Cours de Réseaux

4 – La sous-couche de contrôle d'accès au canal

Rappel : le modèle hybride

5	Couche application
4	Couche transport
3	Couche réseau
2	Couche liaison de données
	(Sous-couche contrôle d'accès au canal)
1	Couche physique

La sous-couche de contrôle d'accès au canal

Media Acces Control (MAC)

- Seulement dans les réseaux duplex ou à multi-diffusion, en particulier les LANs
- Gestion des droits à émettre sur un canal partagé
- Éventuellement gestion de plusieurs canaux de communication sur un médium (multiplexage)
- Objectif : gestion dynamique pour mieux utiliser la bande passante du médium.

Paramètres du problème

- Temps :
  - discret : le fil de temps est coupé en créneaux. Envoi de trames seulement dans des créneaux.
    Nécessite un moyen de synchronisation.
  - continu : à priori les participants peuvent commencer à envoyer une trame à tout moment.
- Écoute de porteuse (*carrier sense*) :
  - pas d'écoute : exemple connexion sans fil.
  - avec écoute : exemple cuivre, fibre optique.

Sans écoute de porteuse

ALOHAnet : Norman Abramson, université de Hawaï, début des années 70 :
Réseau sans fils entre des stations fixes.
Topologie d'étoile : un nœud central (hub).
Un canal pour l'envoi des stations vers le hub, un envoi multi-diffusion par le hub.

ALOHA pur (1)

Temps continue.

Chaque station envoie sur le canal partagé une trame quand elle veut.

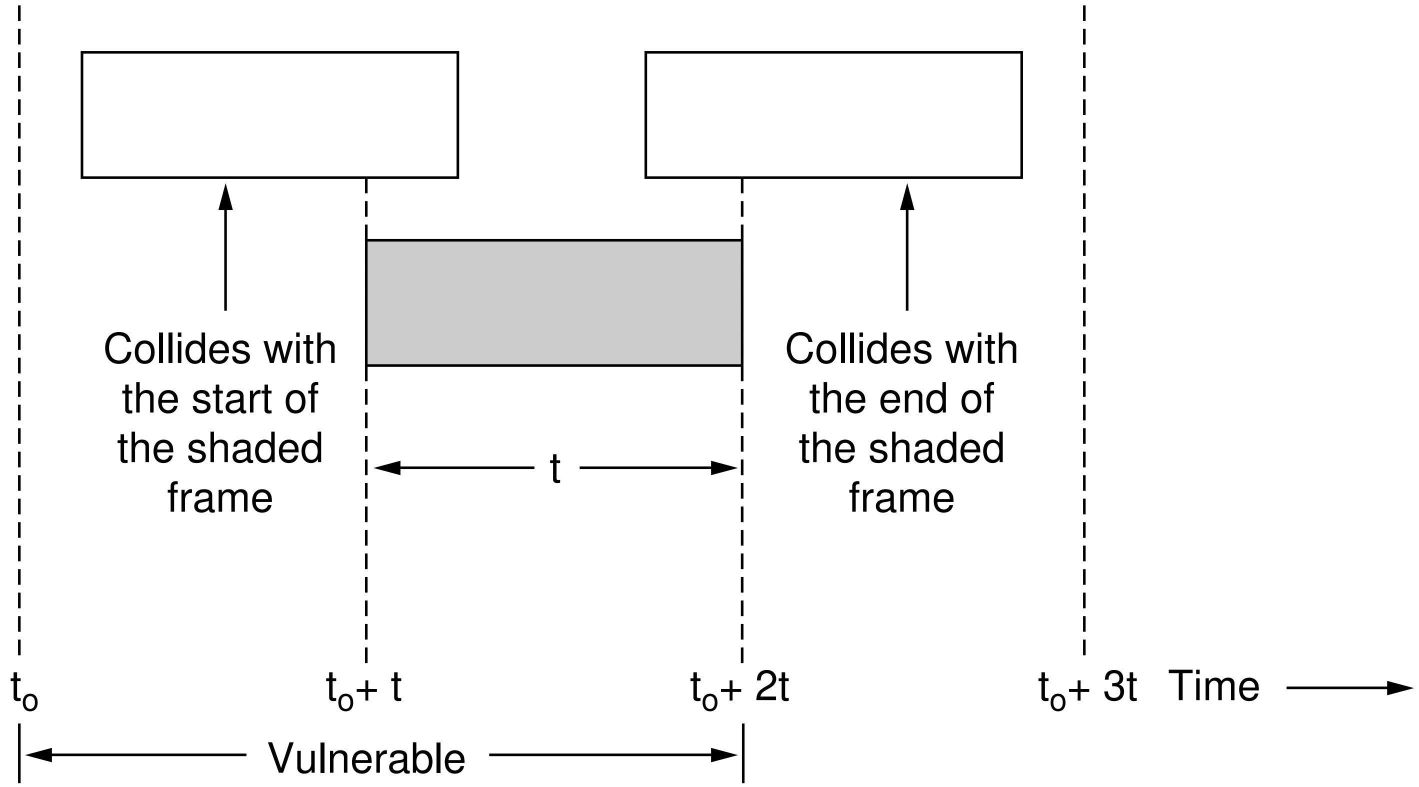
Le hub renvoie sur le canal de multi-diffusion un acquittement (pas de collision possible sur ce canal).

En cas d'erreur : station attend un temps aléatoire avant retransmission.

– Inconvénient : mauvaise utilisation de la bande passante.
– Avantage : Flexibilité.

Modèle pour le réseau Ethernet (voir plus tard).

ALOHA pur (2)



Collides with
the start of
the shaded
frame
t
Collides with
the end of
the shaded
frame
t_o
t_o+ t
t_o+ 2t
t_o+ 3t
Time
Vulnerable

ALOHA discrétisé

Temps partagé : le hub envoie régulièrement des signaux de synchronisation.

Les stations peuvent commencer un envoi seulement au début d'un créneau.

