Réseaux locaux

Pierre David
pda@unistra.fr

Université de Strasbourg – Master CSMI

2023 – 2024

Plan

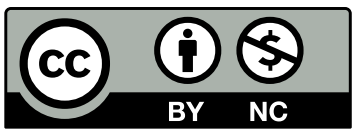
Aloha

CSMA

CSMA/CD et Ethernet

CSMA/CA et WiFi

Licence d'utilisation



Couches 1 et 2

Problèmes :

- comment partager un médium unique ?
- comment coder l'information ?
- comment adresser un message à un destinataire ?

Technologies :

- Token Ring
- Token Bus
- Ethernet
- WiFi

Plan

Aloha

Contexte

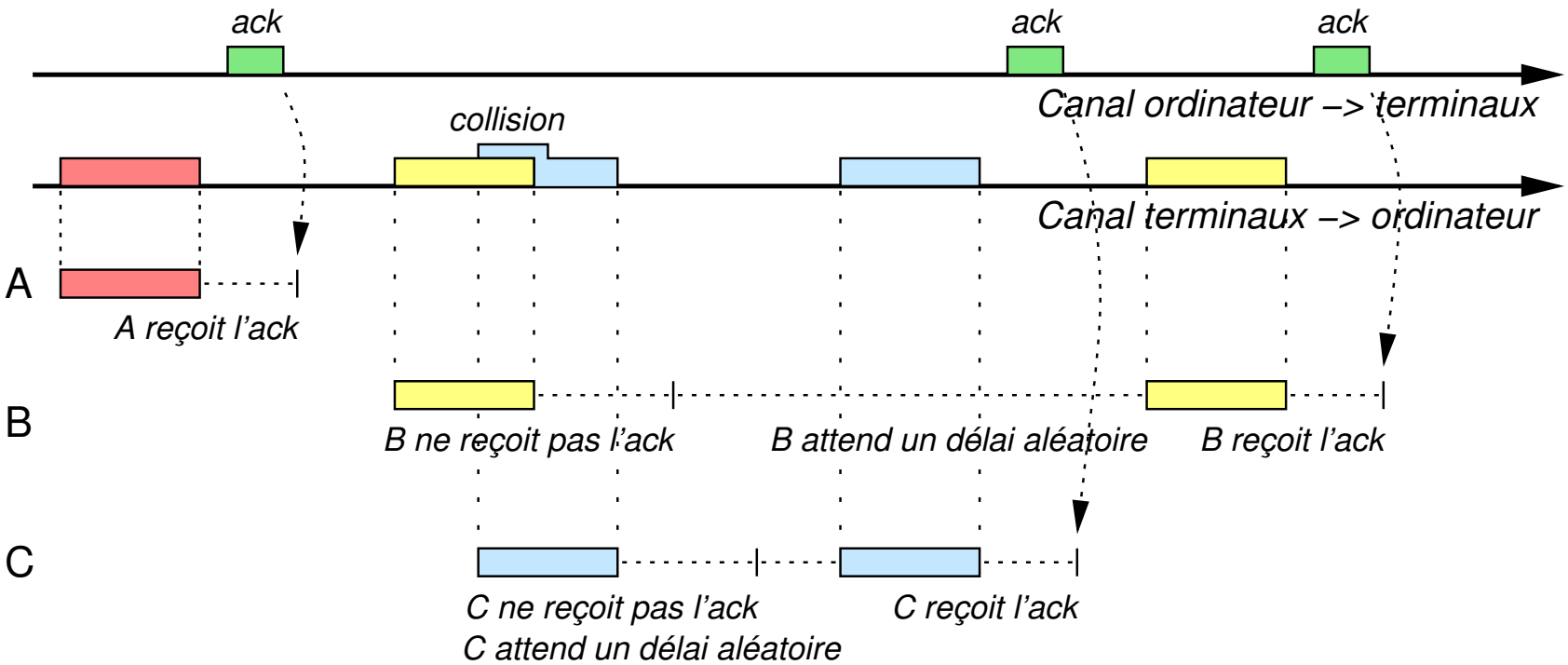
- 1969
- Université d'Hawai – Norman Abramson
- Aloha = Bonjour
- Réseau en étoile
  - ordinateur central à Honolulu
  - terminaux dans les îles
- pas de câbles $\Rightarrow$ transmission radio (100 km)
- un canal pour les communications terminaux $\rightarrow$ ordinateur
  canal partagé $\Rightarrow$ collisions
- un canal pour les communications ordinateur $\rightarrow$ terminaux
  un seul émetteur possible $\Rightarrow$ pas de collision

Aloha pur

Algorithme des terminaux :

1. s'il y a des données à émettre, les émettre
2. si acquittement de l'ordinateur, alors ok
3. si pas d'acquittement reçu dans un délai court
   - 3.1 attendre un délai aléatoire
   - 3.2 goto 1

Aloha pur



Performances : utilisation maximum du médium = 18 %

Aloha discrétisé

Meilleure utilisation du canal : Slotted Aloha (ou Aloha discrétisé)

1. 1972
2. temps découpés en slots
   $\Rightarrow$ référence temporelle (ex : signal de synchronisation)
3. émission en début de slot
4. moins de collisions : utilisation du medium à 36 %

Plan

CSMA

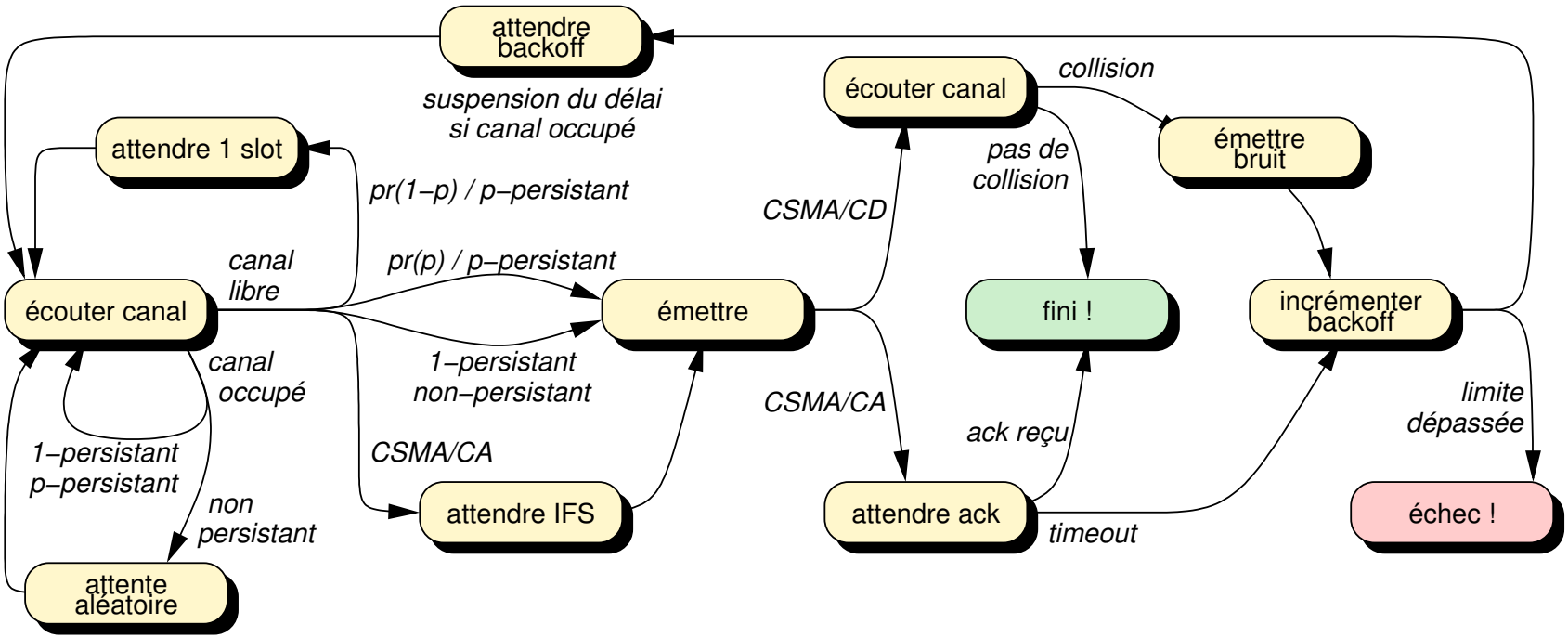
- CSMA : Carrier Sense Multiple Access
- une station écoute le canal **avant** d'émettre

CSMA

Si la porteuse est actuellement occupée, la station souhaitant émettre :

- CSMA non persistant :
  - attend une durée aléatoire
- CSMA 1-persistant :
  - émet dès la fin de l'émission en cours
- CSMA *p*-persistant :
  - émet avec une probabilité *p* à la fin de l'émission en cours (sinon attend le début du slot suivant)
  - uniquement pour les canaux découpés en slots

CSMA


attendre backoff
suspension du délai si canal occupé
attendre 1 slot
pr(1−p) / p−persistant
écouter canal
canal libre
pr(p) / p−persistant
émettre
CSMA/CD
écouter canal
collision
émettre bruit
pas de collision
fini !
incrémenter backoff
limite dépassée
canal occupé
1−persistant non−persistant
CSMA/CA
CSMA/CA
ack reçu
1−persistant p−persistant
non persistant
attendre IFS
attendre ack
timeout
échec !
attente aléatoire

