



Département Telecom & RSI – 1^{ère} année

Module RE110 & RE112: Introduction aux Réseaux

Introduction aux Réseaux – 3^{ème} partie

Les réseaux locaux

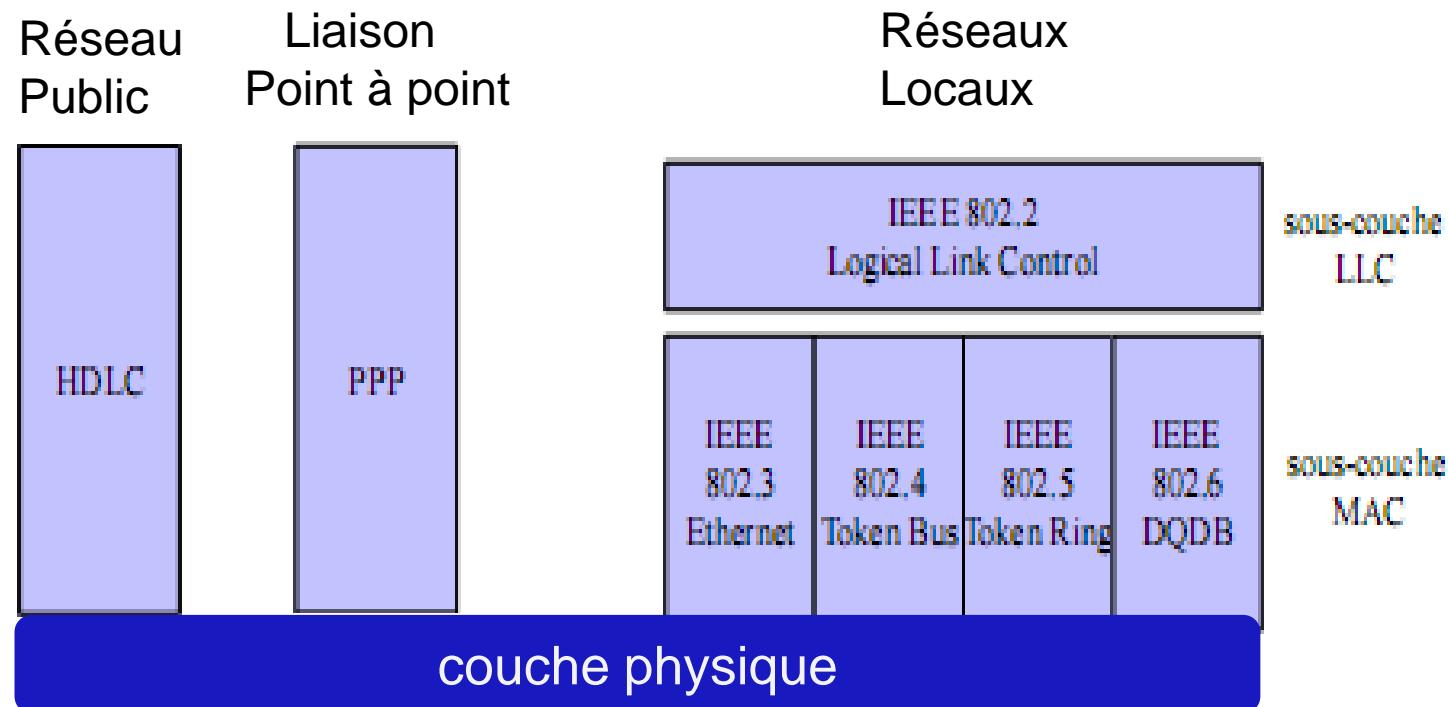
A. NAHALI

Plan

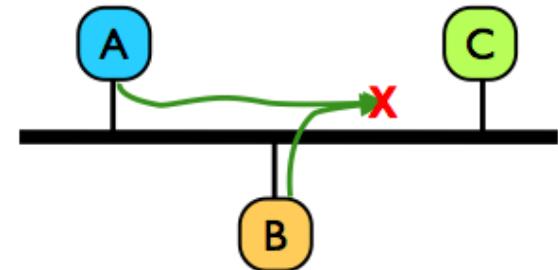
■ Les réseaux locaux:

- **Principes**
- Sous-couche MAC
- Ethernet
- Ethernet et la commutation
- Annexes (HDLC et sous-couche LLC)

Couche Liaison – Exemples de protocoles



Réseaux locaux à diffusion



- Sur un réseau à diffusion, toutes les stations sont en compétition pour transmettre sur un canal partagé
- Si deux stations émettent concurremment sur un canal de diffusion, les trames transmises sont détruites (Collisions)
- Gérer l'accès concurrent au canal

Plan

■ Les réseaux locaux:

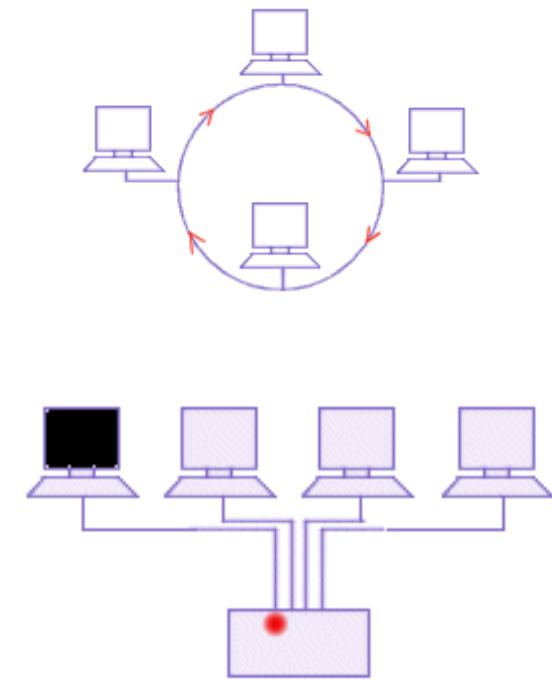
- Principes
- **Sous-couche MAC**
- Ethernet
- Ethernet et la commutation
- Annexes (HDLC et sous-couche LLC)

Sous-couche MAC (Medium Access Control)

- Cette couche est très importante dans les réseaux locaux qui fondent souvent leur communication sur le principe de canal à accès multiple
- Trois techniques pour gérer l'accès au lien partagé:
 - Par multiplexage (Time Division Multiplexing, Frequency Division Multiplexing): allocation statique d'une partie du canal à un utilisateur (utilisée dans les artères du réseau téléphonique, GSM, téléphonie mobile, ...)
 - Par consultation : maître-esclave et méthode d'accès à jeton (Token ring)
 - Par compétition : ALOHA, CSMA et variantes

Par consultation: méthode d'accès à jeton

- Principe de la communication tour à tour TOKEN RING LAN
- Chaque machine du réseau a la possibilité de parler à son tour
- Pour avoir le tour de parole, il faut posséder le jeton
- Le jeton circule en boucle d'une machine à une autre
- Lorsqu'une machine est en possession du jeton, elle peut émettre pendant un temps déterminé, puis relâche le jeton pour la machine suivante



Par compétition

- La façon de gérer le canal est telle que des collisions peuvent se générer
- Si une collision se génère, une station attend une période aléatoire avant de retransmettre
- Garantie probabiliste d'accéder au canal avec succès
=> latence variable

⇒ Protocole CSMA/CD

Par compétition

- Qu'est-ce qu'une collision?
- Le signal électrique met un certain temps à parcourir le câble (délai), et chaque répéteur suivant introduit un bref temps de latence lors de la transmission de la trame entre deux ports.
- En raison du délai et du temps de latence, il est possible que plusieurs stations commencent la transmission au même moment ou « quasiment » au même moment, ce qui engendre une **collision** des données envoyées

Par compétition: CSMA/CD

- Principe de CSMA (Carrier Sense Multiple Access):
- Quand une station doit envoyer des données, elle commence en écoutant le support de transmission
 - Si une autre station est en train de transmettre, la station attend que le canal se libère
 - Sinon elle transmet la trame

Par compétition: CSMA/CD

- Principe de CD (Collision Detection):
- Quand une station envoie des données, elle continue d'écouter le canal, afin de détecter tout bruit perturbateur, indice de collision
 - Si collision, la station gère la collision

Amélioration de CSMA : deux stations peuvent mettre fin à une transmission dès qu'elles s'aperçoivent de l'existence d'une collision \Rightarrow économie de temps et de bande passante

Par compétition: CSMA/CD

Emetteur

- Ecoute du canal
- Si le canal est libre
Alors
transmission de l'information
et écoute simultanée du canal
pour détecter une éventuelle collision

Si collision détectée

Alors

- Arrêt immédiat de la transmission
et notification de la collision à toutes les stations

-- Gestion de la collision

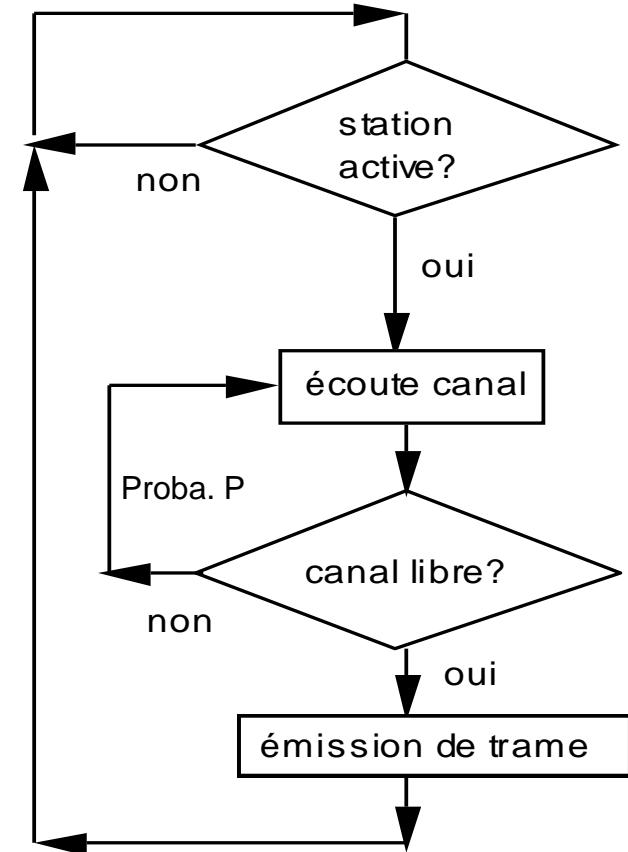
Sinon continuer la transmission

Procédure de Backoff exponentiel

1 CSMA

2 CD

3



Par compétition: CSMA/CD

Gestion de la collision

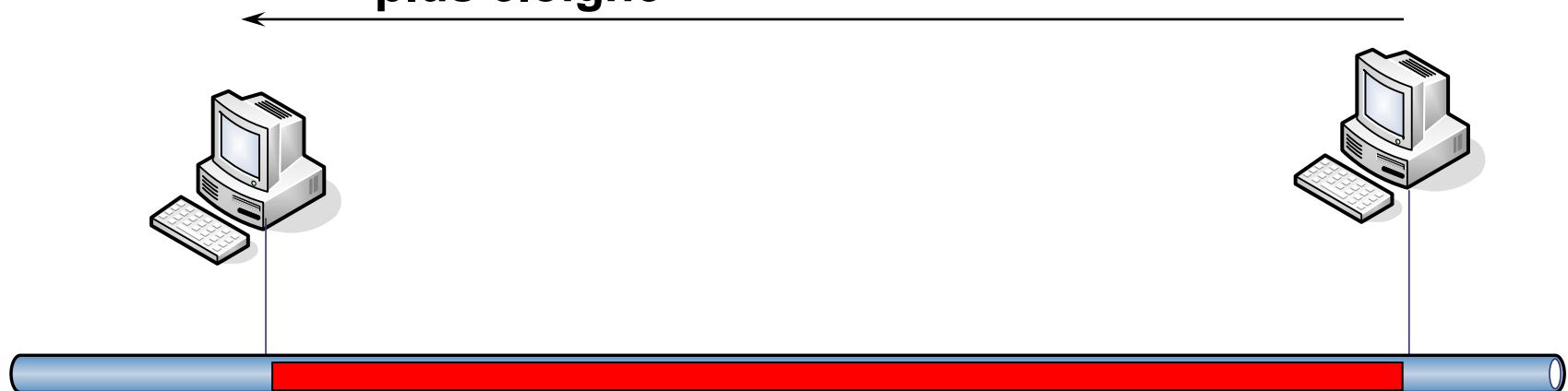
Si pendant l'émission, on détecte le signal d'autres stations \Rightarrow La station arrête de transmettre la trame et gère les collisions

- a) La station arrête de transmettre la trame, et transmet 32 bit prédefinis à 1 (JAM) puis
- b) La station entre dans la phase de backoff exponentiel
- c) Après l'attente aléatoire due à la phase de backoff exponentiel, repartir à la phase d'écoute

Par compétition: CSMA/CD

Détection de la collision

Temps d'émission entre les stations les plus éloigné

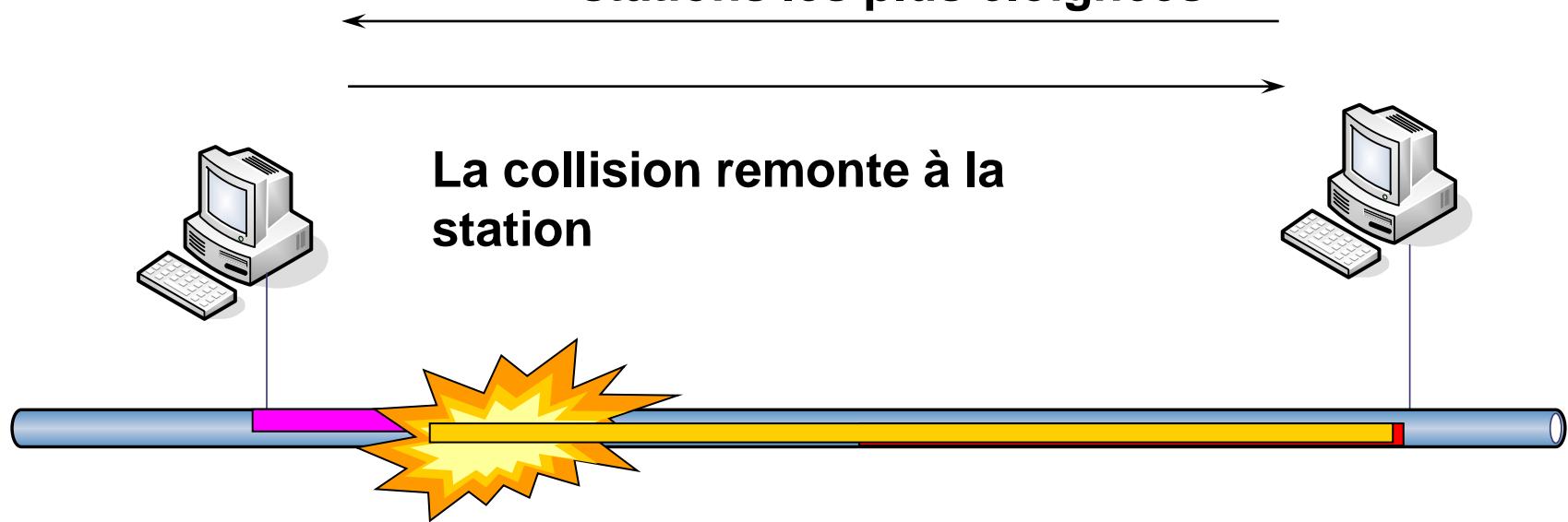


Occupation du canal suffisamment longtemps pour assurer qu'aucune autre station ne transmettra en même temps

Par compétition: CSMA/CD

Détection de la collision

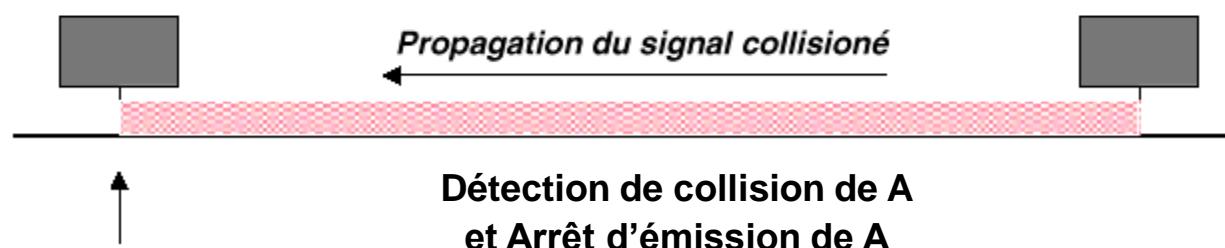
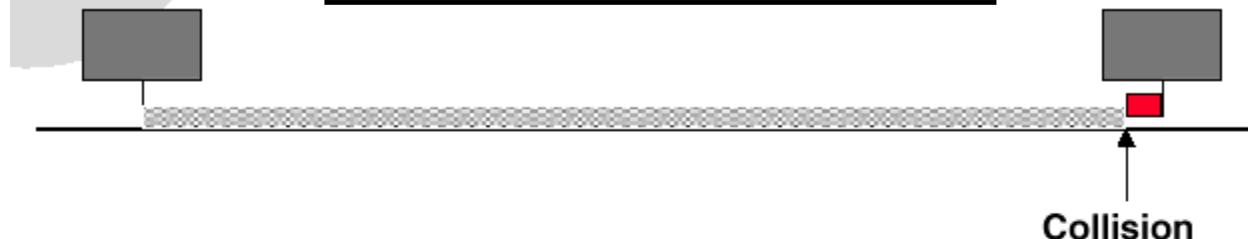
Temps d'émission entre les stations les plus éloignées



Cette collision n'est pas perçue par l'émetteur → problème d'occupation du canal

Par compétition: CSMA/CD

Détection de la collision



Temps max écoulé = Aller + Retour (RTT Round Trip Time) = Distance / V

Temps d'émission = T_e = Longueur de la trame / Débit du canal

Quelle est la condition pour que CSMA/CD fonctionne correctement ?

$$T_{\text{émission}} \geq 2 * T_{\text{propagation}}$$

Par compétition: CSMA/CD

- Détection de la collision:
- L'émission d'une trame en utilisant CSMA/CD doit durer un temps au moins égal au double du délai de propagation entre stations les plus extrêmes
- Ce délai dépend :
 - Des délais de propagation du signal sur les câbles (200 000 km/s environ)
 - Des retards introduits par les équipements de raccordement
 - Des retards dus à l'électronique des cartes réseau des stations