– Avantage : moins de collisions (50% par rapport à ALOHA pur).
– Inconvénient : nécessite synchronisation, plus de temps d'attente avant l'envoi d'une trame.

ALOHA discrétisée

Probabilité de succès : Soient k stations. Pour chaque créneau, probabilité p qu'une station donnée veut accéder le canal.

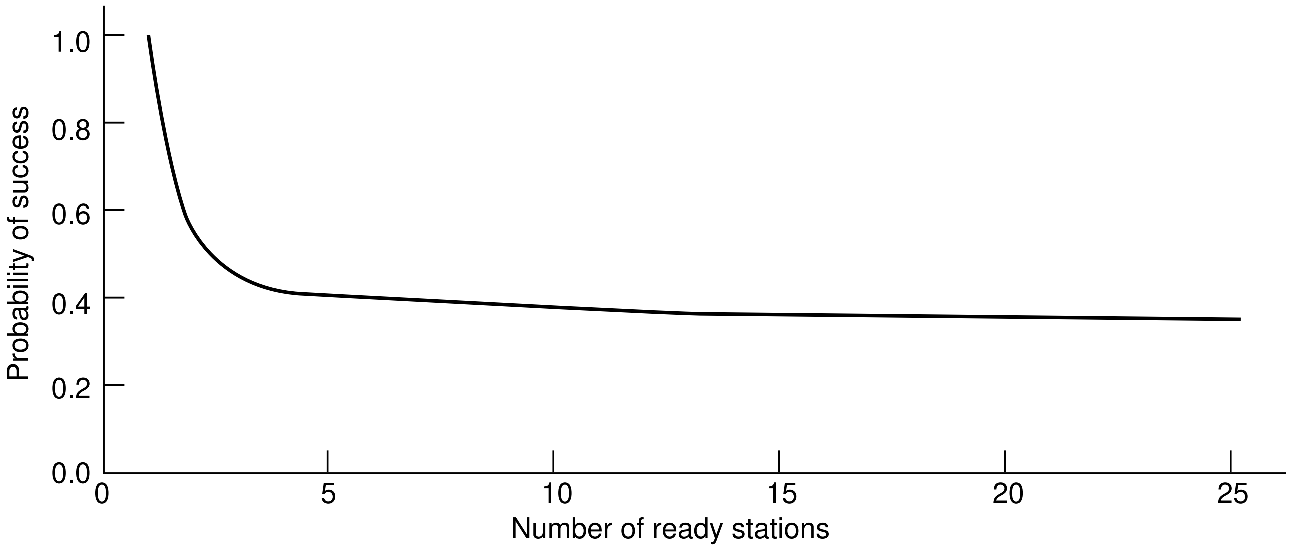
Probabilité que pour un créneau donné envoi d'un trame sans collision, c-à-d qu'il y a exactement un compétiteur :

$$kp(1-p)^{k-1}$$

Maximum pour $p = \frac{1}{k}$.

Probabilité de succès en ALOHA discrétisée

Probabilité dans le cas optimal ($p = \frac{1}{k}$) :



Écoute de porteuse : CSMA/CD

Carrier Sense Medium Access with Collision Detection

Pas d'émission quand la porteuse est déjà occupée.
Les collisions sont toujours possibles.
Soit $\tau =$ temps maximal de propagation d'un signal. Si pas de collision après temps $2\tau \Rightarrow$ émetteur a la main sûre sur le canal.

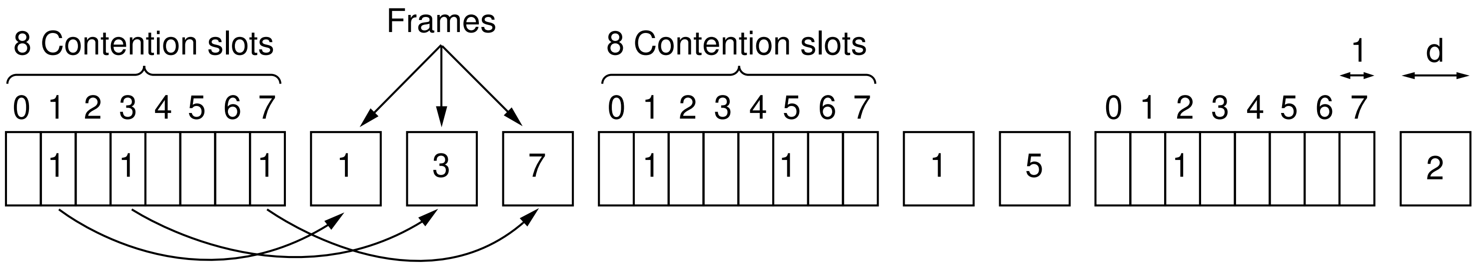
Quand le canal est pris, ou en cas de collision : attendre pour une période de durée randomisée.

Protocoles sans collision : Bit-Map (1)

Soient N stations

Pendant un premier temps : Les stations annonces dans l'ordre leur intention d'émettre (N créneaux à 1 bit)

Puis, les émetteurs émettent dans l'ordre.



