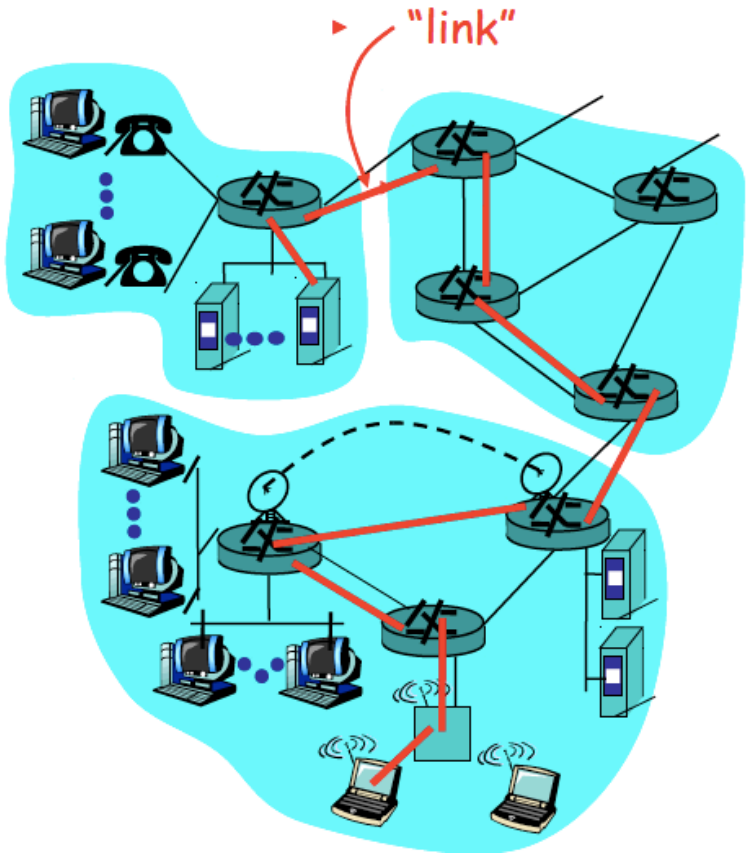
Réseaux - Mif05

Couche liaison de données
L'exemple de la technologie Wi-Fi

Isabelle Guérin Lassous
Isabelle.Guerin-Lassous@univ-lyon1.fr
http://perso.ens-lyon.fr/isabelle.guerin-lassous

Introduction

- Vocabulaire
  - Nœud
    - Terminal, routeur, commutateur, …
  - Lien de communication
    - Permet de relier des nœuds voisins
    - Canal/Médium de communication
- Couche liaison de données
  - Assure le transfert de données entre deux ou plusieurs nœuds voisins



C. Kurose & Ross

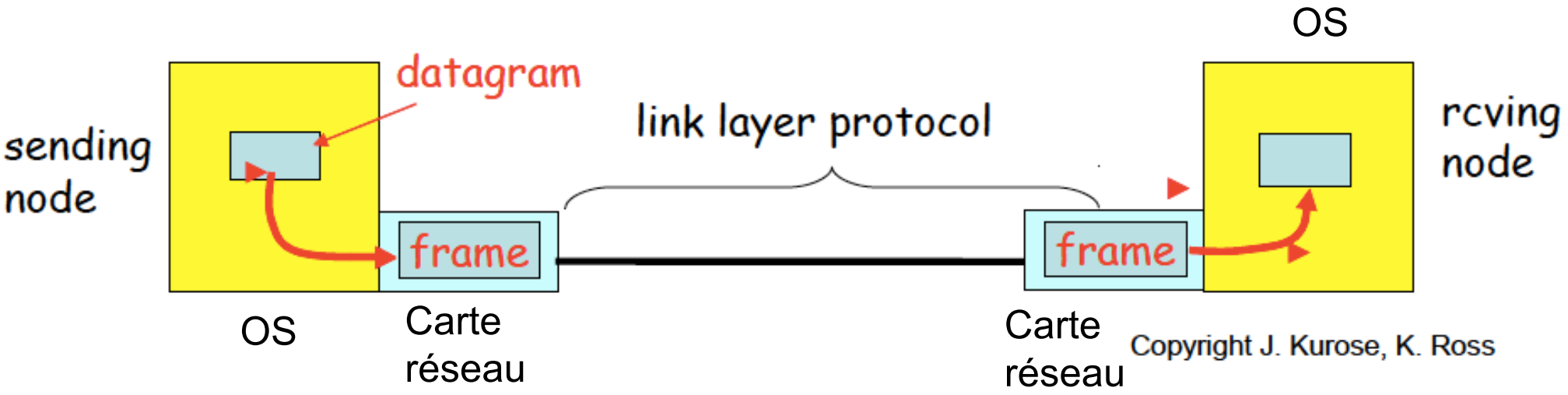
Introduction

- Protocoles liaison de données
  - Ethernet, PPP, Frame Relay, IEEE 802.11 (WiFi)
- Les protocoles liaison de données peuvent fournir des services différents

