

Réseaux et Sans-fils et de capteurs

LIG - Semestre 2

Enseignante: Dr. Wafa AKKARI
wefa.akkari@gmail.com, wafa.akkari@ensi-uma.tn

Plan Général du cours (1)

I. Introduction

1. Définition des réseaux sans fils
2. Fonctions des couches

II. Réseaux locaux sans-fil

1. Rappel de WiFi (IEEE 802.11)
2. Bluetooth (IEEE 802.15)
3. WiMax (IEEE 802.16)

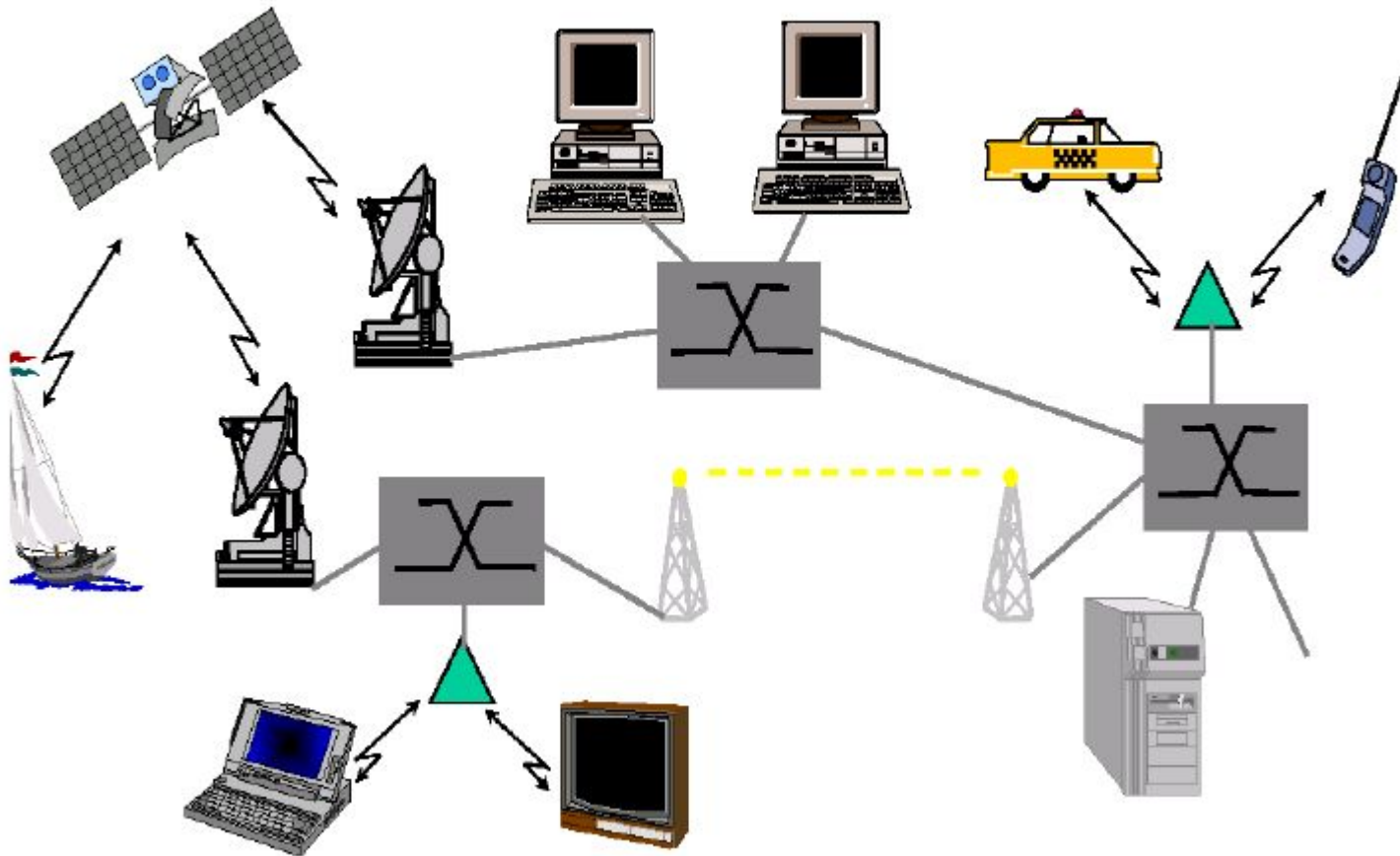
III. Téléphonie Mobile

1. GSM
2. GPRS
3. UMTS

Plan Général du cours (2)

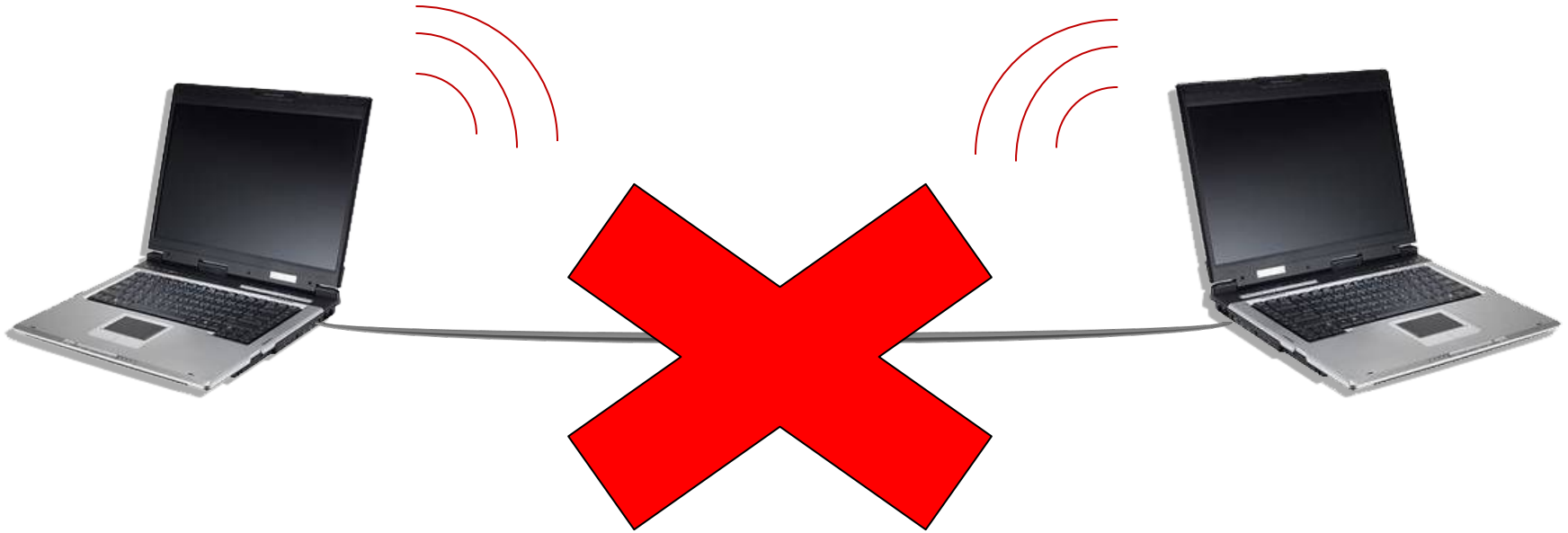
- I. Les réseaux de capteurs
 - 1. Définitions
 - 2. Caractéristiques
 - 3. Applications
 - 4. WSN VS MANET
 - 5. Architecture et Composants d'un nœud capteur

Le sans fils omniprésent?



Introduction aux réseaux sans fil

❑ But principal d'un réseau sans fil



• But secondaire

- connexion temporaire
- matériel de secours

les réseaux sans fils

❑ Définition: " réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement".

❑ Protocoles : Des protocoles sans fils connus... et inconnus :

- ✓ IR, Bluetooth, RFID¹, Zigbee
- ✓ GPS, GPRS, UMTS (3G), Satellite
- ✓ WiFi, Wimax

¹ Rq: Radio Frequency Identification (RFID) Ce sont des réseaux d'étiquettes actives ou passives qui permettent de détecter si un objet se trouve dans un certain périmètre autour du lecteur d'étiquettes. Cependant la portée de ces étiquettes et de ces lecteurs d'étiquettes n'est pas très importante (de l'ordre de quelques mètres).

Les bénéfices des WLAN

- ❑ Mobilité
 - ✓ Liberté de mouvement des usagers et des terminaux
- ❑ Zones difficiles à câbler
 - ✓ Traverser une rivière, une autoroute, une voirie, etc.
- ❑ Moins de risques de rupture de liens que dans le filaire (coupure du câble, abîmer les connecteurs, etc.)
- ❑ Délais de mise en service du réseau plus faibles
- ❑ Des économies à long terme

Domaines d'application des WLAN

- ❑ Tous les métiers dont la mobilité est nécessaire pour augmenter la productivité
 - ✓ Hôpitaux (gestion des fichiers patients, ...)
 - ✓ Restaurants (communications rapides entre serveurs et cuisiniers, ..)
 - ✓ Home and small office (éviter de câbler, coûts réduits, ...)
 - ✓ Etc. ...
- ❑ Environnement d'installation difficiles des médias filaires

les réseaux sans fils

- ❑ Intérêt du sans fil:
 - ✓ Facilité de déploiement
 - ✓ Interopérabilité avec les réseaux filaires
 - ✓ Débits adaptés à un usage professionnel
 - ✓ Grande souplesse et faiblement structurant (chantier, exposition, locaux temporaires)
 - ✓ Non destructif (monuments historiques, sites classés)
 - ✓ Grande mobilité
 - ✓ Coût

les réseaux sans fils

❑ Contraintes:

✓ Limites des ondes radio

- sensibles aux interférences (microondes, autre réseau...)
- occupation progressive des bandes de fréquence : autorégulation

✓ Sécurité : données circulant librement

- nécessite de déployer des solutions de sécurité adaptées

✓ Réglementation

- fréquences et puissances d'émission contrôlées par l'Etat

✓ Débit : mutualisé et variable

- Partagé entre les utilisateurs et dépendant des conditions d'usage
- Globalement dix fois inférieur au filaire

Contexte: les réseaux MANETs

Caractéristiques:

Limitations

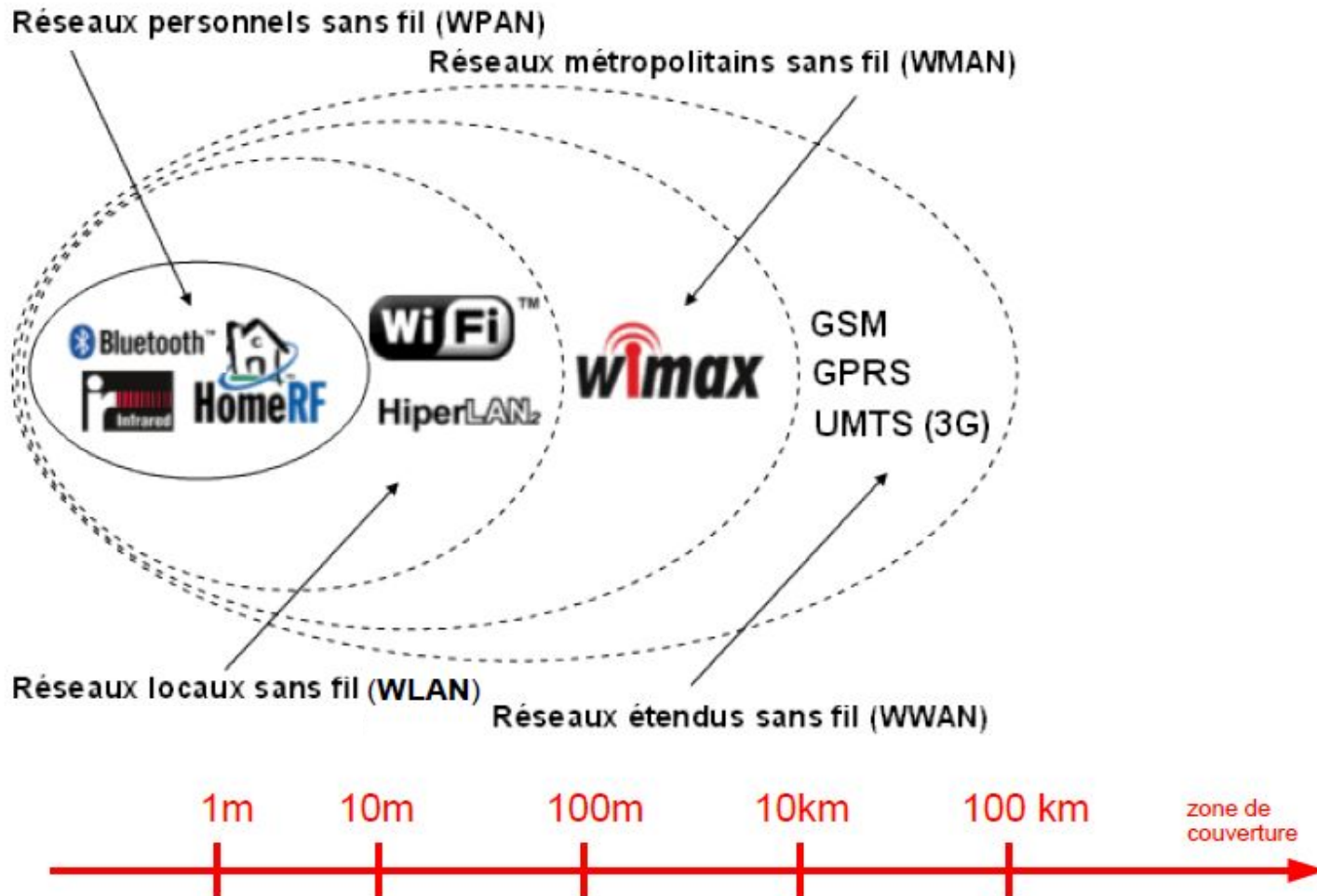
- | | |
|---|---|
| Ressources énergétiques restreintes | Support de transmission partagé |
| ✓ Mobilité | |
| • Batteries à capacité limitée | - Taux d'erreur élevé |
| ✓ Liens sans fils | - Faible débit |
| ✓ Hétérogénéité des nœuds | - Sécurité |
| ✓ Absence d'infrastructure | + - Ressources énergétique restreintes |
| • Activités supplémentaires pour les nœuds (routage) | - Rayon de transmission |
| ✓ Auto-organisés et distribués | - Topologie variable |
| □ durée de vie limitée des nœuds | - Interférences |
| ✓ Taille des réseaux | - Routage du trafic |
| ✓ Multi-sauts | |

