Institut Supérieur de Technologies
Master I RIM

Réseaux sans fil

B. Tanguy KABORE

Doctorant IT

tanguykabore@yahoo.fr

Plan

- Introduction
- WLAN: IEEE 802.11
- WiMAX
- Réseau Mobile
- RCSF

Module 1: Introduction et WLAN

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.

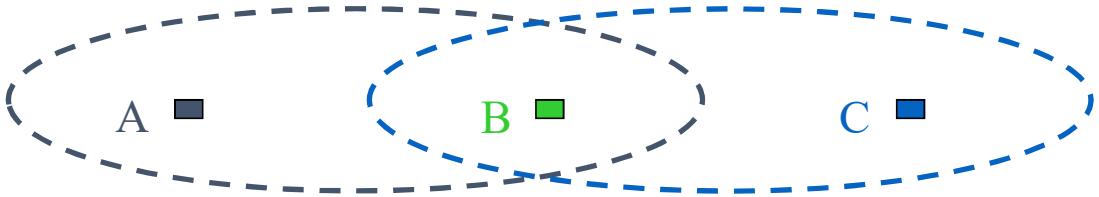
Utilisation des WLAN

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

Les problèmes d'accès

❑La technique du CSMA est inapplicable

- Problème de la station cachée

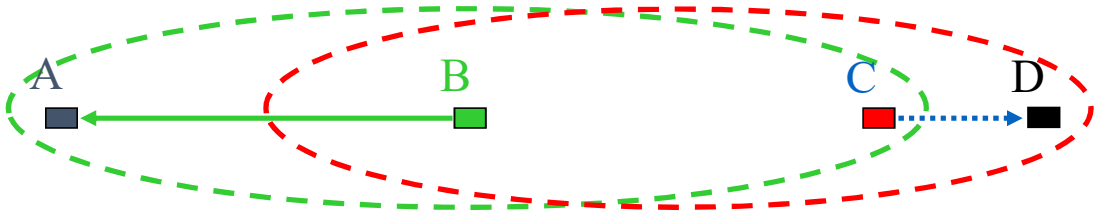


– *A émet vers B*

– *C écoute et C émet vers B*

⇒*Interférences*

- Problème de la station exposée



– *B émet vers A*

– *C écoute et reporte son émission*

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 fil ne garantit pas l'absence de collision à la réception.

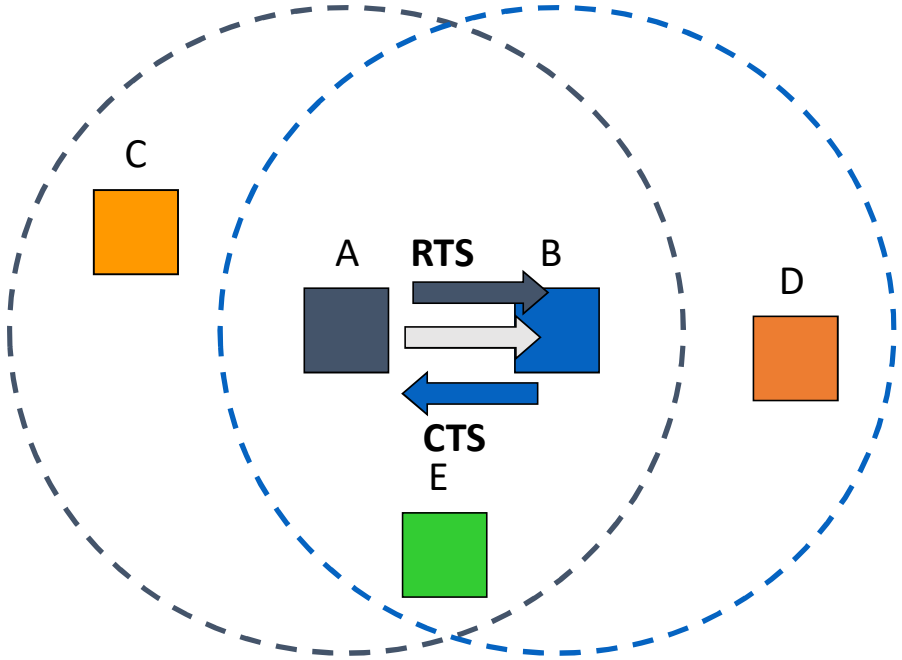
Le protocole MACA

- *Multiple Access with Collision Avoidance*
- Développé en 1990, il est à la base des travaux sur la norme 802.11

- **Principe**
  - Avant de transmettre, l'émetteur émet une trame RTS (*Request To Send*).
  - Les stations entendant le RTS s'interdise de transmettre pendant le temps nécessaire à la transmission.
  - Le récepteur signale qu'il accepte la transmission par une trame CTS (*Clear To Send*).