Services / Principes Théoriques

Adaptateur

- Protocole liaison de données souvent implémenté dans un adaptateur
  - Network Interface Card
  - Processeur, mémoire, bus, etc.
- Réalise les services de niveau 2
- Mode semi-autonome



Tramage

- Constitution d'un paquet de niveau liaison de données
- Encapsulation du datagramme dans une trame
  - Champs supplémentaires
    - En-tête de niveau 2
    - Informations sur la couche 2 comme ?
  - Assurer la communication entre 2 nœuds voisins
  - Réaliser les services de niveau 2
- Délimitation d'une trame
  - Fanion (bit), marqueur de début et fin (caractères)
  - Se fait au niveau physique pour certains protocoles
    - Wi-Fi

Détection d'erreurs

- Erreurs possibles sur le lien de communication
  - Atténuation
  - Bruit
  - Collisions / interférences
  - Echo
- Mécanisme réalisé
  - Au niveau hardware (en général)
  - Optionnel
    - Mais souvent réalisé au niveau 2

Principe de la détection d'erreurs

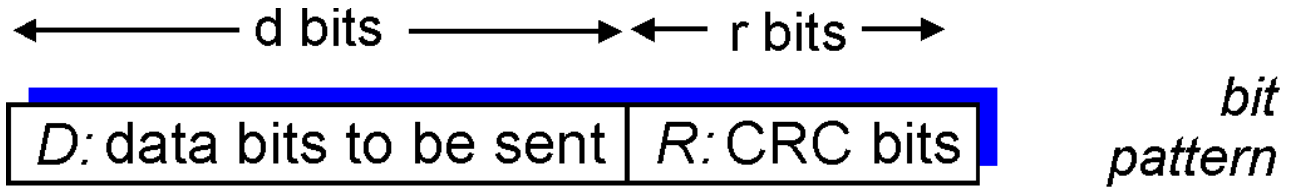
- Ajout de données de contrôle dans la trame par le nœud source
  - Champ détection d’erreurs
  - Checksum – somme de contrôle
- Test de validité du paquet par le récepteur
  - Utilisation du champ détection d’erreurs par le récepteur
  - Réponse positive
    - Paquet considéré comme sans erreur
  - Réponse négative
    - Paquet considéré comme avec erreur
- Pas fiable à 100%
  - Compromis sur la taille du champ détection d’erreurs

CRC

Cyclic Redundancy Code

- D
  - Données à protéger
- G
  - Générateur négocié entre la source et la destination
  - Contient (r+1) bits
  - Bit le plus à gauche à 1
- R
  - CRC = reste de la division de $D.2^r$ par G
  - $D.2^r$ = r bits à 0 ajoutés à D
  - DR est divisible par G
- Récepteur
  - Division des bits reçus par G
  - Si le reste est nul ➔ succès

- Arithmétique binaire modulo-2 (sans retenue)



bit pattern

$D * 2^r$ XOR R

mathematical formula

CRC
Cyclic Redundancy Code

- 1 seule erreur toujours détectée dès que deux 1 dans G
- 2 erreurs toujours détectées dès que trois 1 dans G
- Nombre impair d'erreurs détectées dès que G se termine par 11
- Erreurs d'au plus r bits consécutifs détectées
- Erreurs d'exactement (r+1) bits consécutifs détectées
  - avec probabilité $1-0,5^{(r-1)}$
- Erreurs de plus de (r+1) bits consécutifs détectées
  - avec probabilité $1-0,5^{r}$

- Très utilisé
- Taille du générateur
  - 2 à 65 bits
  - Ethernet, 802.11 : 33 bits
    - 100000100110000010001110110110111