les réseaux sans fils

- ❑ Critères de classification:
 - ✓ Radio : fréquence, modulation et puissance
 - ✓ Protocole de communication et de sécurité
 - ✓ Terminaux supportés
 - ✓ Architecture (topologie) du réseau
 - ✓ Débit
 - ✓ Portée
 - ✓ Coût

les réseaux sans fils

✓ Catégories des réseaux sans fils



Environnement de Propagation Radio

- ❑ Notion de propagation radio: Les ondes radio se propagent en ligne droite dans plusieurs directions depuis leur source d'émission
- ❑ Leur vitesse dans le vide est de $3 \cdot 10^8$ m/s
- ❑ Lorsqu'elle rencontre un obstacle, l'onde est divisée et son énergie est répartie :

Signal Propagation Ranges

❑ Rayon de transmission (transmission range)

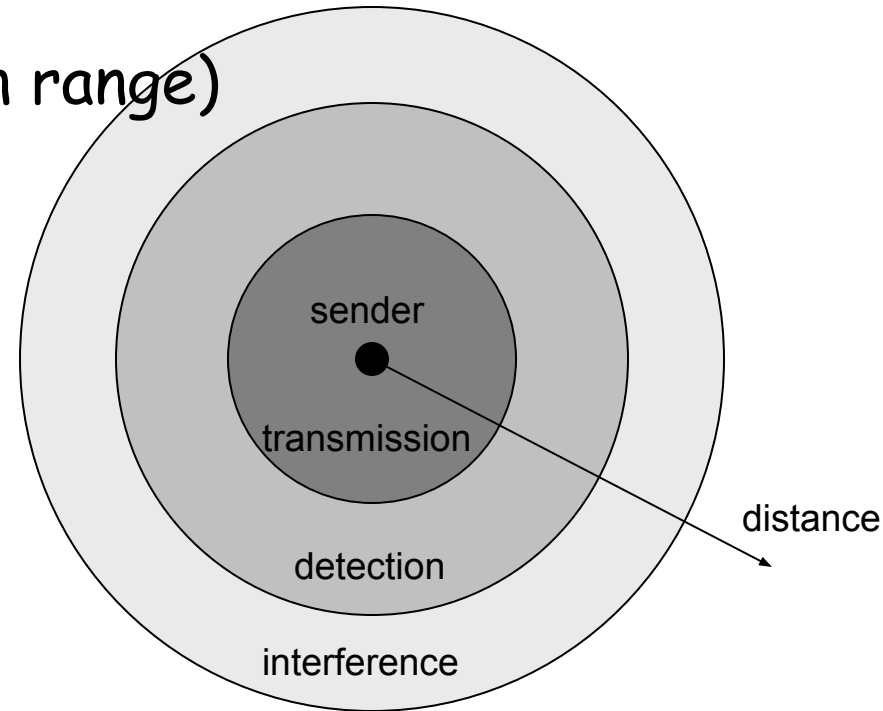
- ✓ communication possible
- ✓ Taux d'erreur faible

❑ Rayon de détection (Detection range)

- ✓ détection du signal possible
- ✓ communication impossible

❑ Rayon d'interférence (Interference range)

- ✓ Les signaux peuvent ne pas être détectés
- ✓ Les signaux ajoutent du bruit



Note: These are **not** perfect spheres in real life!

Environnement de Propagation Radio

❑ Causes de distorsion du signal (Nature du Canal radio):

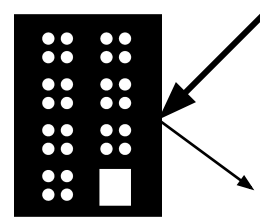
- Atténuation (dûe à la distance)
- Réflexion et Réfraction (nature et densité de surface)
- Diffraction
- Shadowing: blocage du signal



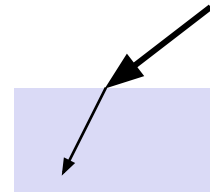
Diffraction



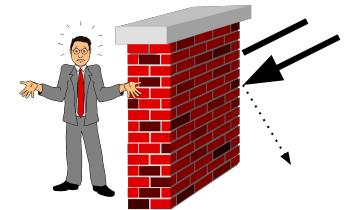
Diffraction



Réflexion



refraction



Shadowing

Environnement de Propagation Radio

- ❑ Atténuation
 - ✓ Lorsqu'elle traverse un obstacle, une partie de l'énergie de l'onde est absorbée
- ❑ Amplification
 - ✓ Lorsqu'il est capté par une antenne, la puissance du signal de l'onde est amplifié (répéteur du filaire)
- ❑ L'atténuation (ou le gain) est le rapport entre la puissance du signal avant et après modification

Environnement de Propagation Radio

(1) Atténuation (Path Loss)

- L'amplitude du signal diminue en fonction de la distance.

$$\frac{P_t}{P_r(d)} = PL(d) = PL(d_0) \left(\frac{d_0}{d} \right)^{-\eta} \quad (1)$$

où:

P_t : Puissance d'émission.

P_r : Puissance de réception.

d_0 : Distance référence.

d : Distance entre émetteur et récepteur.

η : est l'exposant d'atténuation.

- Le pathloss en [dB]:

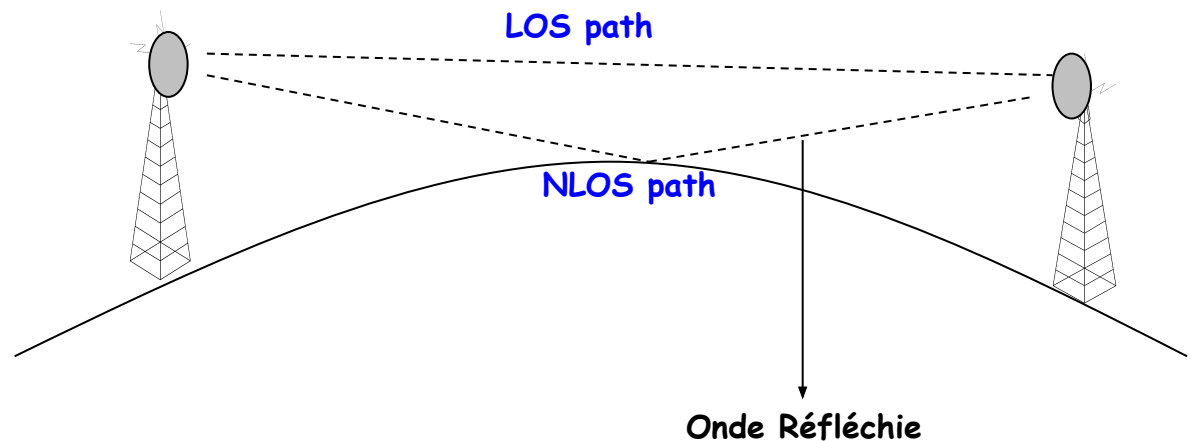
$$PL(d)[\text{dB}] = PL(d_0)[\text{dB}] + 10\eta \log_{10} \left(\frac{d}{d_0} \right) \quad (2)$$

Environnement de Propagation Radio

(2) Effets Multipath

(i) Shadowing

(ii) Fading



Environnement de Propagation Radio

(2) Effets Multipath

(i) Shadowing:

- ❑ La propagation sur le canal Phy est affectée non seulement par la distance mais aussi par des obstacles.
- ❑ D'où le phénomène de Shadowing, souvent dominant les Comm. à faible portée, telles que dans les WSNs.
- ❑ Le coefficient de Shadowing est caractérisé par une distribution Lognormale. D'où, la nouvelle formule du Pathloss:

$$PL(d) = PL(d_0)[\text{dB}] + 10\eta \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \quad (3)$$

X_σ , étant une variable aléatoire gaussienne centrée et de variance σ^2 .

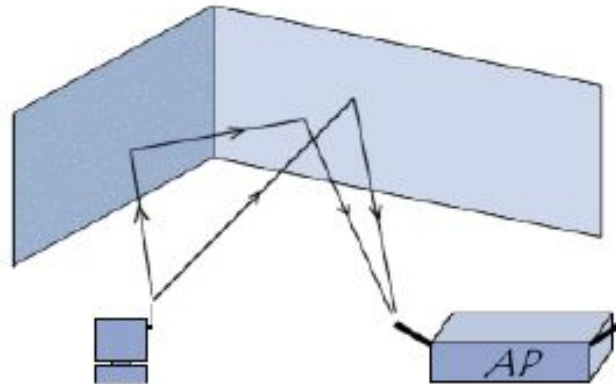
(ii) Fading:

- ❑ Présent surtout dans les zones urbaines, avec NLOS.
- ❑ Caractérisé par une distribution de type Rayleigh.

Environnement de Propagation Radio

❑ Chemins multiples (multipath)

- ✓ Par réflexions successives, une onde peut atteindre une station en empruntant des chemins multiples et générer des interférences
- ✓ La présence de deux antennes sur un point d'accès permet de contrôler et de séparer les signaux



Environnement de Propagation Radio

(3) Capacité du Canal

Source de distortion du Canal:

- (i) Bruit: intrinsèque du composant électronique (N_0).
- (ii) Interférence: dû au partage du canal dans un environnement multi-utilisateur.

Capacité du Canal

(i) Avec Bruit Blanc:

- Rapport Signal-Bruit

$$SNR(d) = \psi(d) = P_t - PL(d) - P_n \quad (4)$$

(ii) Avec Interference:

- Rapport Signal-(Bruit+Interférence)

$$SNIR \text{ [dB]} = 10 \log_{10} \left(\frac{P_r}{N_0 + \sum_{i=1}^k I_i} \right) \quad (5)$$

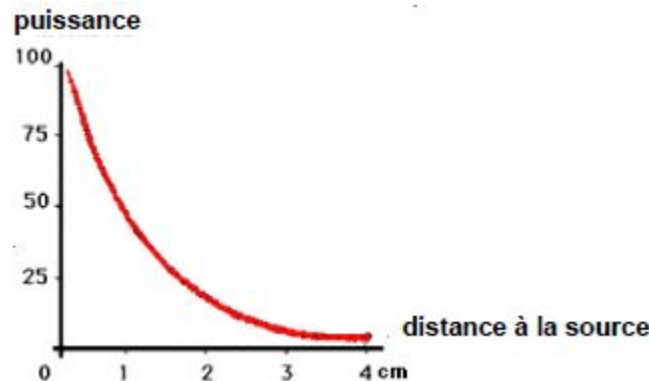
- Formule de Shannon (Débit Maximal):

$$R = W \log_2 \left(1 + \frac{SNIR}{\Gamma_0} \right) \quad (6)$$

Environnement de Propagation Radio

❑ Absorption des ondes

- ✓ L'énergie d'une onde électromagnétique est progressivement dégradée au cours de sa propagation dans l'air
- ✓ L'onde électromagnétique qui voyage rencontre des électrons qu'elle va exciter. Ceux-ci vont ré-émettre à leur tour du rayonnement ce qui perturbera le signal et donc l'atténuera.
- ✓ Les signaux se dégradent avec la distance et avec les obstacles, limitant ainsi la portée et le débit de la liaison



Environnement de Propagation Radio

❑ Ondes, fréquences et couverture

- ✓ Plus la fréquence est élevée plus le phénomène d'absorption est élevé, donc plus la distance de couverture est faible.
 - C'est pour cela que les communications radio se font sur des fréquences d'une centaine de MHz.
 - Pour le WiFi, par exemple on peut difficilement faire plus de 10km avec du matériel « classique ».
- ✓ Plus la fréquence est élevée, plus le débit de données peut être important mais plus la couverture est faible.
- ✓ Puissance élevée : couverture plus grande , mais la consommation d'énergie est plus grande.