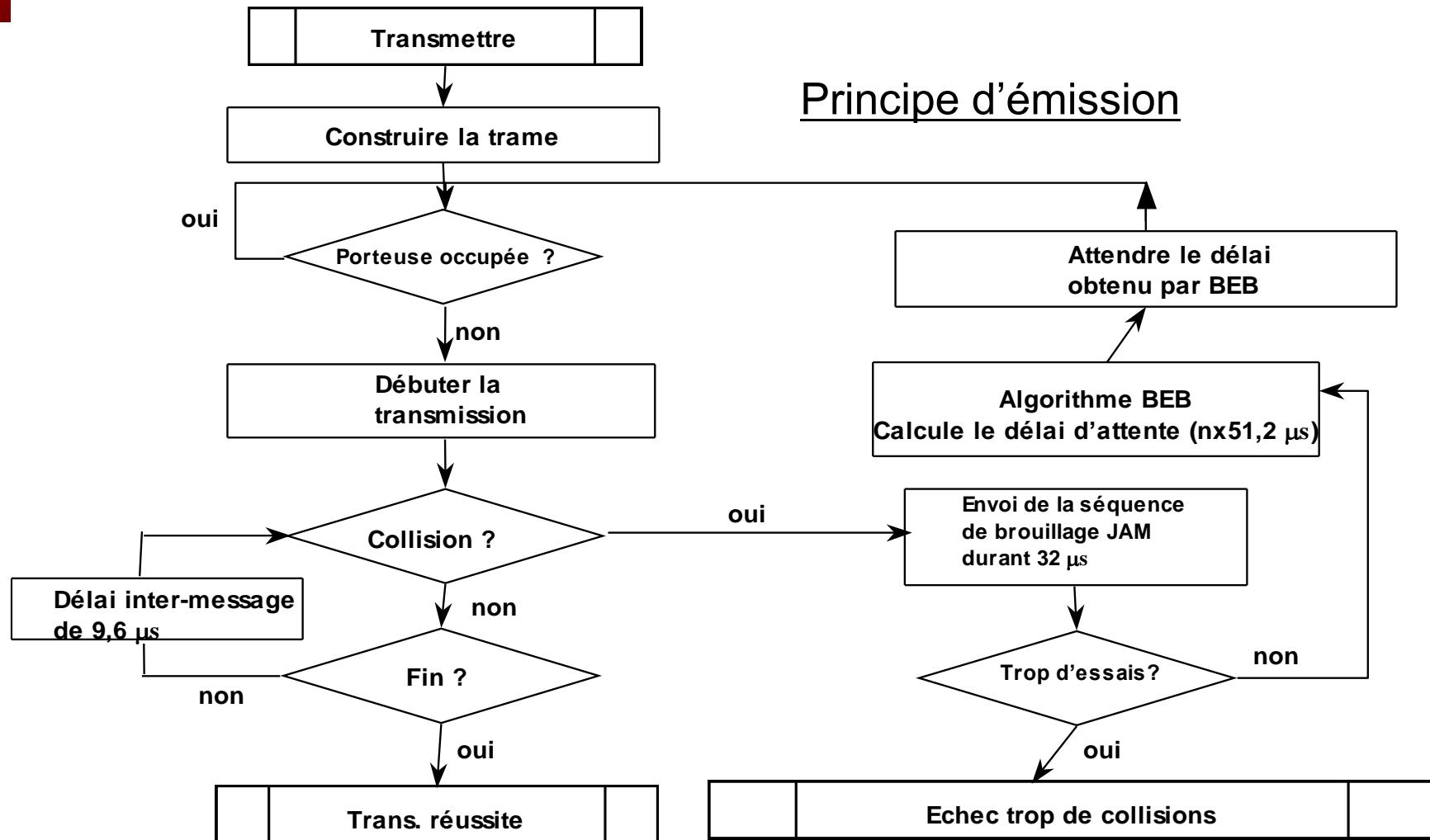
Par compétition: CSMA/CD

- Pour toutes les vitesses de transmission Ethernet égales ou inférieures à 1000 Mbits/s, la norme stipule qu'une transmission ne peut pas être inférieure à une tranche de temps (slot time) nécessaire pour la détection de collision
- La tranche de temps pour l'Ethernet 10 et 100 Mbits/s est de 512 temps-bit, soit 64 octets
- La tranche de temps pour l'Ethernet 1000 Mbits/s est de 4096 temps-bit, soit 512 octets
- La tranche de temps est calculée en se basant sur des longueurs de câble maximales dans l'architecture de réseau légale la plus étendue

Par compétition: CSMA/CD

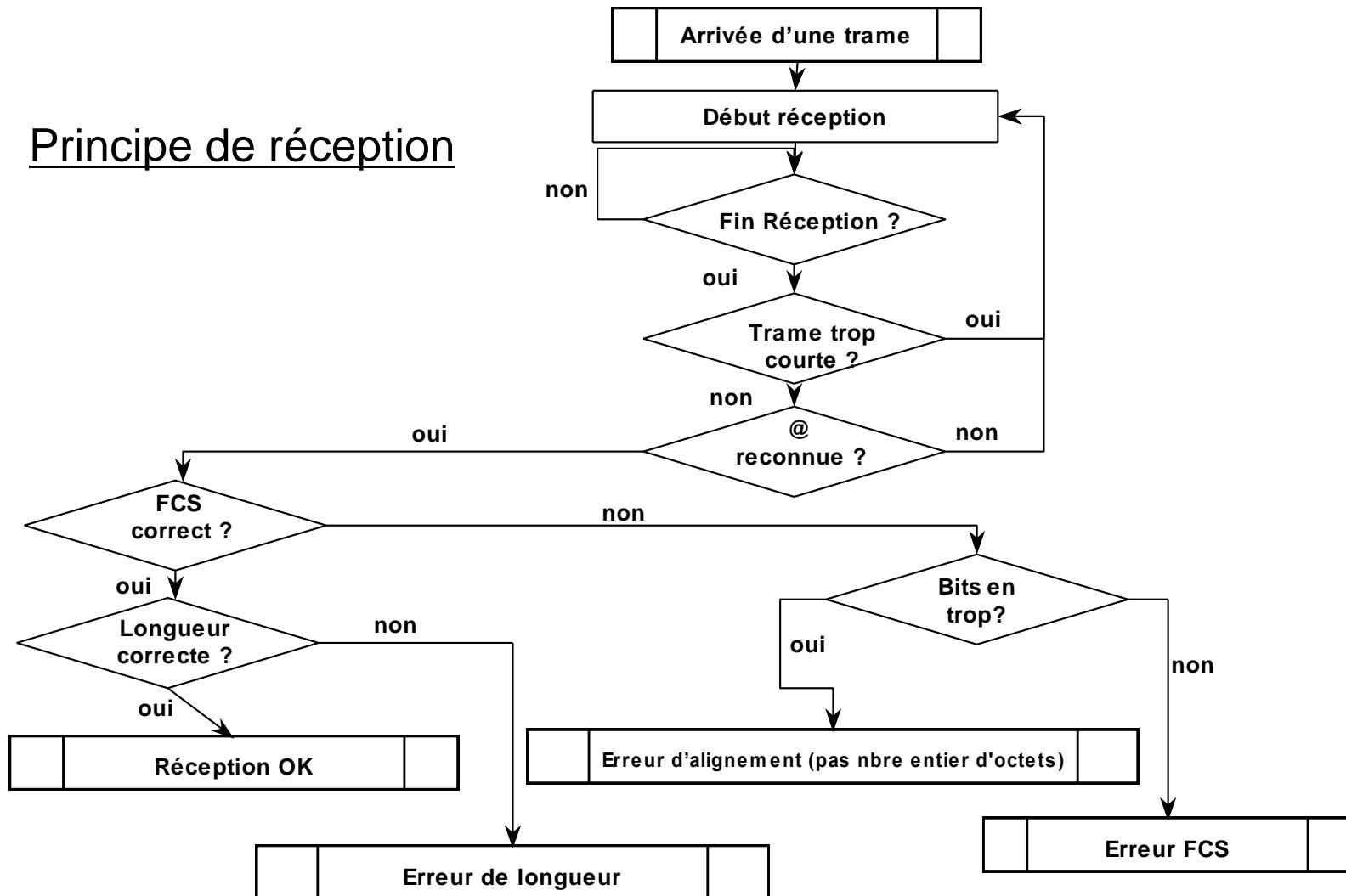
- Gestion de la collision: Back-off exponentiel
- Le temps est divisé en intervalles fixes, slot \Rightarrow égal au temps de propagation aller-retour le plus défavorable
- Après i collisions, le nombre de slots d'attente est prélevé dans l'intervalle de 0 à $2^i - 1$
- Après 10 collisions, l'intervalle de sélection est plafonné à 1023 slots
- Après 16 collisions, une erreur est passée au niveau réseau

Par compétition: CSMA/CD

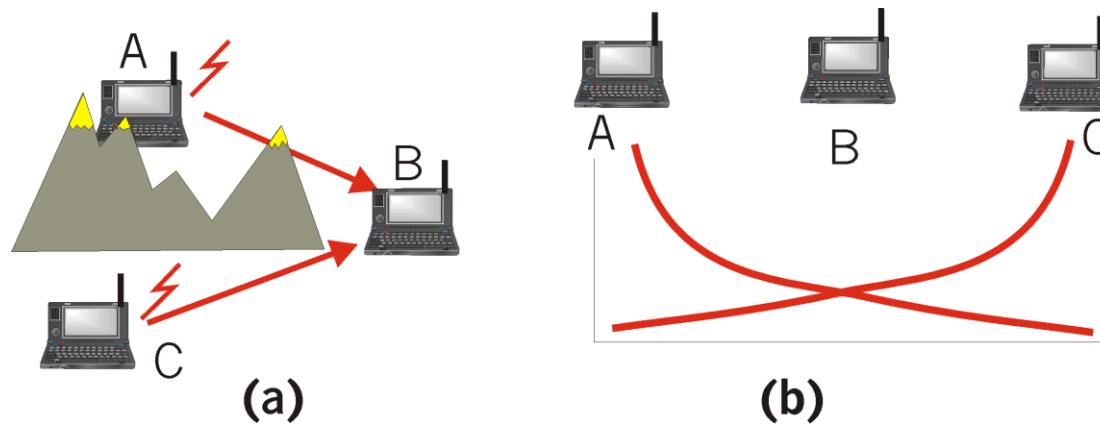


Par compétition: CSMA/CD

Principe de réception



Réseaux sans fil: pas de détection de collisions



Pas de détection des collisions car:

- Un obstacle physique peut empêcher A de détecter que C est en train de transmettre
- Fading : le signal s'atténue en se propageant dans l'air

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

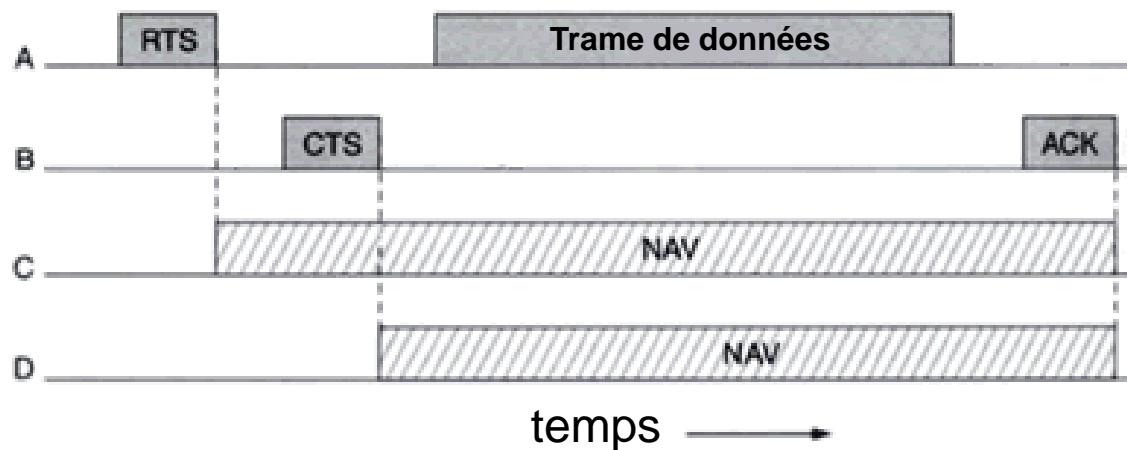
- LAN sans fil (ex. IEEE 802.11 Wifi /IEEE 802.16 WiMax)
- La station écoute le canal avant de transmettre (CSMA)
- Si le canal est libre pour un intervalle de temps déterminé (Distributed Inter Frame Spacing-DIFS), alors la station peut transmettre
- Quand la station réceptrice a reçu correctement et totalement la trame, elle envoie un acquittement à l'émetteur en attendant une courte période avant de transmettre (Short Inter Frame Spacing-SIFS)
- Si une station écoute le canal et qu'il est occupé, elle utilise un algorithme similaire au backoff exponentiel pour décider quand transmettre
 - La station écoute si le canal est libre pour une période égale à DIFS
 - La station calcule une période additionnelle d'attente, la période est calculée avec la méthode du backoff exponentiel
 - Quand la période d'attente se termine, la station transmet la trame

CSMA/CA avec RTS/CTS

- Quand A veut envoyer des données à B, il lui envoie une trame RTS de demande de permission d'émettre
- B répond par une trame CTS d'invitation à émettre
- Dès que A reçoit la trame CTS, elle commence à émettre et arme un temporisateur
- B répond par un acquittement
- La réception de l'acquittement par A met fin à l'échange
- Si l'acquittement n'est pas reçu, la station recommence la procédure

CSMA/CA avec RTS/CTS

- Les autres stations (C, D) peuvent évaluer la durée de la transmission à partir des informations contenues dans la trame RTS ou CTS \Rightarrow les autres stations attendent cette période sans essayer de transmettre



Plan

■ Les réseaux locaux:

- Principes
- Sous-couche MAC
- **Ethernet**
- Ethernet et la commutation
- Annexes (HDLC et sous-couche LLC)

Ethernet - IEEE 802.3

- Ethernet est aujourd’hui la technologie de réseau local dominante sur le plan mondial
- Ethernet est une famille de technologies de réseau local que le modèle de référence OSI rend plus facile à appréhender
- Les spécifications Ethernet prennent en charge différents médias, bandes passantes et autres variantes des couches 1 et 2
- Le format de trame de base et le système d’adressage sont les mêmes pour toutes les variantes d’Ethernet
 - Tous les réseaux locaux doivent traiter le problème de base qui est l’attribution de noms à chaque station ou nœud
- La technologie Ethernet a connu de profondes évolutions:
 - version initiale → Fast → Gigabit → MultiGigabit

Historique

ALOHANET: ancêtre d'Ethernet

- L'idée était de permettre à deux hôtes d'utiliser le même média sans aucune interférence entre les signaux
- Ce problème d'accès multiple de l'utilisateur à un média partagé a été étudié au début des années 70 à l'Université d'Hawaï
- Un système nommé **Alohanet** a été développé pour donner à plusieurs stations des îles Hawaï un accès structuré à la fréquence radio partagée dans l'atmosphère
- Ce travail a par la suite constitué la base de la méthode d'accès Ethernet connue sous l'acronyme CSMA/CD

Historique

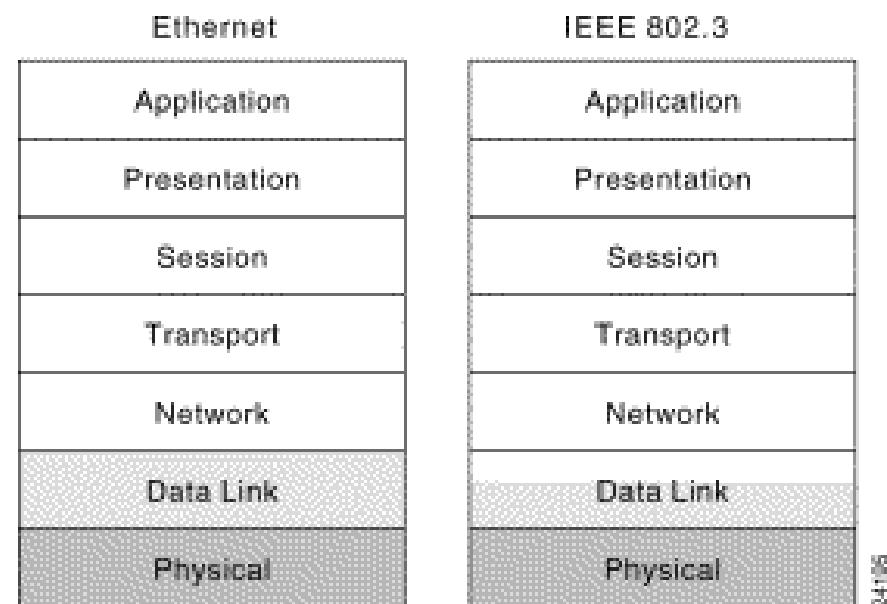
- 1974 : Inventeur XEROX : Spécification de Ethernet
- 1976 : INTEL et DIGITAL proposent Ethernet v2 et en font un standard du marché
- 1980 : IEEE normalise :
 - La technique d'accès d'Ethernet (CSMA/CD 802.3)
 - La gestion des collisions
 - Notifications (bourrage de la ligne - JAM)
 - Algorithme de reprise après collision (Binary Exponential Backoff)
 - Les algorithmes d'émission et de réception
 - Les grandeurs physiques IEEE 802.3 (délais, distances, ...)
 - La structure de la trame Ethernet 802.3
 - Les spécifications des supports physiques
- > 2000 : Ethernet et ses dérivées représentent 90% du marché des LAN

Succès du déploiement

- Le succès d'Ethernet est dû aux facteurs suivants:
 - Simplicité et facilité de maintenance
 - Capacité à incorporer de nouvelles technologies
 - Fiabilité
 - Faible coût d'installation et de mise à niveau
- L'introduction de Gigabit Ethernet a étendu la technologie de réseau local originale à un tel point qu'Ethernet est maintenant une norme des réseaux MAN et WAN

Ethernet – Normalisation IEEE 802.3

- **802.3** : concerne uniquement la couche **physique** et la couche **MAC**
- **Ethernet** : couche physique + MAC + LLC + topologie + support + technique de transmission = spécification complète d'un **LAN**

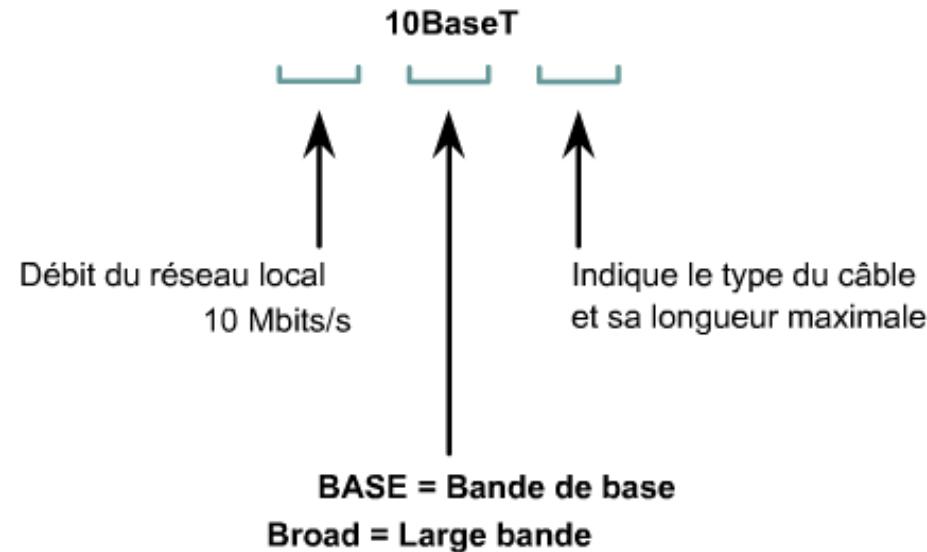


Règles d'attribution des noms

- Ethernet n'est pas une technologie de réseau unique mais une famille de technologies
- Les vitesses d'Ethernet s'échelonnent entre 10, 100, 1000 ou 10000 Mbits/s
- Le format de trame de base et les sous-couches IEEE des couches OSI 1 et 2 restent cohérents quelle que soit la forme d'Ethernet
- Chaque fois qu'Ethernet doit être étendu pour ajouter un nouveau média ou une nouvelle capacité, l'IEEE publie un nouveau supplément à la norme 802.3
- Les nouveaux suppléments sont identifiés par une ou deux lettres (ex. 802.3u). Une description abrégée, appelée identificateur, est également affectée au supplément

Règles d'attribution de noms

- La description abrégée comporte les éléments suivants :
 - Un chiffre qui indique le nombre de **Mbits/s transmis**
 - Des lettres pour indiquer le mode de transmission en **bande de base** ou **large bande**
 - Une ou plusieurs lettres de l'alphabet indiquant le **type de média** utilisé. Par exemple, *F* = câble à fibre optique et *T* = *paire de cuivre torsadée non blindée*
- Note: bande de base exclusivement aujourd'hui
 - Broad est obsolète