Récupération d'erreur

- Si destinataire reçoit un paquet qu'il considère en erreur
  - Quelle action ?
- Rejeter le paquet et ne rien faire d'autre
  - Que suppose-t-on dans ce cas ?
- Prévenir la source qui peut retransmettre le paquet
  - Envoi d'un ACK négatif
    - Ou plutôt seuls les paquets correctement reçus sont acquittés
  - Plusieurs approches
    - Émission & attente d'un ACK
    - Utilisation d'une fenêtre d'émission
  - Si pas d'ACK reçu (timer a expiré)
    - Retransmission du paquet
- Corriger soi-même les erreurs (correction d'erreurs)
  - Utilisation de codes correcteurs
    - Code de Hamming
  - Peu utilisé en pratique au niveau de la couche 2

Types de liens de communication

- Lien unidirectionnel
- Lien bidirectionnel
  - Half-duplex
  - Full-duplex

Accès aux liens de communication

- Lien point-à-point
  - Seulement deux stations connectées par ce médium
  - Lien souvent full duplex
- Lien partagé
  - Plusieurs stations peuvent être connectées au lien
  - Un paquet transmis se propage vers toutes les stations
  - 2 transmissions simultanées peuvent provoquer des collisions
- Protocole MAC
  - Medium Access Control
  - Algorithme qui permet une utilisation partagée du médium, i.e. indique quand un nœud peut transmettre

Protocole MAC idéal

- Hypothèse
  - Médium partagé avec une bande passante de D b/s
- Efficacité
  - Quand un nœud est seul à vouloir parler, il doit pouvoir utiliser tout le médium
    - À quel débit ?
- Equité
  - N nœuds veulent transmettre
    - Débit moyen de chacun ?
- Décentralisé
  - Pas de coordinateur
  - Pas d'horloge
- Simple

Classification (possible)

- Basé sur la notion de canal
  - Découpage « strict » du médium de communication en sous-parties (sous-canaux)
  - Allocation avant transmission
- Basé sur la notion de paquets
  - Envoi du paquet ➔ prise de contrôle du médium
  - Utilisation de tout le médium de communication alloué quand un paquet doit être envoyé

Techniques multicanaux

- Time Division Multiple Access
  - TDMA
    - Découpage en temps
    - Synchronisation nécessaire
- Frequency Division Multiple Access
  - FDMA
    - Découpage en fréquence
    - Débit éventuellement faible

Techniques multicanaux

- Code Division Multiple Access
  - CDMA
    - Utilisation de codes
      - Communications parallèles sur le lien partagé
    - Contrôle de puissance nécessaire

Techniques multicanaux

- Si nombre de sous-canaux > nombre d'utilisateurs
  - Allocation fixe simple
- En général
  - Nombre d'utilisateurs >> nombre de sous-canaux
- Sous-canal à trouver dynamiquement
  - On demande à une entité spécifique
    - e.g. station de base dans les réseaux cellulaires mobiles
  - Problème de l'œuf et de la poule
    - Il faut communiquer pour demander une allocation
    - Il faut un protocole MAC pour savoir quand on doit accéder au médium
    - Utilisation d'un protocole à accès aléatoire pour obtenir un sous-canal

Protocoles à accès aléatoire

- Quand un nœud veut envoyer un paquet
  - Utilisation complète du médium (nécessaire pour la communication)
  - Pas de coordination a priori entre les nœuds
- Collision possible
  - Comment détecter les collisions ?
  - Comment gérer les collisions ?
- Exemples
  - ALOHA
  - CSMA

ALOHA

Bonjour !

Protocole à accès aléatoire développé pour le 1er réseau sans fil par commutation de paquets

Acquittements envoyés par le récepteur + retransmissions de la source après un temps aléatoire