Le protocole MACA

❑Exemple



- A émet un RTS contenant @A, @B et durée de la transaction

⇨ C et E se tairont jusqu'à la fin de la transaction

- B répond par un CTS contenant @A, @B et durée de la transaction

⇨ D et E se tairont jusqu'à la fin de la transaction

- A émet les données

Le protocole MACA

- Le risque de collision n'est pas nul : il existe lors de l'envoi de RTS
  - RTS et CTS = trames courtes pour minimiser la probabilité de collision
  - Si collision, elle est détectée par l'absence de CTS en retour : retransmission d'un RTS après un temps aléatoire
- Amélioration MACAW (1992)
  - Introduit des ACK
  - Ecoute de la porteuse avant émission des RTS
  - Contrôle de congestion

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 !

Technologies

Wi-Fi 

Acronyme de ***Wi****rless* ***Fi****delity* ou ***Wi****rless* ***PHY***, est plus précisement connu sous la norme IEEE 802.11.

Bluetooth 

"Dents bleues" a été développé en 1994 par le suédois ERICSSON. Remplace les liaisons filaires courtes de types périphériques, GSM, PDA et autres.

IrDA 

Infrared Data Association à l'identique du *Bluetooth*, il permet la connexion de périphériques et autres équipements portables, grâce à une liaison **optique infrarouge**.

Les réseaux

WPAN - Réseau Personnel sans Fils
Réseaux domestiques de faible portée.
Technologies applicables:
Bluetooth, IrDA

WLAN – Réseau Local sans Fils
Réseaux locaux d'entreprise nécessitant une portée supérieure aux réseaux domestiques.
Technologies applicables:
Wi-Fi, DECT pour la téléphonie, …

Les réseaux

WMAN – Réseau Métropolitain sans Fils

Réseaux métropolitains de type *WirelessMAN de forte portée.*

Technologies applicables:

WiMAX, …

WWAN - Réseau Étendu sans Fils

Réseaux étendus de très forte portée à usage principalement téléphonique.

Technologies applicables:

WiMAX, GSM, …

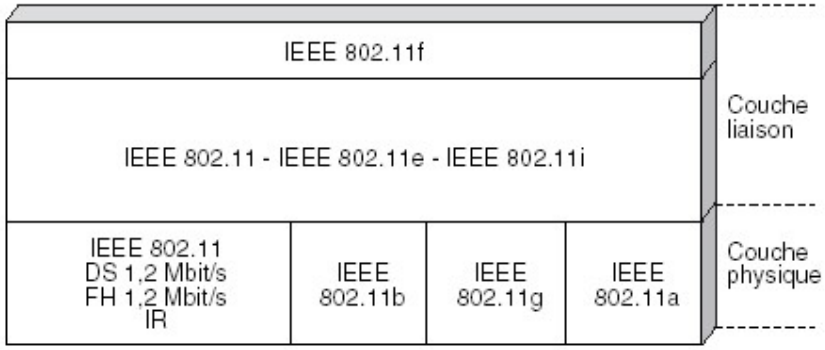
Norme IEEE 802.11 ? WiFi?

- La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil.
- WiFi 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

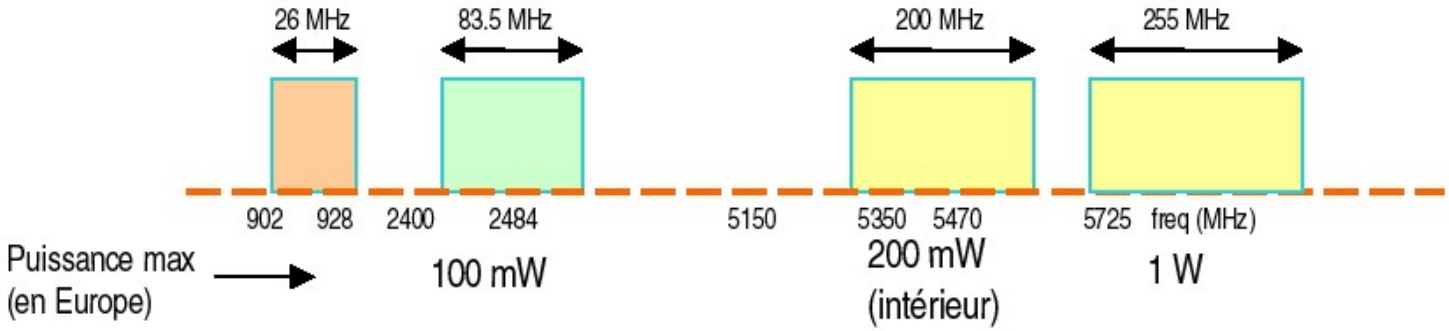
- La norme IEEE 802.11 est en réalité la norme initiale, développée en 1997, offrant des débits de 1 ou 2 Mbps.
- Des révisions ont été apportées à la norme originale afin d'optimiser le débit, la sécurité ou l'interopérabilité.
- Les extensions de la norme IEEE 802.11 utilisent toute le même protocole d'accès au canal : le protocole CSMA/CA. 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