Ethernet – Normalisation cablâge - Exemples

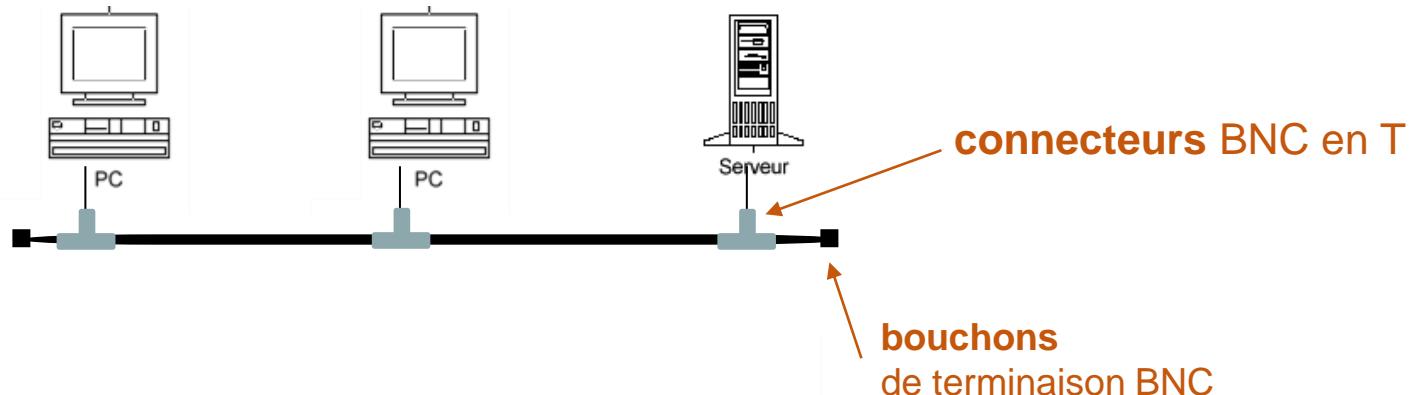
Type	Norme	Commentaire
10Mb/s	10 base 5	Coaxial jaune 500m
10Mb/s	10 base 2	Coaxial fin 200m
10Mb/s	10 broad 36	Large bande, 3.6km
100Mb/s	100 base T	Paire de fils torsadés
100Mb/s	100 base F	Fibre optique

Plusieurs variantes de Ethernet existent

- Elles **utilisent** toutes :
 - 802.3 CSMA/CD,
 - half-duplex au minimum
 - Bande de base
- Elles **diffèrent** par :
 - Le type de support (UTP “Unshielded Twisted Pair”, STP “Shielded Twisted Pair”, Coax, Fibre optique)
 - Le type de topologie (bus, étoile, arbre)
 - Le débit (1, 5, 10, 1000 Mbps)

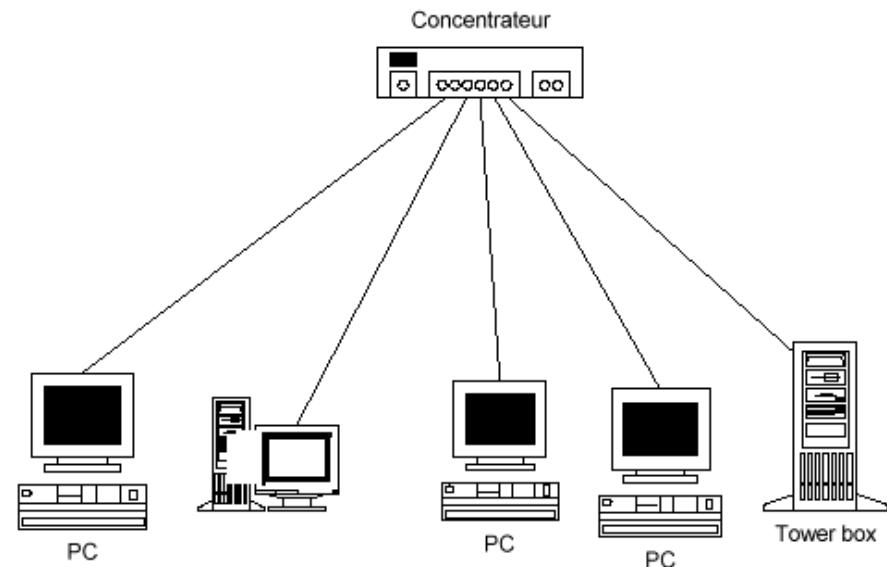
Ethernet - 802.3a 10Base2

- Moyen physique de connexion inter-nœuds: câble coaxial fin (thinnet):
- 10 Base 2
 - Débit 10 Mbit/s
 - 2 indique environ 200 mètres qui est la distance maximale entre deux nœuds quelconques du réseau sans répéteur de signal entre eux
- Sans répéteur: au plus 30 nœuds connectés au bus
- Avec un répéteur: on peut connecter deux segments ayant chacun 30 nœuds et une longueur de 185 mètres
- Un répéteur régénère et resynchronise le signal au niveau du bit
- Au plus 4 répéteurs peuvent être utilisés

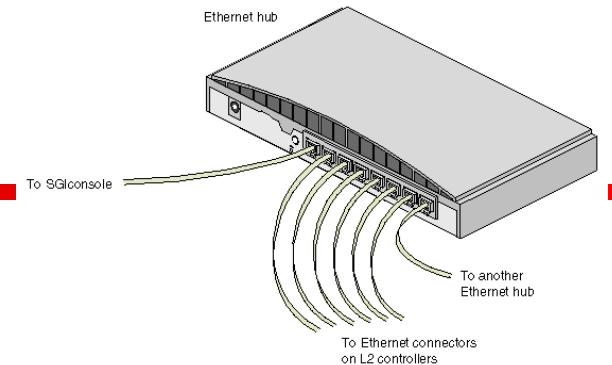


Ethernet - 802.3i 10BaseT

- 10BaseT
 - 10Mbits/sec
 - T ⇒ Fils de cuivre en paires
Torsadées blindés (STP) ou
non (UTP)
- Connecteurs RJ-45
- Concentrateur (Hub)
- Topologie étoile physique
MAIS bus logique



Concentrateur (Hub)



- Dispositif de la couche physique qui retransmet sur tous les ports en sortie chaque bit en entrée
⇒ répéteur multiport
- Si un nœud fonctionne mal, le concentrateur le déconnecte
- Donne des informations statistiques au nœuds connectés

Cables

Les types de câble coaxial

Il existe deux types de câbles coaxiaux :

Le câble coaxial fin

Le câble coaxial épais

Quel est le rôle du câble coaxial ?

Le rôle d'un câble coaxial est de transmettre des données issues de signaux numériques et analogiques, à haute ou basse fréquence.

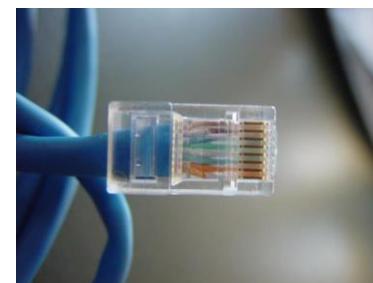
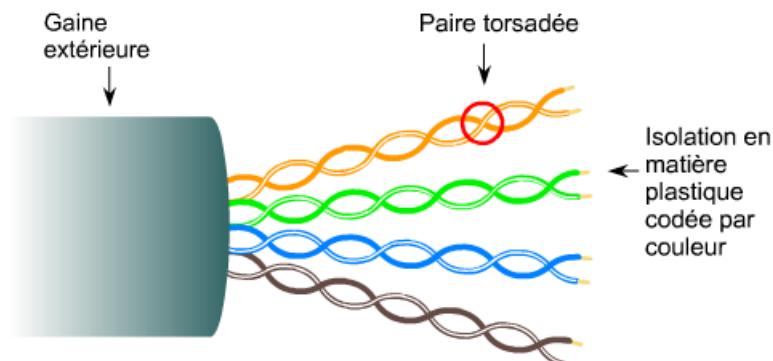
Ainsi, ce dernier permet de brancher une antenne à un appareil comme une télévision ou une radio, et de pouvoir recevoir les ondes envoyées.



Cables

Les supports les plus courants : la paire torsadée

- Une ligne de transmission symétrique qui permet la propagation d'un signal électrique analogique ou numérique.
- Une ligne formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but principal de limiter la sensibilité aux interférences et la diaphonie dans les câbles multi paires.

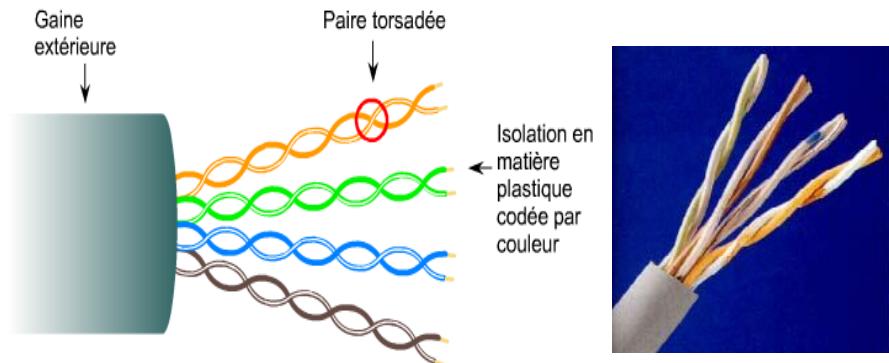


RJ45

Câbles

Câble à paires torsadées non blindées

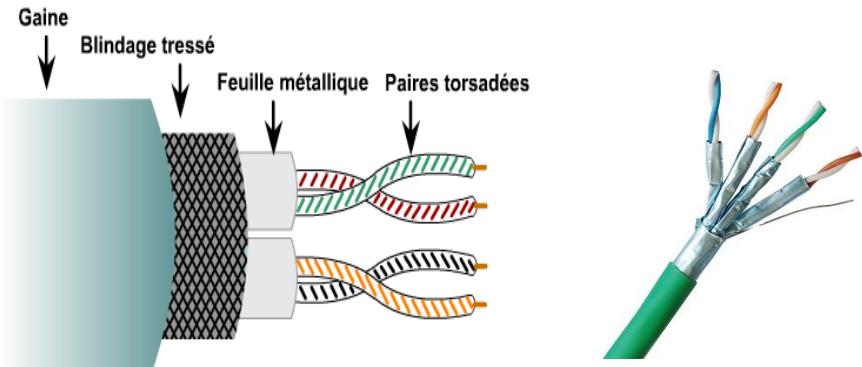
- Média constitué de quatre paires de fils, présent dans divers types de réseau
- Chacun des huit fils de cuivre du câble est protégé par un matériau isolant
- Les paires de fils sont tressées entre elles



Câble à paires torsadées non blindées (UTP)

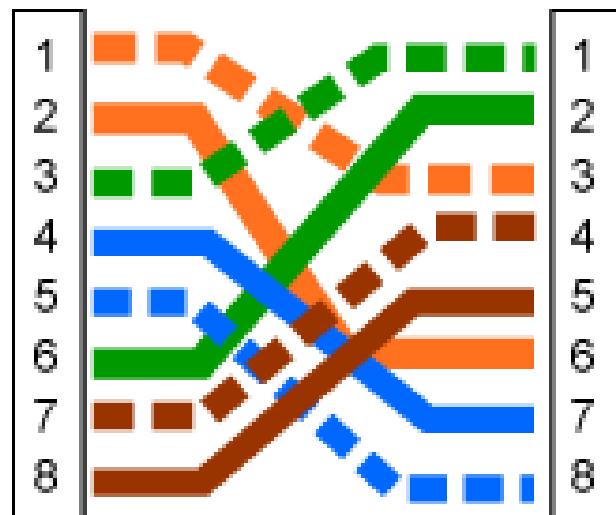
Câble à paires torsadées blindées

- Chaque paire de fils est enveloppée dans une feuille métallique et les deux paires sont enveloppées ensemble dans un revêtement tressé ou un film métallique
- Réduction du bruit électrique à l'intérieur du câble ainsi qu'à l'extérieur du câble



Câble à paires torsadées blindées(STP)

Câble croisé vs câble droit



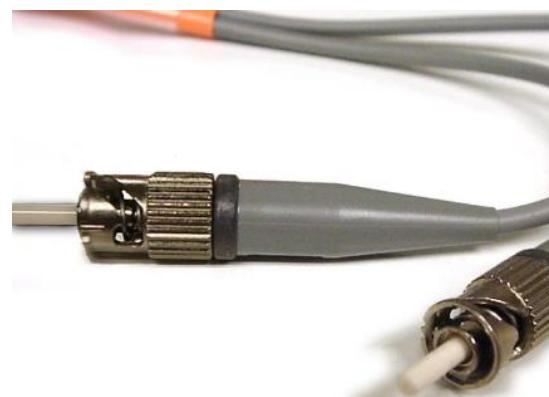
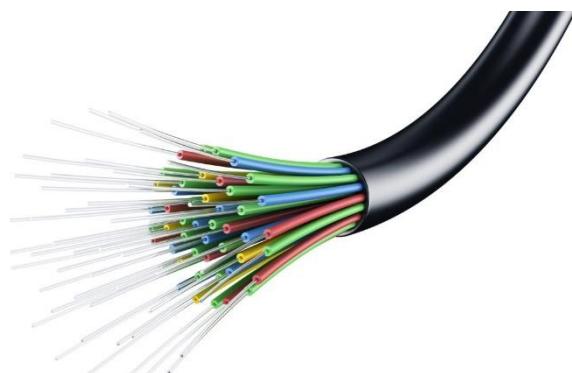
1	Blanc/orange
2	Orange
3	Blanc/vert
4	Bleu
5	Blanc/bleu
6	Vert
7	Blanc/brun
8	Brun

Seuls quatre fils (1, 2, 3 et 6) sont actifs dans un câble d'interconnexion Ethernet (10BaseT et 100BaseTX)

Autres supports

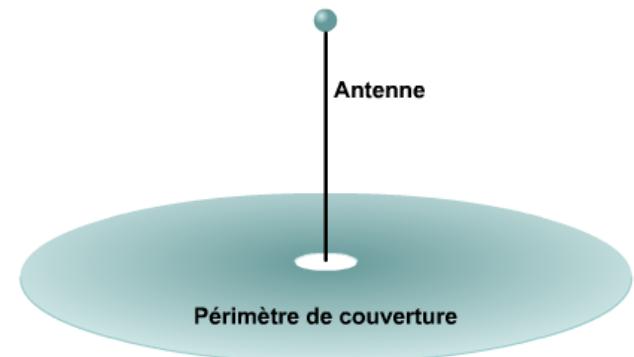
■ Les supports les plus courants : Fibre Optique

- Une fibre optique est un fil de verre extrêmement fin.
- Il a la capacité de conduire la lumière
- Il est utilisé pour transmettre des données numériques ou pour des explorations visuelles dans le milieu médicale.



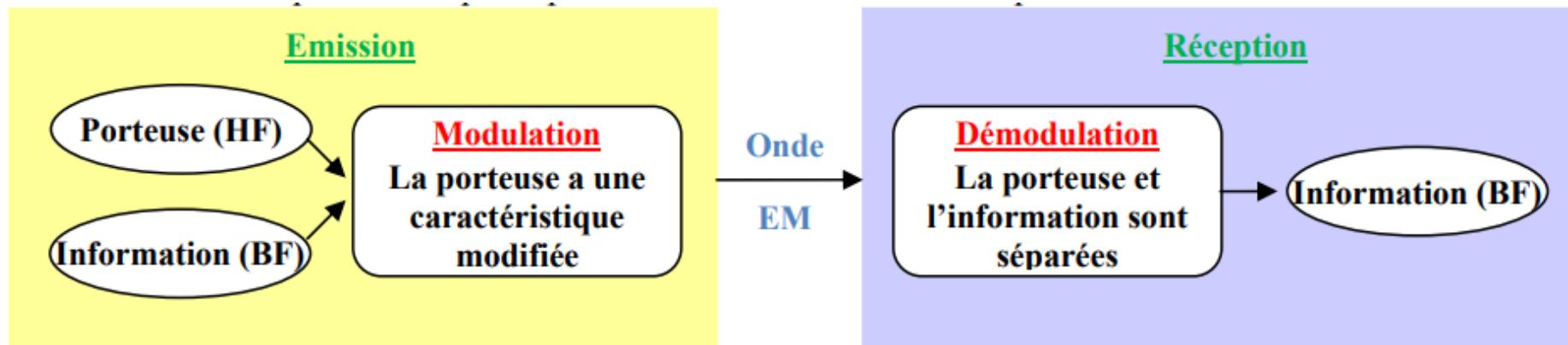
Autres supports

- **Les supports les plus courants : Ondes Radios**
- une onde électromagnétique dont la fréquence est inférieure à 300 MHz (*sont comprises entre 9 kHz et 300 GHz*).
- Elles sont produites en injectant dans une antenne un courant électrique variable à haute-fréquence



Autres supports

■ Les supports les plus courants : Ondes Radios



Ethernet – Format de la trame

8 octets	6 o	6 o	2 o	46 – 1500 o	4 o
Préambule	Adresse destination	Adresse Source	Type	Données	CRC

- **Préambule** : premier 7 octets 10101010, dernier octet 10101011
- **Adresses** : si le récepteur reçoit une trame avec son adresse dans le champ destination ou avec l'adresse de broadcast, il dés-encapsule et passe le paquet contenu à l'intérieur de la trame à la couche réseau si la trame est correcte. Sinon, la trame est rejetée.
- **Type** : indique le protocole de réseau (généralement IP, mais aussi autre protocoles possibles)
- **CRC** : détection des erreurs

Ethernet – Format adressage (adresses MAC)

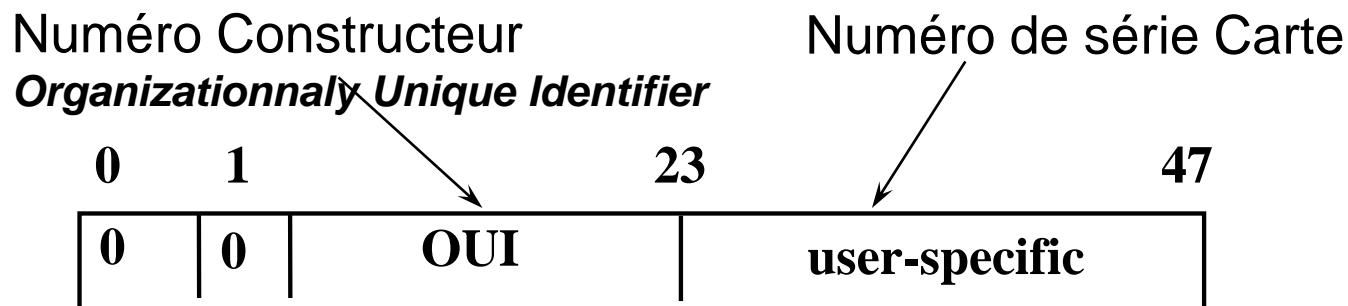
- 6 octets $\Rightarrow 2^{48}$ adresses MAC possibles
- Généralement dénotée à travers la notation hexadécimale, chaque octet correspond à une paire de nombres hexadécimales \Rightarrow exemple 5C:66:AB:90:75:B1 (séparée par : ou -)
- Une adresse MAC est forgée dans le NIC (Network Interface Card) de la machine quand elle est créée et est permanente
- Chaque NIC dans le monde a son unique MAC adresse
=> adresse physique

Ethernet – Unicité adresses MAC

- L'IEEE gère l'espace d'adresses MAC
- Un constructeur (ex. Cisco) a 2^{24} adresses MAC à utiliser pour construire ces cartes réseaux
- IEEE établie les premiers 24 bits de l'adresse MAC
- Le constructeur alloue les 24 bits suivants de l'adresse d'une façon unique pour chaque carte

Ethernet – Format adresse universelle MAC

- 00:00:0C:XX:XX:XX : Cisco
- 08:00:20:XX:XX:XX : Sun
- 08:00:09:XX:XX:XX : HP
- 00:14:BF:XX:XX:XX : Cisco-Linksys
- 3C:15:C2:XX:XX:XX : Apple



Ethernet - Récapitulatif

Paramètres	Valeurs
Tranche canal	→ 512 temps bits (64 octets)
Slot-time (10 Mbps)	→ 51.2 µs
Silence inter messages	→ 9.6 ms
Nombre d'essais total	→ 16 (15 retransmissions)
Limite tirage BEB	→ 10
Taille mini. du brouillage	→ 32 bits
Taille maxi. des trames	→ 1518 octets
Taille mini. des trames	→ 64 octets (46 octets pour Data)
Taille des adresses	→ 6 octets