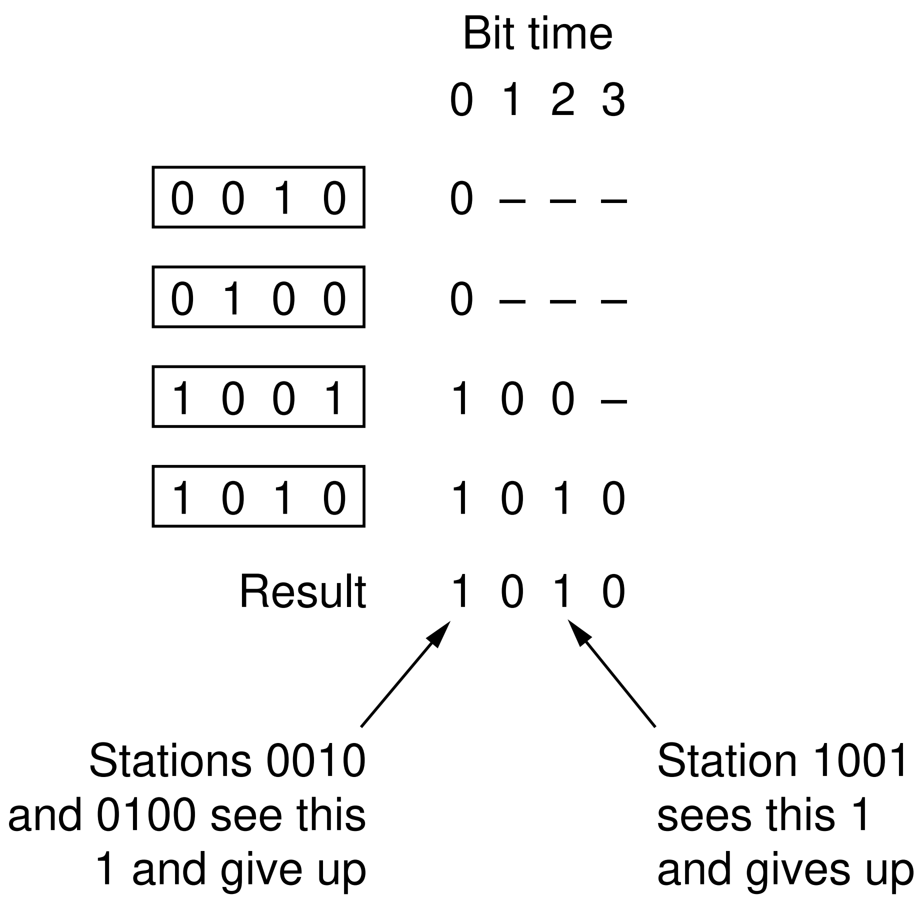
Protocoles sans collision : Bit-Map (1)

- Temps perdu pour les créneaux de contention.
- Il faut que tout le monde soit d'accord sur le nombre de participants.
- Favorise les stations avec un grand numéro dans le cas d'une faible occupation du canal (pourquoi ?).
- Borne supérieure pour le temps d'attente d'une station.

Protocoles sans collision : comptage binaire (1)

À chaque tours, élection de la station la plus prioritaire parmi celles qui souhaitent émettre.
Toutes les stations souhaitant d'émettre envoient de façon synchrone leur numéro (commençant par le bit le plus fort).
Quand une station voit un signal sur une position où elle à 0 dans son adresse elle se retire.

Protocoles sans collision : comptage binaire (2)



Protocoles sans collision : comptage binaire (3)

– Favorise la station avec le numéro le plus élevé.
– Pas de garantie d'un temps maximale d'attente.
– Amélioration : après chaque émission changement de numérotation : la station qui vient d'émettre obtient le numéro le plus bas.

Réseaux avec jetons (1)

Topologie d'un anneau

Les stations envoient toujours dans le même sens à leur voisin

À chaque moment un seul émetteur

Après avoir reçu une trame t de station $n-1$, la station n doit

– envoyer une trame à $n+1$ (soit t, soit sa propre trame)

– envoyer un jeton à $n+1$

En théorie meilleure performance que les protocoles avec collision (Ethernet)

Réseaux avec jetons (2)

Exemples :

– Token Bus par General Motors
  aujourd'hui complètement dépassé.
– IBM Token Ring
  aujourd'hui rarement utilisé.
– FDDI (Fiber Distributed Data Interconect) sur les réseaux à fibre optique
  encore en utilisation.

Protocoles à contention limitée

- Protocoles sans contention : perte dans le cas d'une collision.
  $\Rightarrow$ bonne performance pour faible trafic, performance dégradée en cas d'un trafic important
- Protocoles sans collision : coût supplémentaire pour contention
  $\Rightarrow$ performance diminué pour faible trafic, bonne performance en cas cas d'un trafic important

Comment combiner les avantages des deux approches ?

Parcours arborescent adaptatif (1)

Les numéros des stations sont arrangés dans un arbre binaire
Procédure try : entrée un arbre, résultat $\in \{\texttt{success}, \texttt{silent}\}$

- permet à tous les nœuds en t de parler
- Si silence : résultat `silent`
- Si un seul nœud parle : résultat `success`
- Si conflit :
  - match try(t.left) with :
    - `success` : résultat `sucess`
    - `silent` : try(t.right)
  - résultat : `success`

Parcours arborescent adaptatif (2)

Amélioration :

En cas d'un fort trafic ce n'est pas la peine d'essayer avec l'arbre complet car il y aura de toute façon un conflit.

⇒ On essaye séquentiellement les sous-arbres à un certain niveau.

Choisir le niveau en fonction du trafic observé sur le réseau.

Protocoles WDMA (1)