Rappels sur les réseaux locaux sans fils : WiFi(802.11b)



❑ Le WiFi

- ✓ permet à des équipements informatiques de se connecter et d'échanger des données par voie radio
- ✓ s'intègre dans la pile IP (souscouche)



Rappels sur les réseaux locaux sans fils : WiFi(802.11b)



❑ Quelques données:

- ✓ **Débit** : Association de 11 Mbps. 50% de débit effectif.
- ✓ **Portée** : de quelques centaines de mètres à plusieurs km.

Ce résultat sera fonction de :

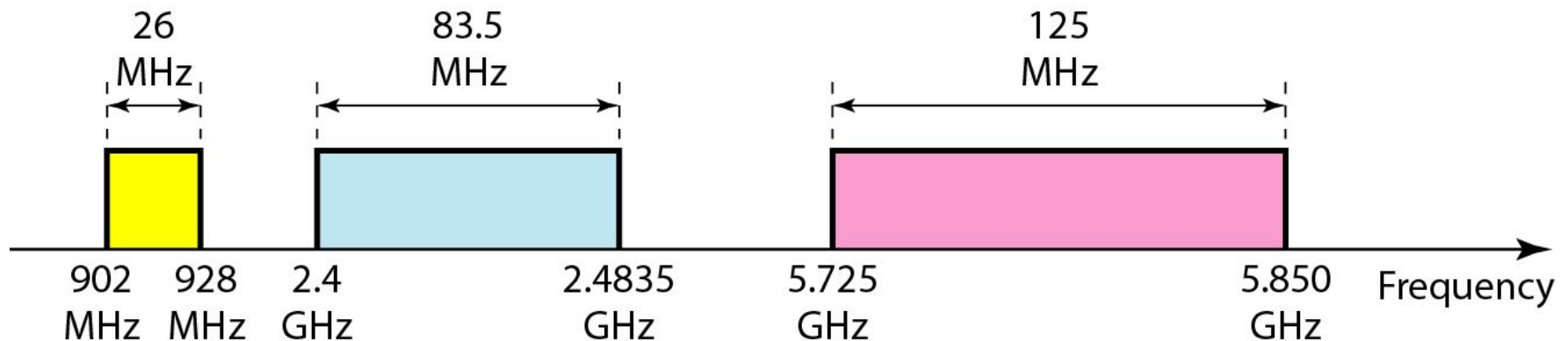
- la **puissance**_{em} : couples AP + antennes choisis
- la **sensibilité**_{rec} : inv proportionnelle au débit choisi
- **Affaiblissement**_{ligne} : masques radio et interférences
- ✓ **Puissance autorisée par l'ART (Autorité de Régulation des Télécommunications (<http://www.art-telecom.fr/>))**: 100 mW en sortie d'antenne pour les réseaux privés et indépendants.
- ✓ **Santé** : rayonnement 10 fois inférieur à celui d'un téléphone portable.

WiFi: 802.11

- ❑ IEEE 802.11: WLAN ("Wireless LAN"): se décompose en plusieurs normes avec des caractéristiques différentes (fréquence, débit, portée du signal radio, ...).
- ❑ IEEE 802.11b (Wi-Fi 2): 2,4 GHz.
 - ✓ Déployé principalement dans les aéroports, les gares, les campus universitaires et les entreprises (permet de connecter des laptops et d'autres équipements)
 - ✓ Les stations Wi-Fi 2 ont une portée de quelques dizaines de mètres à l'intérieur d'un bâtiment et de quelques centaines de mètres à l'extérieur.
 - ✓ Si la liaison n'est pas satisfaisante, le débit nominal de 11 Mbit/s peut se replier sur des débits inférieurs : 5,5 Mbit/s, 2 Mbit/s et 1 Mbit/s.
- ❑ IEEE 802.11g (Wi-Fi 5): Débits plus élevés que le Wi-Fi 2 (6 à 54 Mbit/s), compatible avec le Wi-Fi 2 (2.4 GHz).

La transmission sans fils

- ❑ Les WLANs utilisent des ondes radio ou infrarouges.
- ❑ Ils utilisent les bandes de fréquence sans licence suivantes:
 - ✓ ISM "Industrial Scientific and Medical" : 3 sous-bandes cédées en 1985 par l'armée US,



- ✓ U-NII "Unlicensed-National Information Infrastructure".
- ❑ Plusieurs techniques de transmission ont été définies afin de limiter les problèmes dus aux interférences et afin d'augmenter le débit

La transmission sans fils

❑ Caractéristiques :

- ✓ Plus la puissance d'émission est élevée, meilleure est la couverture, mais la consommation d'énergie est plus grande.
- ✓ Plus la fréquence radio est élevée, meilleur est le débit, mais la couverture est moins bonne.
- ✓ Plus le débit est élevé, plus la couverture radio est faible.
- ✓ Les signaux se comportent différemment dans l'environnement selon leur fréquence ; dans la gamme des micro-ondes :
 - les gouttes de pluie atténuent davantage les signaux à haute fréquence,
 - les micro-ondes sont en partie réfléchies par la plupart des objets. Un signal peut être réfléchi plusieurs fois, le récepteur capte donc plusieurs signaux avec de légers décalages de temps,
 - au-delà de 5 GHz (le haut du spectre des micro-ondes), les ondes ne pénètrent quasiment plus les objets. L'émetteur et le récepteur doivent être en vue directe sans obstacle « *clear line of sight* ».

Environnement de Propagation Radio

- ❑ Notion de propagation radio: Les ondes radio se propagent en ligne droite dans plusieurs directions depuis leur source d'émission
- ❑ Leur vitesse dans le vide est de $3 \cdot 10^8$ m/s
- ❑ Lorsqu'elle rencontre un obstacle, l'onde est divisée et son énergie est répartie.

Signal Propagation Ranges

❑ Rayon de transmission (transmission range)

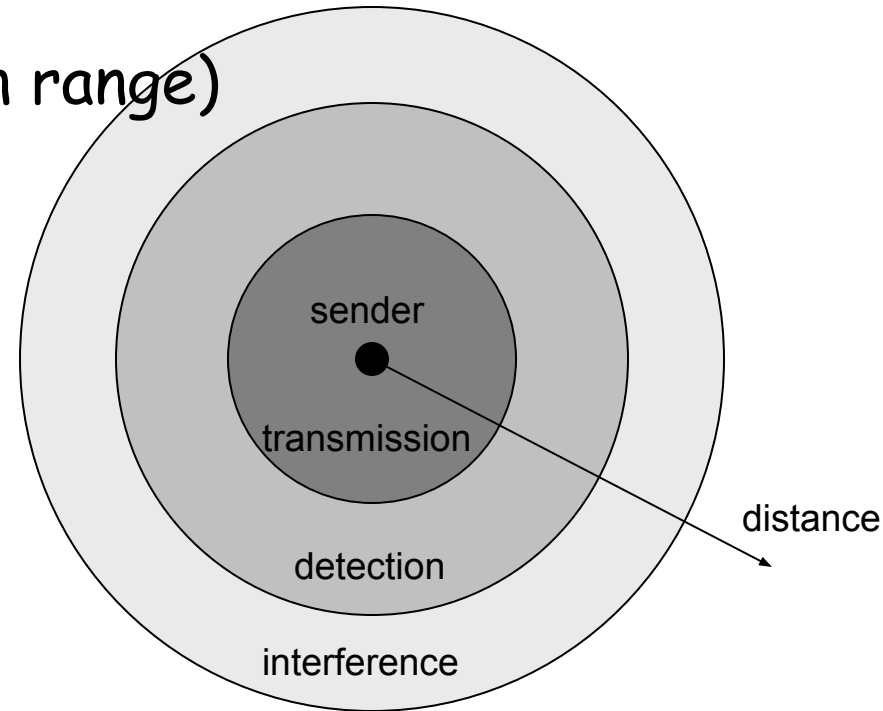
- ✓ communication possible
- ✓ Taux d'erreur faible

❑ Rayon de détection (Detection range)

- ✓ détection du signal possible
- ✓ communication impossible

❑ Rayon d'interférence (Interference range)

- ✓ Les signaux peuvent ne pas être détectés
- ✓ Les signaux ajoutent du bruit



Note: These are **not** perfect spheres in real life!

Environnement de Propagation Radio

❑ Causes de distorsion du signal (Nature du Canal radio):

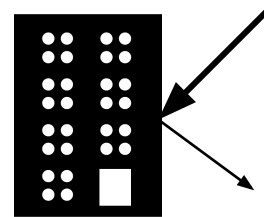
- Atténuation (dûe à la distance)
- Réflexion et Réfraction (nature et densité de surface)
- Diffraction
- Shadowing: blocage du signal



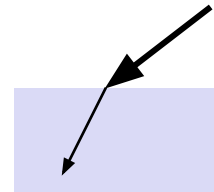
Diffraction



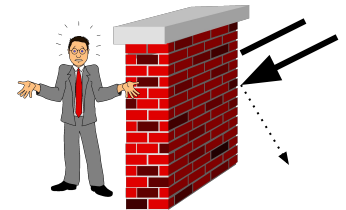
Diffraction



Réflexion



refraction



Shadowing

Environnement de Propagation Radio

❑ *Ondes, fréquences et couverture*

- ✓ Plus la fréquence est élevée plus le phénomène d'absorption est élevé, donc plus la distance de couverture est faible.
 - C'est pour cela que les communications radio se font sur des fréquences d'une centaine de MHz.
 - Pour le WiFi, par exemple on peut difficilement faire plus de 10km avec du matériel « classique ».
- ✓ Plus la fréquence est élevée, plus le débit de données peut être important mais plus la couverture est faible.
- ✓ Puissance élevée : couverture plus grande , mais la consommation d'énergie est plus grande.

Origines des WLAN

- ❑ Nouveau besoin des utilisateurs : la mobilité
 - ⇒ Développement et commercialisation d'équipements portables munis de liaisons radio ou infrarouges

WLAN (Wireless LAN, LAN sans fil) :
Système local offrant un moyen de communication direct entre plusieurs ordinateurs portables par liaison radio.

- Insuffisance des méthodes d'accès existants pour les réseaux filaires
 - ⇒ Besoin de protocoles d'accès spécifiques

Utilisation des WLAN

- ❑ Mobilité : augmente l'efficacité et la productivité
- ❑ Installation dans zones difficiles à câbler
 - ✓ Immeubles anciens
 - ✓ Halls, salles de réunion, cafés, lieux publics
 - ✓ Réseaux temporaires
- ❑ Temps d'installation réduits
- ❑ Facilité d'emploi pour les utilisateurs
- ❑ Maintenance facile, coût de câblages faibles
- ❑ Réseaux ad-hoc : réunions, interventions militaires et humanitaires et en cas de catastrophes naturelles

Matériel pour WLAN

Le matériel employé:

- ✓ Points d'accès (eq. switch)
- ✓ Cartes clientes (éq. carte réseau)
- ✓ Antennes et connectiques
- ✓ Matériel Ethernet



Les problèmes spécifiques aux transmissions sans fil

- ❑ **Interférences** : Les bandes de fréquences utilisées sont les mêmes que les fréquences de travail des fours micro-ondes, et d'autres normes (Bluetooth)
- ❑ **Sécurité** : Les informations transitent « dans l'air ». Sans précaution particulière, tout récepteur équipé d'une antenne peut : lire les données, les modifier, se connecter au réseau. 3 problèmes : confidentialité, intégrité, authentification.
- ❑ **Roaming** (handover): un utilisateur mobile peut quitter la portée d'un point d'accès.
- ❑ **Consommation de puissance** : Les équipements mobiles ont une batterie de faible capacité. L'énergie doit être économisée.
- ❑ **Réglementation des émissions** : on n'émet pas à n'importe quelle fréquence ni à n'importe quelle puissance !