Plan

CSMA/CD

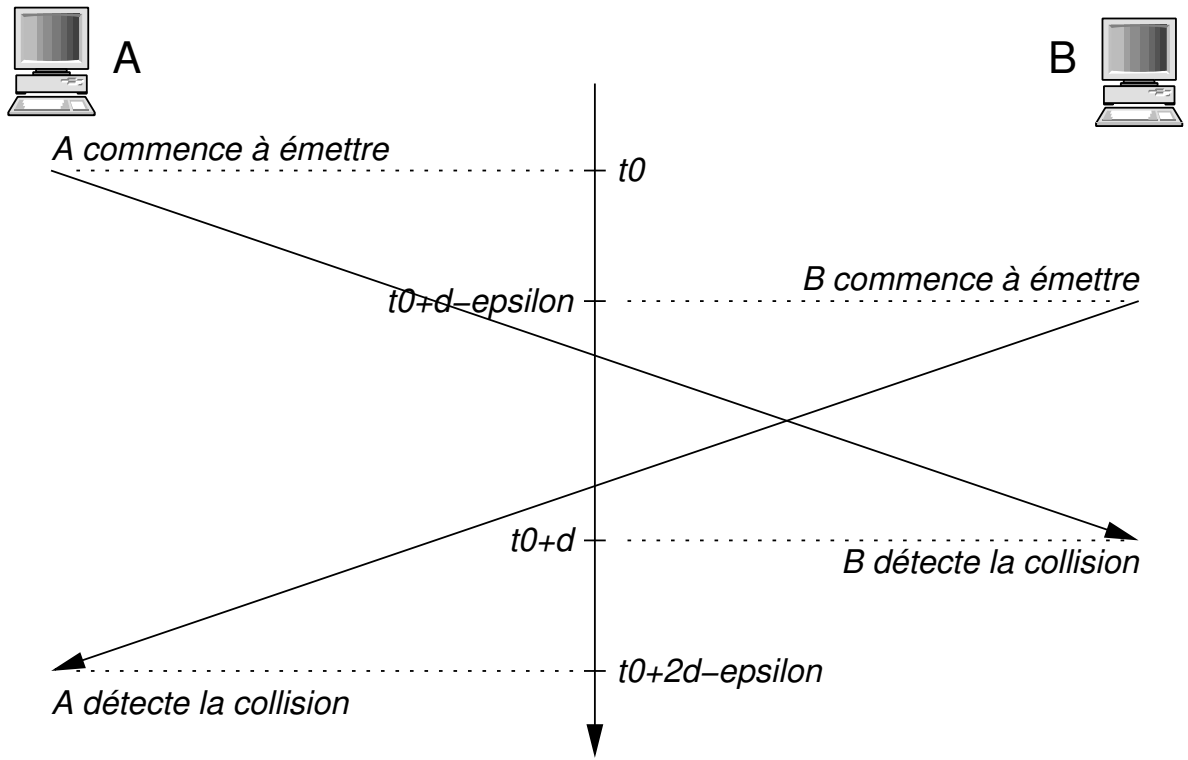
CD = Collision detection

1. si trafic en cours, attente d'un délai aléatoire
   (Ethernet : aléa $\in [1..16]$ slots)
2. si pas de trafic, alors émission
3. si écoute pendant l'émission indique une collision alors arrêt immédiat, attente aléatoire et goto 1
   (Ethernet : émission d'un signal de brouillage de 48 bits pour signaler la collision aux autres stations)
4. abandon au bout d'un certain nombre d'échecs

CSMA/CD

Influence de la bande passante et du délai de transmission

Soit *d* le délai de transmission entre les deux stations les plus éloignées (i.e. longueur maximum du câble)



Une station doit attendre 2*d* après la fin de l'émission pour être sure qu'un message a pu être transmis sans collision

Ethernet – Historique

1973	Xerox PARC, Bob Metcalfe, 3 Mb/s
1979	alliance DEC, Intel et Xerox
1982	10 Mb/s
1983	norme IEEE 802.3 (10Base-5)
1985	norme 10Base-2
1990	norme 10Base-T (RJ-45)
1995	Fast Ethernet (100Base-TX)
1998	Ethernet 1 Gb/s
2002	Ethernet 10 Gb/s
2010	Ethernet 40 et 100 Gb/s

Bob Metcalfe expliquant Ethernet :

`https://www.youtube.com/watch?v=Fj7r3vYAjGY`

Support physique – 10Base-5

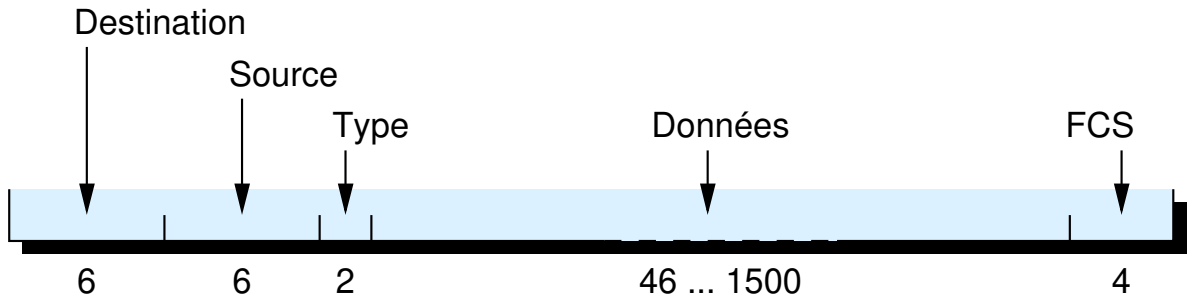
- 10 Mb/s (version originale en 1973 : 3 Mb/s)
- câble coaxial (jaune) $\Rightarrow$ *ThickNet*
- connexion de segments via des répéteurs
  - maximum 500 m par segment
  - maximum 4 répéteurs
    ($\Rightarrow$ distance max entre deux stations = 2500 m)
  - maximum 3 segments avec des stations
    ($\Rightarrow$ 2 segments pour prolonger le réseau)
  - maximum 100 stations par segment
- résistances terminales de 50 Ω pour absorber le signal
- repères tous les 2,5 m (distance choisie pour ne pas correspondre à la longueur d'onde)
- transceivers, prises vampire

Support physique – 10Base-2

- 10 Mb/s
- câble coaxial (noir) $\Rightarrow$ *ThinNet*
- prises BNC en T (attention à l'insertion ou au retrait)
- bouchons = résistances terminales de 50 Ω
- distance max d'un segment = 185 m
- 30 stations maximum par segment
- mêmes règles que 10Base-5 pour les répéteurs
  $\Rightarrow$ distance max = 925 m (= 5 $\times$ 185 m)

Ethernet – En-tête

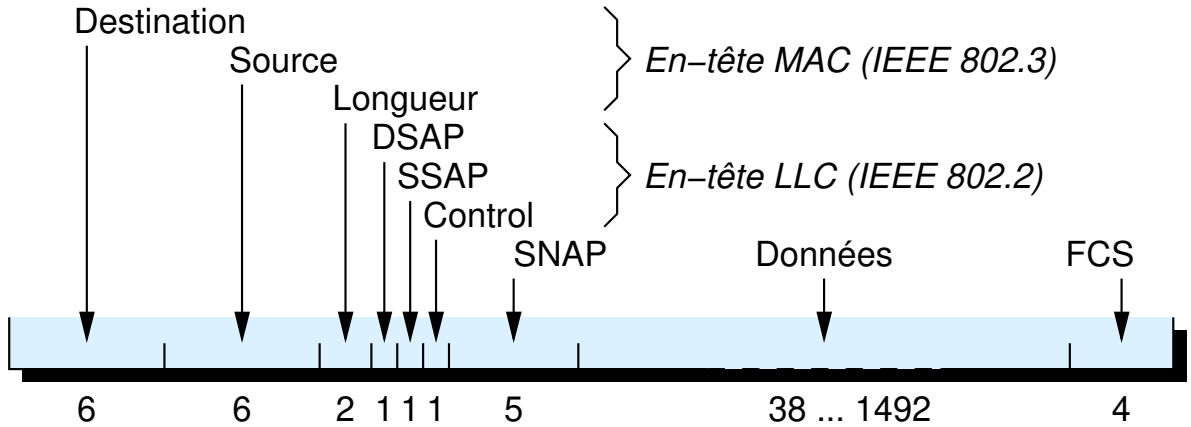
Format Ethernet II (ou Ethernet DIX) :



- Type : alloué par l'IEEE
- FCS : Frame Check Sequence (= Cyclic Redundancy Check)

Ethernet – En-tête

Format Ethernet IEEE 802.3 :



- DSAP/SSAP : Destination/Source Service Access Point
- Control : type de trame LLC
- SNAP : Sub-Network Access Protocol

Ethernet – En-tête

Deux formats différents pour Ethernet ?

- Ethernet 802.3 presque jamais utilisé en pratique
- Comment distinguer ?
  - Ethernet II si Type > 1500
  - Ethernet 802.3 si Longueur $\leq$ 1500

  $\Rightarrow$ suppose que l'IEEE n'attribue pas de type $\leq$ 1500 (vrai)

Ethernet

Préambule :

- avant la trame elle-même
- 7 octets à 01010101
- 1 octet à 01010111 (Start frame delimiter)
- synchronisation des stations

Inter Frame Gap :

- préparer la réception de la trame suivante
- 9,6 μs (i.e. 12 octets à 10 Mb/s)
- 0,96 μs (i.e. 12 octets à 100 Mb/s)
- etc.

Ethernet – Longueur de trame

Longueur maximum : limitée arbitrairement à 1500 octets

- trame longue $\Rightarrow$ délai d'attente pour les autres stations
- trame longue $\Rightarrow$ probabilité de corruption d'un bit
- trame longue $\Rightarrow$ mémoire dans la carte réseau
  $\Rightarrow$ raison réelle de la limitation

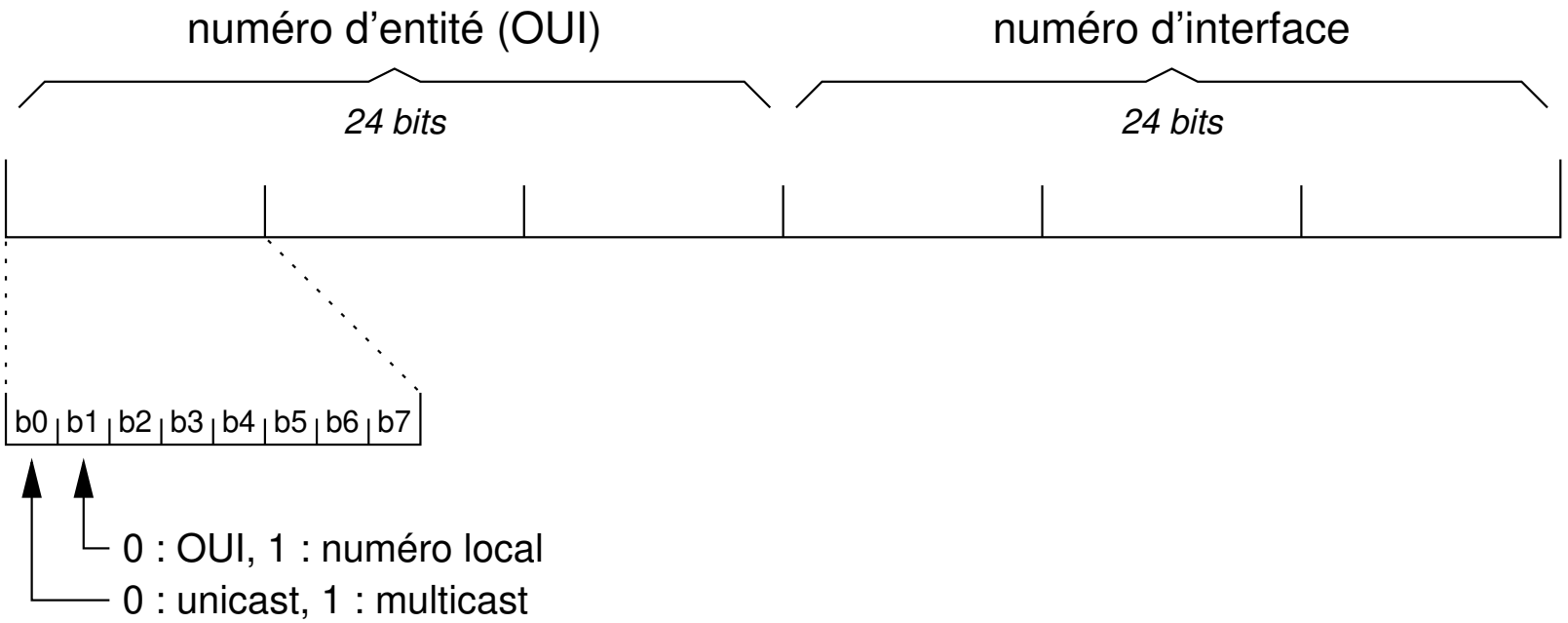
Ethernet – Longueur de trame

Longueur minimum = 46 octets, pour que les trames (hors préambule) fassent plus de 64 octets. Pourquoi ?