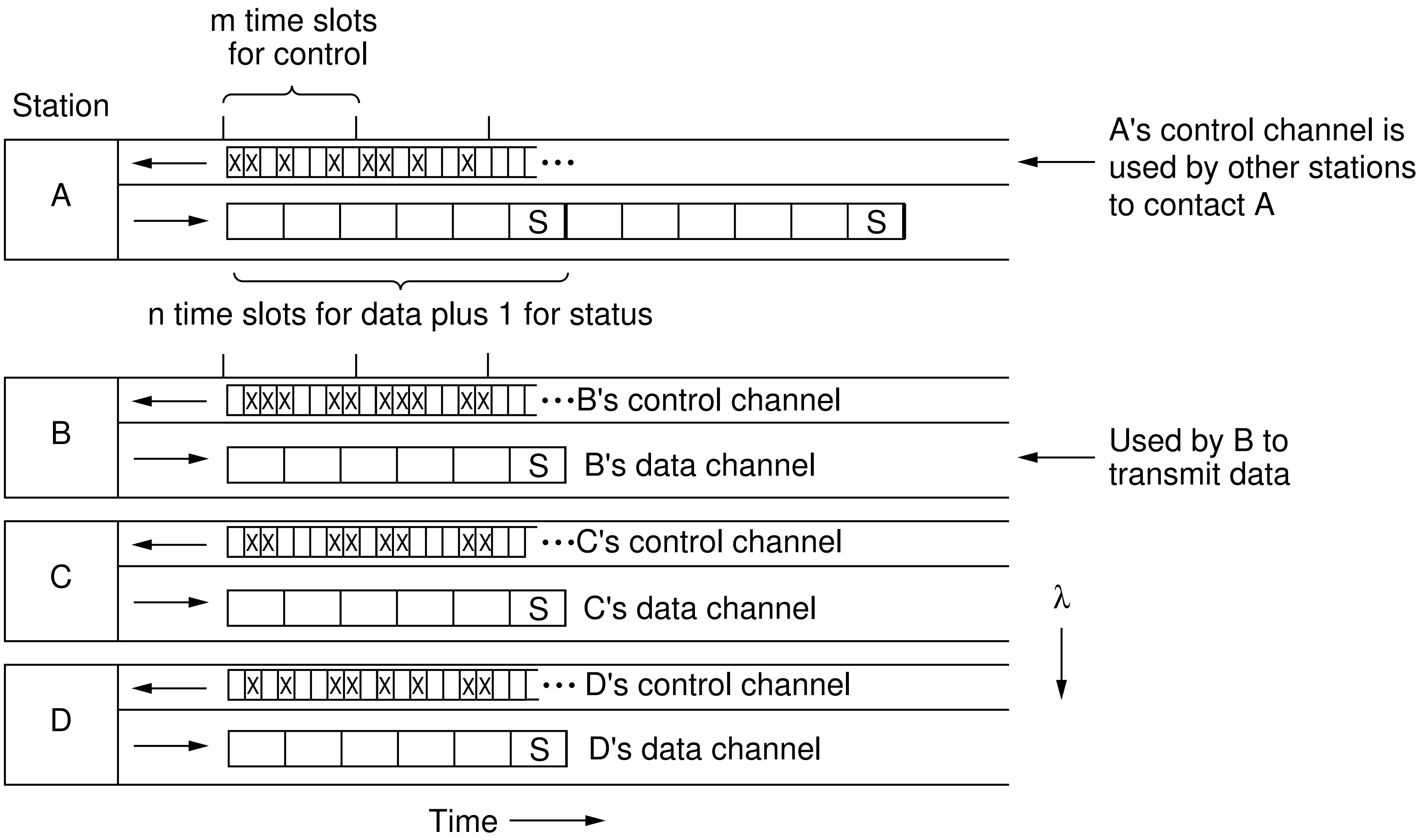
Wavelength Division Multiple Access
Multiplexage de fréquence dans la transmission par fibre optique

Chaque station possède
– un canal de contrôle (faible bande passante) qu'elle écoute.
– un canal de données (large bande passante) sur lequel elle envoie ses trames.

Tout le monde peut envoyer sur tous les canaux de contrôle, et écouter tous les canaux de données.

Les canaux sont coupés en créneaux.

Protocoles WDMA (2)



Protocoles WDMA (3)

Quand A veut envoyer à B (une seule trame, ou établir une connexion) :

– A écoute le canal de données de B et attend la trame *status* qui lui indique quels sont les créneaux disponibles dans le canal de contrôle de B.
– A choisit un créneau n disponible sur le canal de contrôle de B et envoie une demande de connexion (collision possible)
– B confirme dans la trame *status* que A a la main sur le créneau n de son canal de contrôle à B

Protocoles de WDMA (4)

- A envoie dans le créneau n du canal de contrôle de B : « je t'envoie une trame de contrôle dans le créneau m » (conflit possible)
- B écoute le canal de données de A et récupère la trame dans le créneau m

Aussi pour établir des connexions de longue durée.

Variantes possibles.

Protocoles LAN sans fil (1)

Problème : pas d'écoute (fiable) de porteuse.

- Problème de la station cachée : L'émetteur A ne se rend pas compte d'une collision chez le récepteur B qui est aussi dans la portée d'une tierce station C.
- Problème de la station exposée : L'émetteur A entend une station B et pense qu'il n'a pas le droit d'émettre pour B qui est portant hors de la portée de C