Bande de fréquence

Bande 2,4 GHz (métropole)
Norme 802.11b (Wifi et Bluetooth)

Limite des puissances PIRE en Wi-Fi:

Fréquences en MHz	Intérieur	Extérieur
2,400 GHz à 2,454 GHz	100 mW	100 mW
2,455 GHZ à 2,4835 GHz		10 mW

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'AES (Advanced Encryption Standard) 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 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 liaison de données).
802.11e	Introduction de qualité de service au niveau de la couche liaison de données.
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.

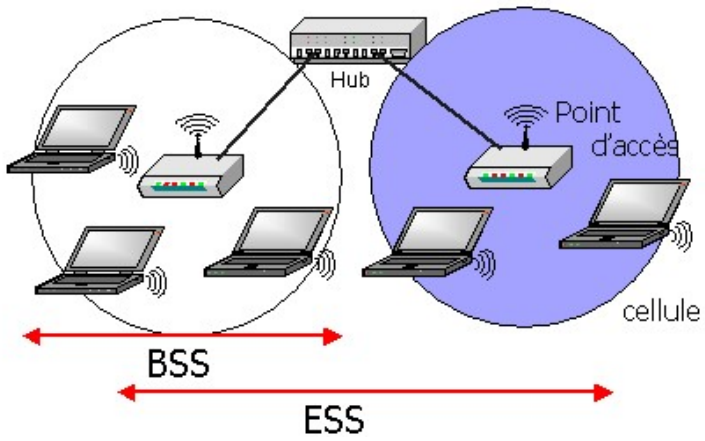
Architecture physique : deux modes de configuration

- Mode infrastructure
  - Les hôtes sans 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

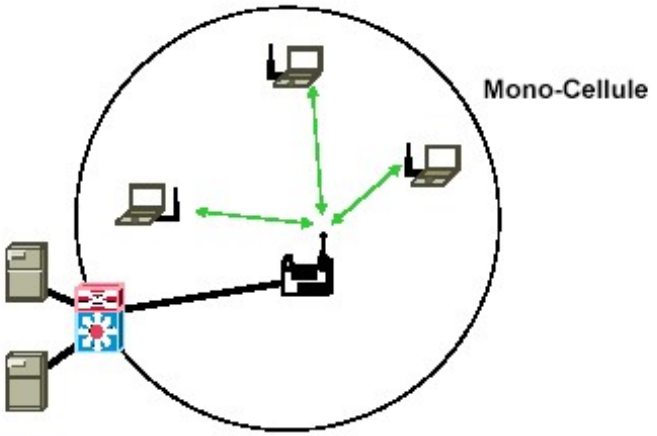
❑ Des points d'accès sont connectés au réseau local filaire. Chacun définit une cellule.

- 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*).

