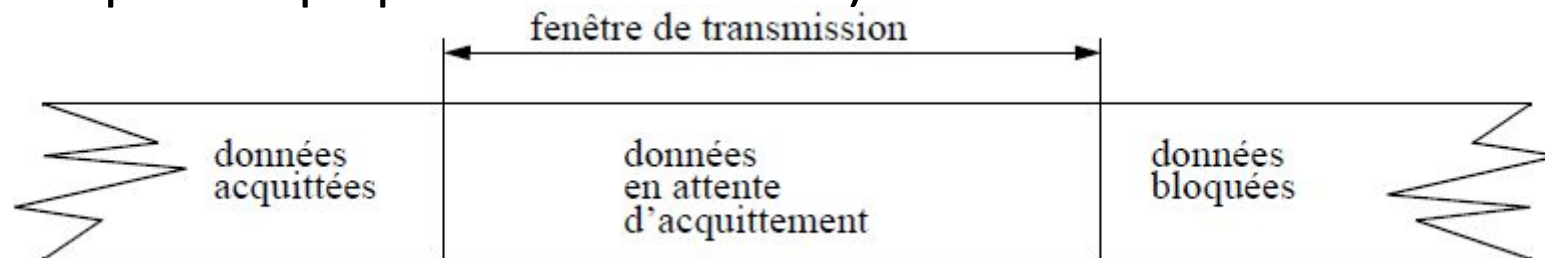
+ L'utilisation d'une bonne estimation améliore les performances

# TCP: Contrôle de Flûx

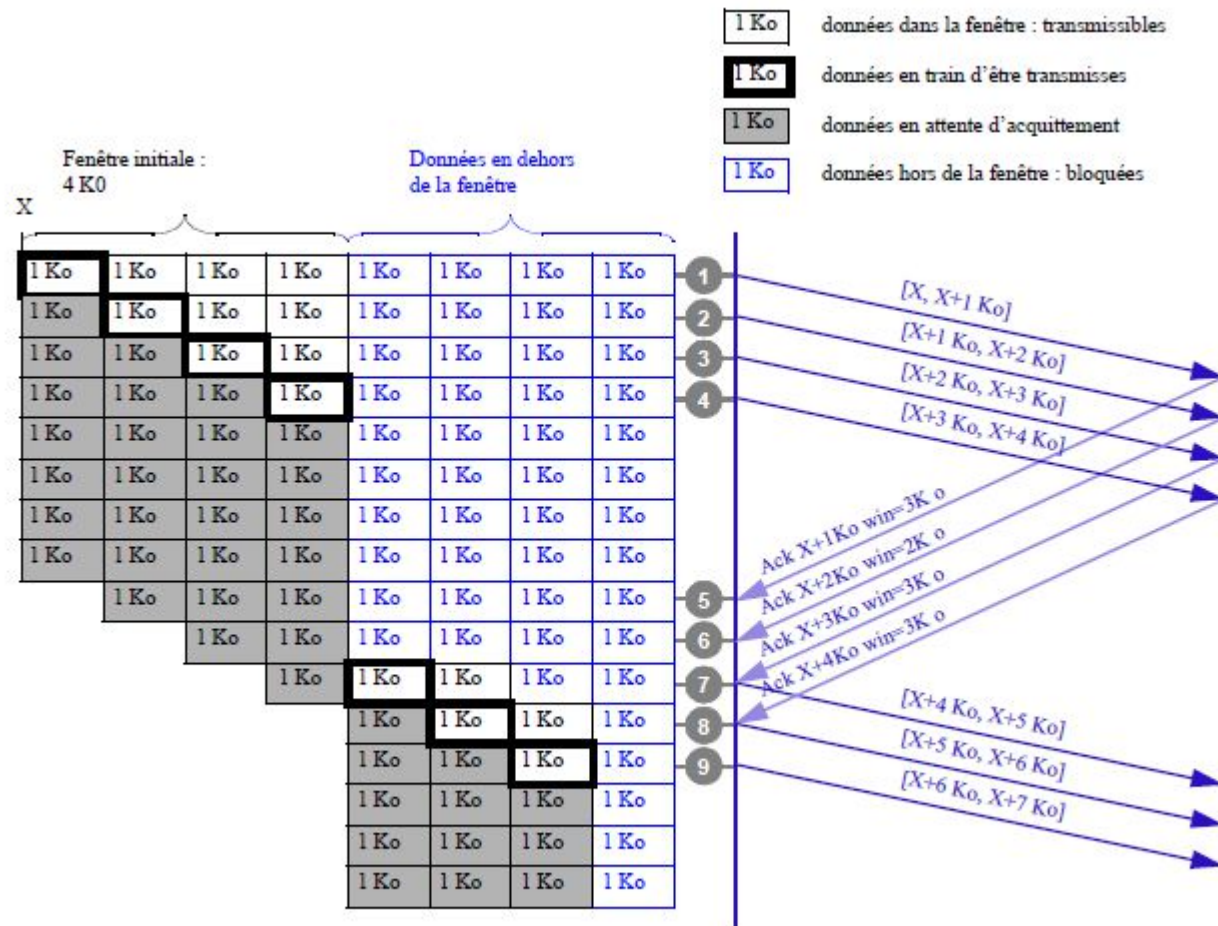
- Adapter dynamiquement le trafic émis à la configuration du réseau et au récepteur.



Basé sur la taille d'une fenêtre de retransmission (nombre d'octets non acquittés qui peuvent être émis)



# TCP: Fenêtre d'anticipation



# Congestion

Le débit du réseau varie (dépend des autres utilisateurs), il peut y avoir congestion des routeurs.

- Les congestions font perdre des paquets, qui seront retransmis, et qui à leur tour feront des congestions, qui feront perdre des paquets et qui ...
  - La perte d'un paquet provient plus souvent d'une congestion que d'une erreur de transmission.
  - La perte d'un paquet peut se détecter quand l'émetteur reçoit plusieurs acquittements identiques.
  - La perte de plusieurs paquets se détecte quand la temporisation de retransmission se déclenche.
- Pour s'adapter au débit, faire varier la taille de la fenêtre d'anticipation.

# Travaux pratiques

- **Déploiement de réseaux IP sous Linux et MS Windows**
- **Partage d'une connexion en utilisant SQUID & IPTABLES**
- **Déploiement des services DHCP et DNS**
- **Déploiement de réseaux IP sous IOS Cisco**
- **Configuration de LANs & Interconnexion de niveau 2 sous IOS Cisco**