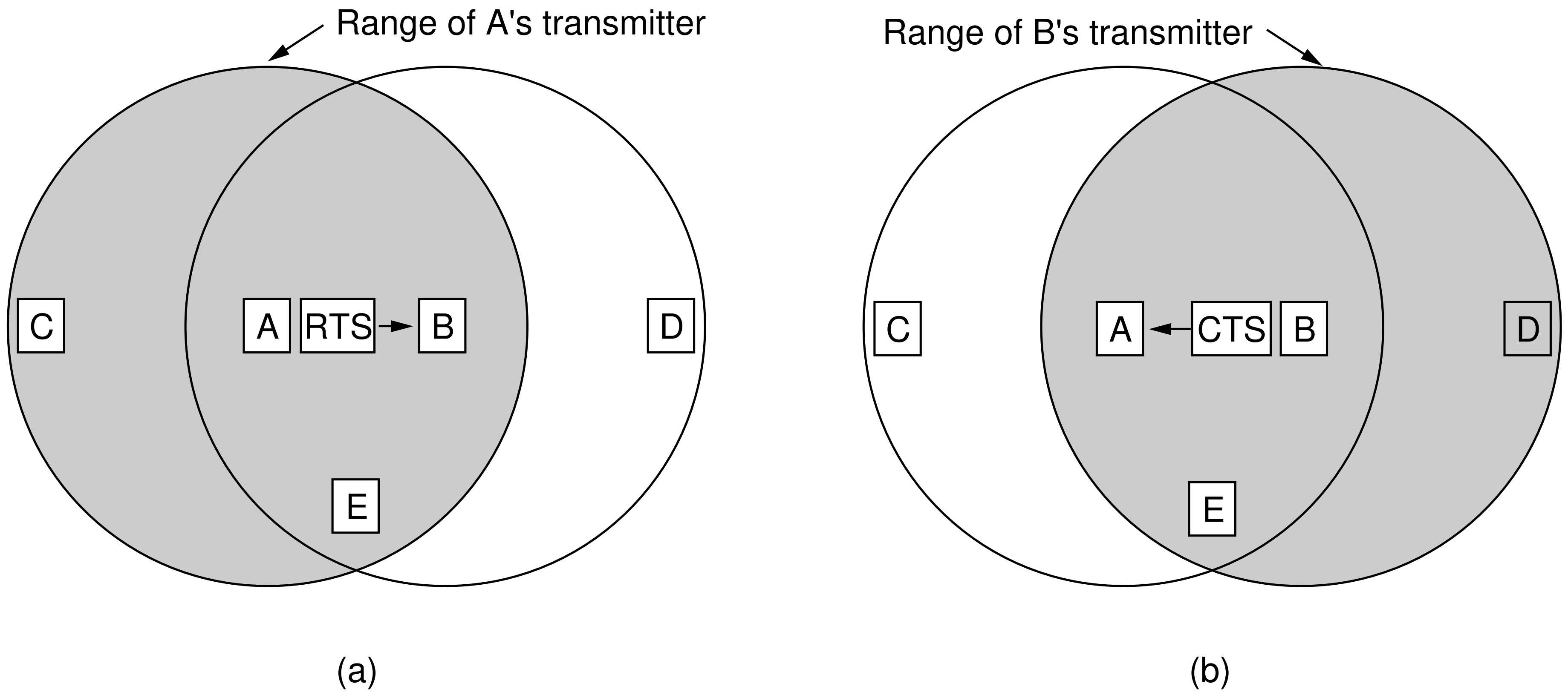
Protocoles LAN sans fil (2)

Racine du problème : Seulement les collisions côté récepteur sont importantes, mais l'émetteur ne connaît que les collisions de son côté.

Solution : MACA (Multiple Access with Collision Avoidance) :

- Émetteur envoie un signal RTS (request to send), contient la longueur de la trame.
- Récepteur renvoie un signal CTS (clear to send), aussi avec la longueur de la trame.

Protocoles LAN sans fil (3)



Les collisions sont toujours possible.

Ethernet (1)

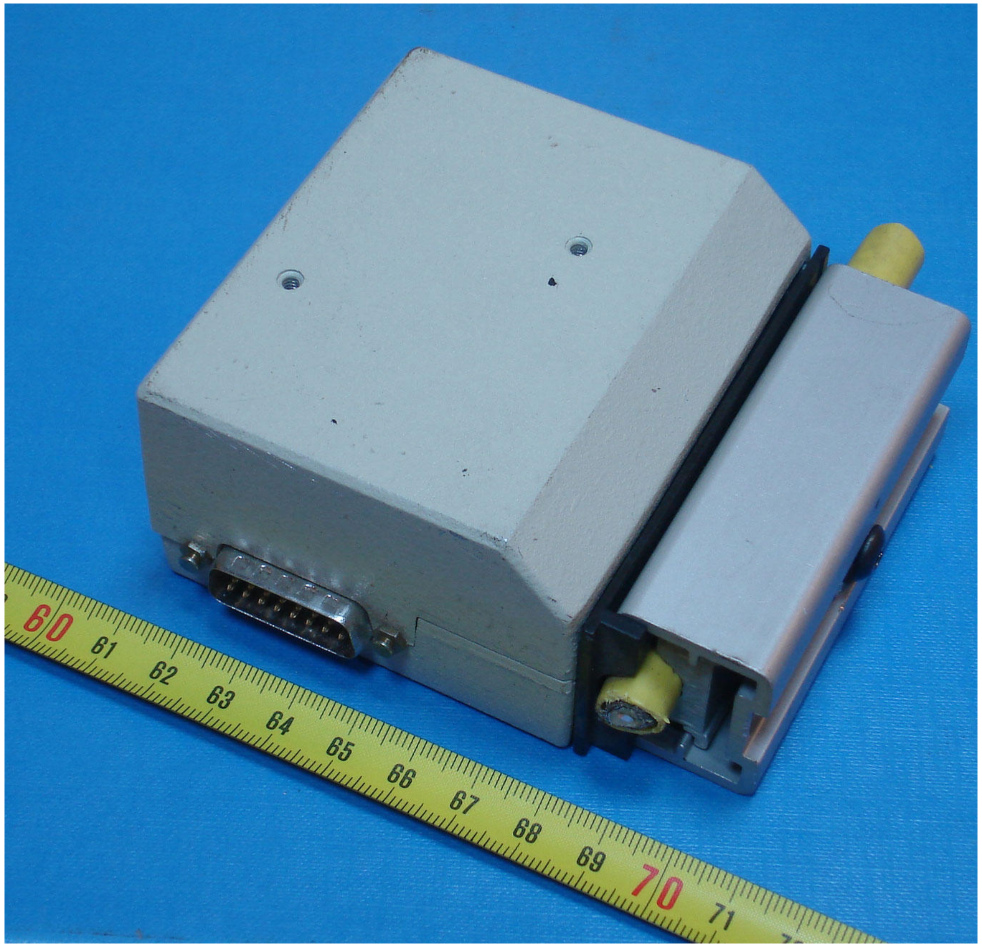
- Robert Metcalfe, 1978, XEROX Parc
- basé sur le modèle ALOHA
- aujourd'hui utilisé dans la grande majorité des LANs (cuivre ou fibre optique)
- classiquement 10Mb/sec