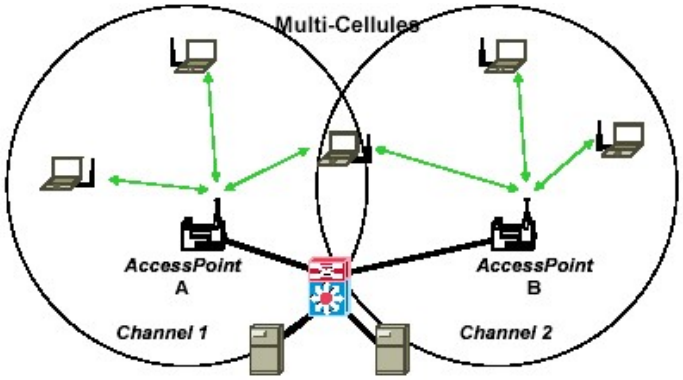


Exemples de configurations avec infrastructure

- La plus courante : monocellule interconnectée avec un réseau filaire

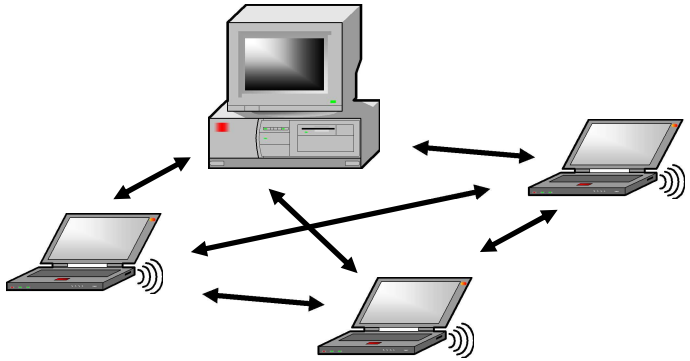


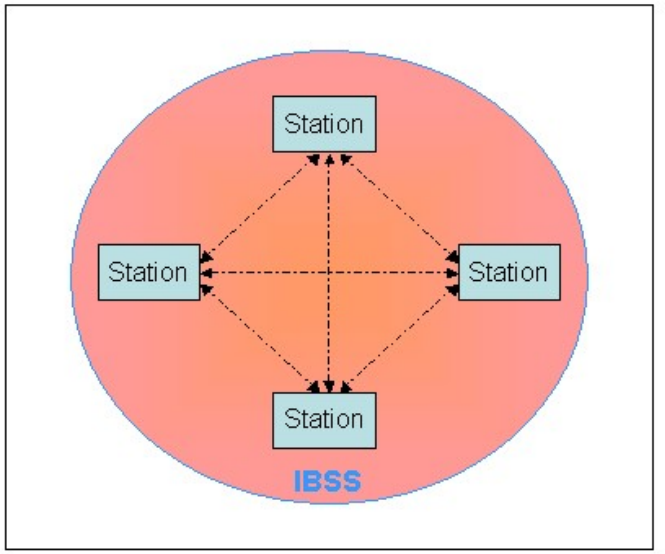
- Multicellules : plusieurs canaux, couverture étendue, mais problème du *handover*



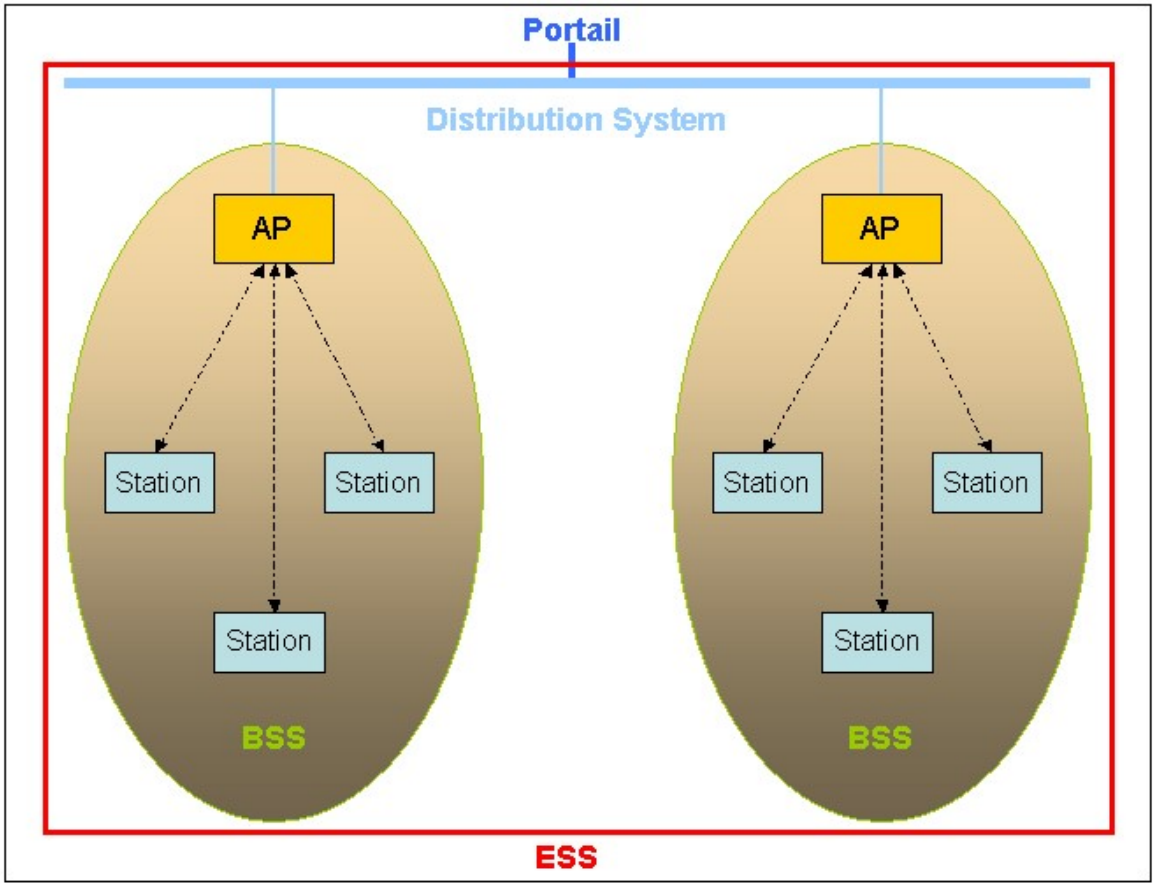
Le mode sans infrastructure (ad hoc)