- la collision doit être détectée par l'émetteur, donc la collision doit arriver avant la fin de l'émission
- sur 2,5 km via 4 répéteurs, le signal met environ 51,2 μs pour faire un aller et retour d'un bout à l'autre
- à 10 Mb/s (10^7 b/s), un bit est émis en 10^{-7} s = 0,1 μs
- l'émetteur doit donc envoyer au minimum 51,2 / 0,1 = 512 bits = 64 octets pour émettre pendant 51,2 μs

Si moins de 46 octets de données : bourrage

Ethernet – Adresses



OUI = Organizationally Unique Identifier

`http://standards-oui.ieee.org/oui/oui.txt`

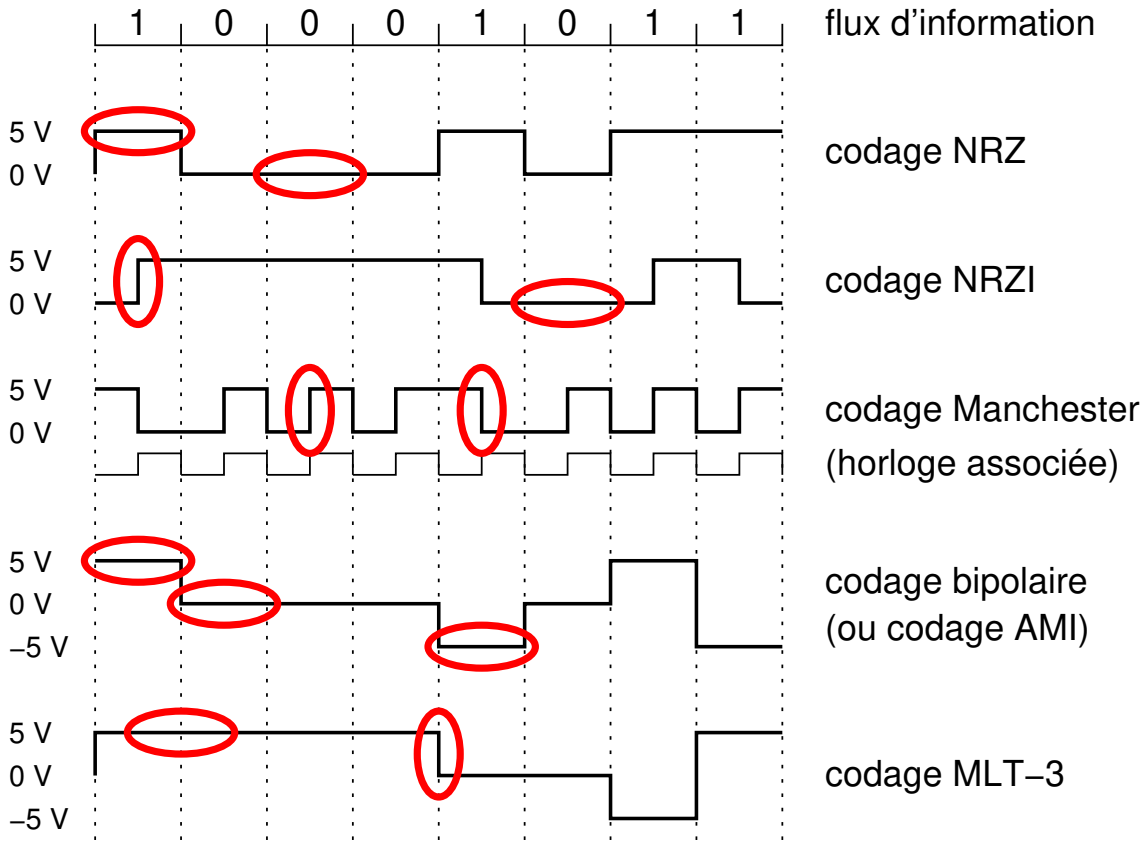
Ethernet – Adresses

- premier bit = 0 : adresse ordinaire
  - 3 octets = OUI = numéro d'entité (ex: fabricant de cartes Ethernet), alloué par l'IEEE
  - 3 octets = alloués par le fabricant

  $\Rightarrow$ adresse d'interface Ethernet **unique**
- premier bit = 1 : adresse de groupe
  - cas particulier : tous les bits à 1 = adresse de **diffusion générale** (ou *broadcast*)
  - $2^{24} - 1$ autres cas : adresse **diffusion restreinte** (ou *multicast*)

Ethernet – Codage

Ethernet classique utilise le codage Manchester :



Envoi du préambule = signal de 10 MHz pendant 6,4 μs

$\Rightarrow$ synchronisation de l'horloge du destinataire

Ethernet – Retransmissions

En cas de collision :

- la station qui détecte la collision envoie un signal de brouillage (48 bits) pour avertir les autres stations
- retransmission : modèle CSMA 1-persistant avec attente aléatoire exponentielle :
  - le temps est divisé en slots de taille 51,2 μs (aller-et-retour sur le chemin le plus long)
  - après la i^e collision, une station doit attendre un nombre aléatoire de slots $\in [0, 2^i - 1]$
  - lorsque $i > 10$, le nombre de slots maximum est plafonné à $2^{10} - 1 = 1023$
  - lorsque $i > 16$, l'émission est abandonnée

$\Rightarrow$ délai total borné à $\sum_{i=1}^{10}(2^i - 1) + 6(2^{10} - 1) =$
$2^{11} + 6 \times 2^{10} - 17 = 8175$ slots de 51,2 μs $\simeq$ 0,4 s

Avantages et inconvénients d'Ethernet

Avantages :

- simple
- pas de configuration
- robuste (aux interférences)

Inconvénients :

- les collisions augmentent avec la charge
- envoi non déterministe (possibilité de famine)
- pas de priorité (toutes les stations sont égales)
- taille minimum = 64 octets (overhead)

Support physique – 10Base-T

- 10 Mb/s
- câble point à point $\Rightarrow$ topologie en étoile
- paire torsadée non blindée, catégorie 3
- connecteur RJ-45
- connexion via des concentrateurs (*hubs*) Ethernet
- distance max = 100 m (90 m + 10 m de jarretières)

Variante 10Base-F : utilisation de la fibre optique

Support physique – Câbles

Paire torsadée : deux fils enroulés en hélice l'un autour de l'autre

- distance constante entre les fils
- diminue la diaphonie (interférence entre les fils)

Câbles multi-paires (couramment 4 paires).

Blindage de métal entre paires, ou autour du câble :

Nom	Blindage entre paires	Blindage entre paires et câble
UTP	non	non
STP	oui	non

U = Unshielded, S = Shielded, TP = Twisted Pair
Note : il existe d'autres types de câbles.

Support physique – Câbles

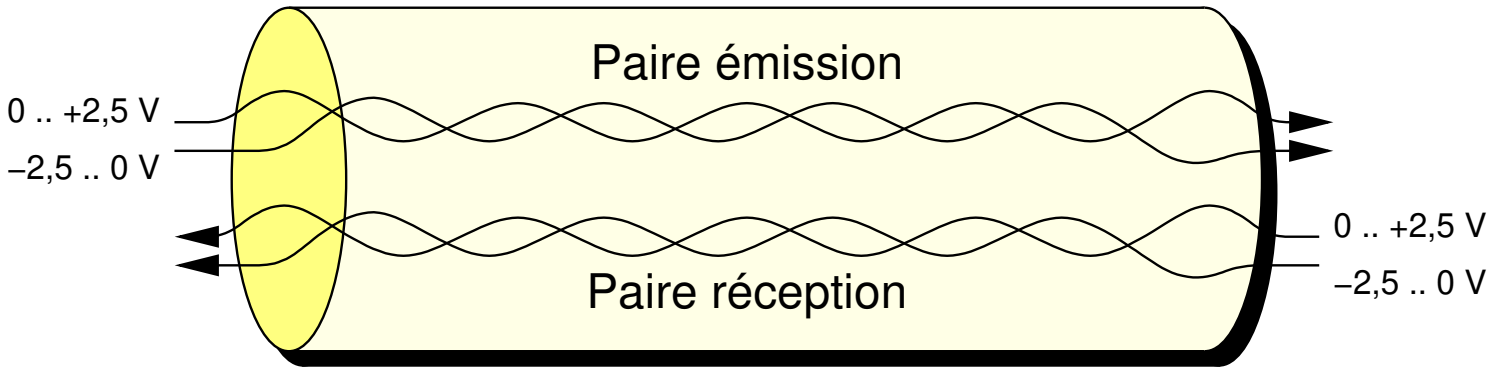
Catégorie :

- Catégorie 3 (basé sur UTP) : téléphone, 10Base-T, 100Base-T4, etc.
- Catégorie 5 (basé sur UTP) : 100Base-TX, 1000Base-T, (très courant)
- Catégorie 5e (basé sur UTP) : idem Cat5, avec tests de certification plus sévères
- Catégorie 6 (basé sur UTP) : 10GBase-T
- Classe F (appelé aussi Catégorie 7), basé sur SFTP : 1000Base-TX

SFTP = câble écranté

Support physique – Câbles

Avec Ethernet 10Base-T :



Croisement des paires émission/réception :

- hub $\leftrightarrow$ station : pas de croisement
- station $\leftrightarrow$ station ou hub $\leftrightarrow$ hub : croisement nécessaire