Plan

■ Les réseaux locaux:

- Principes
- Sous-couche MAC
- Ethernet
- **Ethernet et la commutation**
- Annexes (HDLC et sous-couche LLC)

Ethernet commuté

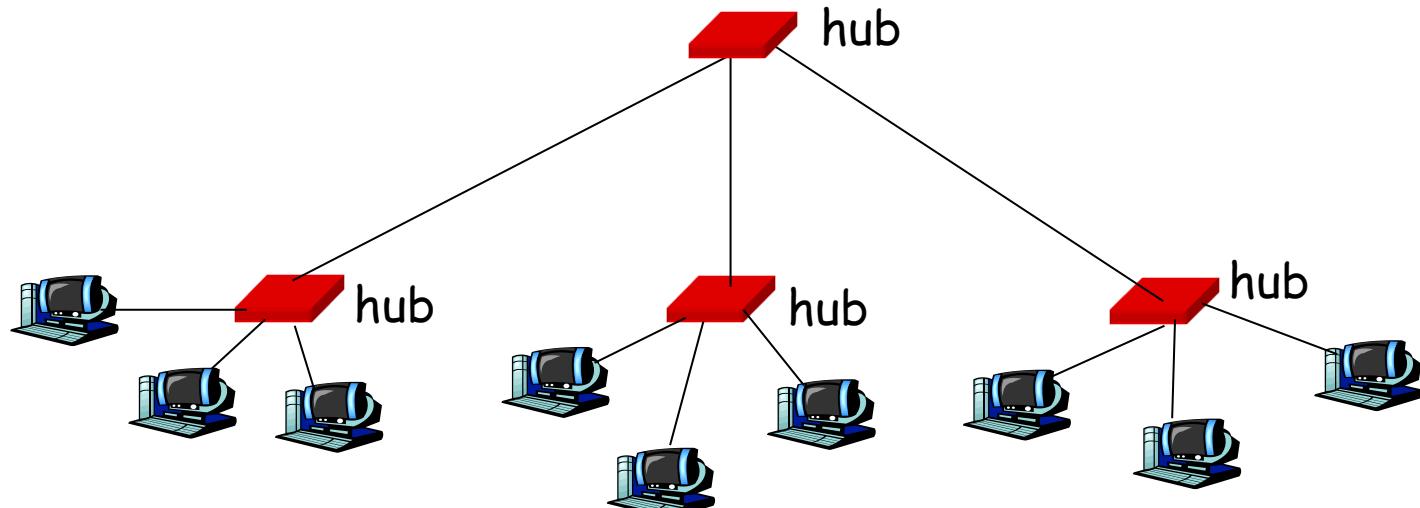
- Un réseau Ethernet partagé fonctionne parfaitement dans des conditions optimales d'utilisation
- Lorsque le nombre des équipements qui tentent d'accéder au réseau est peu élevé, le nombre de collisions se maintient à un niveau acceptable
- En revanche, lorsque le nombre des utilisateurs augmente, le nombre croissant de collisions peut considérablement réduire les performances du réseau
- Les problèmes de broadcast et de collision sont des événements connus dans les réseaux modernes
- Afin d'en limiter les effets, des domaines de collision doivent être créés en installant des **équipements de niveau 2**

Domaine de collision

- On appelle domaines de collision des segments du réseau physique dans lesquels des collisions peuvent se produire
- Les collisions rendent le réseau inefficace
- Chaque fois qu'une collision survient sur un réseau, les transmissions s'interrompent momentanément
- La durée de cette interruption est variable et est fonction d'un algorithme de réémission temporisée pour chaque équipement du réseau
- Les types d'équipements assurant l'interconnexion des segments de médias définissent les domaines de collision

Interconnection avec des hubs

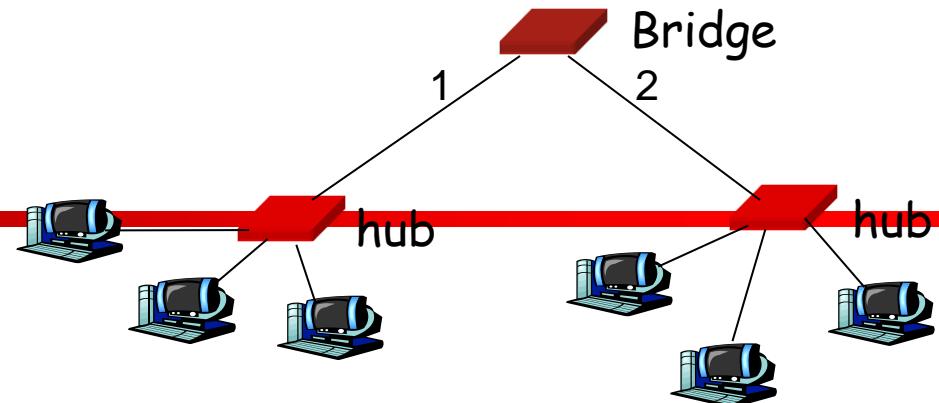
- Backbone hub interconnecte des segments LAN
- Etend la distance max entre nœuds
- Mais **un seul large domaine de collision**
- Ne peut pas interconnecter segments LAN Ethernet 10BaseT et 100BaseT



Séparer les domaines de collision

- Plus le nombre de nœuds situés sur un segment Ethernet augmente, plus le média est utilisé
- Ethernet étant un média partagé, un seul nœud à la fois peut transmettre des données
- L'ajout de nœuds entraîne un besoin croissant de bande passante et occasionne des charges supplémentaires sur le média. En outre, la probabilité de collisions est plus forte, ce qui entraîne davantage de retransmissions
- L'une des solutions consiste à fragmenter le segment principal en plusieurs parties et à le diviser en **domaines de collision distincts**

Pont (Bridge)

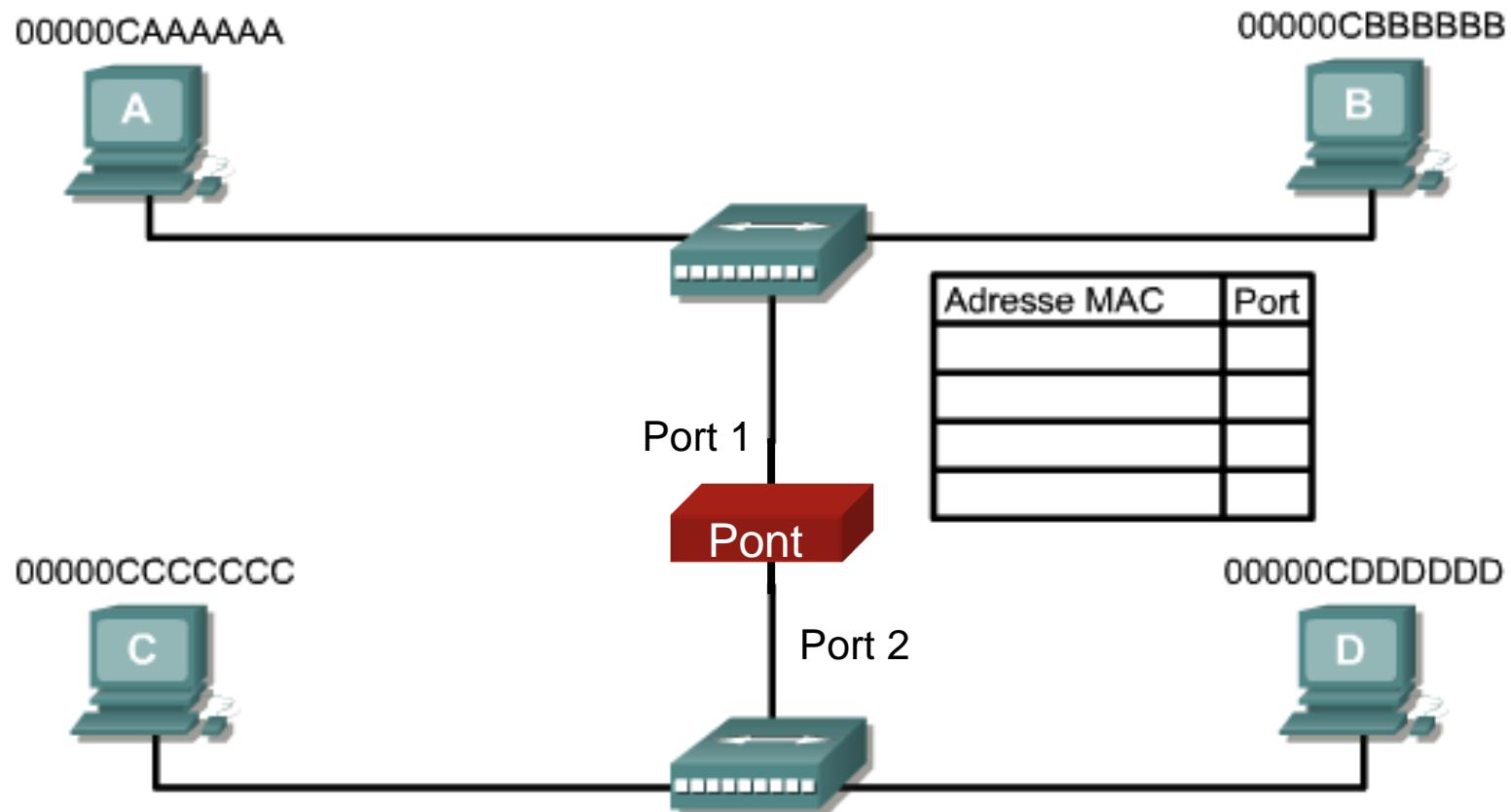


- Un pont est un dispositif plug-and-play (l'administrateur doit seulement connecter le segment LAN à l'interface du dispositif) de la couche liaison
⇒ Travaille sur les trames et non sur le single bit
- Lorsqu'une trame est reçue, le pont analyse l'adresse LAN de la destination dans la trame et forward la trame dans l'interface qui achemine vers le destinataire
 - Il exécute le CSMA/CD protocole pour transmettre la trame
- Le pont permet d'interconnecter plusieurs LAN en maintenant les domaines de collision séparés
- Permet l'interconnexion de technologies Ethernet différentes

Bridge - Forwarding

- **Table de pontage** : Pour savoir vers quelle interface acheminer la trame, le pont gère une table dont il garde des informations sur un sous-ensemble des nœuds dans le LAN
- Chaque entrée de la table contient:
 - L'adresse LAN du nœud (adresse MAC)
 - Le numéro de l'interface (port) qui achemine vers le nœud
 - Le temps auquel cette entrée a été créée
- Lorsqu'un pont vient d'être installé, sa table est vide. Le pont apprend comme acheminer grâce à la réception des trames
- Le pont efface une entrée de la table de pontage si aucune trame est reçue par le nœud correspondant pour une période donnée (aging time)

Fonctionnement d'un pont



Fonctionnement d'un pont

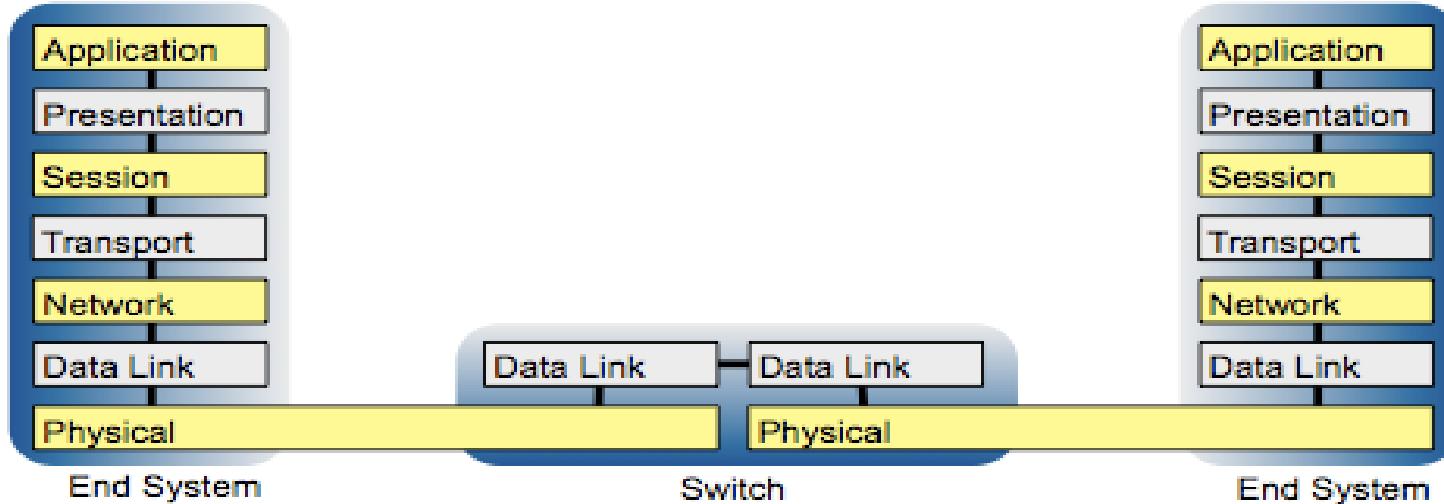
- L'hôte A émet une requête vers l'hôte B. Les données étant transmises sur l'ensemble du segment de domaine de collision, le pont et l'hôte B traitent la trame
- Le pont ajoute l'adresse source de la trame à sa table de pontage
 - Sachant que l'adresse se trouve dans le champ d'adresse source et que la trame est reçue sur le port 1, la trame doit être associée au port 1 dans la table
 - L'adresse de A et l'interface correspondante forment ainsi une entrée de la table de pontage

Fonctionnement d'un pont

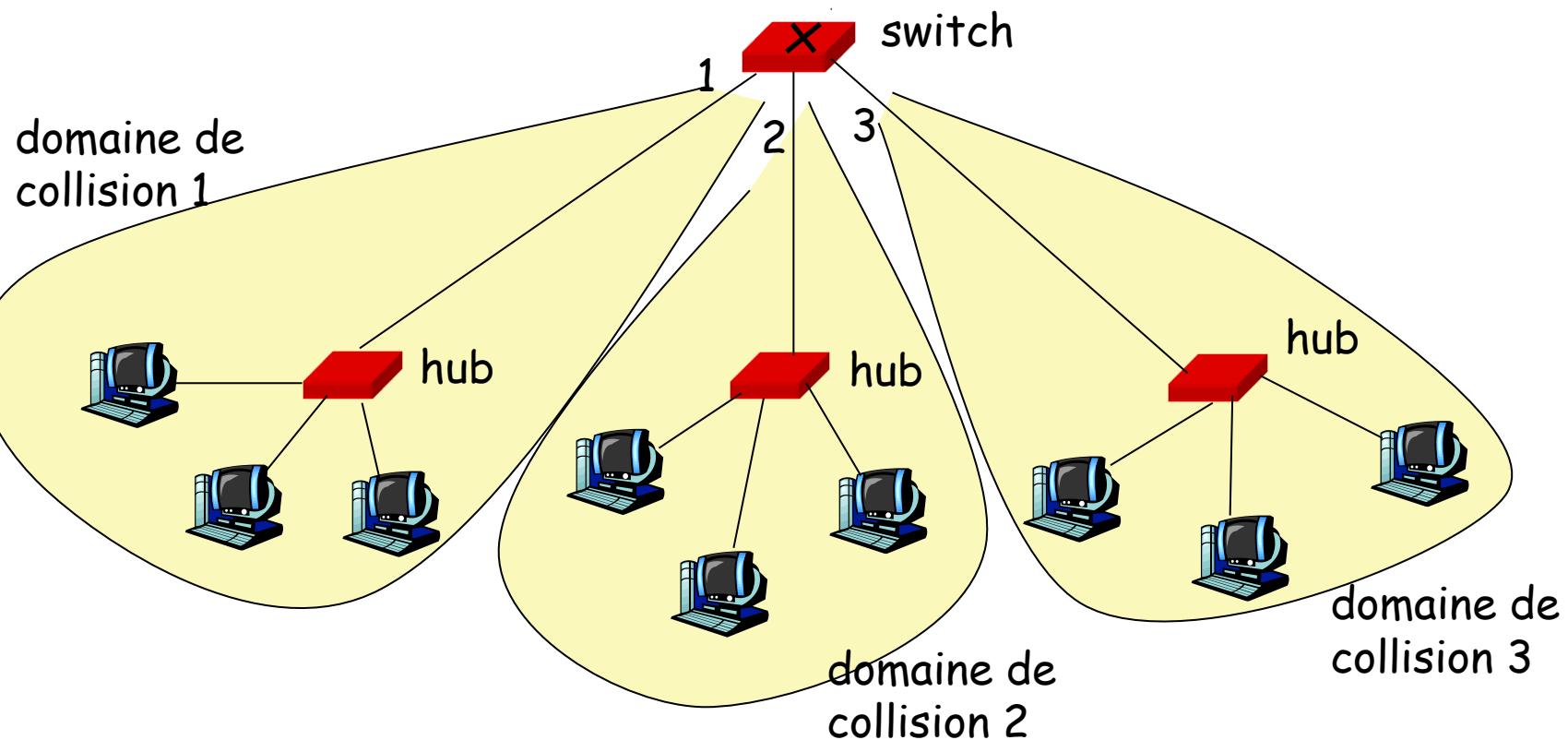
- L'adresse de destination de la trame est comparée à toutes les adresses de la table de pontage.
- Bien que les deux adresses se trouvent dans le même domaine de collision, si l'adresse de destination ne se trouve pas dans la table, la trame est transférée vers le segment suivant
 - L'adresse de l'hôte B n'est pas encore enregistrée
- Et ainsi de suite jusqu'à l'apprentissage total des machines dans les segments Ethernet

Pont (bridge) et commutateur (switch)

- En règle générale, un pont comprend deux ports et subdivise un domaine de collision en deux segments
- **Un commutateur est en fait un pont multiport** très rapide qui peut contenir des douzaines de ports. Chaque port crée son propre domaine de collision
 - Lorsqu'un réseau comporte 20 nœuds, 20 domaines de collision doivent exister si chaque nœud est connecté à son propre port de commutation
- Les décisions prises par un pont/commutateur dépendent uniquement des adresses MAC (ou adresses de couche 2) et n'affectent pas les adresses de couche 3 (ou adresses logiques)



Commutateur/Switch



Domaine de collision

- Le domaine de collision est le segment sur lequel les périphériques sont en concurrence les uns avec les autres pour communiquer
- Tous les ports d'un concentrateur appartiennent au même domaine de collision
- Chaque port d'un commutateur constitue un domaine de collision
- Le commutateur décompose le segment en domaines de collision plus petits, ce qui facilite les choses pour les périphériques

Domaine de diffusion

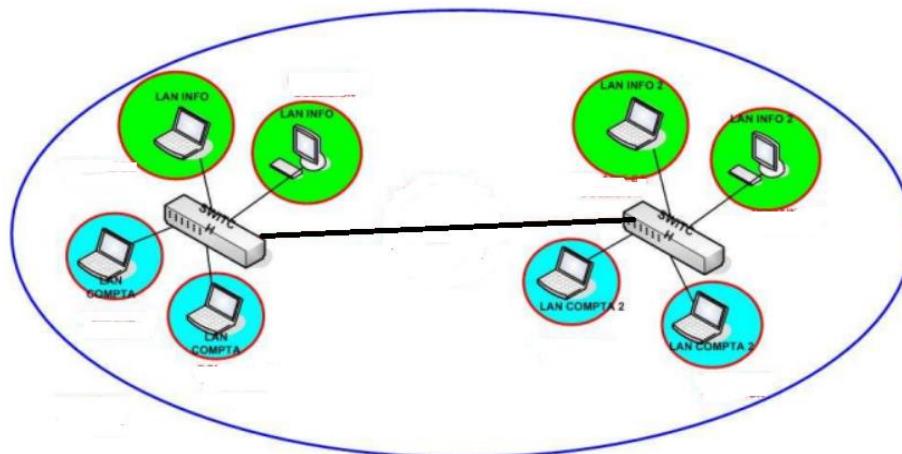
- Le domaine de diffusion représente l'étendue du réseau dans laquelle une trame de diffusion peut être « entendue ».
- Les commutateurs envoient les trames de diffusion à tous les ports. C'est pourquoi ils ne segmentent pas les domaines de diffusion.
- Tous les ports d'un commutateur (avec la configuration par défaut) appartiennent au même domaine de diffusion
- Si deux commutateurs ou plus sont connectés, les diffusions sont envoyées vers tous les ports de tous les commutateurs (à l'exception de celui qui les a initialement reçues)