Efficacité limitée : débit total = 1/(2.e) (18%) de la bande passante

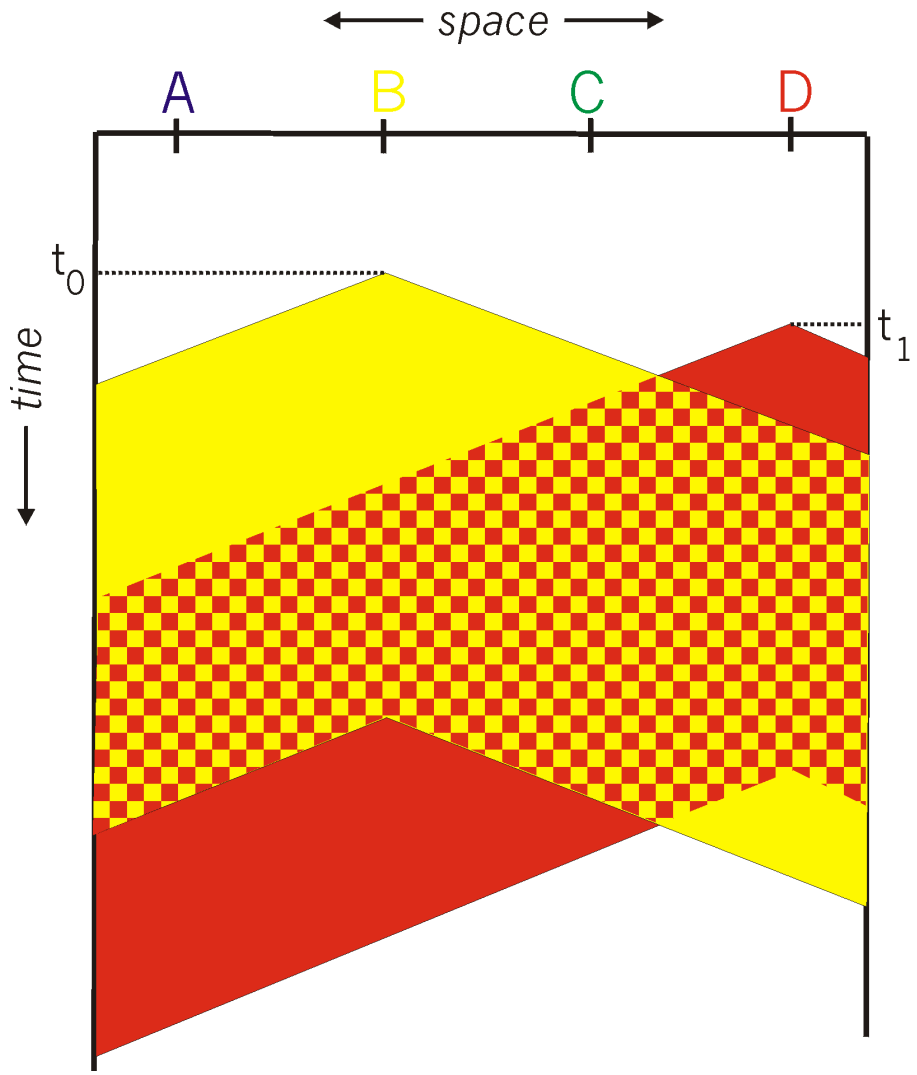
Slotted ALOHA

Slot = efficacité doublée

Nécessite une synchronisation

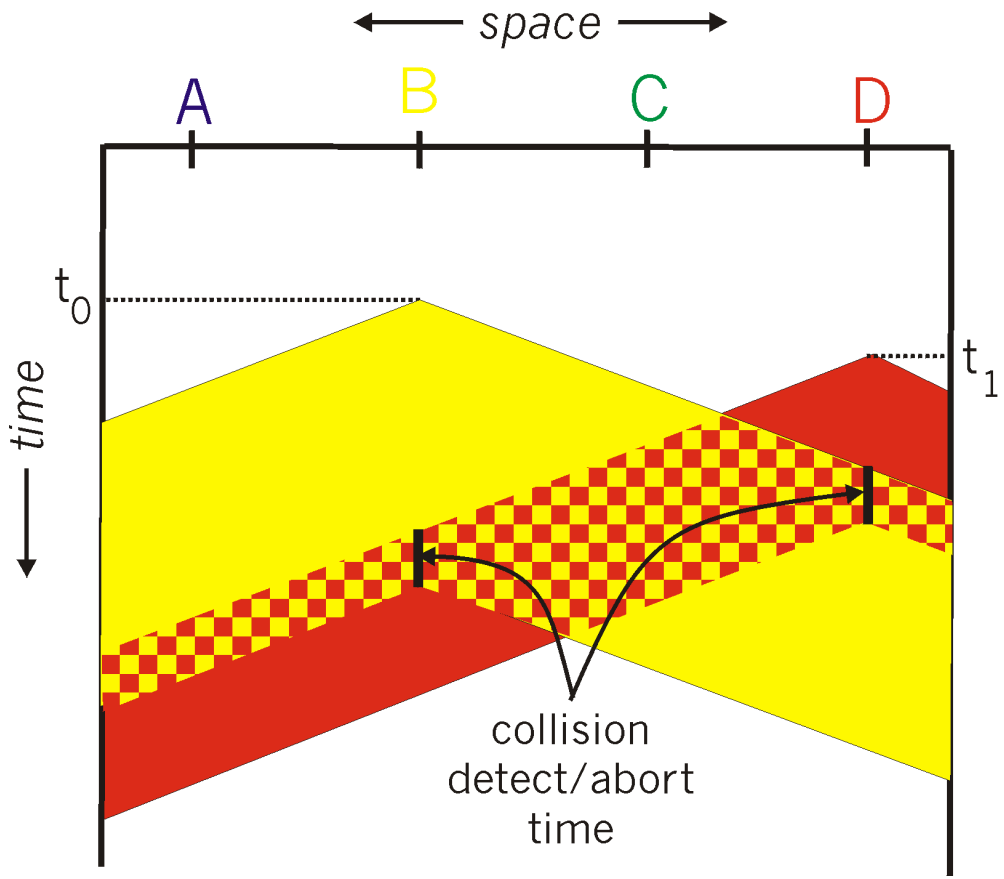
Carrier Sense Multiple Access CSMA

- Que fait-on avant de parler ?
- Collisions encore possibles ?



CSMA/CD

- Collision Detection
  - La station qui transmet détecte une collision
    - Arrêt de la communication
    - Comparaison entre le signal émis et le signal reçu
    - Réalisée par les sources
  - Retransmission après un temps aléatoire



CSMA/CA

- Collision Avoidance
- Sur un médium sans fil
  - Difficile de faire du 'collision detection' (pour le moment)
    - Pourquoi ?
  - Paquet acquitté par le destinataire
- Obligé d'attendre la fin d'une collision