Support physique – Concentrateur

Un concentrateur (*hub*) :

- retransmet une trame reçue, sans la stocker, sur tous les autres ports
  $\Rightarrow$ fonctionne en *half-duplex*
- reconnaît les préambules et détecte les collisions
- diffuse le signal de brouillage en cas de collision

Mais :

- impact sur la sécurité : espionnage du trafic
- autrefois très utilisé (prix)
- aujourd'hui abandonné au profit des commutateurs

FastEthernet (100Base-TX)

- 100 Mb/s
- utilisation de commutateurs
- support = câble catégorie 5, avec utilisation de 2 paires :
  - une paire commutateur $\rightarrow$ station
  - une paire station $\rightarrow$ commutateur

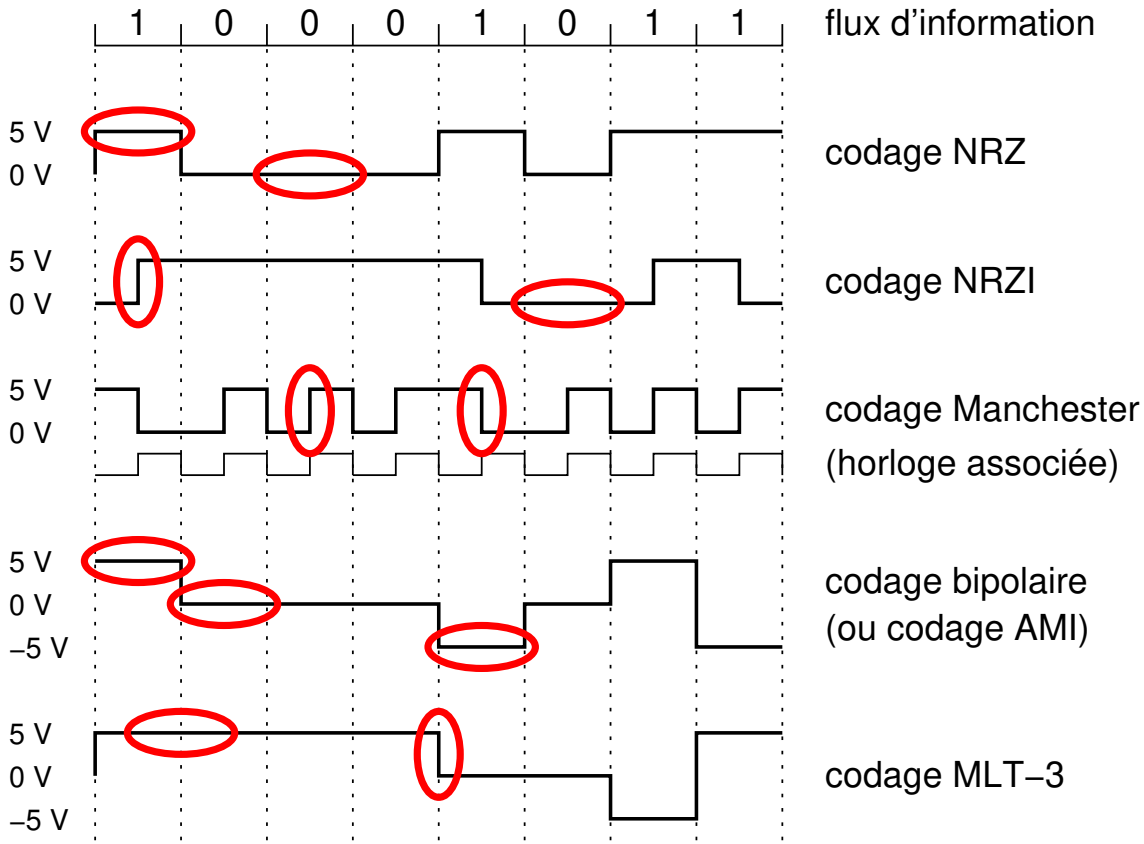
  $\Rightarrow$ liaison full-duplex

100Base-FX : deux paires de fibres multimodes (full duplex, max 2 km)

Support physique – Codage 4B/5B

Problème du codage Manchester : nécessite 100 % de bande passante supplémentaire

100Base-TX : codage 4B/5B avec NRZI



Support physique – Codage 4B/5B

Codage de 4 bits sur 5 : jamais plus de 3 bits consécutifs à 0
$\Rightarrow$ évite une désynchronisation d'horloge

$$0000 \rightarrow 11110$$
$$0001 \rightarrow 01001$$
$$0010 \rightarrow 10100$$
etc

4B5B entraîne un overhead de 25 % seulement (au lieu de 100 % avec Manchester)

FastEthernet – Compatibilité

Mixage avec stations ou hubs en 10Base-T

Autonégociation

GigabitEthernet

1000Base-T :

- 1 Gb/s
- 200 m
- support = câble catégorie 5e ou 6
- autonégociation
- configuration automatique de MDI/MDI-X (Medium Dependant Interface crossover)

Variantes sur fibre optique :

- 1000Base-SX : multimodes, max 550 m (sur 50 μm) ou 220 m (sur 62,5 μm)
- 1000Base-LX : monomode, max 5 km (moins sur multimodes)
- 1000Base-LX10 (1000Base-LH) : monomode, max 10 km
- autres versions non standard (1000Base-EX, 1000Base-ZX, etc.)

GigabitEthernet

Compatibilité avec les hubs :

- CSMA/CD
- 1 Gb/s $\Rightarrow$ une trame de 64 octets est envoyée en 0,512 μs
  $\Rightarrow$ trop rapide pour détecter une collision

D'où :

- longueur minimum de trame = 512 octets
  $\Rightarrow$ bourrage par le matériel (sans intervention du logiciel)
- mode « rafale » pour l'émission de plusieurs petites trames en une seule

GigabitEthernet

Extensions (non standards) :

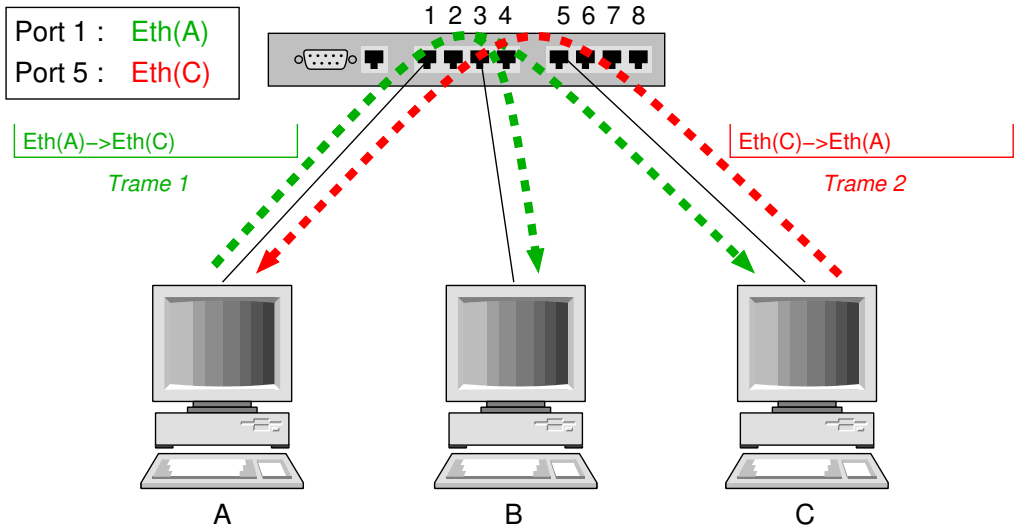
- contrôle de flux (1 Gb/s $\Rightarrow$ 1 bit/ns)
  Trame « pause » : attendre n trames de 512 ns avant d'envoyer une nouvelle trame ($n < 2^{16} - 1$)
- Jumbo frames
  Longueur de trame jusqu'à 9000 octets.

10 Gigabit Ethernet

- jusqu'à 100 m en cuivre (Catégorie 6a)
- jusqu'à 40 km en fibre optique monomode
- plus de support de CSMA/CD (pas de compatibilité avec les hubs)

Commutation

Commutateur = ne transfère que les trames utiles

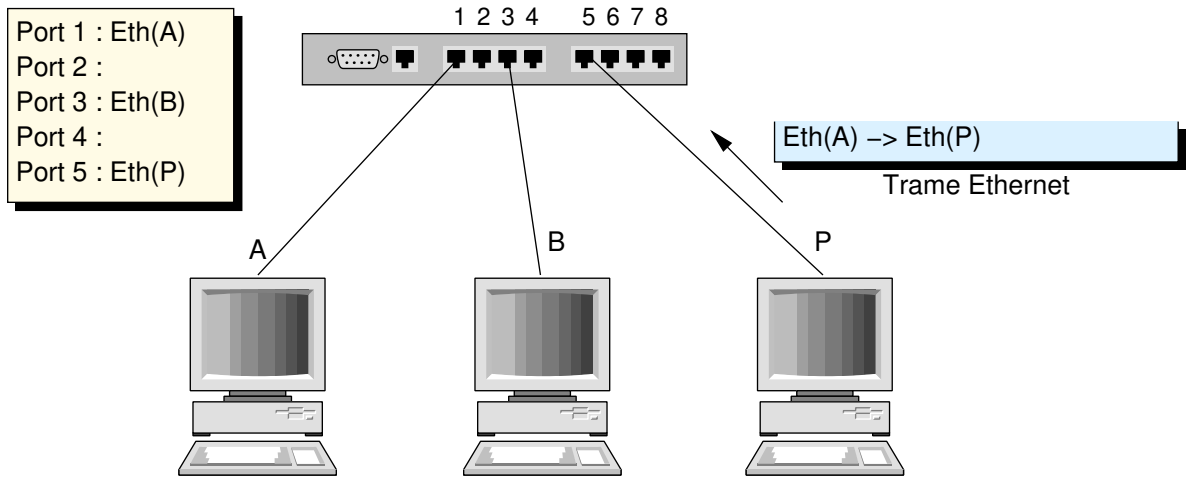


Apprentissage des adresses

- inondation initiale
- écoute de l'adresse source
- expiration des entrées
- commutateurs en cascade

Commutation

Problème de sécurité : *port stealing*



Le pirate émet une trame de niveau 2 contenant A comme adresse source, et sa propre adresse comme adresse de destination

$\Rightarrow$ le commutateur actualise sa table de *forwarding*

$\Rightarrow$ la trame n'est pas propagée $\Rightarrow$ la trame n'est pas détectable

$\Rightarrow$ le trafic à destination de A est capturé par P, et en silence !