Réglementation des émissions en France

- ❑ A l'intérieur des bâtiments
 - ✓ pas d'autorisation préalable
 - ✓ bande 2,4465 - 2,4835GHz pour 100mW
 - ✓ bande 2,4 - 2,4835GHz pour 10mW

- ❑ A l'extérieur des bâtiments dans un domaine privé :
 - ✓ Autorisation obligatoire auprès de l'ART
 - ✓ Bande 2,4465 - 2,4835GHz

- ❑ Sur le domaine public : règles édictées par l'ART (Autorité de Régulation des Télécommunications)

les réseaux locaux sans fils : WiFi(802.11b)



❑ Le WiFi

- ✓ permet à des équipements informatiques de se connecter et d'échanger des données par voie radio
- ✓ s'intègre dans la pile IP (souscouche)



les réseaux locaux sans fils : WiFi(802.11b)



❑ Quelques données:

- ✓ **Débit** : Association de 11 Mbps. 50% de débit effectif.
- ✓ **Portée** : de quelques centaines de mètres à plusieurs km.

Ce résultat sera fonction de :

- la **puissance**_{em} : couples AP + antennes choisis
- la **sensibilité**_{rec} : inv proportionnelle au débit choisi
- **Affaiblissement**_{ligne} : masques radio et interférences
- ✓ **Puissance autorisée par l'ART (Autorité de Régulation des Télécommunications (<http://www.art-telecom.fr/>))**: 100 mW en sortie d'antenne pour les réseaux privés et indépendants.
- ✓ **Santé** : rayonnement 10 fois inférieur à celui d'un téléphone portable.

La norme IEEE 802.11: introduction

Norme IEEE 802.11 ? WiFi?



- ❑ La norme **IEEE 802.11** (ISO/IEC 8802-11) est un **standard international** décrivant les caractéristiques d'un réseau local sans fil.
- ❑ WiFi est un nom commercial correspondant à la norme IEEE 802.11
- ❑ **WiFi ou Wi-Fi** : contraction de *Wireless Fidelity*, correspond initialement au nom donnée à la certification délivrée par la **WI-FI Alliance**, anciennement WECA (*Wireless Ethernet Compatibility Alliance*).
 - ✓ La Wi-Fi Alliance est l'organisme chargé de maintenir **l'interopérabilité** entre les matériels répondant à la norme 802.11.
 - ✓ Le nom de la norme se confond aujourd'hui avec le nom de la certification.
 - ✓ Matériels certifiés par la Wi-Fi Alliance identifiés par le logo

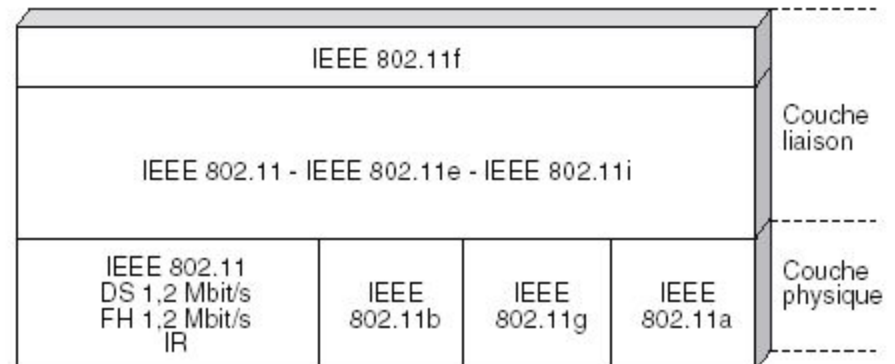


La norme IEEE 802.11



- ❑ La norme IEEE 802.11 est en réalité **la norme initiale**, développée en 1997, offrant des débits de 1 ou 2 Mbps.
- ❑ Des révisions ont été apportées à la norme originale afin d'optimiser le débit, la sécurité ou l'interopérabilité (voir tableau suivant).
- ❑ Les extensions de la norme IEEE 802.11 **utilisent toute le même protocole d'accès au canal** : le protocole CSMA/CA (Carrier Sense Multiple Access). Certaines extensions modifient la couche physique, d'autres rajoutent des fonctionnalités au niveau liaison.

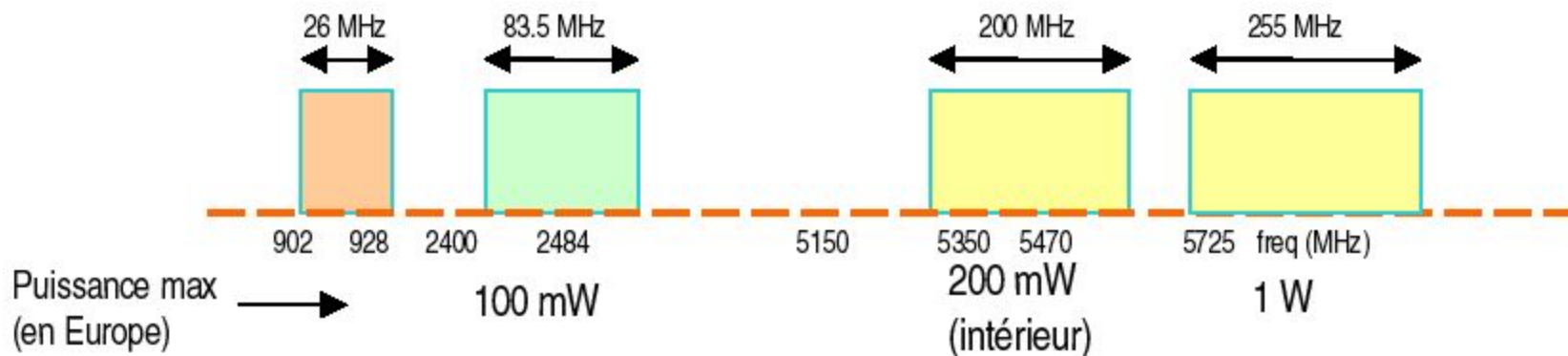
Organisation des différentes extensions de la norme IEEE 802.11



La norme IEEE 802.11



- ❑ Ces normes IEEE 802.11 utilisent les bandes ISM (*Industrial, Scientific and Medical*), allouées à travers le monde pour des opérations sans licences.
- ✓ La bande « des 2.4 GHz » : 83 MHz alloués aux WLAN
- ✓ La bande « des 5GHz » : 200 MHz alloués aux WLAN



La bande ISM

Les principales normes IEEE 802.11

802.11a (WiFi5)	1999	54 Mbit/s théoriques Bande des 5 GHz Incompatible avec 802.11b, g et n
802.11b (WiFi)	Septembre 1999	11 Mbit/s théoriques Bande des 2.4GHz
802.11g	Juin 2003	54 Mbit/s théoriques Bande des 2.4 GHz Compatibilité ascendante avec la norme 802.11b
802.11i	Juin 2004	Améliore la sécurité des transmissions S'appuie sur l' <i>AES (Advanced Encryption Standard)</i> Chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11n	Ratification prévue fin 2006 mais...!	Evolution rétrocompatible des normes 802.11b/g. Débits de 300 Mbit/s

Autres normes IEEE 802.11



802.11d	Pour une utilisation internationale des réseaux locaux 802.11, permet aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11c	Modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau <i>liaison de données</i>).
802.11e	Introduction de qualité de service au niveau de la couche <i>liaison de données</i> .
802.11f	Recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits.
802.11h	Conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie

Les normes concurrentes d'IEEE 802.11

- ❑ Bluetooth (IEEE 802.15) : Pas vraiment concurrente, car Bluetooth concerne les WPAN et non les WLAN.
- ❑ Hiperlan/2 (*High Performance Radio LAN*) : La concurrente européenne de la norme IEEE 802.11. Même couche physique que IEEE 802.11a. Pas d'applications commerciales.
- ❑ Zigbee (802.15.4): destinée pour les réseaux de capteurs

La norme IEEE 802.11: architecture

Architecture physique : deux modes de configuration



☐ Mode infrastructure

- ✓ Les hôtes dans fil sont organisés en cellules autour d'un point d'accès
- ✓ Les points d'accès sont eux-mêmes connectés à un réseau local filaire.
- ✓ La communication entre deux hôtes de deux cellules distinctes passe via les point d'accès par le réseau filaire.

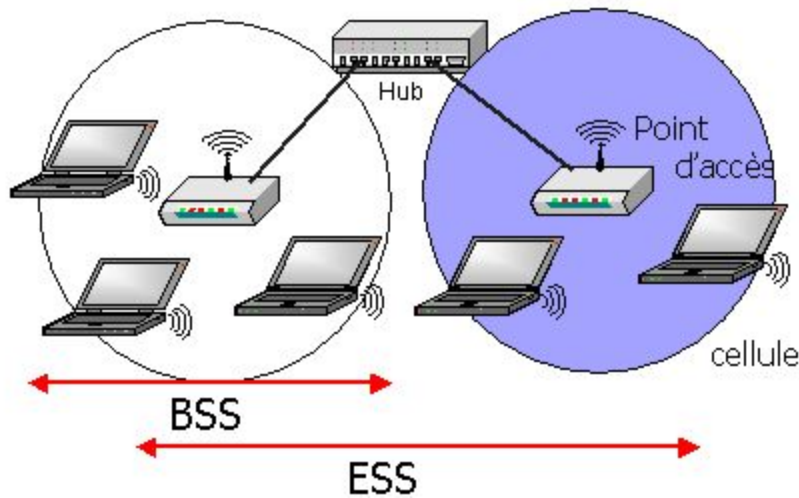
☐ Mode sans infrastructure (= mode ad hoc)

- ✓ Pas de point d'accès
- ✓ Chaque hôte sans fil fait office de routeur pour acheminer les communications

Le mode infrastructure



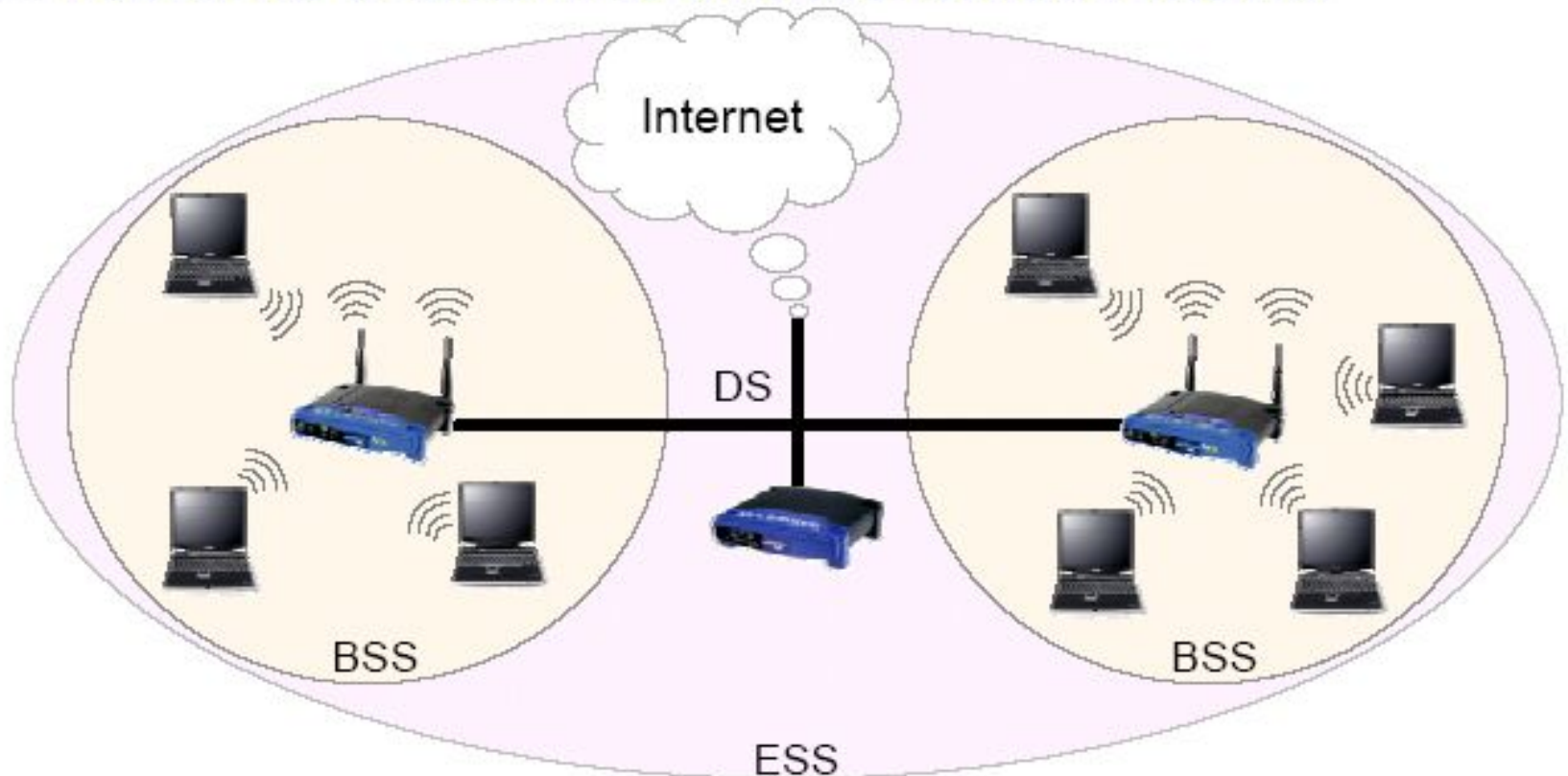
- ❑ Des points d'accès sont **connectés au réseau local filaire**. Chacun définit une cellule.
- ❑ Centralisation de toutes les fonctionnalités au sein de l'AP
 - ✓ **Cellule** = BSS (*Basic Service Set*)
 - ✓ Les communications émises par toutes les stations passent par un **point d'accès** (AP *Access Point*) : il peut y avoir un ou plusieurs AP.
 - ✓ Les AP sont interconnectés par le DS (*Distribution System*), par exemple Ethernet.
 - ✓ Les BSS connectés en sous-réseau constituent l'ESS (*Extended Service Set*).