- 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*).





Le mode infrastructure



Méthodes d'accès au support

- Deux méthodes d'accès au support sont normalisées
  - 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
- 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).

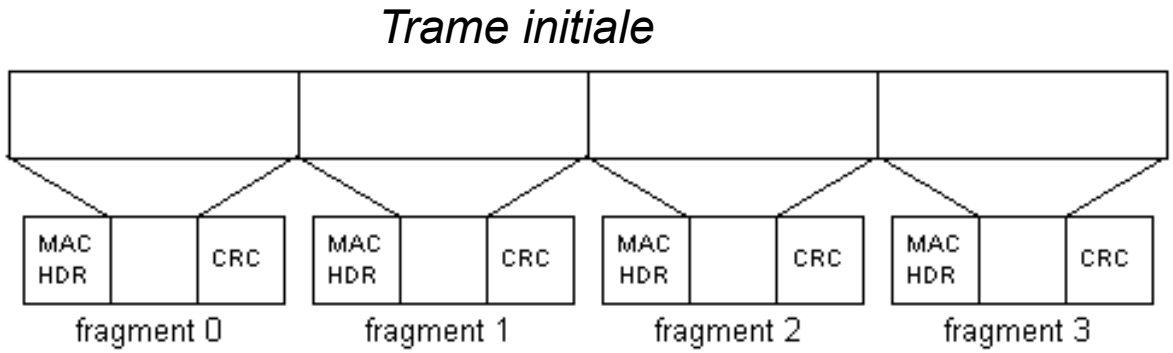
- Pour l'émetteur, ACK reçu = aucune collision n'a eu lieu
- Sinon, l'émetteur retransmet le fragment.

Virtual Carrier Sense

- Le VCS consiste à « réserver » le support avant émission.
- Avant de transmettre, si le support est libre
  - 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.

Fragmentation et réassemblage

- En sans fil, besoin de petits paquets
  - La probabilité d'erreur augmente avec la taille du paquet
  - Moins de BP gâchée par retransmission
  - Nécessaire si FHSS pour limiter le risque d'interruption de la transmission
- Fragmentation et réassemblage gérés au niveau de la couche MAC



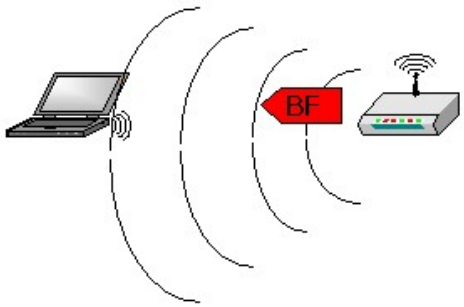
Entrée d'une station dans une cellule

- Après allumage, mode veille ou déplacement géographique, une station veut joindre un BSS

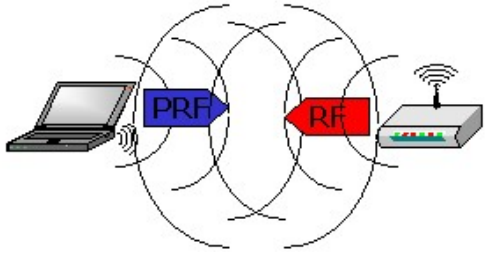
- Synchronisation sur l'AP (ou sur les autres stations dans le mode ad hoc)
  - Par écoute passive : écoute des trames balise (*beacon*) émises périodiquement par l'AP
  - Ou par écoute active : émission d'une requête *Probe Request Frame*, et attente de la réponse de l'AP

- Authentification : L'AP et la station se prouvent leur identité (par connaissance d'un mot de passe). Un « mode ouvert », sans authentification existe aussi.