Domaine de diffusion/ collision

Exercice:

Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes

1. Des ordinateurs et des commutateurs :



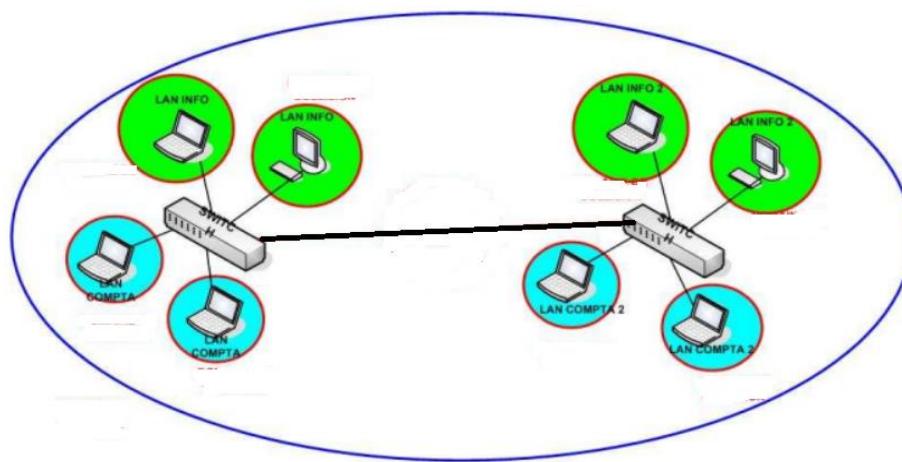
Nombre de domaine de collision :
Nombre de domaine de diffusion :

Domaine de diffusion/ collision

Exercice:

Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes

1. Des ordinateurs et des commutateurs :



Nombre de domaine de collision : 9

(Un switch crée 1 domaine de collision par port)

Nombre de domaine de diffusion : 1

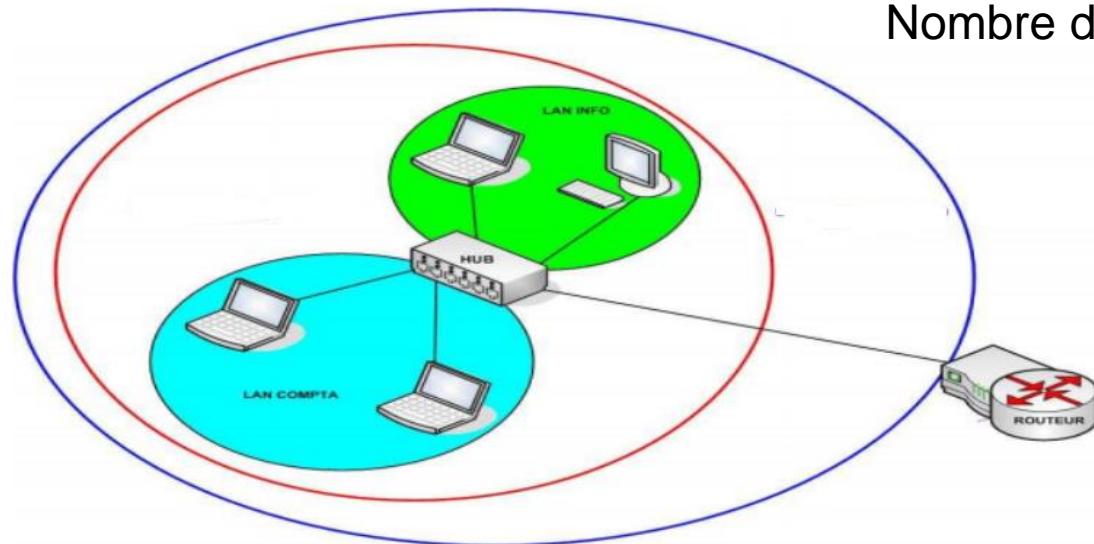
(Les switches ne séparent pas la diffusion)

Domaine de diffusion/ collision

Exercice:

Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes

2. Des ordinateurs, un concentrateur et un routeur



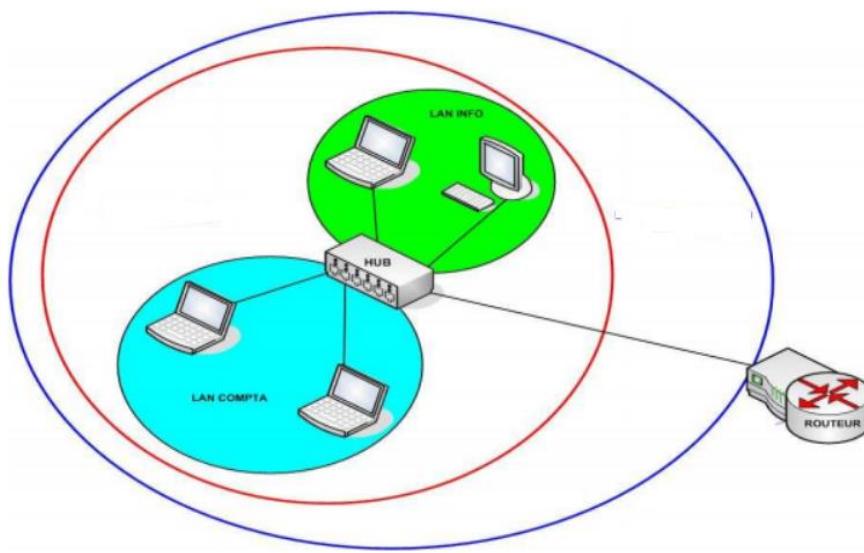
Nombre de domaine de collision :
Nombre de domaine de diffusion :

Domaine de diffusion/ collision

Exercice:

Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes

2. Des ordinateurs, un concentrateur et un routeur

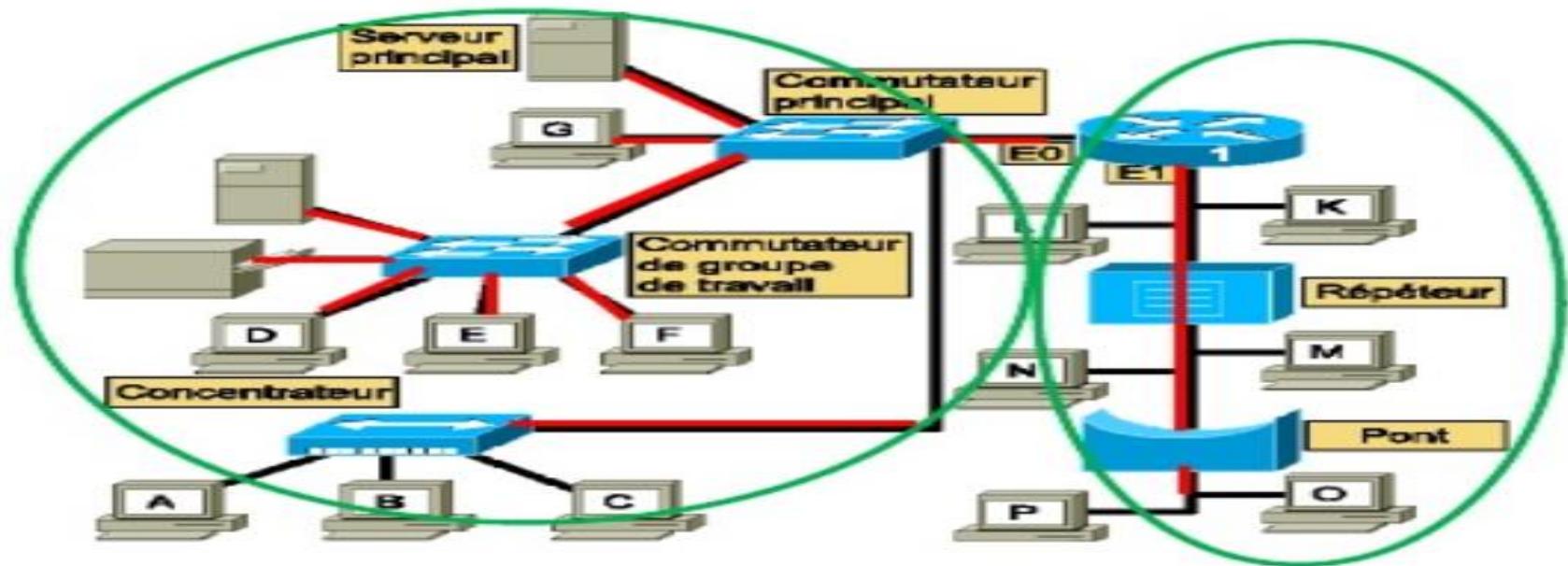


Nombre de domaine de collision : 1
(un hub crée toujours un seul domaine de collision, quel que soit le nombre de machines)

Nombre de domaine de diffusion : 1
(un seul LAN)

Domaine de diffusion/ collision

Exercice: Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes

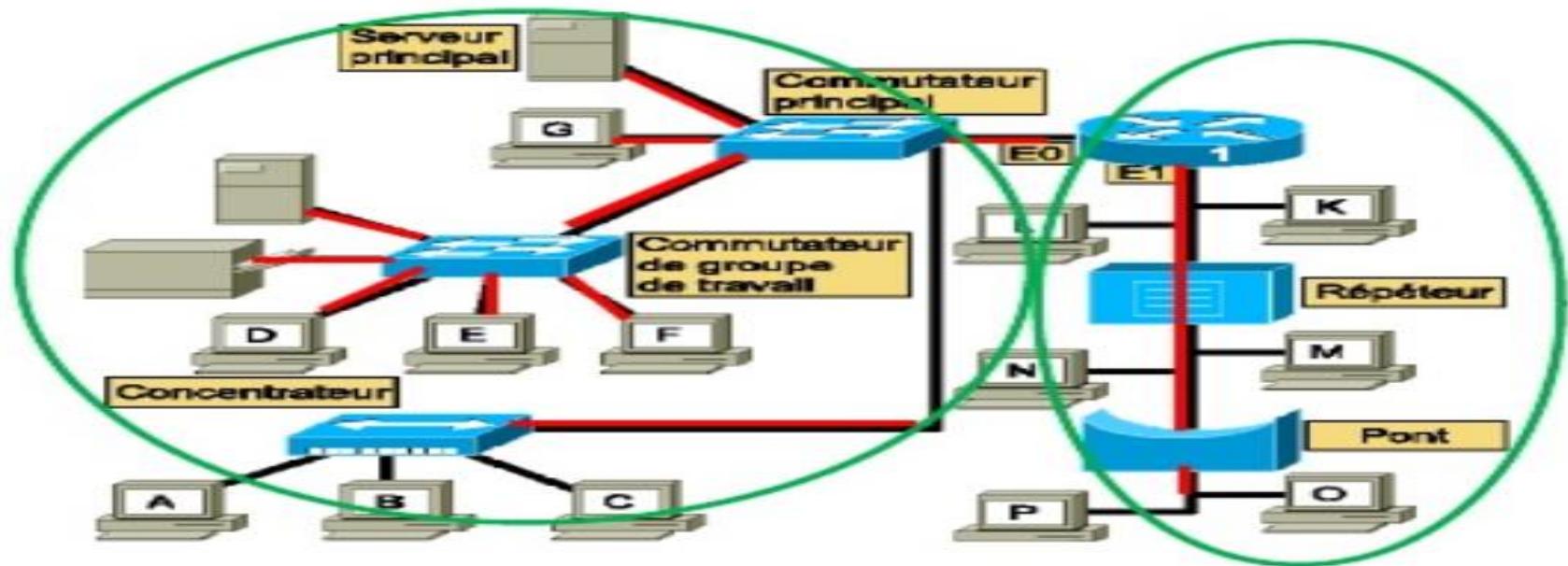


Nombre de domaine de broadcast :

Nombre de domaine de collision (chaque port du switch définit un domaine) :

Domaine de diffusion/ collision

Exercice: Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes



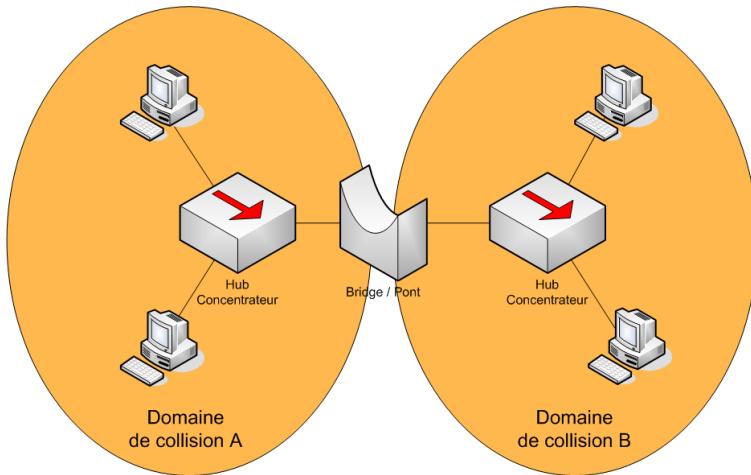
Nombre de domaine de broadcast : 2

Nombre de domaine de collision (chaque port du switch définit un domaine) : 12

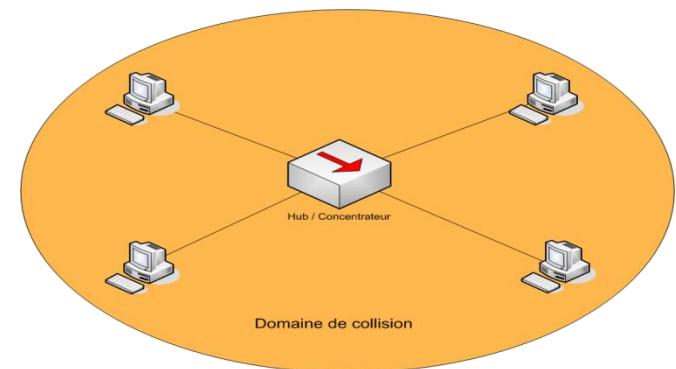
Domaine de diffusion/ collision

Exercice:

Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes



Nombre de domaine de broadcast :
Nombre de domaine de collision :

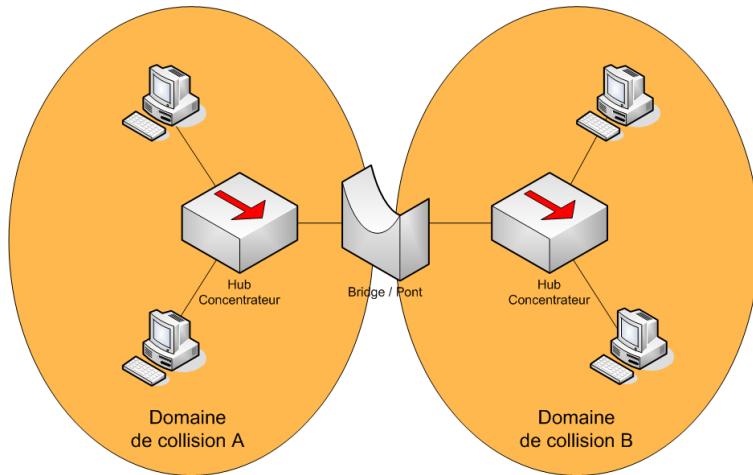


Nombre de domaine de broadcast :
Nombre de domaine de collision :

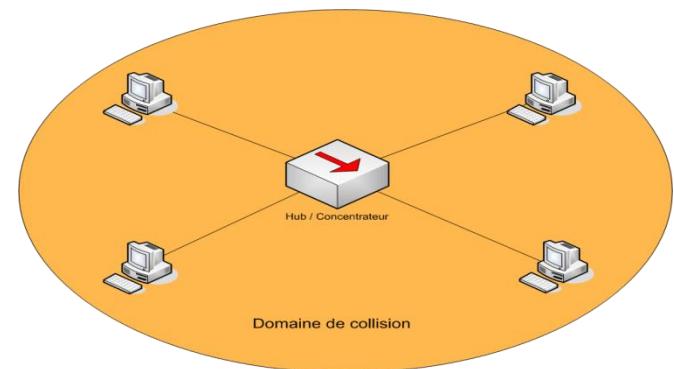
Domaine de diffusion/ collision

Exercice:

Calculer le nombre de domaines de collision et de diffusion pour les architectures réseaux suivantes



Nombre de domaine de broadcast : 1
Nombre de domaine de collision : 2

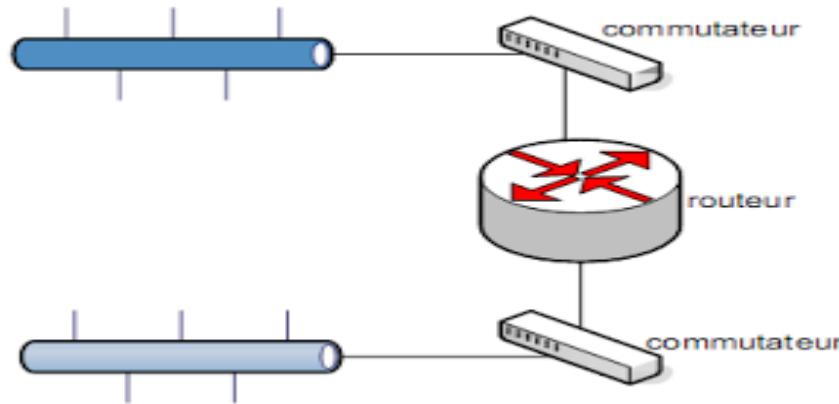


Nombre de domaine de broadcast : 1
Nombre de domaine de collision : 1

Domaine de diffusion/ collision

Exercice:

Soit le réseau suivant :



Nombre de domaine de diffusion
: **2**

Nombre de domaine de collision
: **4**

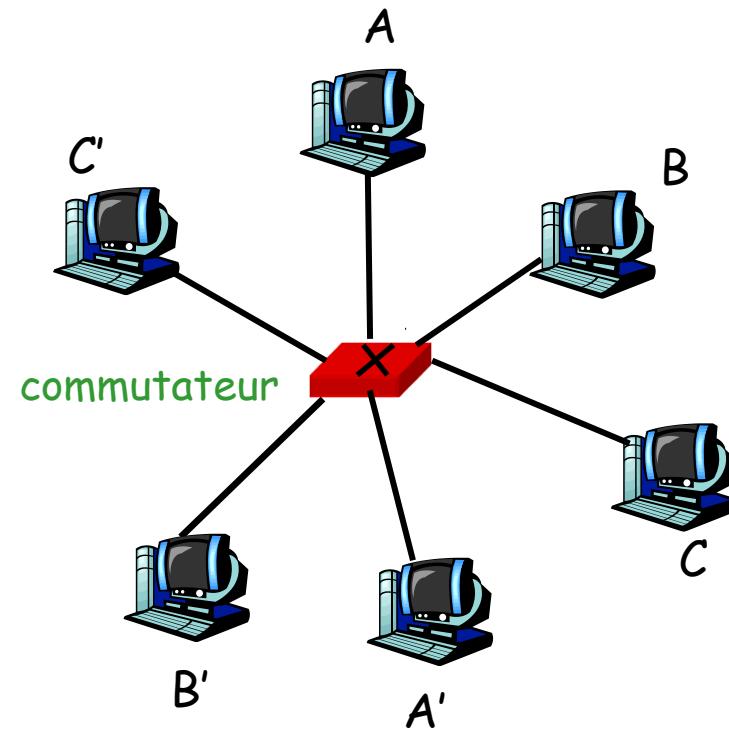
Si on enlève le routeur et qu'on relie les deux commutateurs :