ESS



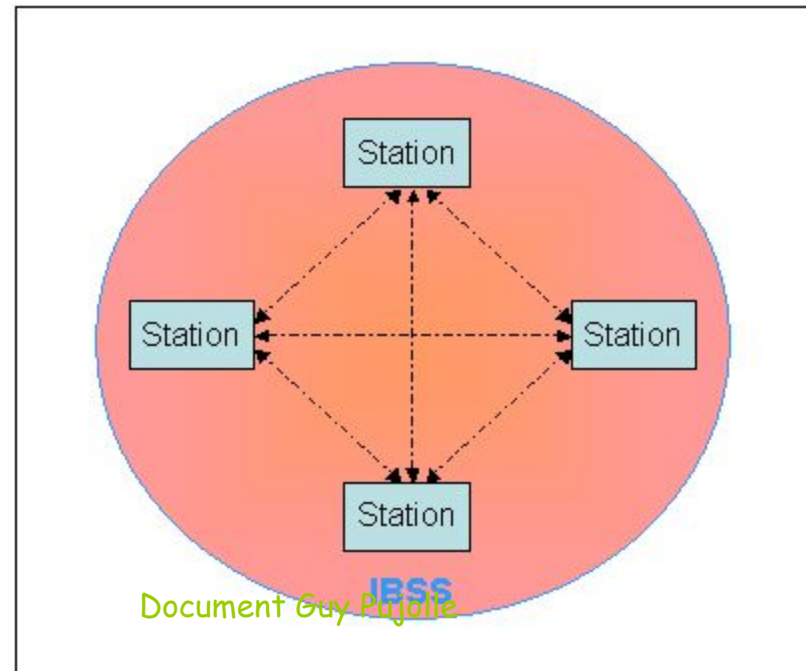
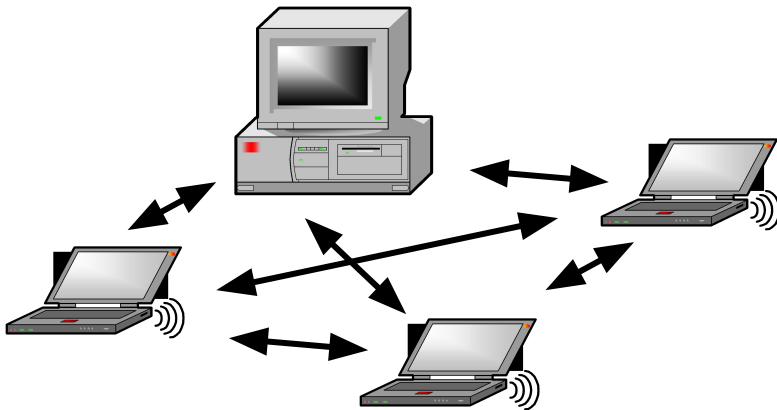
- Wi-Fi** Extended Service Set : plusieurs points d'accès (BSS) connectés entre eux par un système de distribution (DS)
- Wi-Fi** DS : Ethernet ou un autre réseau WLAN
- Wi-Fi** Fourniture d'accès vers un autre réseau : Internet



Le mode sans infrastructure (ad hoc)

❑ **Mode ad hoc** : Mode sans infrastructure.

- ✓ Réalise un réseau poste à poste (chaque poste peut communiquer avec chacun des autres postes).
- ✓ Un poste fait à la fois office d'hôte et de routeur.
- ✓ Également appelé IBSS (*Independent Basic Service Set*).

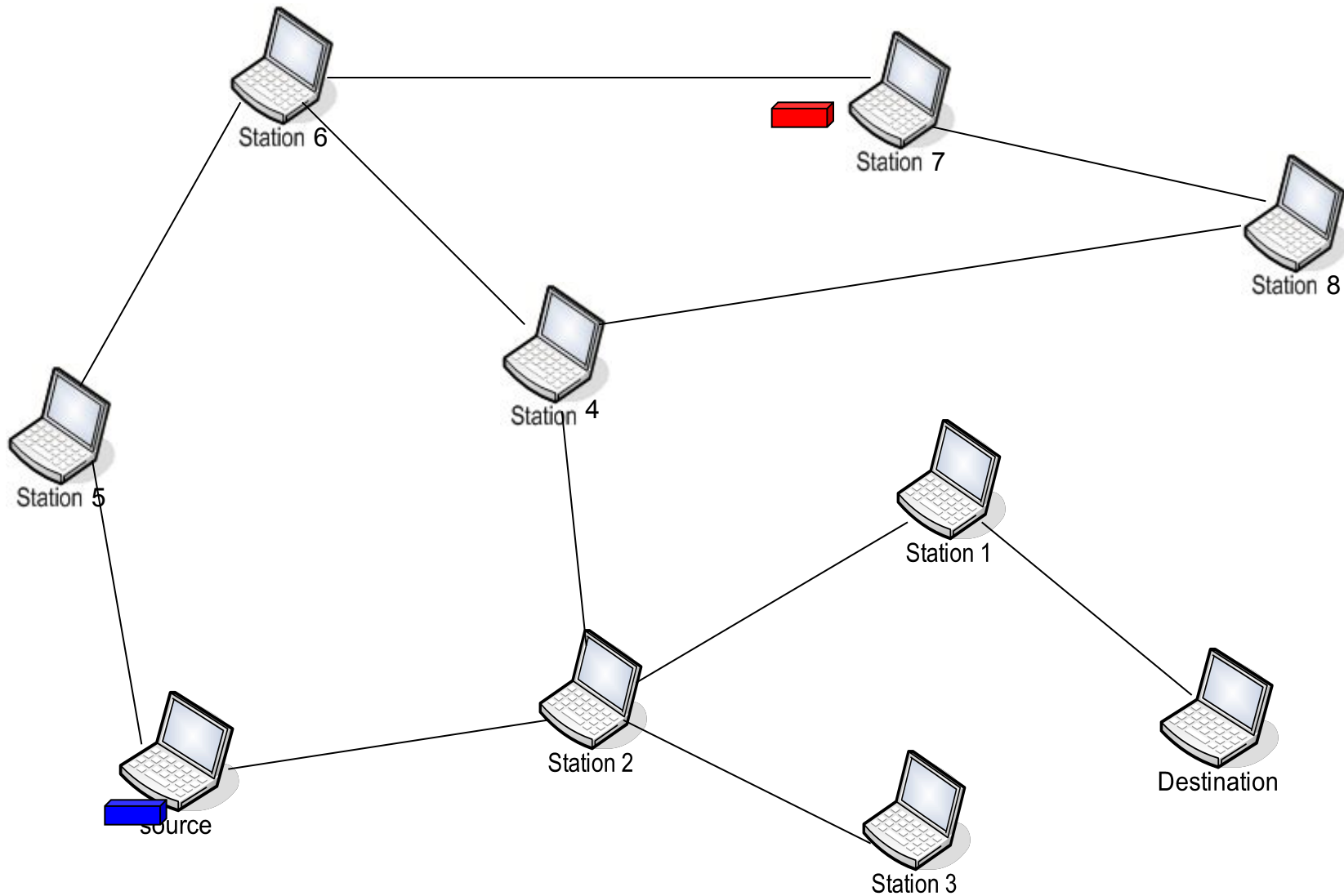


IBSS mode Ad Hoc



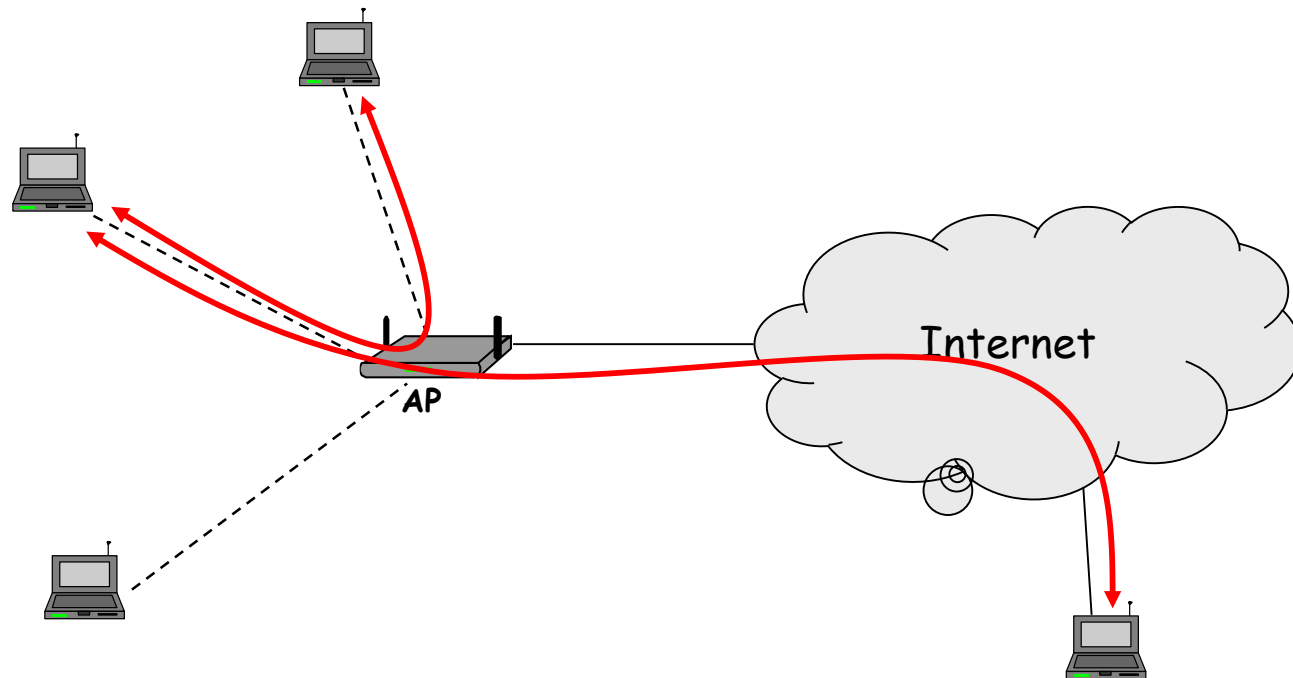
- ❑ Les réseaux Ad-Hoc sont des réseaux caractérisés par:
 - ✓ Une topologie dynamique
 - ✓ Autonomie des nœuds
 - ✓ Fonctionnalités distribuées
 - ✓ Une bande passante limitée
 - ✓ L'absence d'infrastructure
 - ✓ Des contraintes d'énergie
- ❑ Tous les nœuds se comportent comme des routeurs