- Association : échange d'information sur les stations de la cellule et leur capacité, enregistrement de la position des stations par l'AP



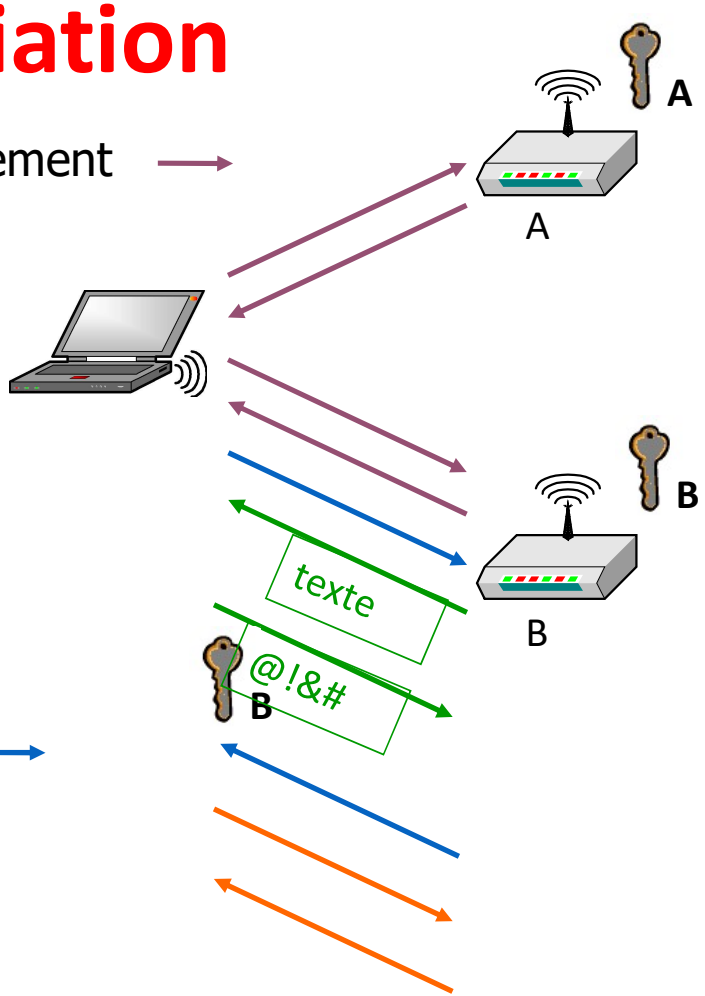
Ecoute passive



Ecoute active

Authentification et Association

- La station diffuse une demande d'enregistrement →
- Les points d'accès répondent →
  - La station évalue la réponse et sélectionne le meilleur point d'accès
- La station émet une trame « demande d'authentification » →
- Le PA envoie un texte →
- La station chiffre le texte avec la clé d'authentification de l'AP →
- Le PA confirme l'authentification du poste →
- La station envoie une demande d'association à l'AP →
- L'AP confirme l'association →



Le handover

- Parfois appelé *roaming*.
- = Passage d'une station mobile d'une cellule à une autre
- N'est effectué qu'entre deux transmissions de paquets
- Peut affecter les performances à cause des retransmissions engendrées par les possibles déconnexions
- La norme ne définit pas la manière d'effectuer le *roaming* mais donne juste des principes à respecter

Les attaques sur les réseaux sans fil

- Trois attaques essentiellement
  - L'écoute (*eavesdropping*) : espionnage
  - Le brouillage (*jamming*) : déni de service
  - Ajout ou modification de données

La sécurité dans la norme IEEE 802.11 initiale

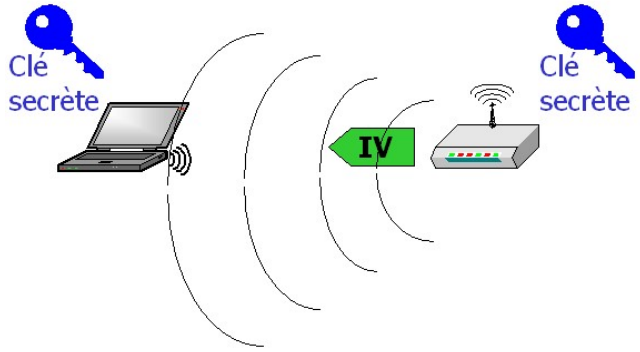
❑ Enjeux

- Empêcher un intrus de se connecter au réseau
- Empêcher l'écoute clandestine des données échangées