Commutation

Une fois le port volé, il est possible de le rendre à A :

- le pirate envoie une requête ARP en demandant l'adresse de A
- la requête est diffusée, donc A répond
- la réponse de A provoque l'actualisation de la table de *forwarding* du commutateur

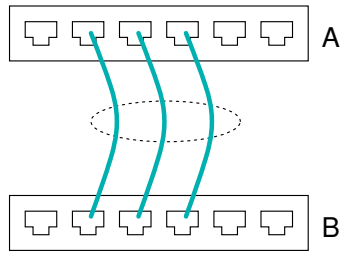
Exemple de protection : commande `switchport port-security` sur les commutateurs Cisco

- configuration statique d'une ou plusieurs adresses MAC
- apprentissage dynamique des adresss MAC, avec interdiction de changement de port

Aggrégation de liens – 802.3ad/802.1AX

Besoin d'aggréger des liens pour :

- augmenter la bande passante
- offrir de la redondance



$\Rightarrow$ aggrégation de liens opérant à la même vitesse

Protocoles :

- EtherChannel (Kalpana, racheté par Cisco) : PAgP (Port Aggregation Protocol) ou LACP
- 802.3ad : LACP (Link Aggregation Control Protocol)
  802.3ad $\rightarrow$ 802.1AX (i.e. indépendant d'Ethernet)

Aggrégation de liens – 802.3ad/802.1AX

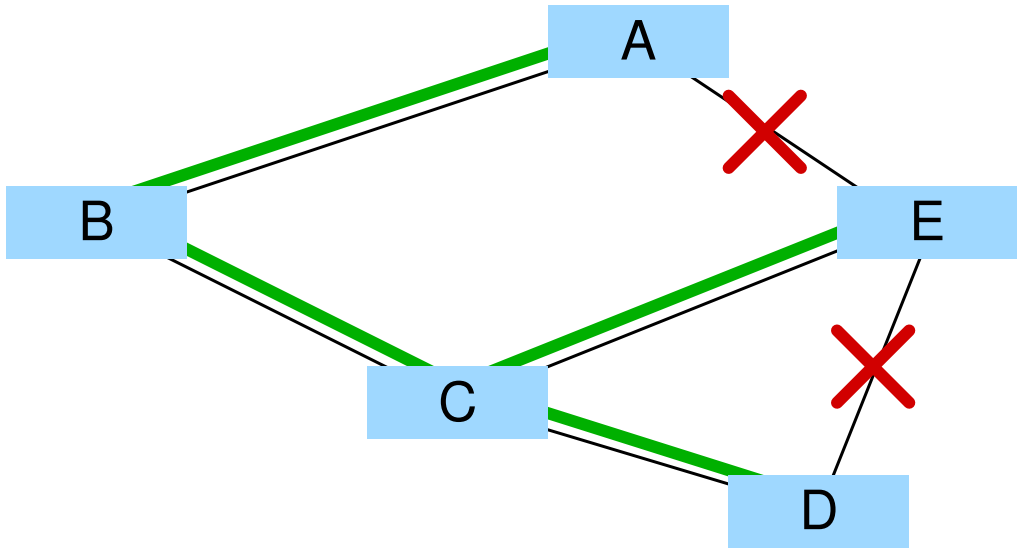
Fonctionnement :

- création d'un port « virtuel » pour l'aggrégation
  $\Rightarrow$ les ports physiques aggrégés ne sont plus utilisés dans les tables de commutation
- partage statique en fonction d'une table de hâchage
  (en fonction des adresses MAC, IP, numéros de ports, etc.)
  $\Rightarrow$ pas de stratégie dynamique de type « *round-robin* »
  $\Rightarrow$ pas de déséquencement des trames
- protocole (LACP) : maintient à jour la liste des ports physiques
  (après configuration initiale)

Spanning Tree – arbre recouvrant – 802.1D

Redondance de niveau 2 : utiliser un réseau maillé et transmettre les trames sans provoquer de boucle

⇒ Constitution d'un arbre recouvrant le graphe avec STP (Spanning Tree Protocol)



⇒ blocage de certains ports pour éviter les boucles

Spanning Tree – arbre recouvrant – 802.1D

Fonctionnement :

1. élection du commutateur racine : plus petite valeur de *bridge-id* = <priorité, adresse MAC>
   (prio = 0x8000, configurable)
2. chaque commutateur détermine le port racine (RP) : distance (coût) minimum vers le commutateur racine
3. sur chaque segment, élection du port désigné (DP) : le port du commutateur le plus direct vers la racine
4. tout autre port (non DP ou non RP) est bloqué

Spanning Tree – arbre recouvrant – 802.1D

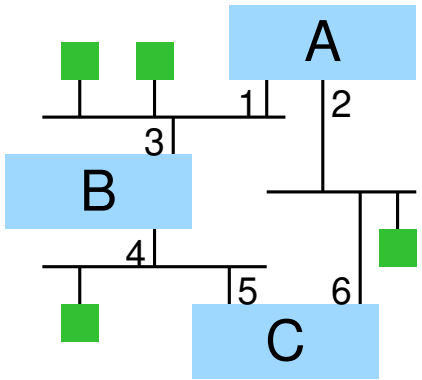
Paquets du protocole STP = Bridge Protocol Data Units :

- configuration : calcul de l'arbre
- notification de changement de topologie
- acquittement de changement de topologie

BPDU envoyés à l'adresse multicast 01:80:C2:00:00:00
$\Rightarrow$ seuls les ponts les reçoivent

Spanning Tree – arbre recouvrant – 802.1D

Fonctionnement :



étape	src	port dest	BPDU RB	BPDU dist	action
1	B	3	B	0	A ignore RB=B/0 via 1
		4	B	0	C apprend RB=B/0 via 5
2	C	6	B	1	A ignore RB=B/1 via 2
3	A	1	A	0	B apprend RB=A/0 via 3
		2	A	0	C apprend RB=A/0 via 6
4	B	4	A	1	C ignore RB=A/1 via 5
5	C	5	A	1	B ignore RB=A/1 via 3

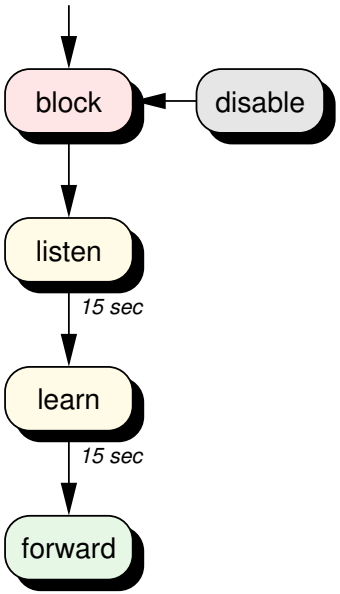
$\Rightarrow$ A est élu racine (*Root Bridge*) car il a le *bridge-id* le plus bas.

$\Rightarrow$ le port racine (*Root Port*) de B = 3, de C = 6

$\Rightarrow$ le port désigné (*Designated Port*) sur le segment AB est A1 (resp. B4 pour BC, resp. A2 pour AC)

$\Rightarrow$ le port C5 est bloqué

Spanning Tree – arbre recouvrant – 802.1D



États d'un port :

- Block : état initial, aucun trafic ne passe, seuls les BPDU sont écoutés
- Listen : état transitoire, seuls les BPDU sont écoutés
- Learn : état transitoire, trafic écouté (mais non transmis) pour constituer la table de commutation
- Forward : état normal de commutation
- Disable : port non pris en compte dans le STP

Temps Block $\rightarrow$ Forward : 30 à 50 s

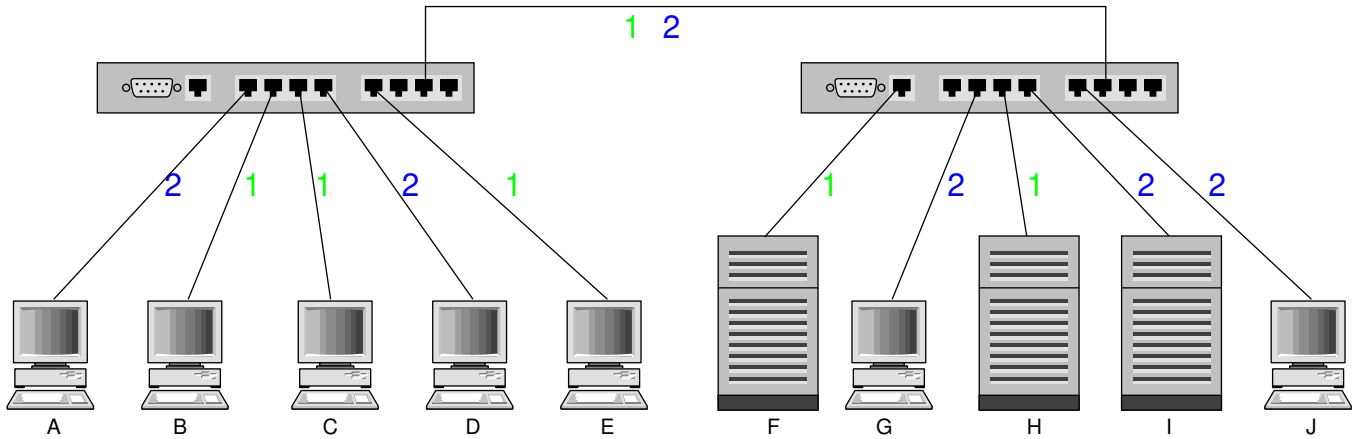
Spanning Tree – arbre recouvrant – 802.1D

802.1D : temps de convergence important (30 à 50 secondes)
$\Rightarrow$ Rapid STP (802.1w) en 2001 :

- acquittements $\Rightarrow$ éviter d'attendre un délai
- possibilité de configurer des ports « edge »
- convergence : 6 secondes
- messages périodiques « hello » : 2 secondes
- expiration rapide : après 3 « hello » non reçus

Réseaux virtuels - 802.1Q

Besoin : gérer des réseaux indépendants en utilisant une infrastructure commune



- Réseau virtuel 1 : B, C, E, F, H
- Réseau virtuel 2 : A, D, G, I, J

Réseaux virtuels - 802.1Q

Définition des VLAN sur le commutateur. En principe :