  - Coûteux en temps
  - Essayer d'éviter au maximum les collisions *a priori*
    - Collision avoidance
- Temps d'attente aléatoire avant la transmission d'un paquet
  - Compromis temps d'attente – réduction des collisions
- Approche utilisée dans le Wi-Fi
  - Détails dans la suite du cours

Un exemple : le Wi-Fi

Solutions de niveau 2

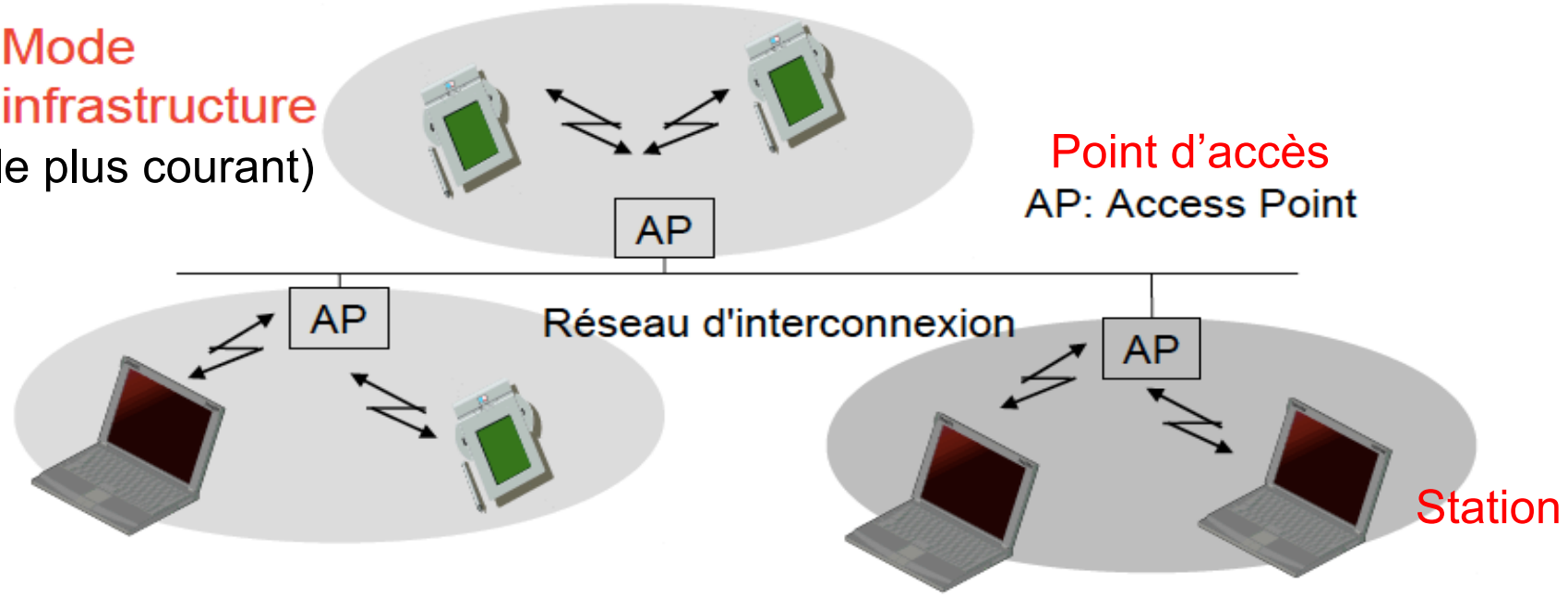
- Diversité des solutions
  - Assemblage de différents services
    - Tramage, Détection d'erreurs, Récupération d'erreurs, MAC
- A bien réfléchir en fonction de
  - Des applications du réseau
  - Du type de médium de communication utilisé
    - Couche physique
  - Du coût
- Standards
  - Définition/choix des différents services
  - Très long travail
  - Beaucoup de participants
  - Toujours en évolution