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

- *Fast Ethernet* (1995) : 100Mb/sec
- *Gigabit Ethernet* (1998) : 1Gb/sec

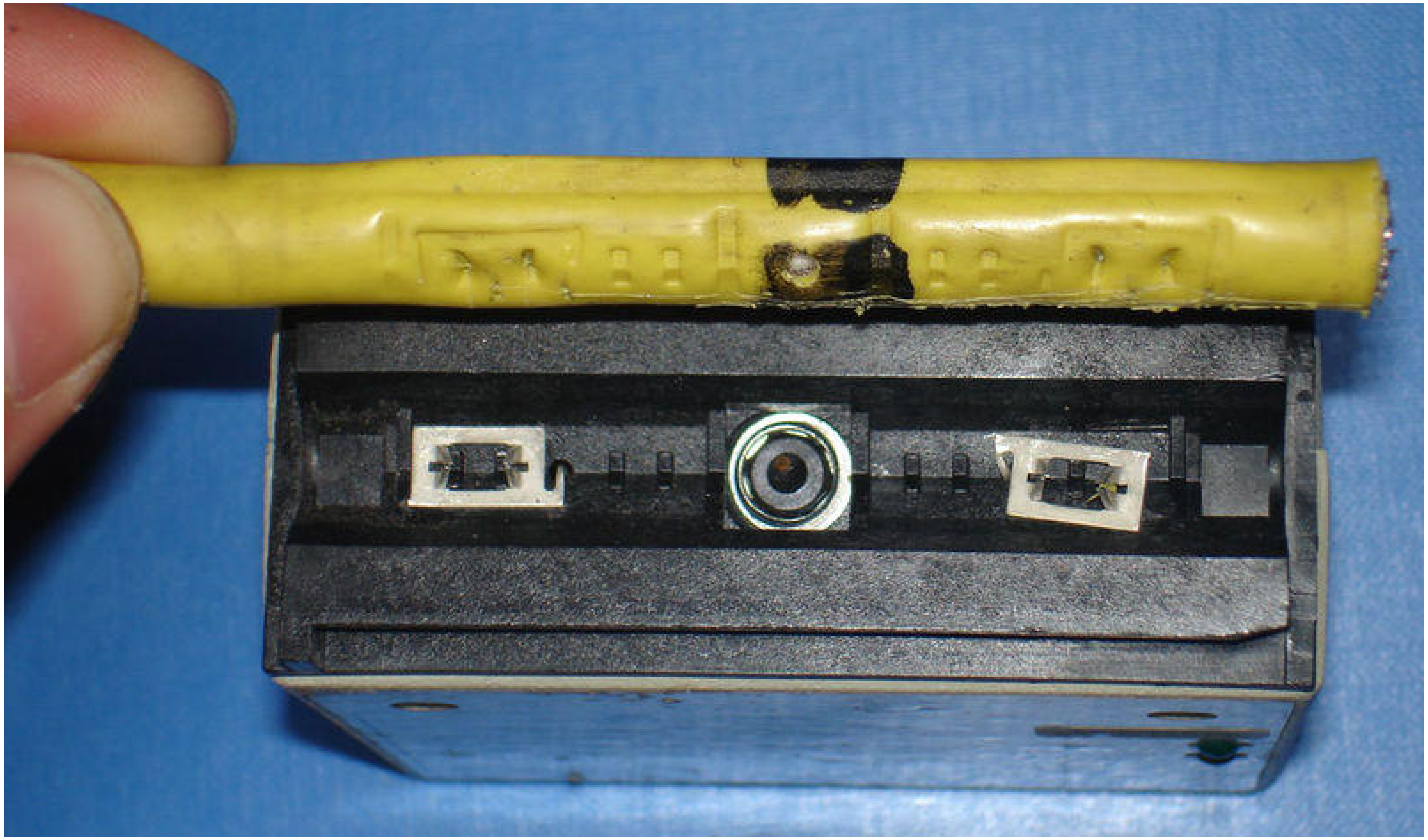
Ethernet (2)

Thick Ethernet (10Base5) avec transceiver

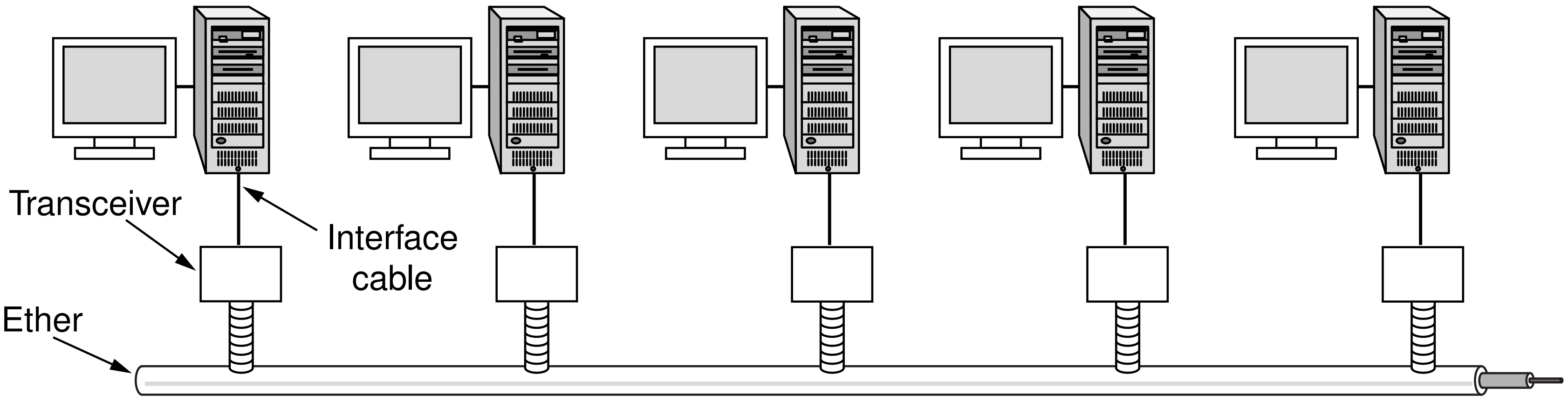


Ethernet (2.1)

Une *prise vampire* (vampire tap) :