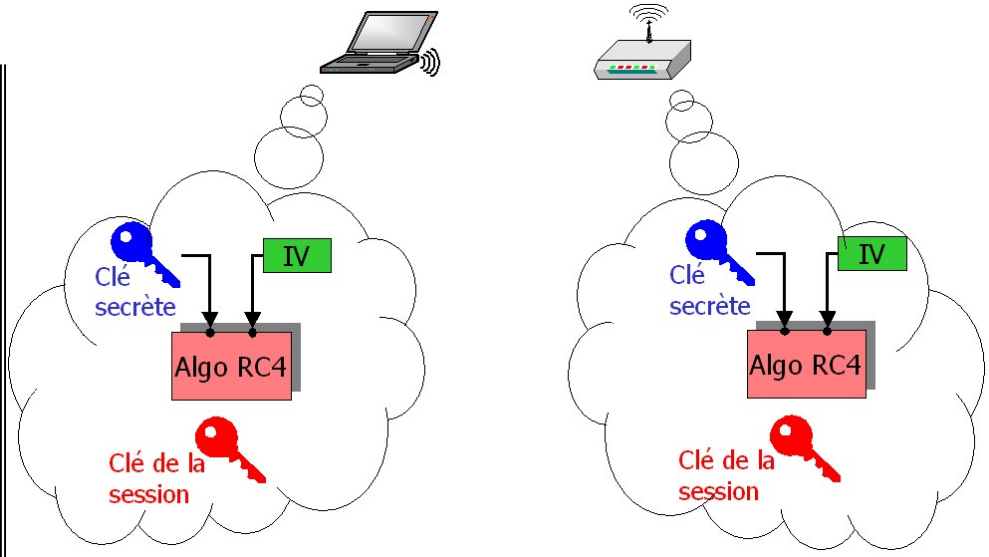
❑ « Solution » de la norme initiale: WEP (*Wired Equivalent Privacy*)

- Une clé secrète (40 bits) est partagée entre l'AP et les stations (échangée par voie sure).
- L'AP transmet en clair un mot initial (IV, Initial Vector)
- La clé combinée à l'IV est utilisée pour générer une clé de 40 bits pseudo-aléatoire via un algorithme
- Les données sont chiffrées à partir de cette clé et ainsi émises
- Clé de 64 ou 128 bits

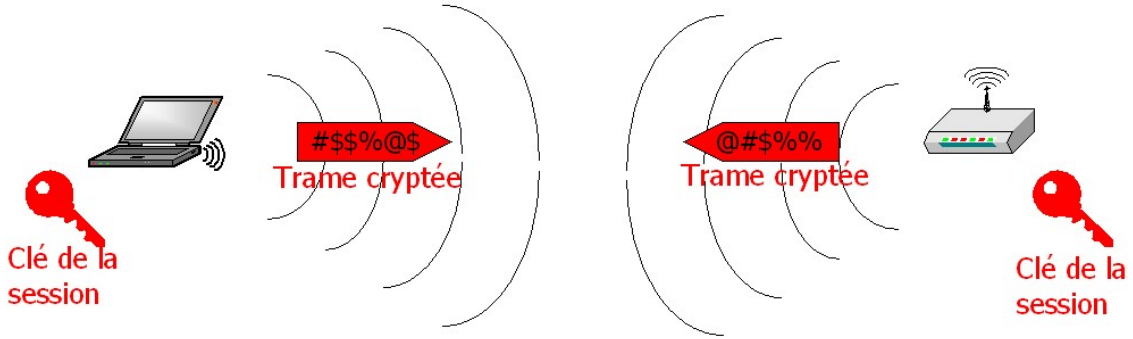
Fonctionnement du protocole WEP



Etape 1 : Echange de l'IV



Etape 2 : Calcul de la clé de la session



Etape 3 : Chiffrement des données

Failles du protocole WEP

- Possibilité de déchiffrer la clé dès que l'on connaît un couple « texte en clair, texte chiffré » de même IV
- Possibilité de trouver la clé WEP par une formule mathématique basée sur des IV « faibles »

- L'extensions IEEE 802.11i apporte des solutions à ces failles de sécurité.