Combien y aura-t-il de domaine de diffusion générale ? **un seul domaine**

Combien y aura-t-il de domaine de collision ? **3 domaines**

Principes commutateur

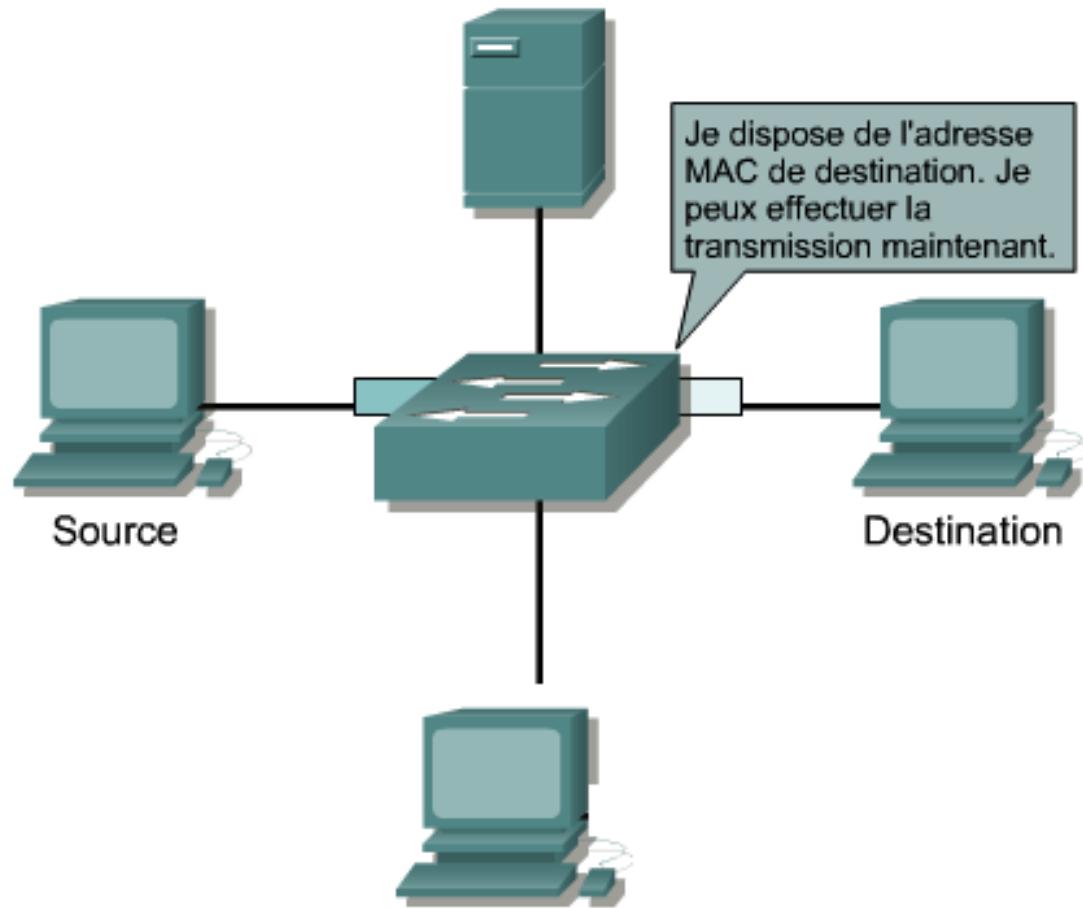
- Réduire les collisions pour accroître les débits
- Utilisation d'une topologie en étoile (migration facile)
- Remplacer le nœud central passif (HUB) par un commutateur
- Full duplex
- A-to-A' et B-to-B' en même temps sans collisions



Commutateur mode Cut-Through

- La commutation d'une trame vers un port de destination est fonction du niveau de latence et de fiabilité
- Un commutateur peut commencer à transférer la trame dès que l'adresse MAC est reçue
- Pour le reste, il se comporte comme un répéteur, une fois la liaison établie avec l'interface de sortie
- Ce mode de commutation des paquets est appelé «**Cut-through**»

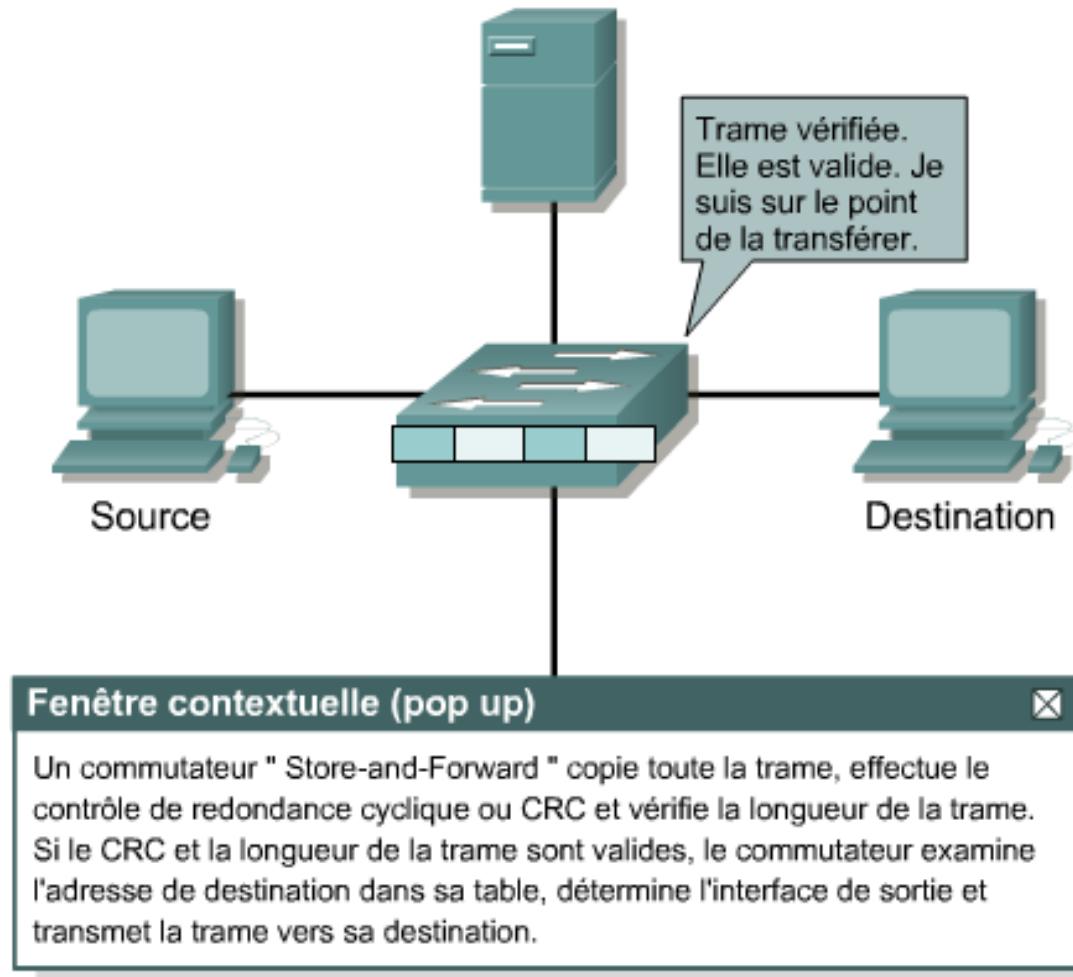
Commutateur « Cut-Through »



Commutateur mode Store & Forward

- Un commutateur peut également attendre de recevoir la trame entière avant de la re-transmettre entièrement vers le port de destination
- Cela permet au logiciel de commutation de vérifier la séquence de contrôle de trame (FCS, *Frame Check Sequence*)
- Si la trame n'est pas correcte, elle est rejetée au niveau du commutateur
- La trame entière est stockée avant d'être transmise => ce mode de commutation des paquets est appelé «**Store-and-Forward**»

Commutateur « Store & Forward »



Ethernet – équipements de réseau

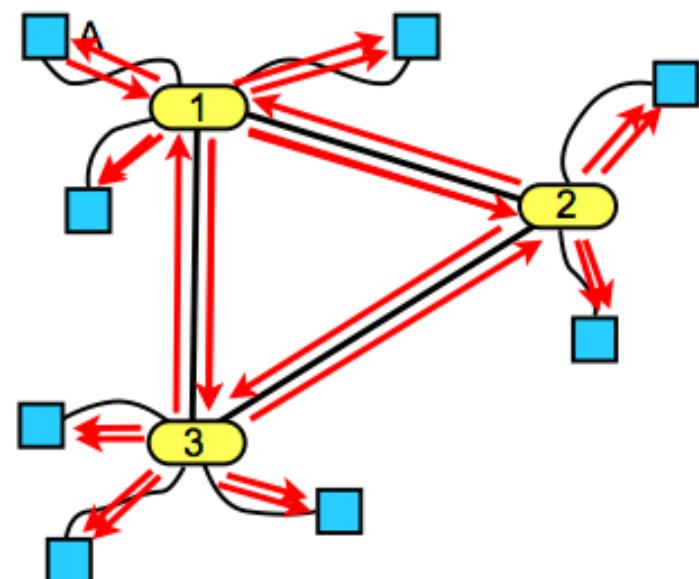
- **équipements de couche 1: répéteurs et concentrateurs (HUB),**
 - Principalement utilisés pour étendre les segments de câble Ethernet
 - Ils permettent d'ajouter davantage d'hôtes
 - Chaque hôte ajouté augmente la quantité de trafic potentiel sur le réseau ⇒ augmente les risques de collision parce que ces équipements ne séparent pas les domaines de collision
- **équipements de couche 2: pont (bridge) et commutateur (switch)**
 - Divisent les domaines de collisions
 - Utilisent les @ MAC des trames
 - Transport simultanée de données sur des domaines de collisions différents

Topologie redondante : problème

- Lorsque plusieurs commutateurs sont placés dans une arborescence hiérarchique simple, il est peu probable que des boucles de commutation se produisent
- Toutefois, les réseaux commutés possèdent très souvent des chemins redondants afin d'assurer une meilleure fiabilité et une meilleure tolérance aux pannes
- Les chemins redondants sont extrêmement utiles mais peuvent avoir des effets secondaires, tels que les **boucles de commutation**

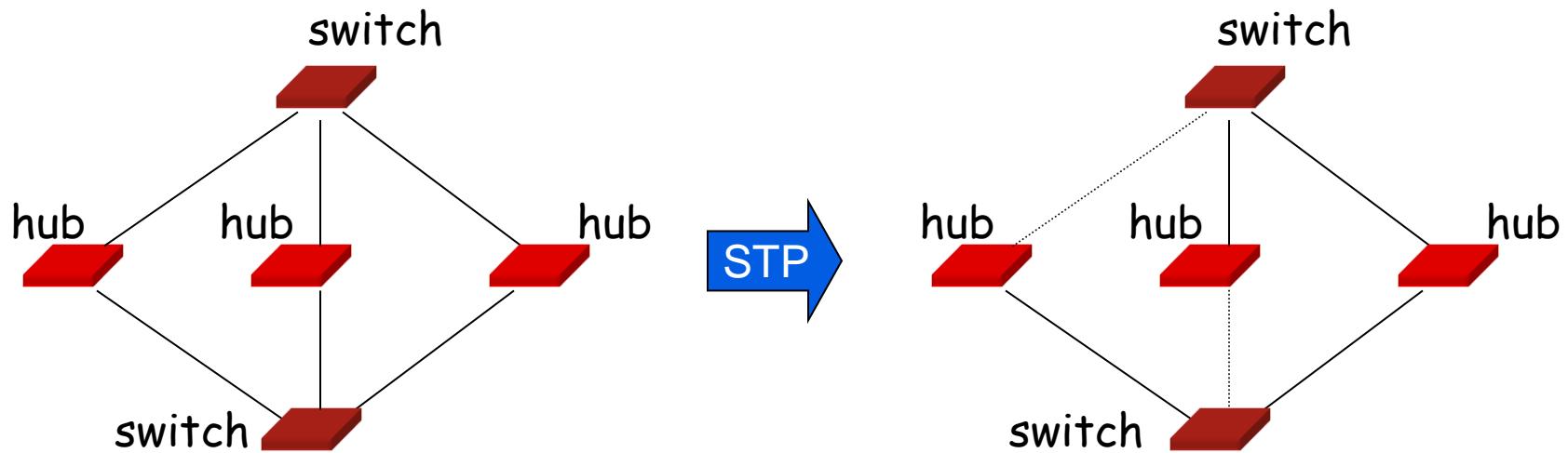
Topologie redondante : exemple de boucle

1. A transmet la trame dont la destination est B
2. Le commutateur 1 ne connaît pas l'interface vers B, donc envoie la trame à tous sauf le domaine d'où la trame est arrivé
3. 2 et 3 ne connaissent pas l'interface vers B donc envoient la trame à tous sauf au port d'où la trame est arrivée (donc pas à 1)
4. 2 et 3 reçoivent de nouveau la trame par 3 et 2 respectivement et donc renvoient la trame dans les interfaces sauf celle d'entrée
5. 1 reçoit la trame et on recommence du pas 2



Spanning Tree Protocole (arbre couvrant)

- Le protocole STP est un protocole normalisé qui permet d'éviter les boucles de commutation
- But : créer un sous-ensemble de la topologie initiale sans boucles
- Un commutateur déconnecte certains ports en accord à la topologie définie par l'arbre couvrant



Plan

■ Les réseaux locaux:

- Principes
- Sous-couche MAC
- Ethernet
- Ethernet et la commutation
- **Annexes (HDLC et sous-couche LLC)**

HDLC (High Data Link Control)

- Présenté en 1976, HDLC, dérivé du protocole SDLC ("Synchronous data link control") proposé par IBM
- Protocole de niveau liaison, il est défini par les normes:
 - ISO 3309 : HDLC frame structure
 - ISO 4335 : HDLC : elements of procedure
- Evolution de HDLC
 - PPP : connexion point-à-point Internet
 - LAP-B (Link Access Procedure) réseaux WAN X.25
 - LAP-D : utilisé dans les réseaux ISDN (Integrated Services Digital Network)

HDLC : Modes de communication

■ **Normal Response Mode (NRM)**

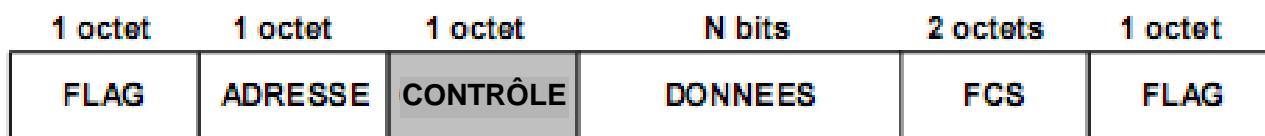
- Une station maître et une station esclave (point à point) ou plusieurs stations esclaves (multipoint)
- Mode asymétrique : une station esclave peut commencer la communication seulement si autorisée par la station maître
- Half-duplex
- *Commandes*= Messages du maître; *Réponses* = messages des esclaves

■ **Asynchronous Balanced Mode (ABM)**

- Connexion équilibrée entre deux stations
- Full-duplex
- Chaque station peut émettre quand elle veut

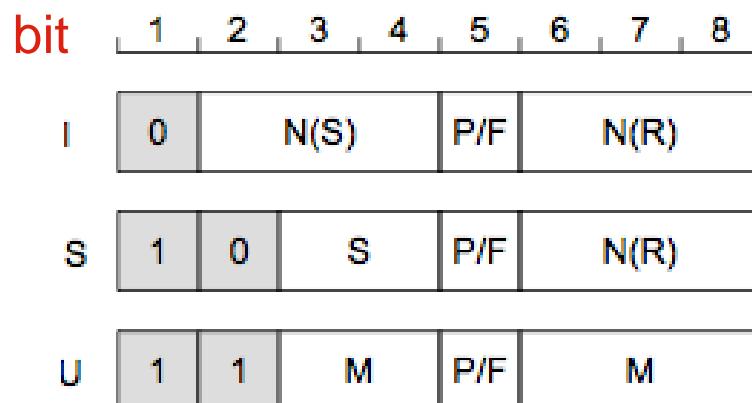
HDLC : format général d'une trame

- Trame L-PDU ("Link protocol data unit")
- Le champ contrôle sert à différencier trois types de trame



HDLC : Types de trames

- Trame d'Information I : pour effectuer le transfert des données
- Trame de Supervision S : pour effectuer les fonctions de supervision de la liaison
 - ex.: demande de retransmission, demande de suspension de la transmission, etc.
- Trame non Numérotées U : pour les fonctions de commande de la liaison (ex. ouverture d'une connexion)



Trame HDLC : Fanion (« flag »)

- Délimite la trame:
 - La trame est de longueur variable puisque le champ de données est de longueur variable
- Format:
 - Octet formé de 6 bits consécutifs à 1, préfixés et suffixés par un bit à 0
- Unicité:
 - Comment assurer l'unicité de la configuration binaire du fanion à l'intérieur de la trame puisque le champ de données de la trame peut comporter n'importe quel octet (le transport des données est transparent) ?
- Transcodage:
 - La trame (sauf les fanions) est transcodée lors de la transmission
 - Toute suite de 5 bits consécutifs à 1 est transcodée en une suite de cinq bits à 1 et d'un bit à 0
 - Augmentation de la longueur de la trame
 - La longueur de la trame transcodée n'est plus un multiple d'octets

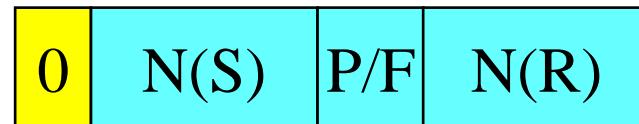
HDLC : Fanion (« flag »)

- Si le récepteur après avoir reçu 5 bits consécutifs à 1
- Reçoit un bit 0 \Rightarrow l'efface immédiatement
- Reçoit un bit 1 \Rightarrow il y a deux possibilités
 - Le bit après le 1 est un 0, le récepteur a détecté un nouveau fanion
 - Le bit après le 1 est un 1, le récepteur a détecté une suite d'abandon et la trame doit être rejetée
- Exemple:
 - Suite binaire originale: 0110001011111110111110
 - Suite transcodée: 011000101111111101111110

HDLC champ adresse

- Champ adresses (8b)
 - A la base mode point-à-point, maitre-esclave (NRM)
 - Les machines s'échangent des commandes et des réponses à ces commandes
 - Nécessaire de savoir si la trame circulant dans la liaison est une commande ou une réponse, ainsi que la provenance de la trame
 - Système à 2 adresses 0000 0001 et 0000 0011 comme suit:
 - Si émetteur d'une commande est ETTD (abonné) vers récepteur ETCD (réseau), alors adresse 0000 0001
 - Si émetteur d'une commande est ETCD (réseau) vers récepteur ETTD (abonné), alors adresse 0000 0011
 - Si émetteur d'une réponse est ETTD (abonné) vers récepteur ETCD (réseau), alors adresse 0000 0011
 - Si émetteur d'une réponse est ETCD (réseau) vers récepteur ETTD (abonné), alors adresse 0000 0001
 - Adresse de diffusion totale ("broadcast"): 11111111
 - Champ d'adresse extensible à 16b

Trame d'information I

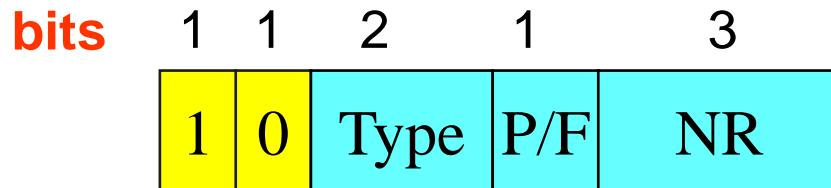


- N(S): Numéro de séquence de la trame, peut prendre une valeur de 0 à modulo-1 où $\text{modulo} \in \{8, 128\}$
 - Au plus modulo-1 trames peuvent être en attente d'acquittement
- N(R): Utilisé pour acquitter les trames reçues, numéro de la première trame qu'on s'attend à recevoir
 - Permet d'acquitter toutes les trames avec numéro < N(R)
 - La perte d'un acquittement peut ainsi être compensée par le prochain acquittement
- P/F: poll/final bit