IBSS mode Ad Hoc



La norme IEEE 802.11: La couche liaison de données- méthode d'accès

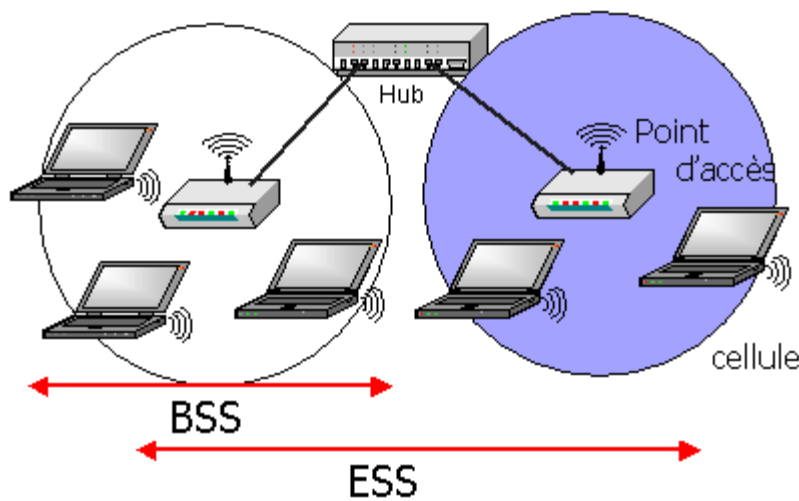
BSS: mode avec infrastructure



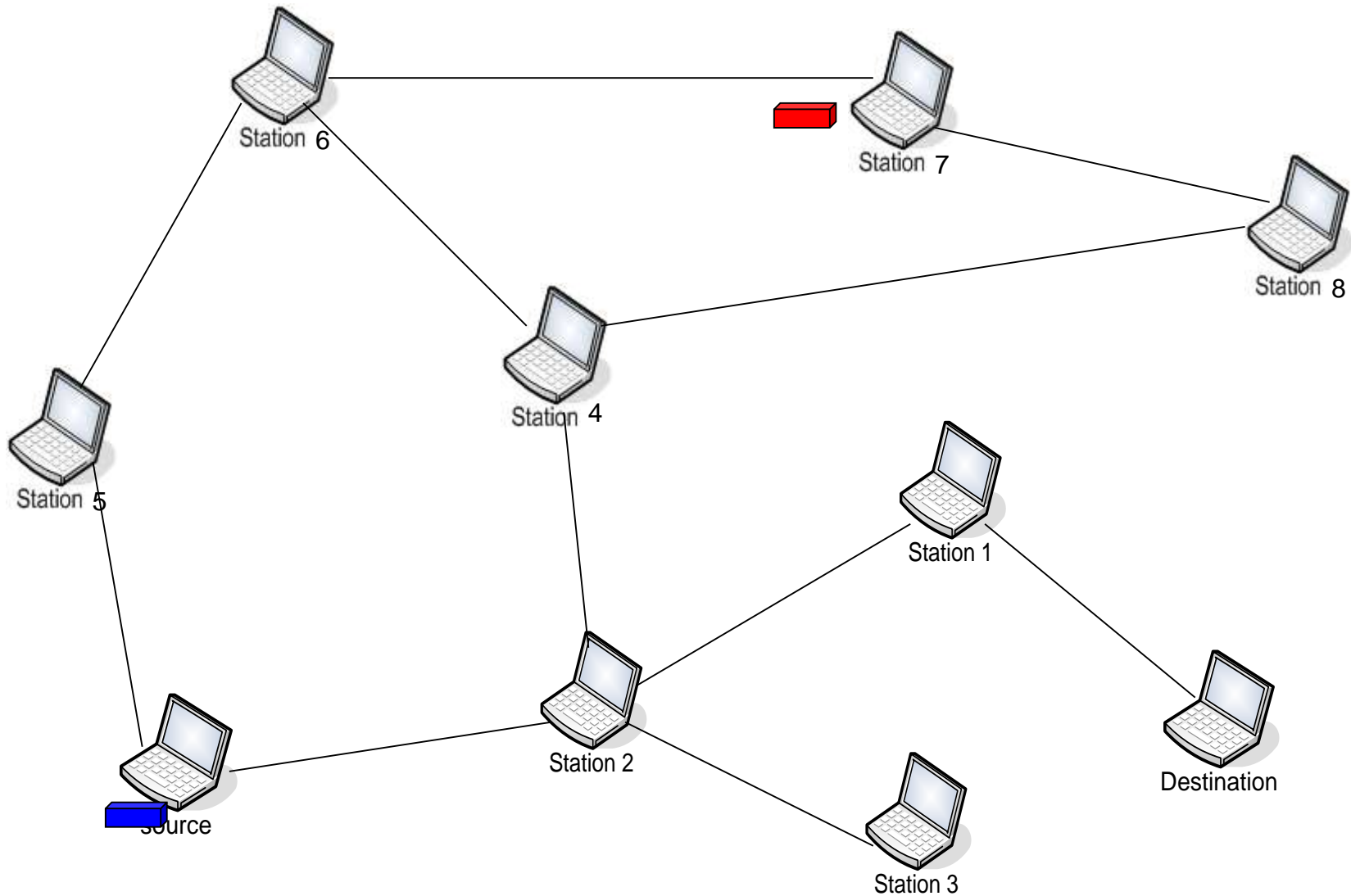
Le mode infrastructure



- ❑ Des points d'accès sont **connectés au réseau local filaire**. Chacun définit une cellule.
- ❑ Centralisation de toutes les fonctionnalités au sein de l'AP
 - ✓ **Cellule** = BSS (*Basic Service Set*)
 - ✓ Les communications émises par toutes les stations passent par un **point d'accès** (AP *Access Point*) : il peut y avoir un ou plusieurs AP.
 - ✓ Les AP sont interconnectés par le DS (*Distribution System*), par exemple Ethernet.
 - ✓ Les BSS connectés en sous-réseau constituent l'ESS (*Extended Service Set*).



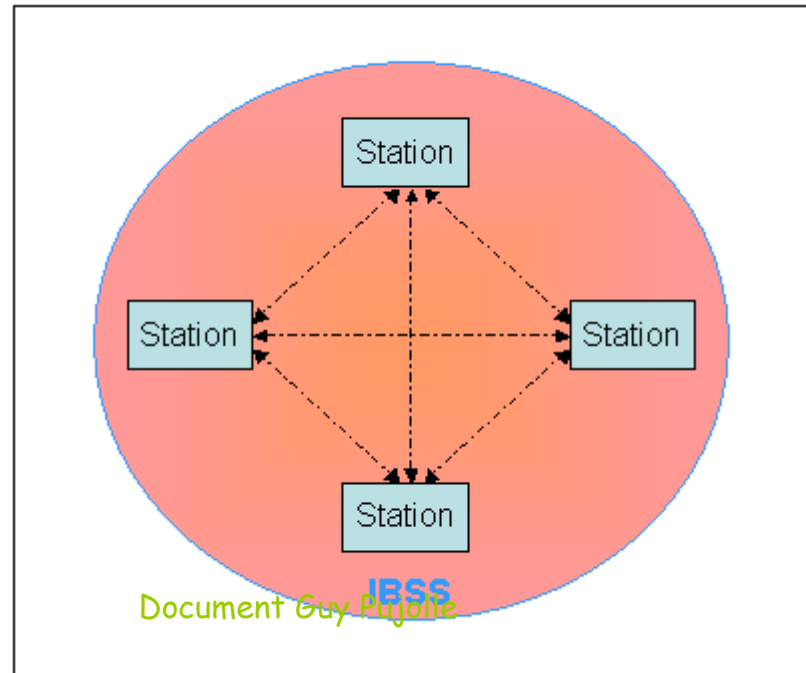
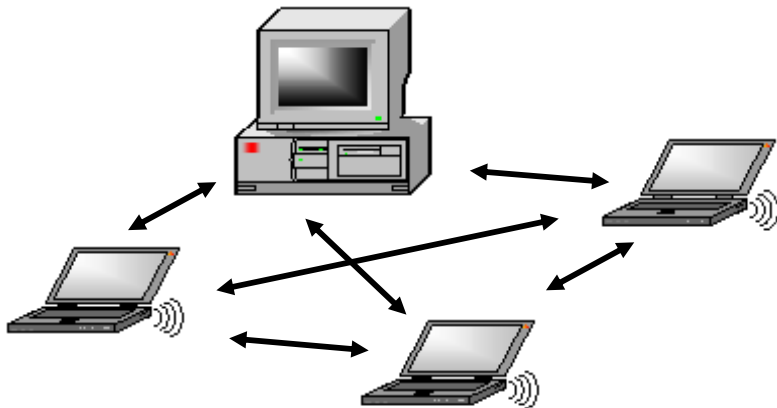
IBSS mode Ad Hoc



Le mode sans infrastructure (ad hoc)

❑ **Mode ad hoc** : Mode sans infrastructure.

- ✓ Réalise un réseau poste à poste (chaque poste peut communiquer avec chacun des autres postes).
- ✓ Un poste fait à la fois office d'hôte et de routeur.
- ✓ Également appelé IBSS (*Independent Basic Service Set*).



IBSS mode Ad Hoc



- ❑ Les réseaux Ad-Hoc sont des réseaux caractérisés par:
 - ✓ Une topologie dynamique
 - ✓ Autonomie des nœuds
 - ✓ Fonctionnalités distribuées
 - ✓ Une bande passante limitée
 - ✓ L'absence d'infrastructure
 - ✓ Des contraintes d'énergie
- ❑ Tous les nœuds se comportent comme des routeurs

Méthodes d'accès au support

- ❑ Deux méthodes d'accès au support sont normalisées (couche liaison de données)
- ❑ La **coordination distribuée** (DCF, *Distributed Coordination Function*) utilise le protocole **CSMA/CA** avec **VCS**.
- ❑ La **coordination centralisée** (PCF, *Point Coordination Function*) est une méthode de temps partagé de type **maître-esclave** : l'AP est le maître et attribue le temps de parole aux stations esclaves.

Méthodes d'accès : Avantages et inconvénients

❑ La méthode centralisée

- ✓ 😊 Elle est mieux adaptée aux flux de type « temps réel ».
- ✓ 😞 Mais son efficacité diminue avec la mise en veille des postes et leur changement de cellule.

❑ La méthode distribuée

- ✓ 😊 Elle est mieux adaptée à un trafic déséquilibré entre les postes.
- ✓ 😞 Elle est moins efficace pour les trafics temps réel.

❑ Le choix est déterminé par le point d'accès qui informe les postes.