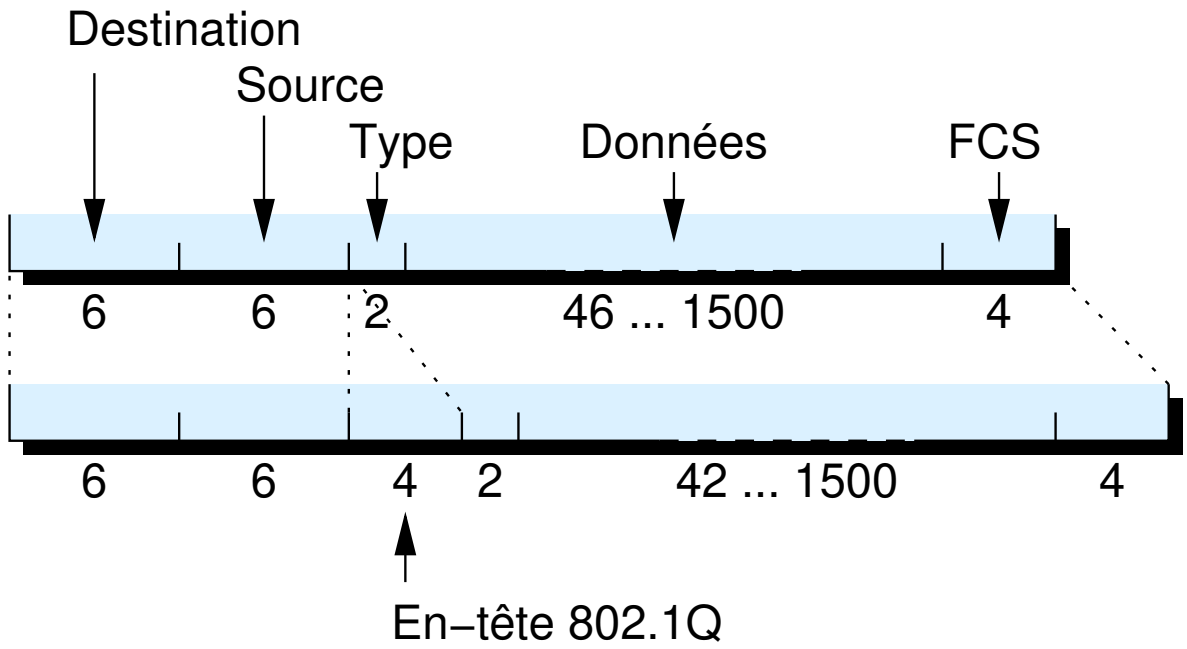
- les ports vers les stations sont configurés dans un VLAN donné
  $\Rightarrow$ protocole Ethernet standard
- les ports vers d'autres commutateurs doivent faire transiter plusieurs VLAN
  $\Rightarrow$ ajout au protocole Ethernet

Dans la pratique :

- les stations peuvent être des serveurs hébergeant plusieurs machines virtuelles dans des VLAN distincts
- un commutateur distant peut ne pas être compatible avec 802.1Q

Réseaux virtuels - 802.1Q

802.1Q (1988) $\Rightarrow$ modification de la trame Ethernet :



En-tête 802.1Q = tag :

16 bits	identificateur de protocole (0x8100)
3 bits	priorité 802.1p
1 bit	trame jetable en cas de congestion
12 bits	identificateur de VLAN

Réseaux virtuels - 802.1Q

Transport de VLAN sur des réseaux d'opérateurs

$\Rightarrow$ extension : « QinQ » (802.1ad, 1998)

- double en-tête 802.1Q
- type = 0x88a8 (anciennement 0x9100)

Réseaux virtuels - 802.1Q

Modifications à Ethernet :

- protocole Ethernet
- étanchéïté des réseaux $\Rightarrow$ commutateur doit avoir une table de commutation par VLAN
- Spanning Tree par VLAN

Plan

Problématique de la propagation radio

Médium partagé, mais...

1. ... une station ne peut recevoir et émettre en même temps
   $\Rightarrow$ transmission *half-duplex*
   $\Rightarrow$ pas de détection de collision
2. la portée n'est pas uniforme
   - problème de la station cachée
   - problème de la station exposée

   $\Rightarrow$ le partage du médium est inégal
   $\Rightarrow$ impossible d'écouter toutes les stations

CSMA/CA – Principes

CA = Collision Avoidance
$\Rightarrow$ éviter *autant que possible* les collisions

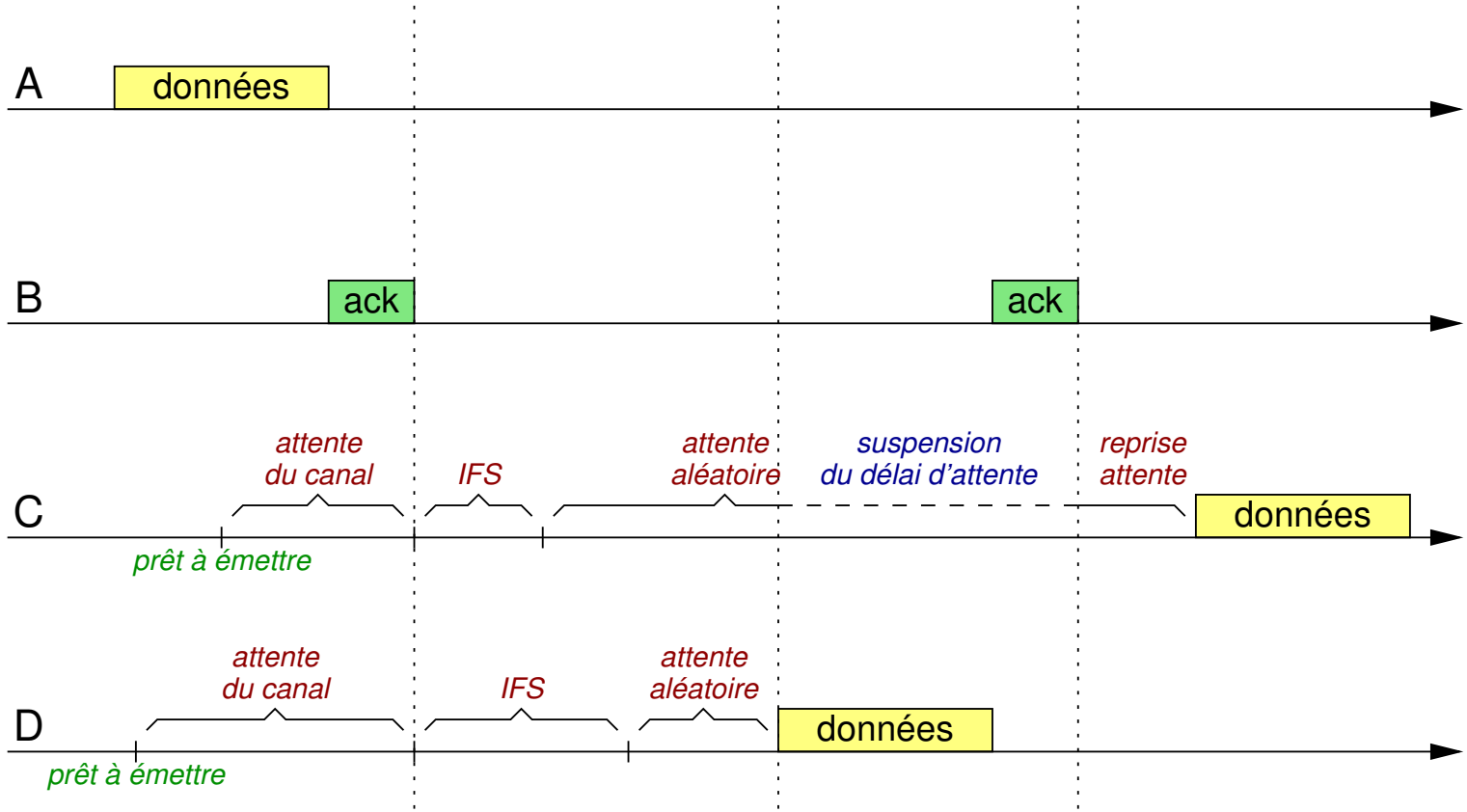
CSMA/CA est un mécanisme général (comme CSMA/CD) pour partager un canal :

- bus : LocalTalk d'Apple
- sans-fil : 802.11 (WiFi) ou 802.15.4 (réseaux de capteurs)

CSMA/CA – Algorithme général

1. une station souhaitant émettre écoute le canal
2. si le canal n'est pas libre, la station attend en écoutant
3. lorsque le canal est libre, la station attend un délai convenu IFS (*Inter-Frame Spacing*)
   $\Rightarrow$ la durée du délai est représentative de la priorité
4. la station choisit alors un délai d'attente aléatoire $\in [0, cw]$ (cw = *contention window*, initialement à 1)
   si le canal devient occupé, le délai n'est plus décompté pendant la durée d'occupation
5. au bout du délai, si le canal n'est pas occupé, la station émet les données
6. si l'acquittement n'est pas reçu, cw est doublé et on recommence au début

CSMA/CA – Algorithme général



CSMA/CA – Algorithme général

Ajustements pour tenir compte de la réalité :

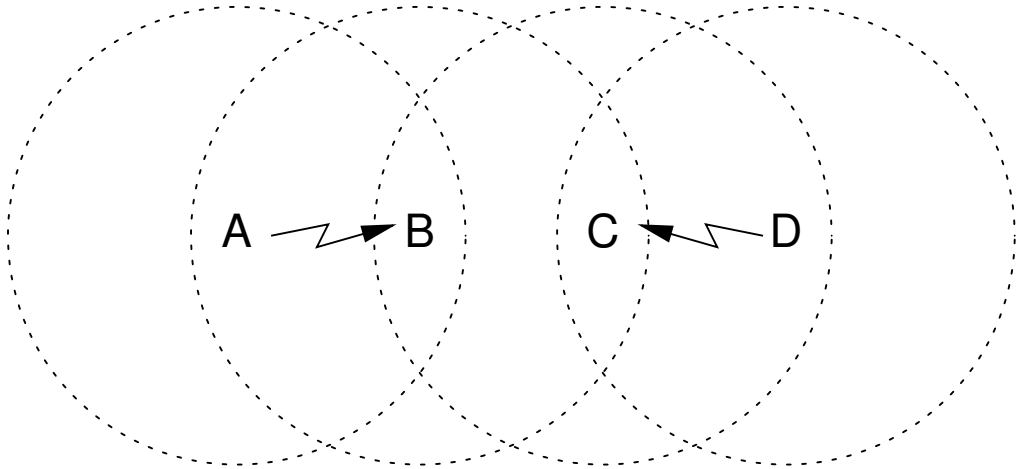
DIFS	Distributed Coordination Function IFS	temps d'attente initial
SIFS	Short IFS	temps entre réception des données et émission de l'acquittement (basculement du tuner)
EIFS	Extended IFS	remplace DIFS si la précédente trame émise était en collision