IEEE 802.11

- Standard pour la couche physique et la couche liaison de données des points d'accès et des stations (mobiles) pour les réseaux locaux sans fil
- Alliance Wi-Fi
  - Certification Wireless Fidelity
    - Interopérabilité entre les différents constructeurs
- Communication par ondes radio
- Evolution du standard
  - 1997 / 1999 / 2007 / 2012 / 2016

Deux architectures d'utilisation

Mode infrastructure
(le plus courant)



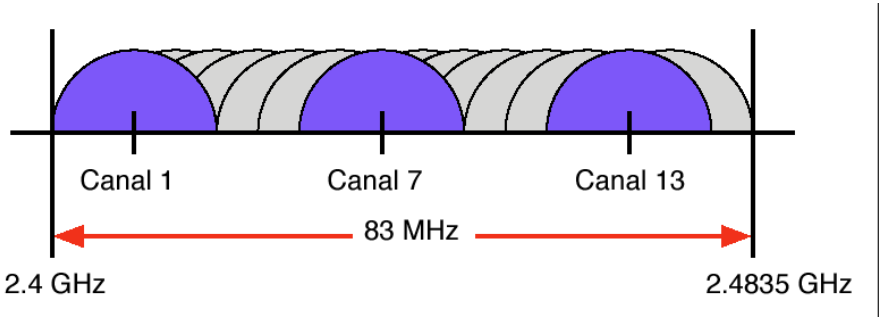
Point d'accès
AP: Access Point

Station

Mode ad hoc

Bandes de fréquences « classiques » du Wi-Fi

- Bande ISM
  - Fréquences libres
- 2,4 GHz
  - 14 canaux de 20 MHz
- 5 GHz
  - 22 canaux (en France) de 20 MHz indépendants
- Communication entre 2 nœuds se fait sur un seul canal
  - Canal de 20 MHz ou canal agrégé de 40, 80 ou 160 MHz
- Un nœud ne peut émettre que sur un canal à la fois



Les capacités d'émission du Wi-Fi
Quelques exemples

Nombre d'antennes utilisées

Largeur du canal

Intervalle de garde

Modulation and coding schemes

MCS index[a]	Spatial Streams	Modulation type	Coding rate	Data rate (in Mbit/s)[16][b]							
				20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7
0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130
1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260
2	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390
3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520
4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780
5	2	64-QAM	2/3	104	115.6	216	240	468	520	936	1040
6	2	64-QAM	3/4	117	130.3	243	270	526.5	585	1053	1170
7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300
8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560

Une capacité d'émission possible

...

Les capacités d'émission du Wi-Fi

- De très nombreuses capacités d'émission
- Laquelle choisir ?
- Règle (simpliste)
  - Plus la capacité d'émission est élevée, moins la transmission est robuste
- Choix de la capacité d'émission doit se faire en fonction de la qualité du canal radio
  - émetteur et récepteur très proches => canal de bonne qualité
    => utiliser une capacité d'émission élevée
  - émetteur et récepteur éloignés et obstacles => canal de mauvaise qualité => utiliser une capacité d'émission réduite
- Choix dynamique
  - Algorithme d'adaptation de débit
  - Appliqué par l'émetteur
  - Propriétaire ou open source