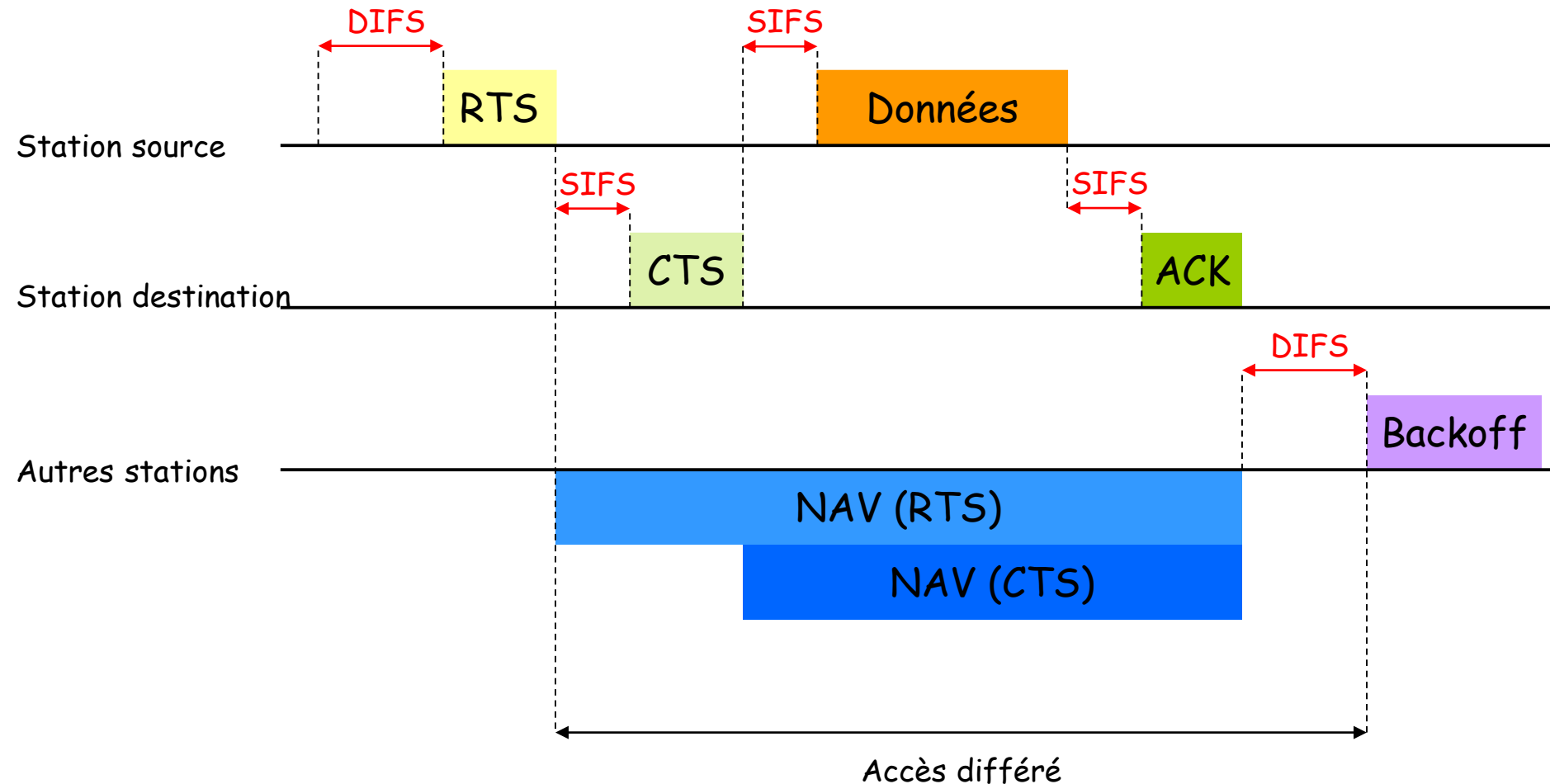
Le protocole CSMA/CA

- ❑ *Carrier Sense Multiple Access with Collision Avoidance*
- ❑ C'est le protocole CSMA avec « en mode fiable ».
- ❑ Quand une station veut émettre, elle écoute le support
 - ✓ S'il est occupé, la transmission est différée (retardée)
 - ✓ Si le support est libre durant un temps spécifique (DIFS), alors la station est autorisée à transmettre.
- ❑ La station réceptrice vérifie le CRC du paquet reçu et renvoie un accusé de réception (ACK).
 - ✓ Pour l'émetteur, ACK reçu = aucune collision n'a eu lieu
 - ✓ Sinon, l'émetteur retransmet le fragment.

La partie « Virtual Carrier Sense »

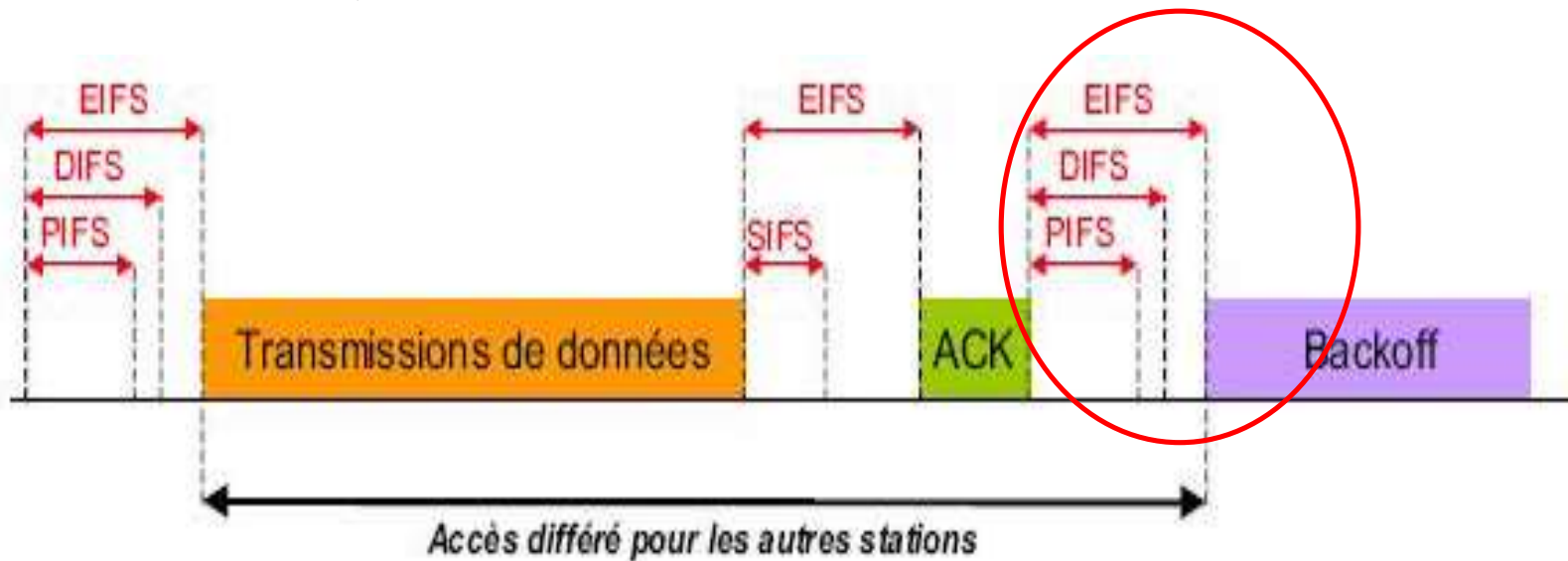
- ❑ Le VCS consiste à « réserver » le support avant émission.
- ❑ Avant de transmettre, si le support est libre après DIFS
 - ✓ L'émetteur émet une trame RTS (@src, @dest, durée transaction(paquet+ACK))
 - ✓ Si le support est libre, le récepteur émet un CTS
 - ✓ Toute station entendant le RTS ou le CTS déclenche son NAV (Network Allocation Vector) et se tait pendant toute la durée de la communication.
- ❑ La probabilité de collision par une station cachée de l'émetteur est limitée à la courte durée du RTS.
- ❑ Si données courtes, pas de RTS ni CTS.
- ❑ Si collision, exécuter un algorithme de Backoff Exponentiel

Bilan : Utilisation des IFS et de l'algorithme du backoff dans le DCF



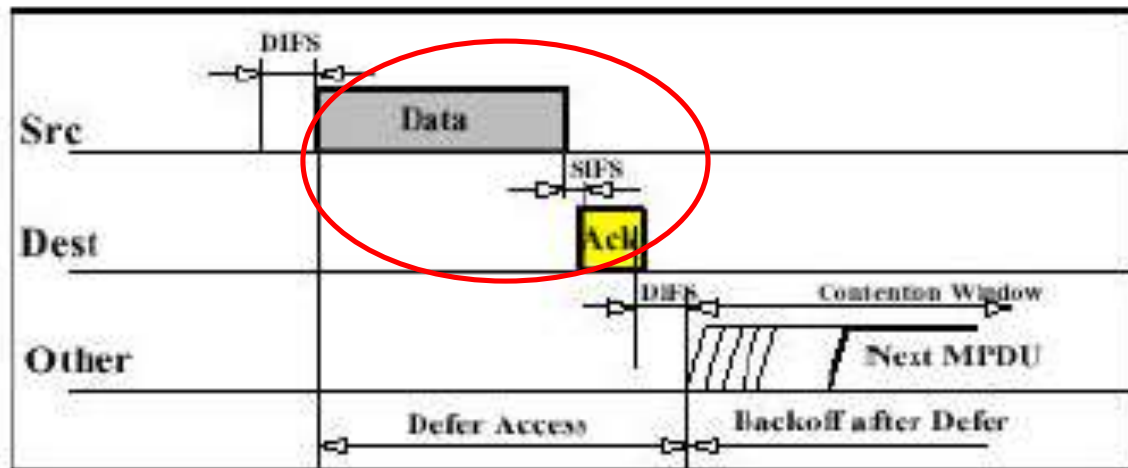
Inter Frame Space

- ❑ 4 types de temps inter-frames
 - ✓ SIFS
 - ✓ PIFS
 - ✓ DIFS
 - ✓ EIFS



Inter Frame Space

- ❑ **SIFS (Short Inter Frame Space)** est utilisé pour séparer les transmissions appartenant à un même dialogue (eg. Fragment - Ack).
- ✓ **C'est le plus petit écart entre deux trames**
- ✓ Il y a toujours, au plus, une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres
- ✓ Valeur fixée par la couche physique et calculée de sorte que l'émetteur puisse commuter en mode réception pour pouvoir décoder le paquet entrant.
- ✓ Pour la couche physique FH de 802.11, 28 microsecondes.



Inter Frame Space

❑ PIFS (*Point Coordination IFS*)

- ✓ Utilisé par l'AP pour gagner l'accès au support avant n'importe quelle autre station
- ✓ Cette valeur est SIFS plus un certain temps (Slot Time), soit 78 microsecondes.

❑ DIFS (*Distributed IFS*)

- ✓ Utilisé par une station voulant commencer une **nouvelle** transmission
- ✓ Calculé comme étant PIFS plus un temps, soit 128 microsecondes.

❑ EIFS (*Extended IFS*)

- ✓ **L'IFS le plus long.**
- ✓ Utilisé par une station recevant un paquet qu'elle ne comprend pas.
- ✓ Ceci est nécessaire pour éviter que la station (celle qui ne comprend pas l'information de durée pour le *Virtual Carrier Sense*) ne provoque de collision avec un futur paquet du dialogue en cours.

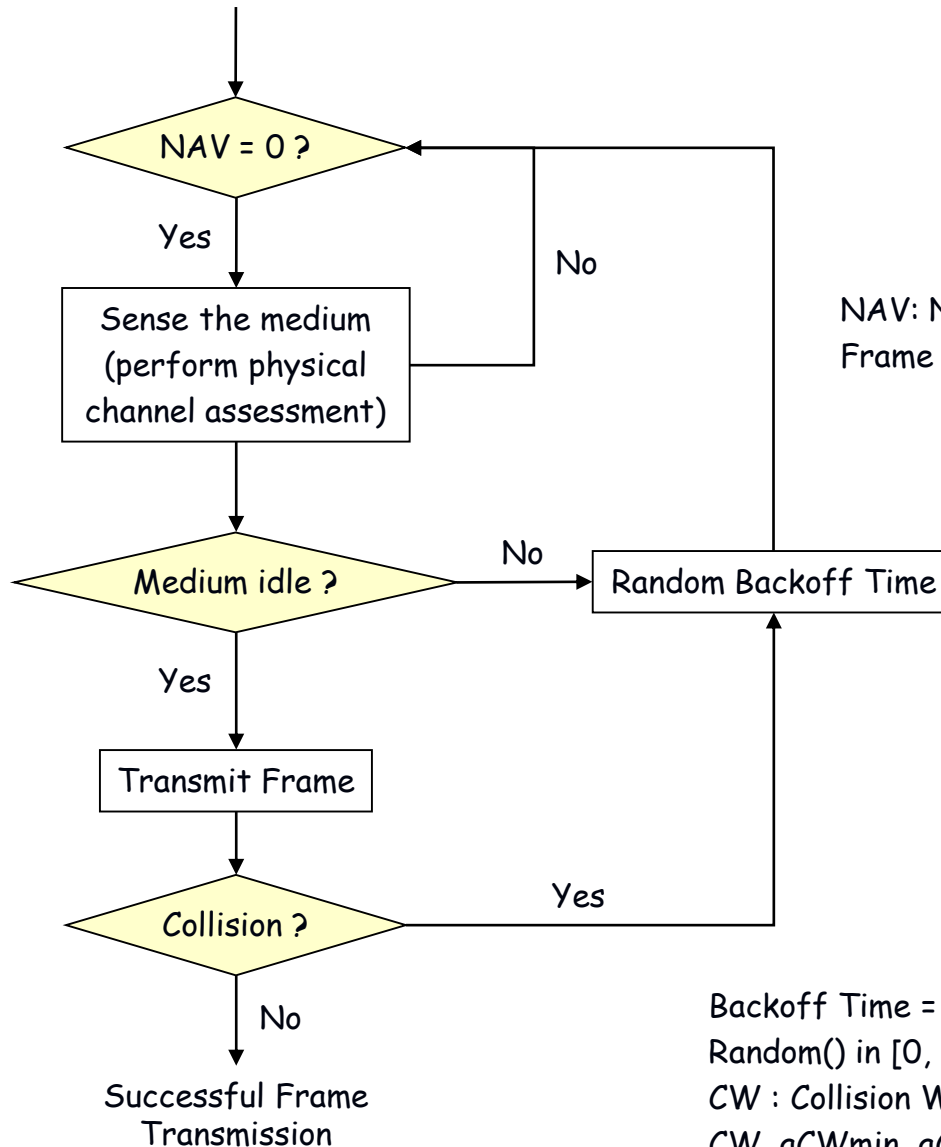
Algorithme de Backoff Exponentiel

- ❑ Algorithme permettant de tirer un temps d'attente aléatoire avant émission
 - ✓ Tirage d'un nombre n appartenant à un intervalle entier déterminé $[0; N_{\max}]$
 - ✓ Attente de $n \times T_{\text{slot}}$ (T_{slot} : temps prédéterminé)
 - ✓ Puis émission si canal libre
 - ❑ Backoff « exponentiel » : à chaque fois qu'une station choisit un slot et provoque une collision, N_{\max} est augmenté exponentiellement.
- ❑ Algorithme est appliqué
 - ✓ Quand une station écoute le support avant la 1ère transmission d'un paquet et qu'il est occupé
 - ✓ Après chaque retransmission
 - ✓ Après une transmission réussie
- ❑ Non utilisé si le support a été libre pendant une durée $> DIFS$