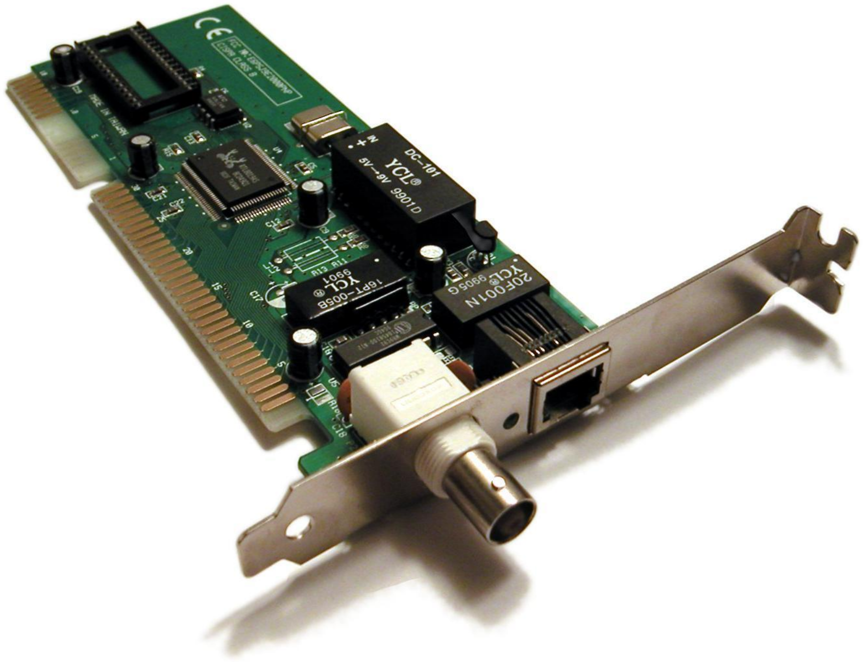
Ethernet (3)



– Transceiver : détection de collision
– Contrôleur : création et réception de trames

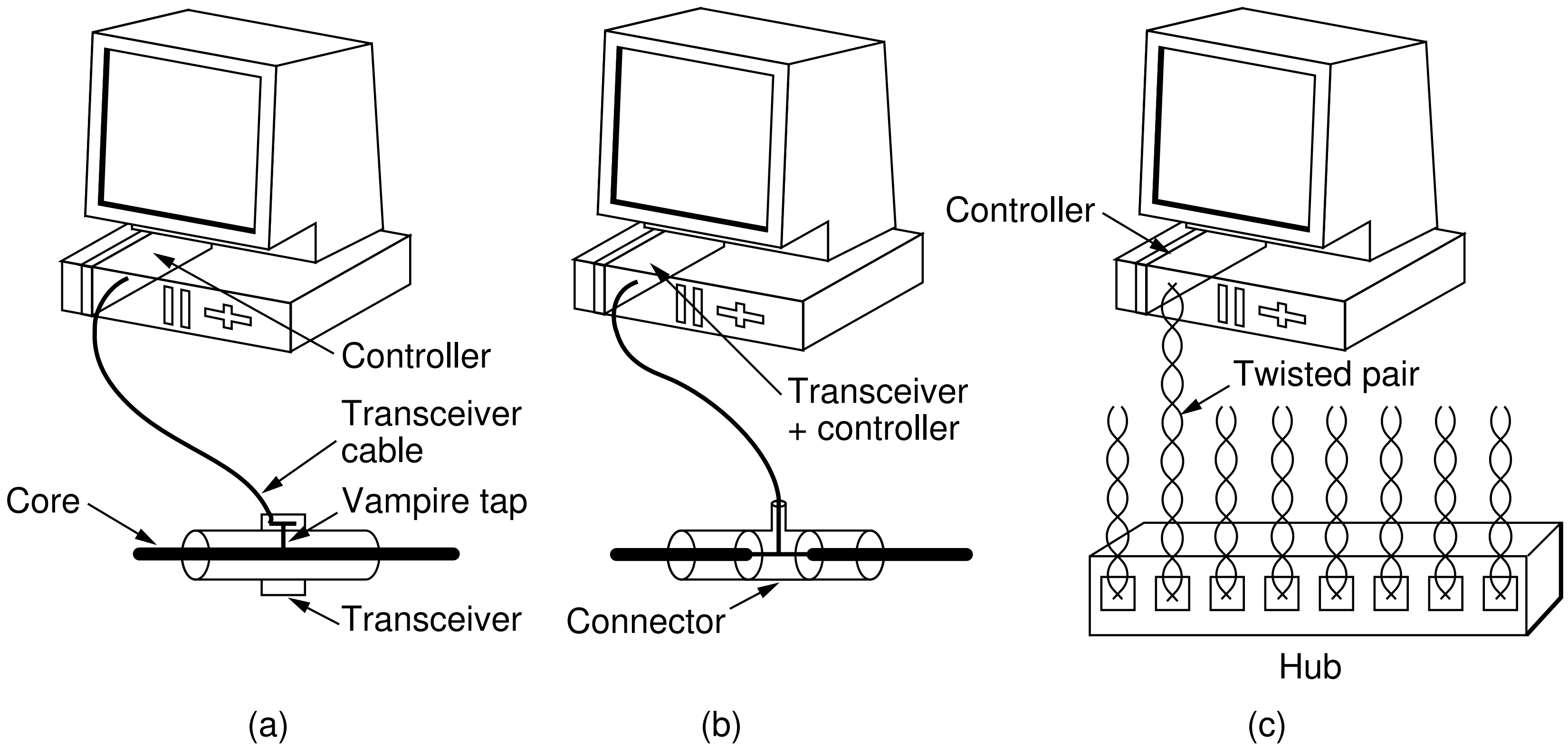
Ethernet (4)

Thin Ethernet (10Base2) : Transceiver intégré sur la carte réseau.