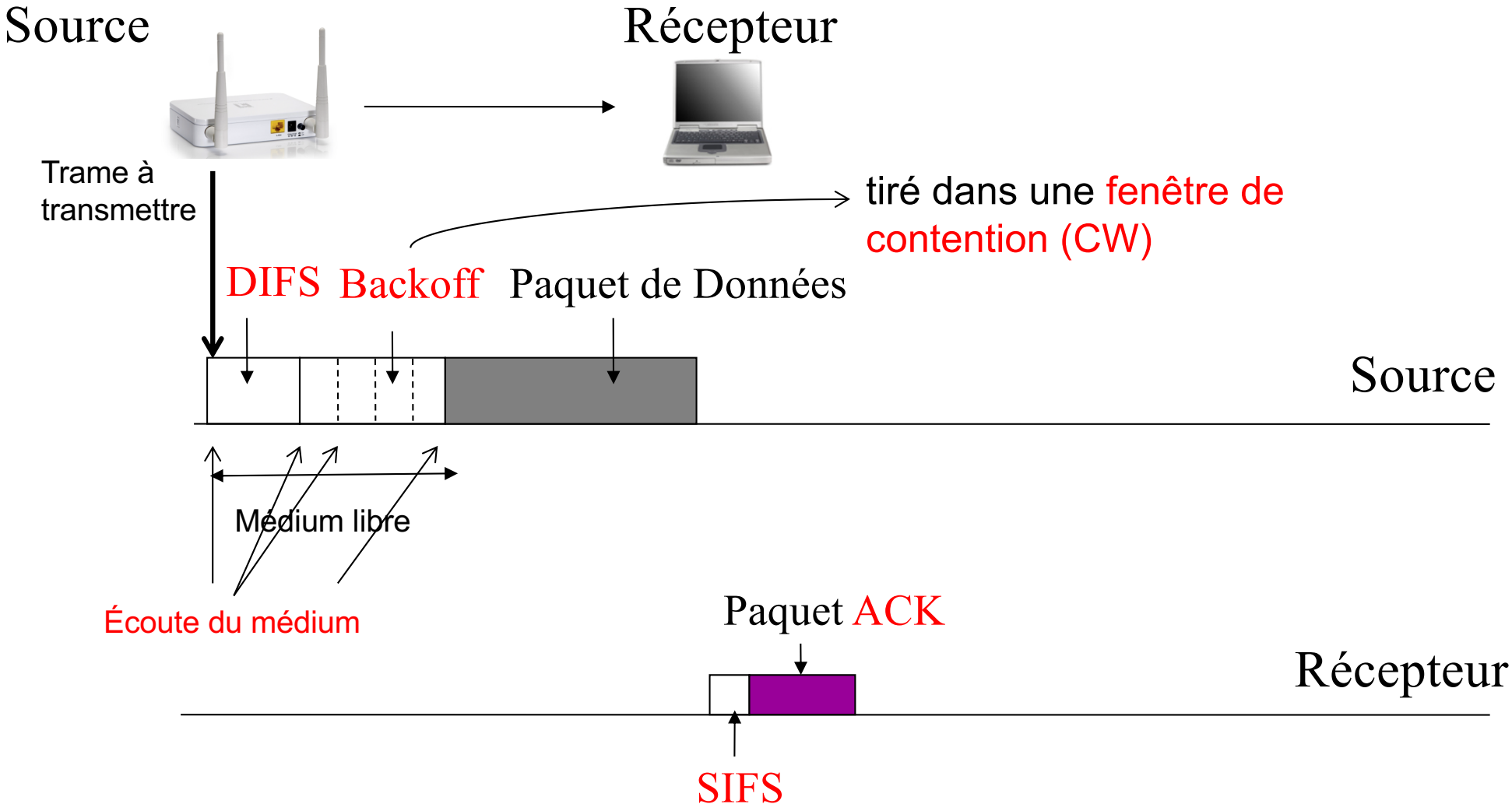
Accès au médium radio

- Deux fonctions possibles dans le standard
- Distributed Coordination Function - DCF
  - Infrastructure / ad hoc
  - CSMA/CA
- Point Coordination Function - PCF
  - Infrastructure