DCF - CSMA/CA

CSMA/CA
DCF

Start (Frame needing transmission)

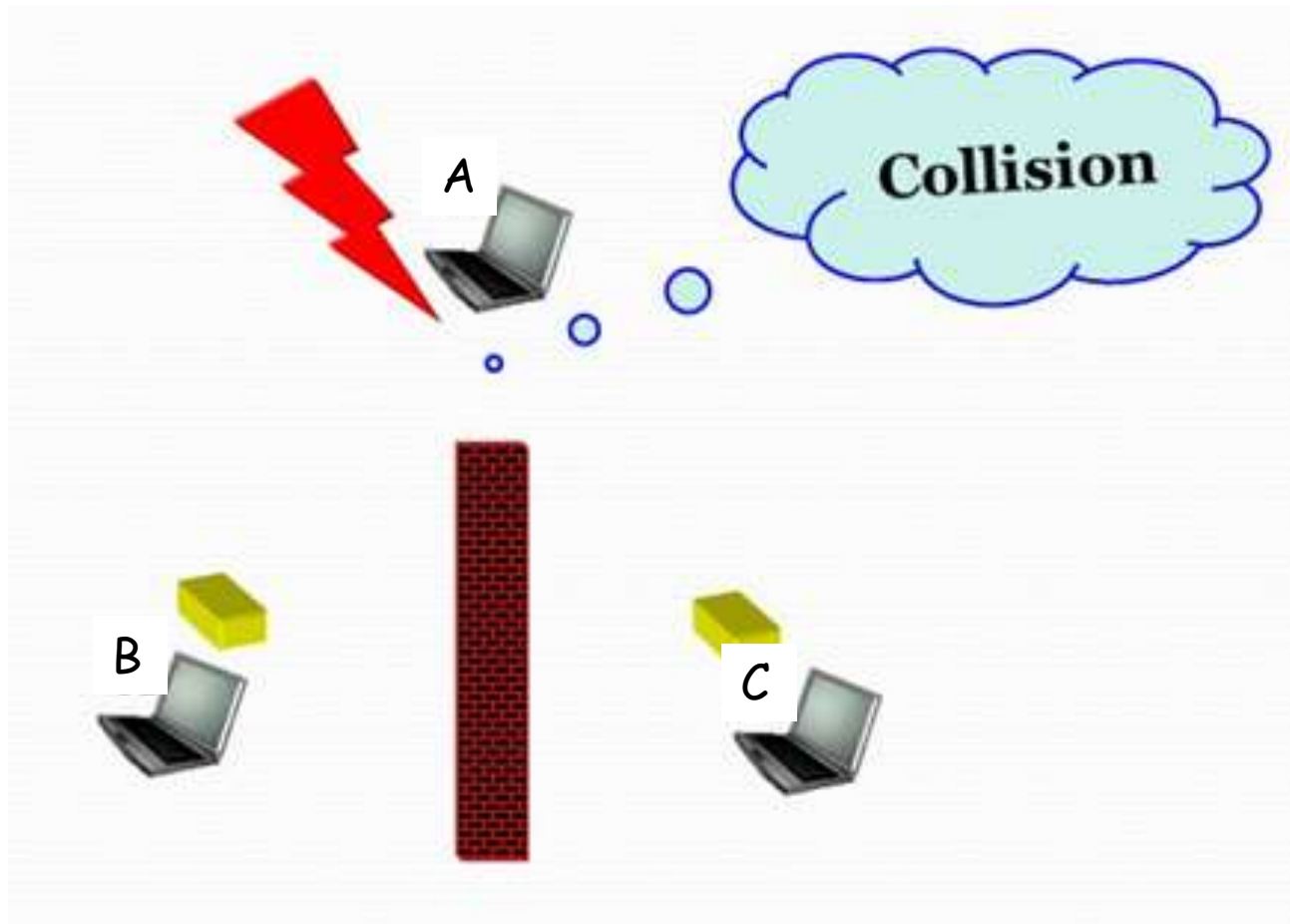


NAV: Network Allocation Vector
Frame Duration Field

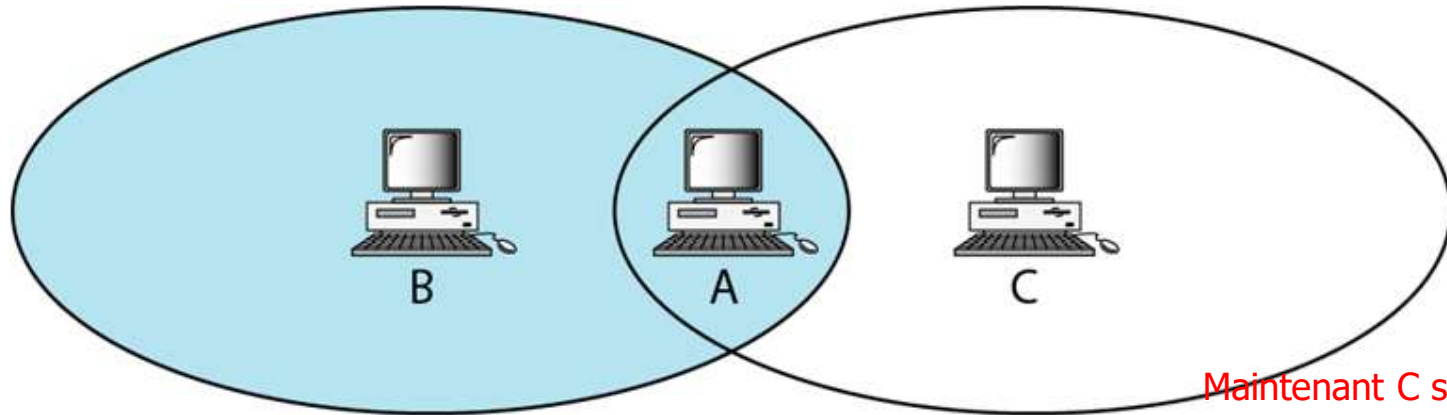
Backoff Time = Random() * aSlotTime
Random() in [0, CW]
CW : Collision Window in [aCWmin, aCWmax]
CW, aCWmin, aCWmax, aSlotTime in MIB

DCF: problème des nœuds cachés

- ❑ B et C ont tous les 2 des données à envoyer vers A
- ❑ B et C écoutent le canal et ils le trouvent libre donc les 2 sources procèdent à leurs transmissions vers A → collision

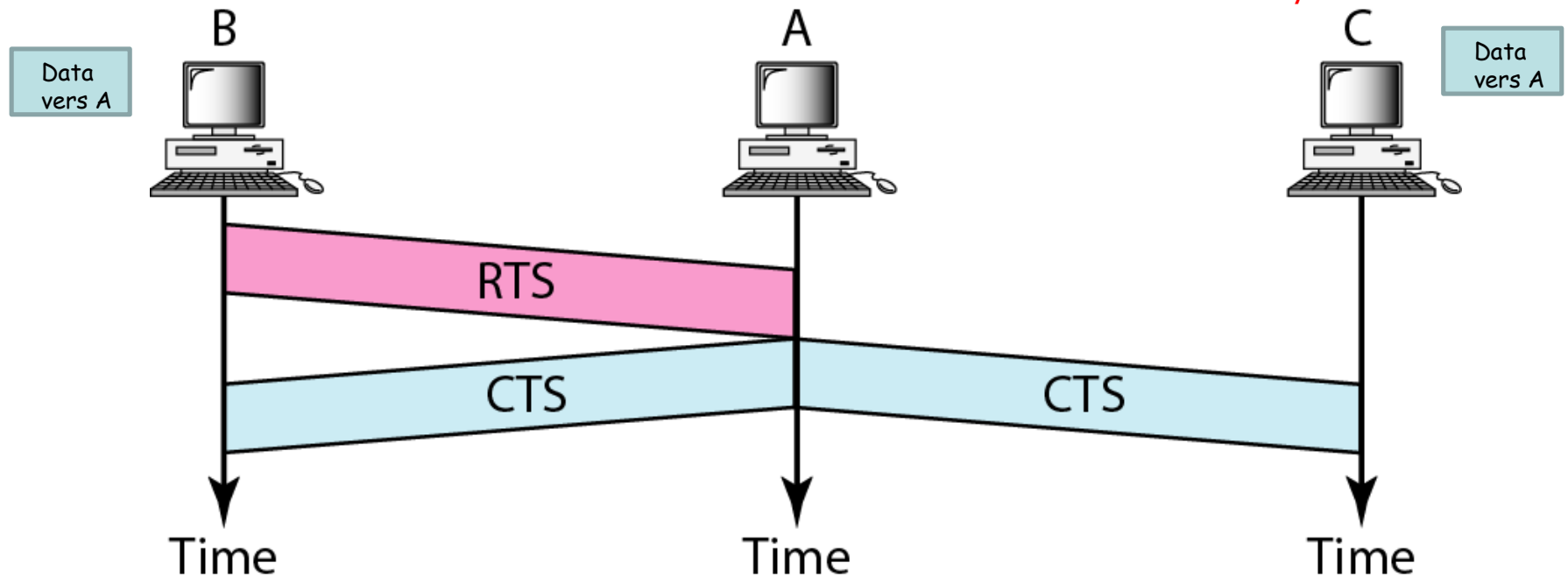


Problème des nœuds cachés: La solution RTS/CTS



Problème du terminal caché

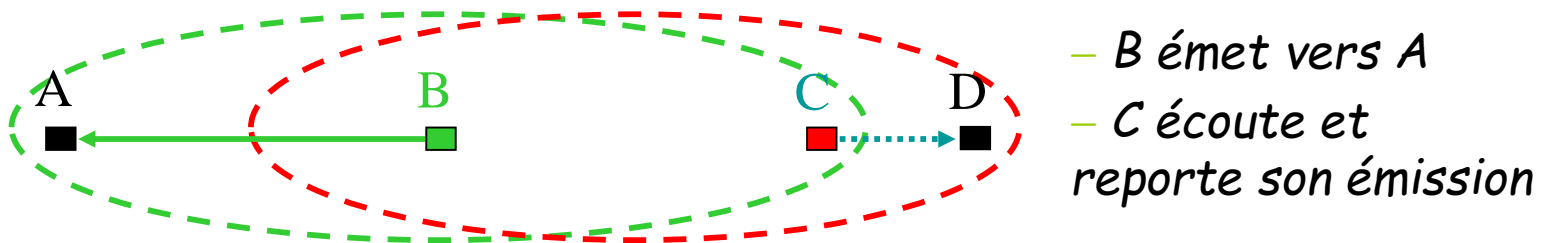
Maintenant C sait que A es en train de communiquer avec B alors, il ne va pas tenter d'envoyer à B



DCF: Problème des nœuds exposés

❑ L'échange RTS/CTS résout le principe de la station cachée, mais l'extension provoque un autre problème : celui de la **station exposée** (*exposed station*).

■ Problème de la station exposée



- un ralentissement de l'ensemble du réseau
- Une sous utilisation des ressources du réseau

PCF : Le temps partagé

- ❑ N'est possible qu'avec un point d'accès (mode infrastructure).
- ❑ L'AP partage le temps d'émission entre toutes les stations souhaitant émettre des données.
- ❑ Il interroge les stations pour savoir qui a des données à émettre (méthode de polling).



- ❑ Pas de collisions, mais une perte d'efficacité due à la scrutation.

Les problèmes d'accès

- ❑ Dans un milieu sans fil, il est possible que toutes les stations ne soient pas à portée radio les unes des autres.
- ❑ La technique du CSMA se base sur le principe que le signal se propage à toutes les stations du réseau à un instant donné.
 - ⇒ Le CSMA dans un environnement sans fils ne garantit pas l'absence de collisions à la réception.

CSMA/CA: critiques

Avantages	Inconvénients
Aide à prévenir les collisions de données	Établi un temps d'attente
Grâce à la rétroaction, les données ne sont pas perdues.	Provoque du trafic supplémentaire
Évite le trafic de données inutile avec l'extension RTS/CTS	Résout le problème des stations cachées uniquement par extension RTS/CTS
	Crée le problème de la station exposée par l'intermédiaire de RTS/CTS.