Ethernet (5)

Types de câblage Ethernet :



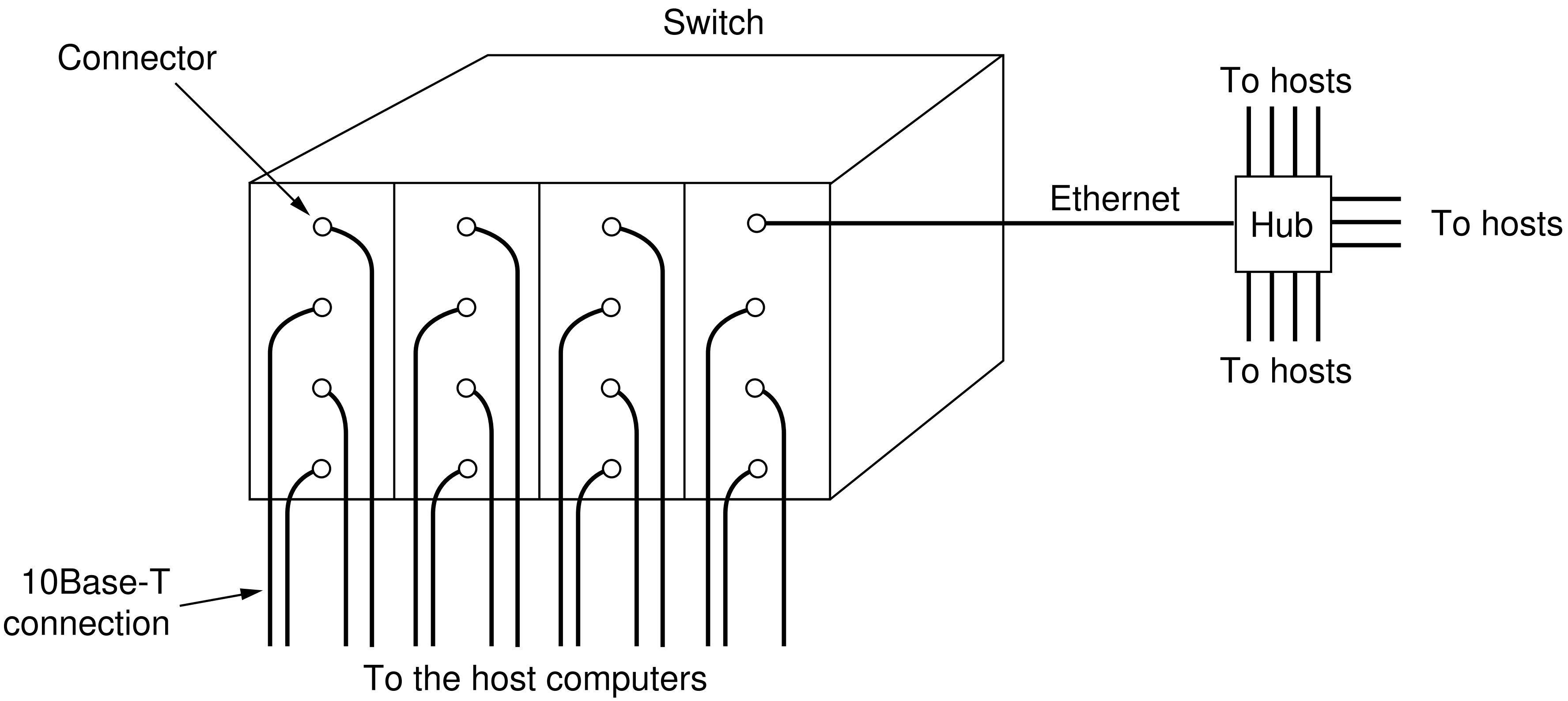
Ethernet (6)

– Répéteur (repeter) : amplificateur de signaux (couche 1)
  Si collision sur un côté envoie un bruit (jam signal) sur l'autre côté.
– Hub : renvoie toutes les trames sur toutes les connecteurs (couche 1)
  Les stations restent responsable de la gestion des collisions.
– Commutateur (switch), ou pont (bridge) : connaît les adresses des machines sur chacun de ses connecteurs, renvoie une trame seulement sur le connecteur ou est le destinataire (couche 2).

Ethernet (7)

Un hub avec 4 connecteurs :

Ethernet (8)



Switch
Connector
To hosts
Ethernet
Hub
To hosts
To hosts
10Base-T
connection
To the host computers

Ethernet (9)

Comportement en cas de collision : *binary exponential backoff*

- en cas de collision : attendre un temps aléatoire entre 0 et t.
- en cas de nouvelle collision : pareil, mais $t := 2 * t$
- après 10 collisions : t plafonné à $2^{10} * t_0$
- après 16 collisions : échec

Ethernet (10)

L'essentiel de la structure d'une trame Ethernet :

- Adresse destination (6 octets). Aussi : adresses de groupes, et *multicast*.
- Adresse de l'émetteur.
- Type (du protocole de la couche réseau).
- Données ($\leq$ 1500 octets)
- Remplissage (pour atteindre une longueur minimale)
- Checksum (CRC)

Les adresses sont globalement uniques (gérées par IEEE)

Des LANs commutés

Raisons pour utiliser des commutateurs :

– répartition de la charge
– connexion de LANs de technologie différente (Ethernet et WiFi)
– limitation de longueur dans un LAN
– isolation des nœuds défectueuses
– sécurité

Configuration des commutateurs

Apprentissage a posteriori (backward learning)

– le commutateur maintient une liste indiquant quelle station est accessible sur quel connecteurs

– si une trame arrive avec destinataire inconnu $\Rightarrow$ envoyer sur tous les connecteurs (sauf la source)

– si une trame arrive où émetteur et destinataire sur le même connecteur $\Rightarrow$ rejeter

– sinon $\Rightarrow$ envoyer sur le connecteur où est le destinataire

– balayer régulièrement les anciennes entrées

Configuration des commutateurs

Problème : éviter des boucles
⇒ algorithme distribué pour calculer un *arbre recouvrant* (spanning tree) par Radia Perlman (voir TP).