SIFS < DIFS < EIFS

De plus, chaque trame contient la durée de l'échange
$\Rightarrow$ ex : l'en-tête des données comprend aussi les durées de SIFS et de l'acquittement

CSMA/CA – Communications radio

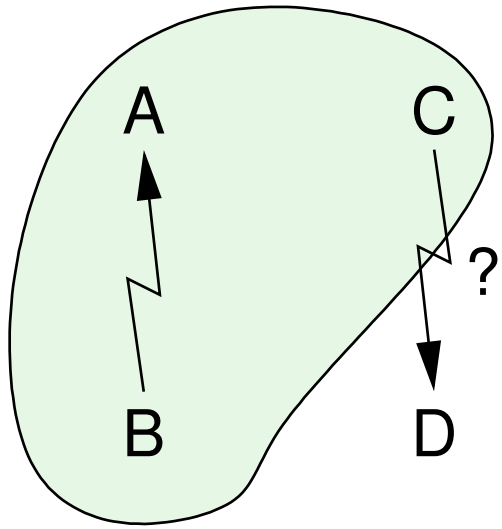
Problématique des communications radio : la station cachée



- A ne peut détecter la collision provoquée par la transmission D $\rightarrow$ C
- le signal reçu par B (A $\rightarrow$ B) est perturbé par la communication D $\rightarrow$ C

CSMA/CA – Communications radio

Problématique des communications radio : la station exposée



portée radio de B

- B émet vers A :
  - C reçoit le signal (par exemple parce qu'il est en hauteur)
  - D ne reçoit pas le signal
- C ne peut donc pas émettre vers D
  - bien que D ne soit pas perturbé par l'émission de B

CSMA/CA – Communications radio

Ces deux problèmes viennent de ce que l'émetteur choisit d'émettre en fonction de ce que l'*émetteur* sait, et non de ce que le *récepteur* peut recevoir

Solution (parmi d'autres) :

1. A envoie un message RTS (*Request To Send*) à B
2. si B reçoit RTS, il renvoie un message CTS (*Clear To Send*) à A
3. A envoie alors la trame de données à B

Mécanisme optionnel sur 802.11, rarement utilisé en pratique (coût trop élevé compte-tenu de la rareté des stations cachées/exposées)

802.11

WiFi = nom « commercial » des normes IEEE 802.11*
Deux modes d'utilisation :

- mode « ad-hoc » : coordination des stations entre elles (sans point d'accès)
- mode « infrastructure » : repose sur un point d'accès
  $\Rightarrow$ le plus courant

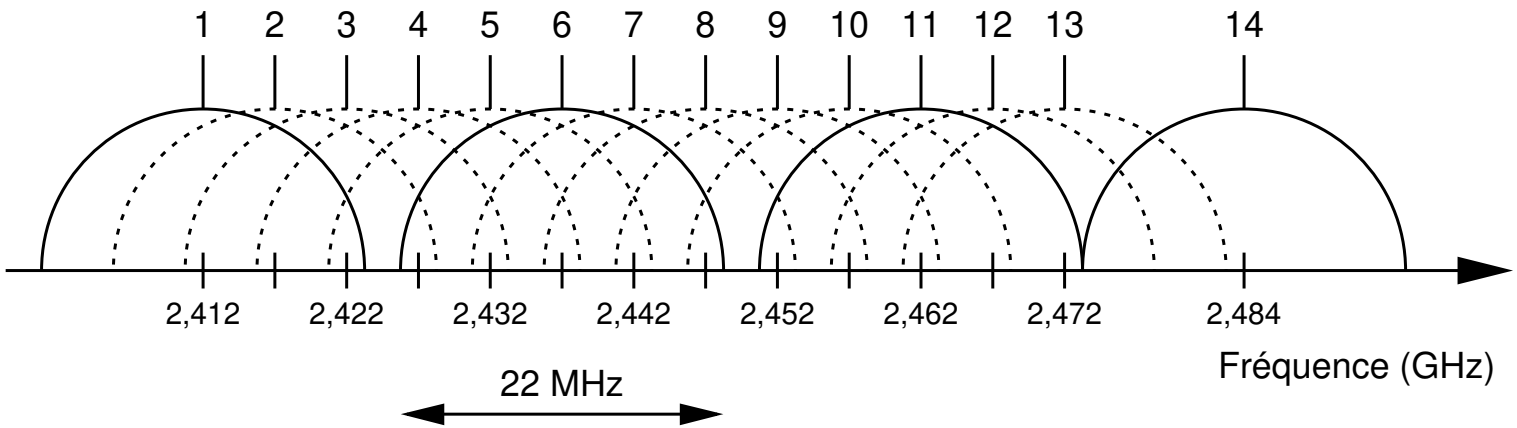
802.11

Norme	Date	Fréquence	Bande passante		Portée	
			max	typique	int	ext
802.11a	1999	5 GHz	54 Mb/s	22 Mb/s	25 m	75 m
802.11b	1999	2,4 GHz	11 Mb/s	5-6 Mb/s	35 m	100 m
802.11g	2003	2,4 GHz	54 Mb/s	22 Mb/s	25 m	75 m
802.11n	2009	2,4/5 GHz	540 Mb/s	200 Mb/s	50 m	125 m
802.11ac	2014	5 GHz	6 Gb/s	-	20 m	50 m

Note : pas de notion de débit typique avec 802.11ac car cela dépend de l'encombrement du spectre et de la distance.

802.11 – Canaux

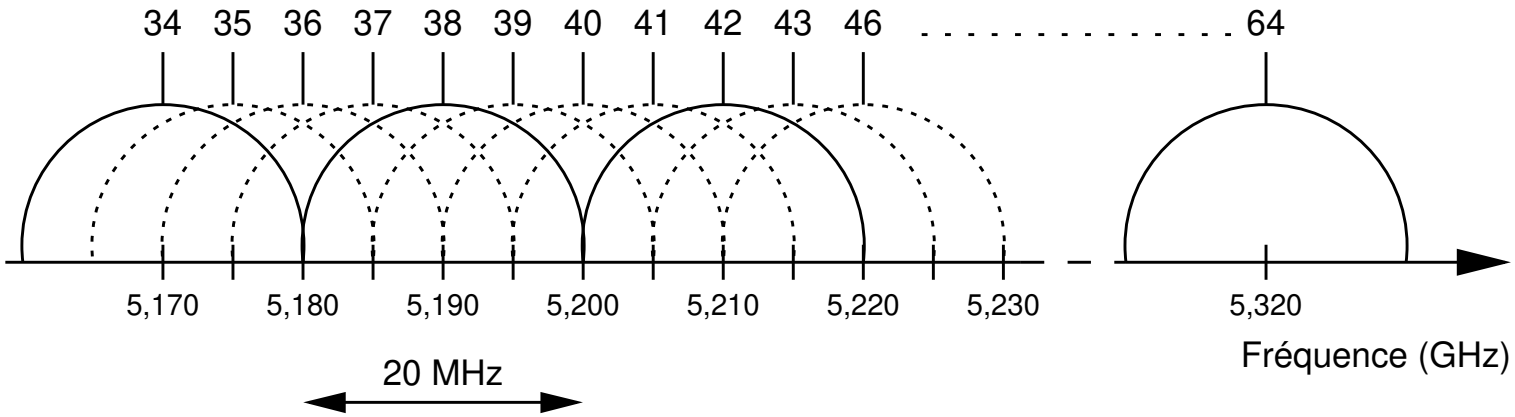
Décomposition du spectre 2,4 GHz en canaux (802.11b) :



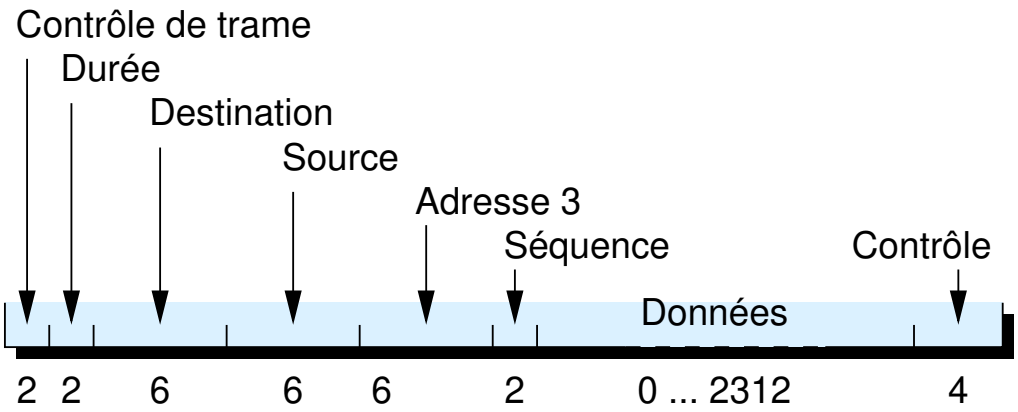
- canal 14 autorisé au Japon seulement
- interférences possibles entre canaux
  $\Rightarrow$ canaux 1, 6 et 11, voire 14

802.11 – Canaux

Décomposition du spectre 5 GHz en canaux (802.11a) :