Bit P/F

- Bit Polling/ Final a une utilisation différente selon les modes de dialogue entre stations
- Normal Response Mode-NMR
 - le bit est mis à 1 par le maître pour interroger une station esclave
 - L'esclave répond avec plusieurs trames, dont la dernière a le bit P/F=1 (Final) \Rightarrow donne de nouveau le contrôle de la liaison au maître
- Asynchronous Balanced Mode (ABM)
 - Généralement est égal à 0, il est mis à 1 pour demander la retransmission des trames à cause d'un timeout

Trames de supervision S : champ contrôle



Sous-champ *Type* pour identifier un des 4 types de trame de supervision :

- La trame de supervision **RNR (Receive Not Ready)**
 - Interdit la transmission des trames suivantes, indique une impossibilité momentanée à accepter des trames de données supplémentaires
 - Confirme la réception des trames de données de $n^o < NR$

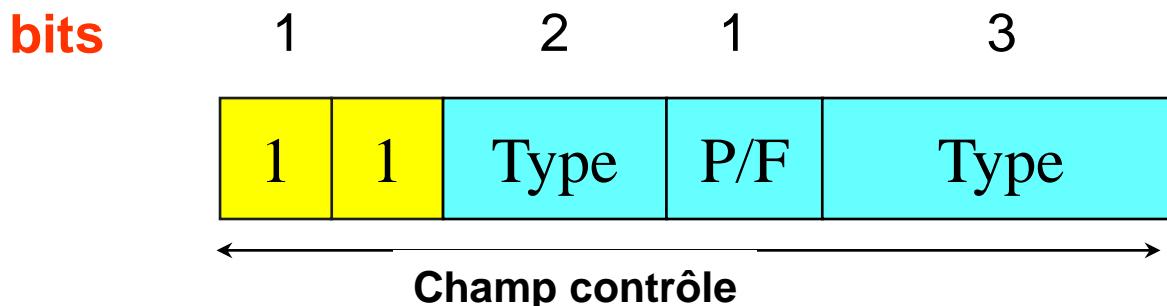
Trames de supervision S : champ contrôle

- RR ("Receive & Ready") :
 - Indique que l'émetteur est prêt à recevoir une trame de données !
 - Confirme la réception des trames de données de n° < N(R)
- Une trame RR peut être utilisée pour indiquer la fin d'un état d'occupation qui a été signalé auparavant par l'émission d'une trame RNR (Receive Not Ready) par la même station

Trames de supervision S: champ contrôle

- REJ ("Reject"): trame d'acquittement négatif
 - Indique qu'une erreur de transmission a été détectée
 - NR contient le numéro de la première trame incorrecte reçue
 - Demande la retransmission des trames d'information numérotées à partir de NR \Rightarrow rejet totale
- SREJ ("Selective Reject"): protection contre les erreurs
 - Demande la retransmission de la trame de $n^o = NR$

Trames non numérotées U



- Les champs *Type* (5 bit) codent les types de trames non numérotées
- Des trames nécessaires à la gestion de la connexion:
 - Trame d'**établissement de la connexion** (commande) :
 - **SABM** ("Set asynchronous balanced mode") - en format normal : un octet pour tous les champs commande et commande/reponse
 - **SABME** ("Set asynchronous balanced mode extended") - en format étendu : deux octets pour tous les champs commande et commande/reponse numérotées et un octet pour celles non numérotées

Trames non numérotées U

- Trame de **libération de la connexion** (commande) **DISC** ("Disconnection")
 - L'émetteur du commande DISC suspend son fonctionnement après avoir reçu une trame d'accusé de réception non numérotée (UA)
- Trame d'**accusé de réception non numérotée UA** (réponse) pour les commandes non numérotées, SABM/SABME et DISC

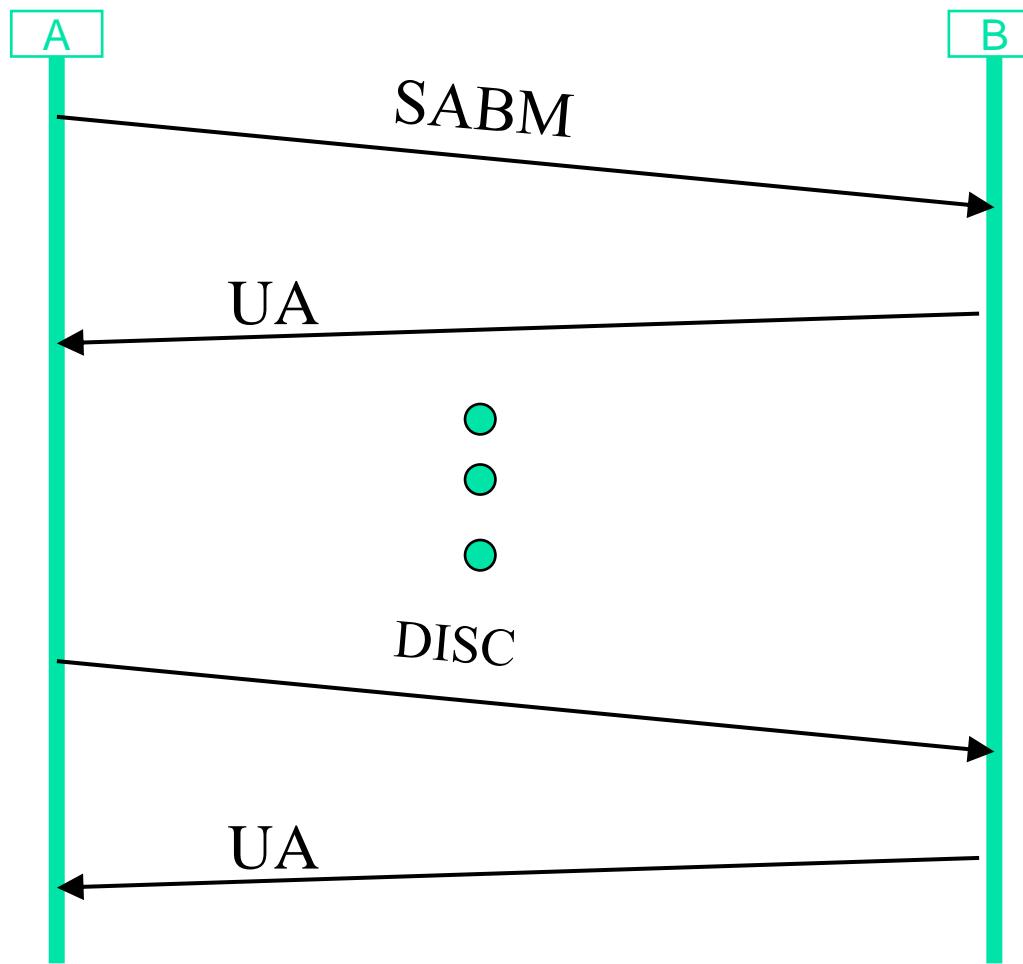
Trames non numérotées U

- Trame d'**indication de connexion libérée**
 - DM ("Disconnected mode")
- Trame de **rejet FRMR** ("Frame reject") (réponse) indiquant une condition d'erreur ne pouvant pas être récupérée par la retransmission d'une trame identique
 - Réception d'un champ de donnée qui dépasse la longueur maximale fixée
 - Réception d'un NR non valide
 - ...

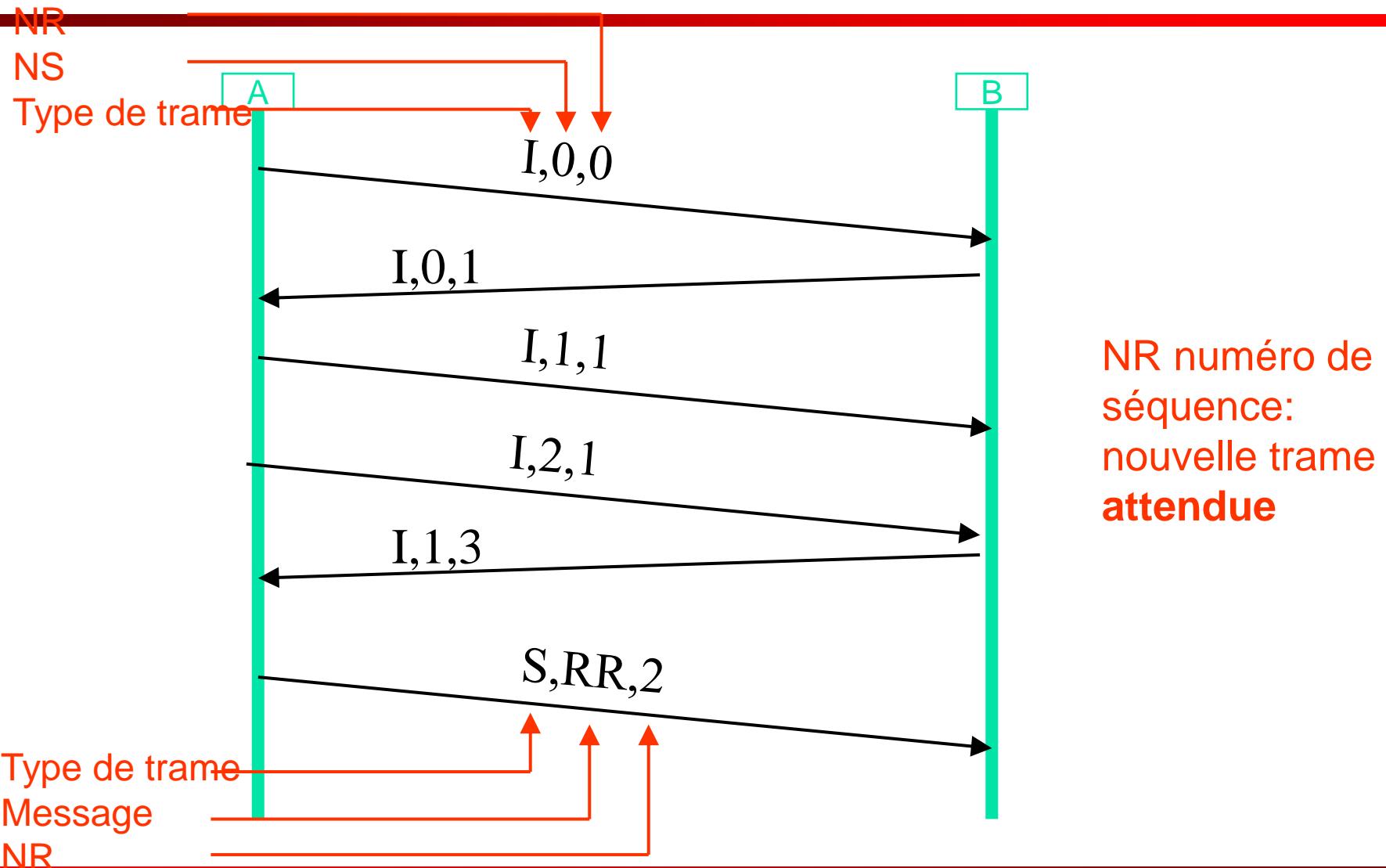
HDLC - Variables et temporisations locales

- Chaque entité tient à jour les trois variables suivantes
 - $V(S)$ = numéro de la prochaine trame d'information à émettre,
 - $V(R)$ = numéro de la prochaine trame à recevoir,
 - $DN(R)$ = numéro du dernier acquittement reçu
- et connaît les constantes suivantes
 - $T1$ = délai de garde au bout duquel une trame non acquittée est réémise
 - $T2$ = délai d'acquittement pendant lequel le récepteur peut retarder l'envoi de l'acquittement d'une trame
 - $N1$ = taille maximum d'une trame
 - $N2$ = nombre maximum de réémissions d'une même trame.
 - W = largeur de la fenêtre
 - ...