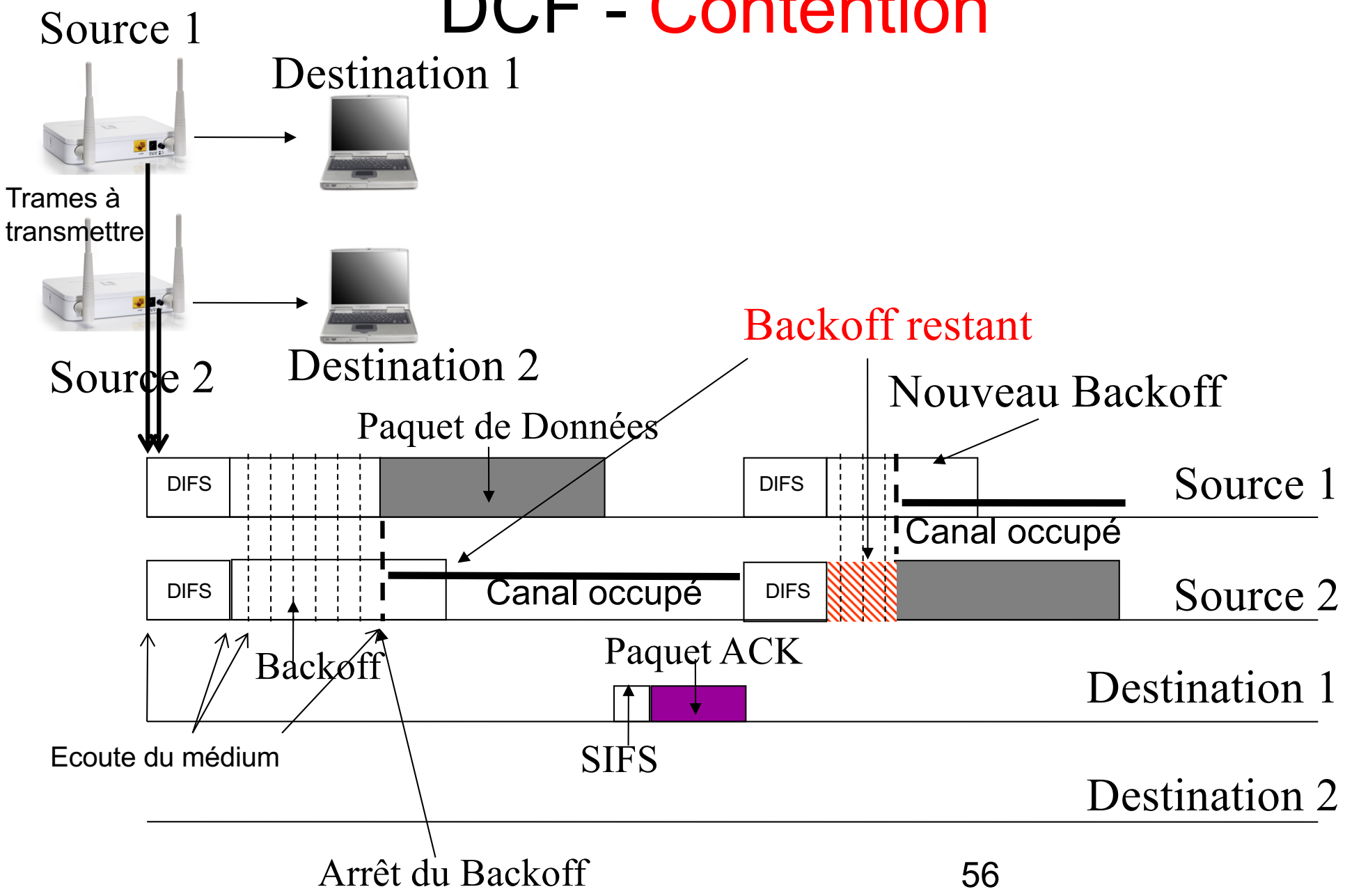
- DCF dans la plupart des cartes et points d'accès

Accès au médium

DCF – mode point-à-point (simple)



DCF - Contention



DCF - Collisions

- Si 2 stations émettent un signal en même temps
  - Il peut y avoir collision au niveau du récepteur
  - Pas d'ACK envoyé/reçu
    - Retransmission du paquet
- Processus d'accès au médium relancé avec une augmentation de la fenêtre de contention
  - Algorithme BEB (Binary Exponential Backoff)
  - Taille CW = 2*Taille CW(précédente)
  - Fenêtre de contention maximale CWmax
- Paquet rejeté si émission échoue plusieurs fois
- Utilisation de CWmin pour le paquet suivant dans la file

Réseaux avancés & Recherche

- M2 RSFM : Wi-Fi avancé

- Beaucoup de recherches autour du Wi-Fi
  - Wi-Fi 6 à venir ; Wi-Fi 7 pour le futur
  - Paramétrage extrêmement complexe
- De très nombreuses technologies radio innovantes
  - reposant sur des couches 2 très différentes

Fin du cours