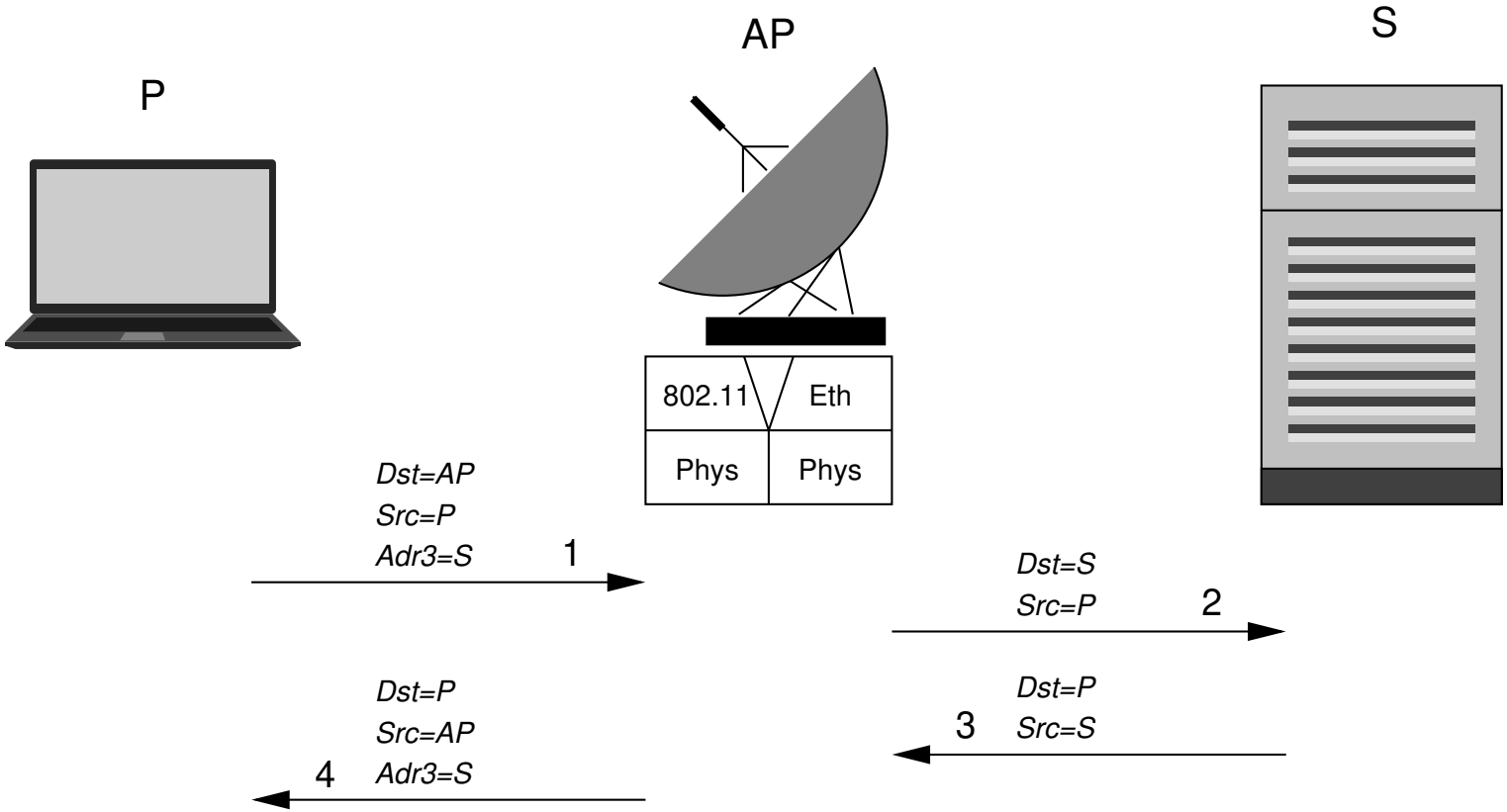


- canaux décomposés en 52 sous-canaux de 300 kHz
- interférences possibles entre canaux
  $\Rightarrow$ canaux 34, 36, 42, etc.
- 802.11a : mécanisme de choix dynamique du canal



- Contrôle de trame :
  - type de trame (données, acquittement, RTS, CTS, etc.)
  - retransmission ou non
  - trame de/vers le réseau extérieur
  - trame chiffrée ou non
  - ...
- Durée : de l'échange complet (ex: y compris SIFS et acquittement) en μs
- Adresse 3 : destination réelle, si passage par un point d'accès
- Séquence : numéro de séquence de la trame

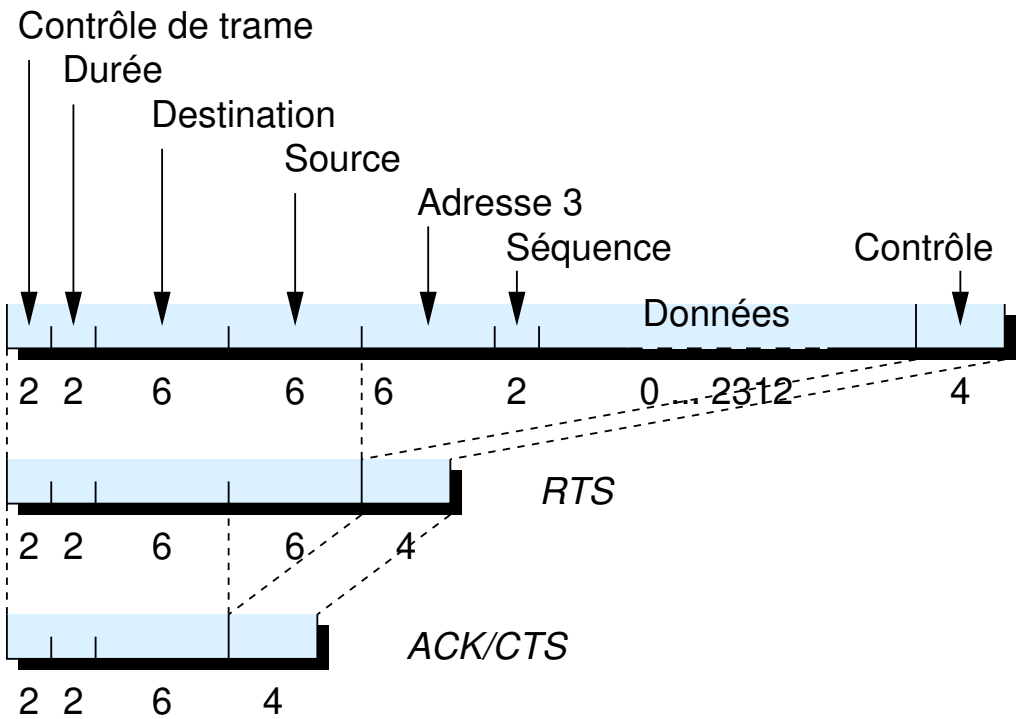
Utilisation de la troisième adresse (en mode « infrastructure ») :



Gestion des duplications :

- chaque trame comporte :
  - un numéro de séquence
  - un bit « retry » (dans le champ « contrôle »)
- le récepteur mémorise, pour chaque adresse source, le numéro de séquence de la dernière trame reçue
  $\Rightarrow$ dupliqué si retry = 1 et numéro de séquence identique
  $\Rightarrow$ ignoré par le récepteur

Les différents types de trames :



802.11

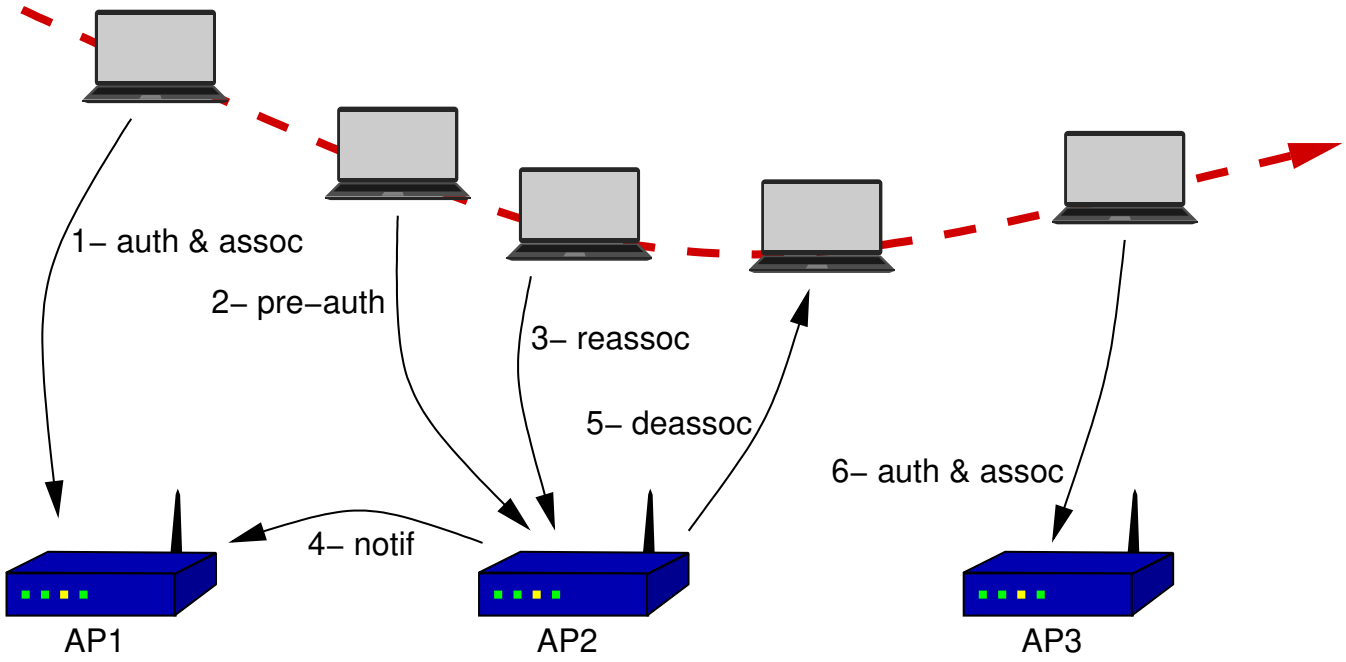
En mode « infrastructure » : message « Beacon » = annonce périodique (toutes les 100 ms) par le point d'accès :

- capacité du point d'accès (débits supportés)
- SSID (Service Set IDentity) : chaîne de caractères terminée par un octet nul
- paramètres radio

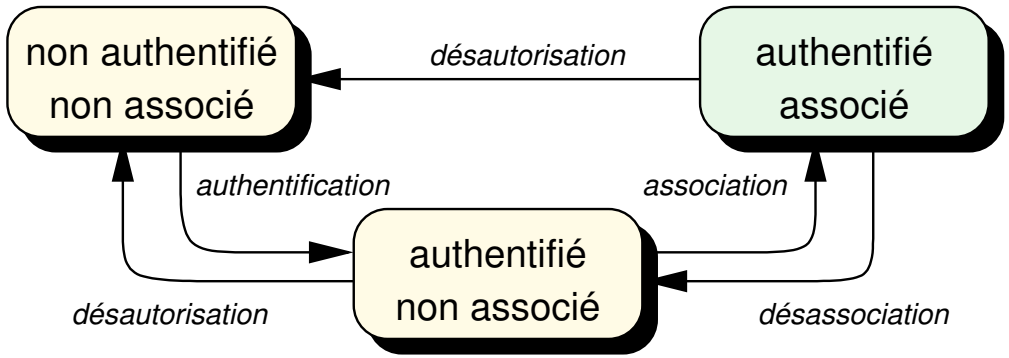
Une station peut également interroger les points d'accès :

- trame « probe request » : la station envoie le SSID souhaité et sa liste de capacités
- trame « probe response » : analogue au « beacon »

802.11 – Association et authentification



802.11 – Association et authentification



Authentification :

- open-system
- shared-key : repose sur un challenge WEP

Association : le point d'accès renvoie un identificateur d'association dans la trame de réponse d'association, et commence à répondre aux requêtes sur le réseau filaire pour l'adresse MAC de la station.