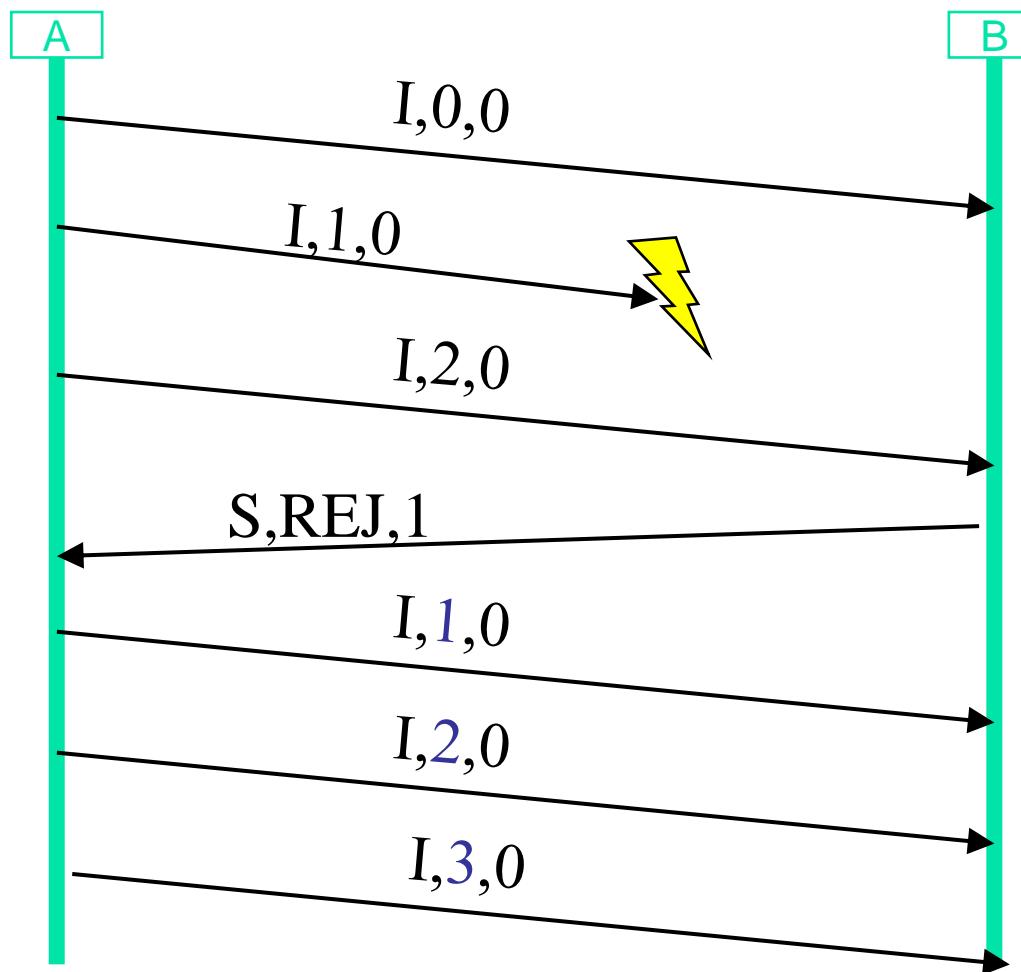
Gestion de connexion



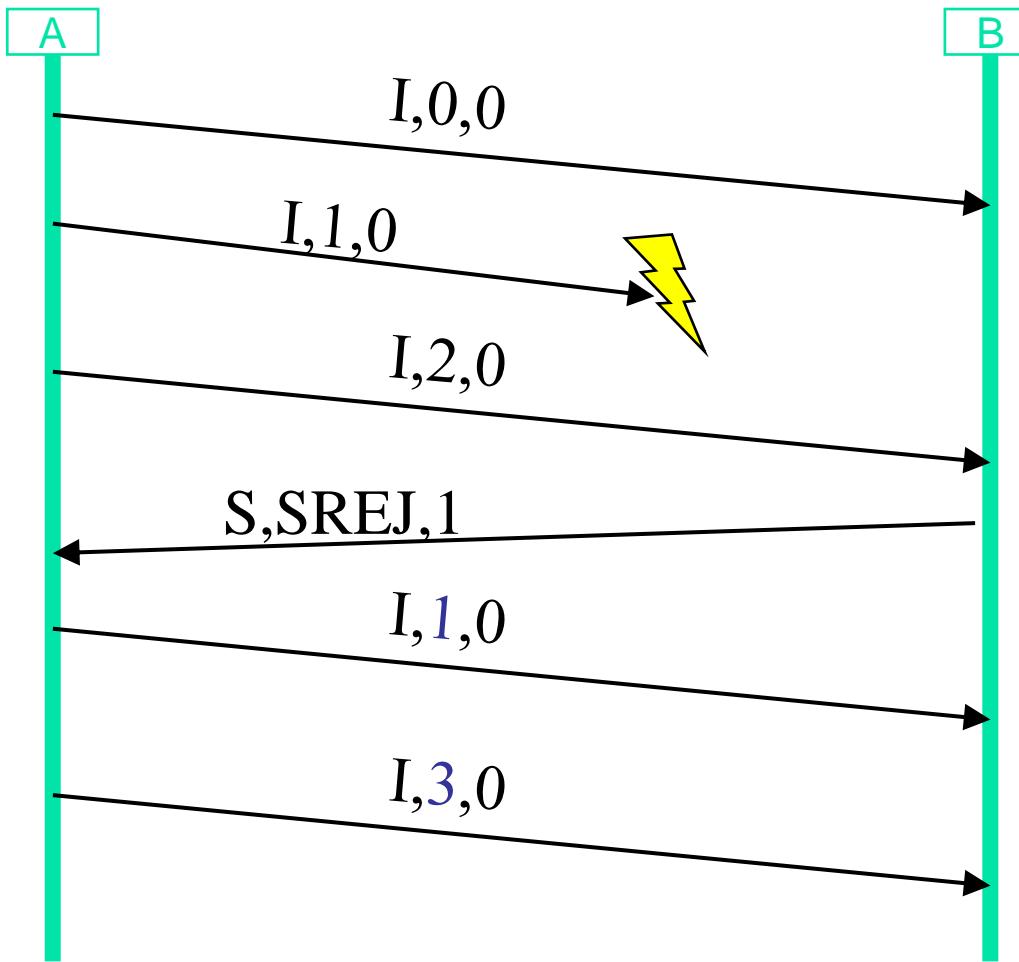
Exemple d'échange de données



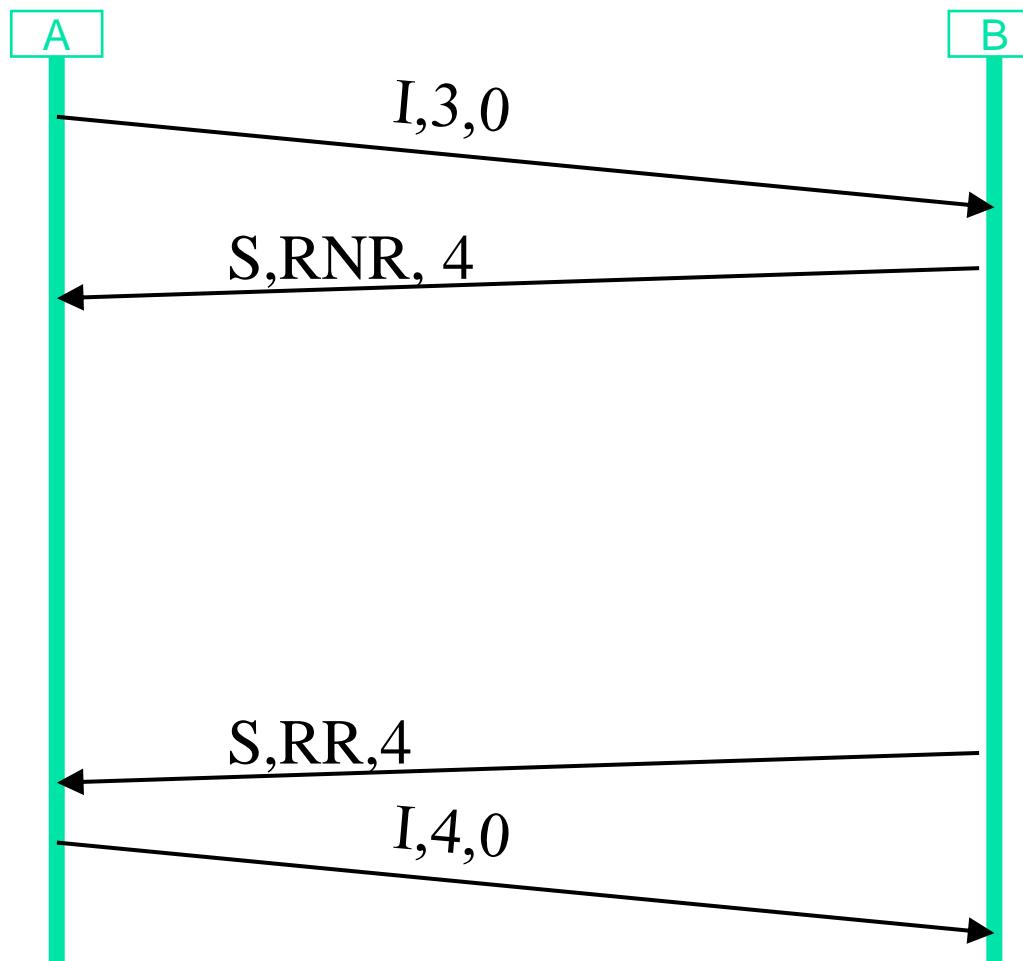
Rejet total



Rejet sélectif



Récepteur occupé



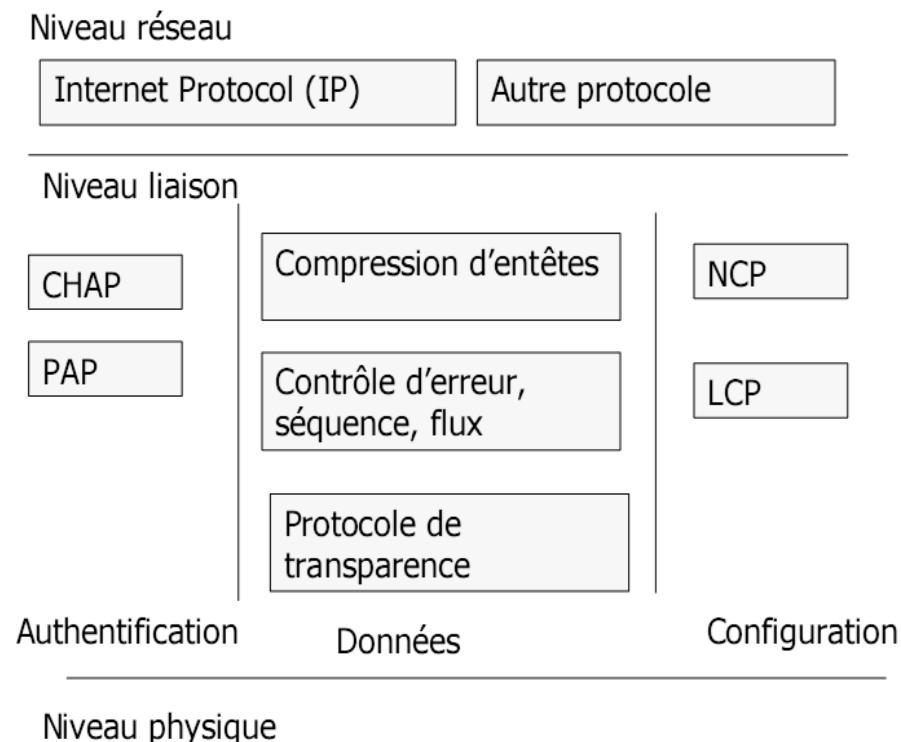
Couche liaison de données dans l'Internet : PPP

Liaison point-à-point dans l'Internet

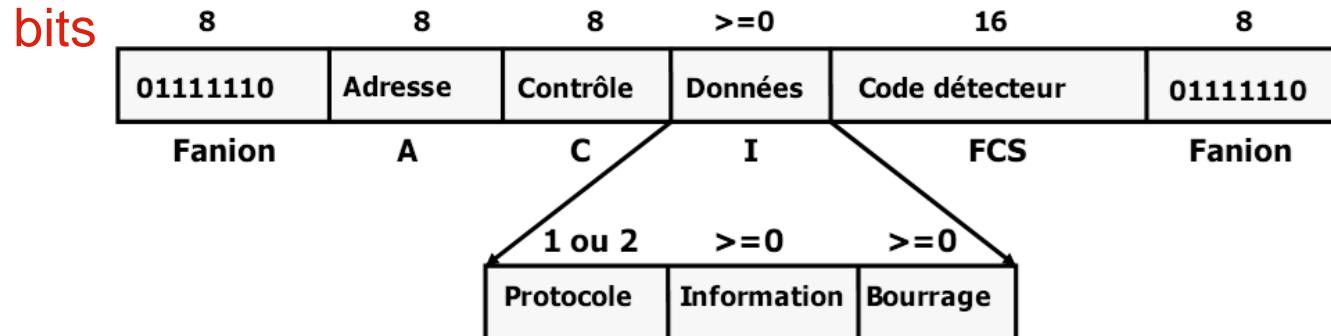
- *Entreprises* : un ou plusieurs réseaux locaux communiquent vers le monde extérieur passant par un ou deux routeurs qui disposent de liaisons point-à-point vers des routeurs distants
- *Personnes* qui souhaite accéder individuellement à Internet en utilisant une liaison téléphonique et un modem

Point-to-Point Protocol (PPP)

- PPP est défini dans RFC 1661, 1662, 1663
- Défini par 3 composants:
 - Un format de trame (proche de celui d'HDLC)
 - Un protocole **LCP (Link Control Protocol)** pour établir, configurer, et tester une connexion
 - Un protocole **NCP (Network Control Protocol)** permettant la négociation de paramètres pour chacun des protocoles réseaux supportés

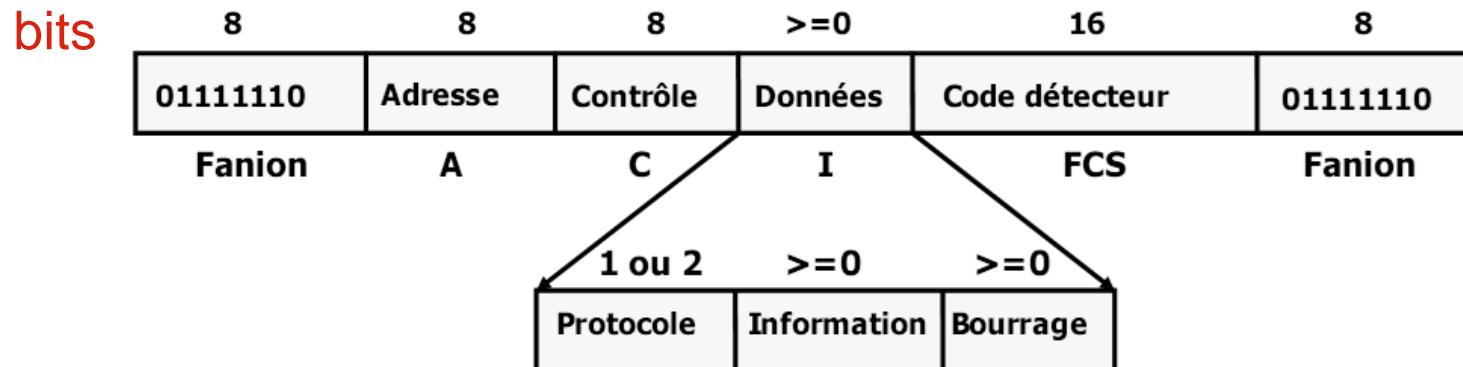


Format de la trame PPP



- PPP orienté caractère : la trame comporte un nombre entier d'octets (HDLC orienté bit)
- Adresse = suite de 8 bits à 1 pour indiquer une adresse de diffusion (broadcast)
- Contrôle = 00000011 pour indiquer une trame non numérotée \Rightarrow PPP par défaut ne fournit pas une transmission fiable
- Adresse et Contrôle sont des champs constants \Rightarrow LCP fournit le mécanisme nécessaire aux deux parties pour négocier une option en omettant ces deux champs

Format de la trame PPP



- Le champ protocole indique le type de paquet que contient le champ données:
 - Protocoles réseaux (exemple IP, IPX, CLNP) commencent par un bit 0, LCP et les différents NCP commencent par un 1
 - 1 ou 2 octets
- Champ données: longueur variant jusqu'à un certain maximum négocié. Si l'on ne négocie pas la longueur en utilisant LCP à l'établissement de la liaison, la valeur par défaut est de 1500 octets

PPP- scénario classique

- Un utilisateur appelle un fournisseur d'accès Internet pour établir une liaison
 1. L'ordinateur de l'utilisateur appelle par téléphone, via un modem, le routeur du fournisseur d'accès
 2. Après que le routeur a décroché et la liaison physique a été établie, l'ordinateur envoie des paquets LCP dans le champ données d'une ou plusieurs trames PPP et ses paquets et leur réponses permettent de sélectionner les paramètres PPP à utiliser
 3. Ces paramètres étant définis, on envoie une série de paquets NCP pour configurer la couche réseau : exemple affecter une adresse IP à l'utilisateur

PPP- Protocole LCP

- Utilisé pendant la phase d'établissement d'une liaison PPP de données pour négocier des options de configuration de la liaison
 - Fournit les moyens de faire une proposition et d'accepter ou rejeter une réponse, complètement ou partiellement
 - Moyen pour assurer la qualité de la liaison
 - Permet de désactiver les lignes lorsqu'on en a plus besoin

Protocole LCP : options de configuration de la liaison

- **Maximum Receive Unit (MRU)** : Taille maximale de la trame PPP. Par default, MRU est 1,500.
- **Authentication Protocol** : Indication du protocole d'authentification qui sera utilisé en phase d'authentification
- **Address and Control Field Compression** : Un flag indiquant que les champs Adresse et Contrôle seront effacés de l'entête de la trame PPP
- ...

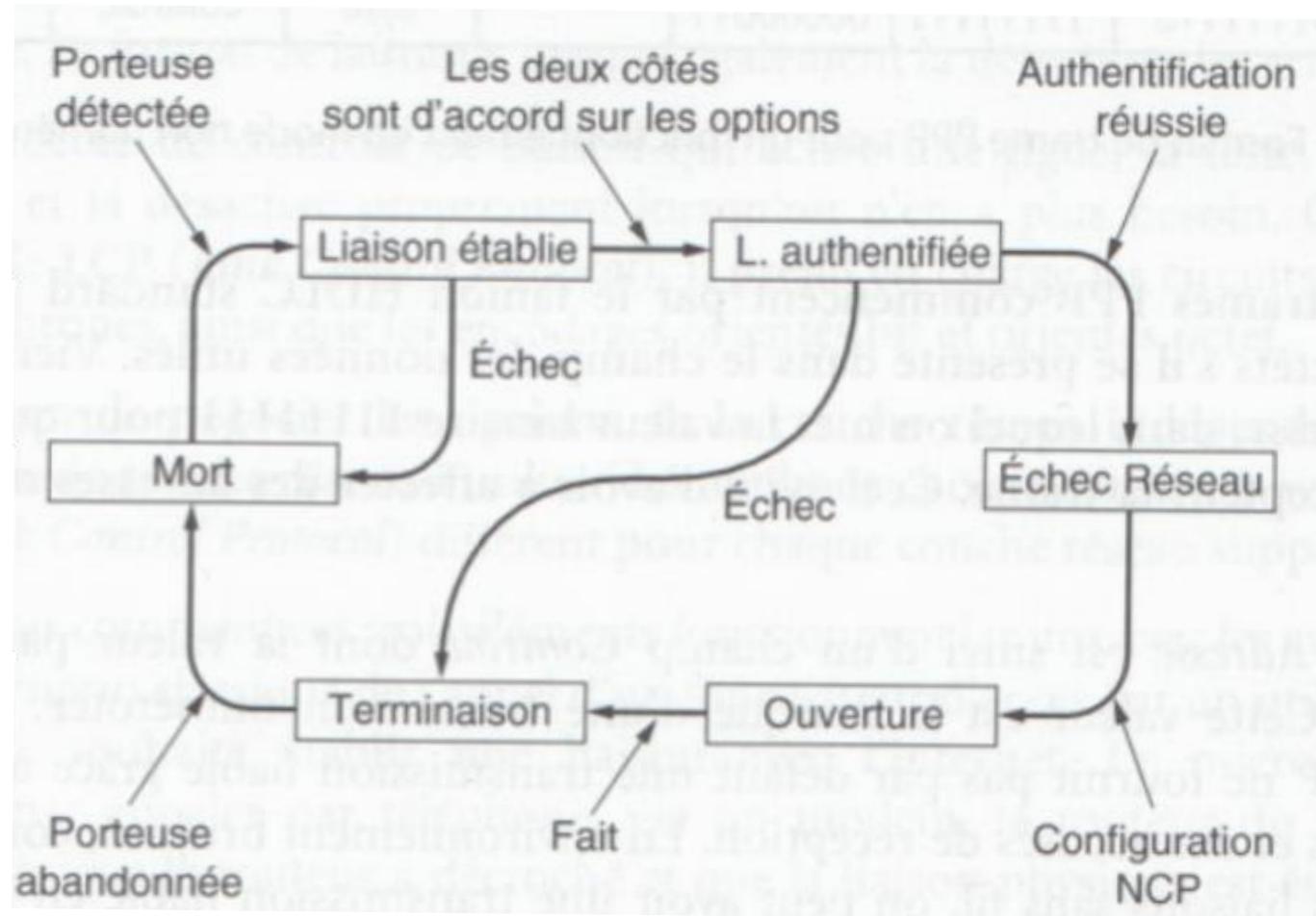
PPP - Protocole LCP

- Moyen pour faire une proposition et d'accepter ou rejeter une réponse
 - Configurer-requête : propose des valeurs d'option au récepteur
 - Configurer-ack : tous les valeurs sont acceptées
 - Configurer-nack : certaines valeurs sont refusées
 - Configurer-rejet : certaines valeurs ne sont pas négociables
 - Terminer-requête : requête pour désactiver la ligne
 - Terminer-ack : ligne désactivée
 - etc

PPP - Protocole NCP

- Le protocole NCP permet la négociation d'options de configuration du niveau 3 réseau dans le cadre du niveau 2 liaison
- Fonctions nécessairement dépendantes du protocole réseau utilisé \Rightarrow existence de protocoles NCP spécifiques par type de réseau
 - RFC 1332 IPCP pour IP
- Envoi de paquets NCP encapsulés dans des trames PPP pour obtenir/libérer une adresse IP

Diagramme simplifié d'activation/désactivation d'une ligne



Plan

■ Les réseaux locaux:

- Principes
- Sous-couche MAC
- Ethernet
- Ethernet et la commutation
- **Annexes (HDLC et sous-couche LLC)**

La couche LLC – Logical Link Control 802.2

- Le but du protocole LLC est de fournir une garantie de livraison des messages appelés LSDU (Link Services Data Unit), la détection et la reprise sur erreur
 - L'envoi d'un datagramme (ou paquet) ne garantit pas à son émetteur que le ou les destinataires ont reçu ce message
- Sous-couche commune des sous-couches MAC (Dérivée de HDLC)
- Propose 3 niveaux de service (qualité):
 - **LLC1** - service sans connexion et sans acquittement
 - **LLC2** - service avec connexion et ack
 - **LLC3** - service sans connexion et avec acquittement au choix

La couche LLC – Logical Link Control 802.2

- Offre l'interface d'accès à la couche Liaison

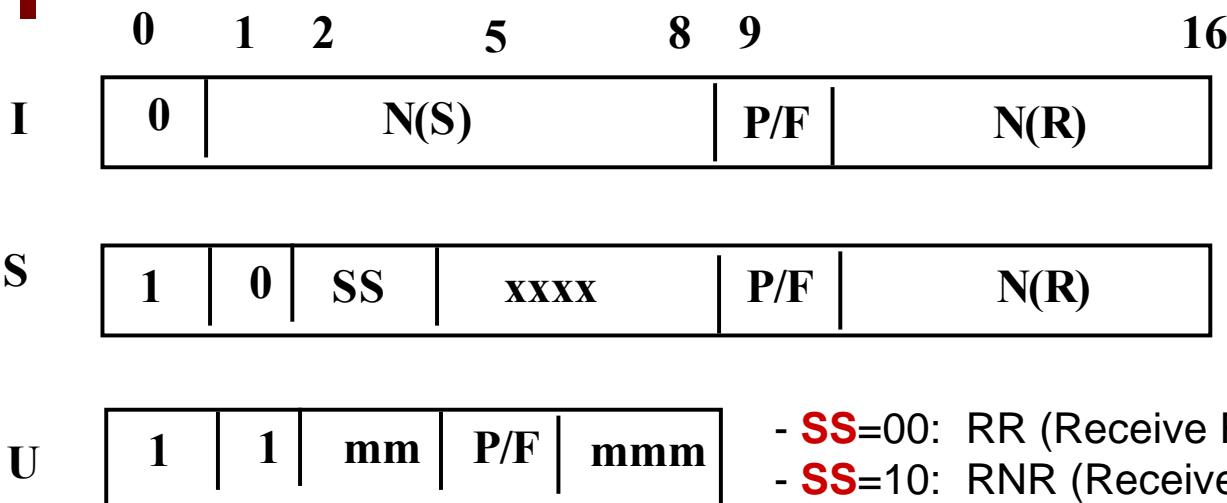
- Primitives sans connexion
 - L_DATA.request
 - L_DATA.indication
- Primitives avec connexion
 - L_CONNECT (request, indication, response, confirm)
 - L_DATA_CONNECT (request, indication, response, confirm)
 - L_DISCONNECT (request, indication)
 - L_RESET (request, indication, response et confirm)
 - L_CONNECT_FLOW_CONTROL (request, indication)

La couche LLC – Logical Link Control 802.2

- Multiplexage
- LLC offre également la possibilité de multiplexer plusieurs connexions réseaux sur une seule liaison virtuelle:
 - Au moyen des **DSAP** (Destination SAP) et **SSAP** (Source SAP) codés sur 1 octet
 - Champ contrôle identique que pour HDLC (distingue les types de trames : U, S, I)



La couche LLC – Logical Link Control 802.2



MM-MMM :

SABME: Demande d'ouverture de Connexion mode asynchrone équilibré étendu,

UA: [Réponse] Acquittement non numéroté

DM : [Réponse] La liaison est déconnectée (Ack négatif suite à un SABME).

DISC : Fermeture d'une connexion : Disjonction

FRMR : Rejet du LPDU en raison d'une erreur (la cause et le diagnostic sont mentionnés),

XID : Echange d'identité entre deux entités LLC,

TEST: Utilisé pour tester une liaison,

UI : Information non numérotée (trames porteuses de données)

La couche LLC – Logical Link Control 802.2

- LLC 2: service avec connexion et avec acquittement
- A l'opposé de LLC 1, qui offre un service très simple de datagramme, le service du type 2, appelé LLC 2, permet de créer et de gérer des échanges sur connexion. Il offre une liaison fiabilisée avec contrôle de flux et reprise sur erreurs, au prix de sa complexité.
- Les fonctionnalités du LLC 2 sont très semblable à celles du HDLC:
 - Tous les **LPDU non numérotés (U)**, à l'exception de l'**UI**, **XID** et **TEST**, sont utilisés pour la gestion de liaison
 - Les **LPDU d'information (I)** numérotés sont utilisés pour créer un flux de données.
 - Les **LPDU de supervision (S)** sont utilisés pour contrôler le flux d'une part (RR, RNR); et effectuer des retransmissions en cas d'erreur (REJ) d'autre part.

La couche LLC – Logical Link Control 802.2

- LLC 3: service sans connexion et avec acquittement
- Le service du type 3, appelé LLC 3 a pour but d'offrir des liaisons en mode *datagramme* sans connexion qui sont *simples* à gérer mais néanmoins *rapides* et *fiables*, comme l'exigent de nombreuses applications temps-réel
- Chaque LPDU est acquitté individuellement. Si l'acquittement n'est pas arrivé au bout du temps imparti, la couche LLC ne prend pas l'initiative de retransmettre le LPDU, mais se contente de confirmer ce résultat négatif à la couche supérieure
- Les LPDU utilisés sont ceux du type 1 (**UI**, **XID**, **TEST**) plus **UA** et **FRMJ**