L'économie d'énergie

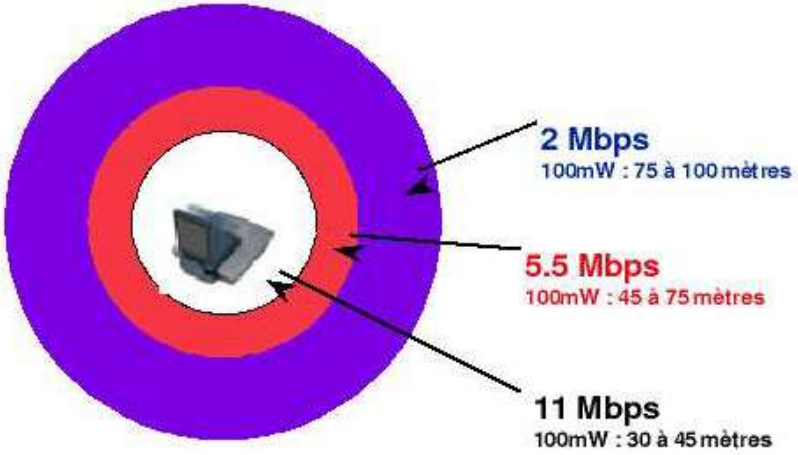
- L'énergie de la batterie est limitée ⇨ économie d'énergie et mise en veille sans perte d'information.
  - L'AP maintien la liste des stations en mode économie d'énergie.
  - L'AP garde les paquets adressés à ces stations
    - jusqu'à ce qu'elles les demandent avec une Polling Request,
    - ou jusqu'à ce qu'elles redeviennent actives.

- Les AP transmettent périodiquement des *beacons* spécifiant quelles stations ont des trames en attente ⇨ Elle peuvent se réveiller pour les récupérer.

- Les trames de multicast et de broadcast sont stockées par l'AP et transmises régulièrement : les stations qui veulent les recevoir se réveillent à cet instant.

La norme IEEE 802.11b

- Le débit se dégrade avec la distance.
  - Selon Cisco :



- En pratique, portée et débit dépendent beaucoup de l'environnement :
  - Type de construction (cloisons, murs)
  - Implantation des antennes
  - Interférences (Bluetooth, fours micro-ondes, autres réseaux Wi-Fi).

La norme IEEE 802.11i

- Aussi appelée norme WPA2
- Vise à améliorer la sécurité des normes IEEE 802.11b et 8092.11g du point de vue du chiffrement et de l'authentification

- Chiffrement : failles du protocole WEP
  - Possibilité de casser la clé par écoute des communications
  - Solution : changer la clé régulièrement ⇨ maintenance lourde !
  - Tous les utilisateurs utilisent la même clé : possibilité d'écouter les communications des autres utilisateurs du réseau

La norme IEEE 802.11i

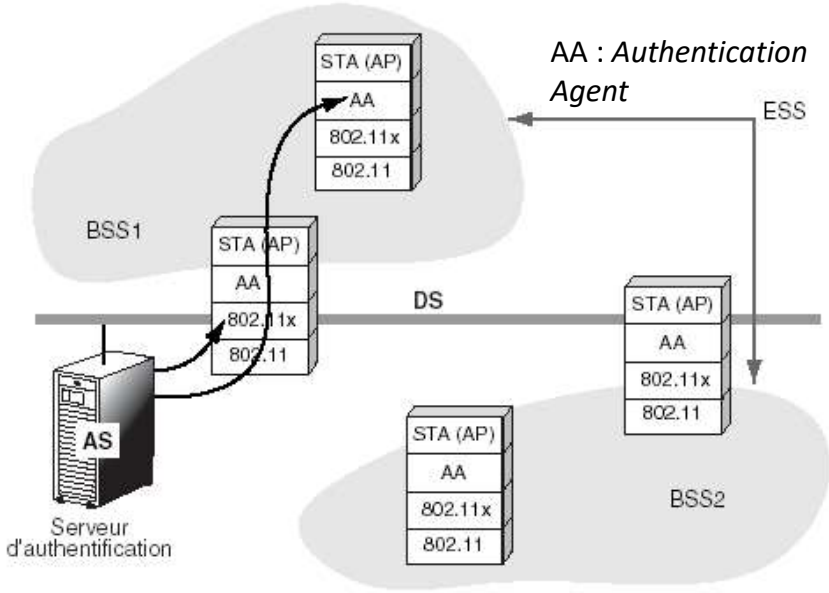
- Solution pour le chiffrement : IEEE 802.11i repose sur le standard WPA (*Wi-Fi Protected Access*)
  - Le protocole TKIP (*Temporal Key Integrity Protocol*) réalise un changement automatique des clés (1 clé par paquet, calculée à partir de la clé de la session, l'IV et l'adresse MAC) et ajoute à chaque trame un code d'intégrité MIC (*Message Integrity Code*) sur l'entête et les données
  - L'algorithme de chiffrement AES (*Advanced Encryption Standard*) est implémenté. Plus robuste que WEP.

La norme IEEE 802.11i

- Problèmes de l'authentification dans IEEE 802.11 : basée sur une clé WEP, méthode peu robuste.

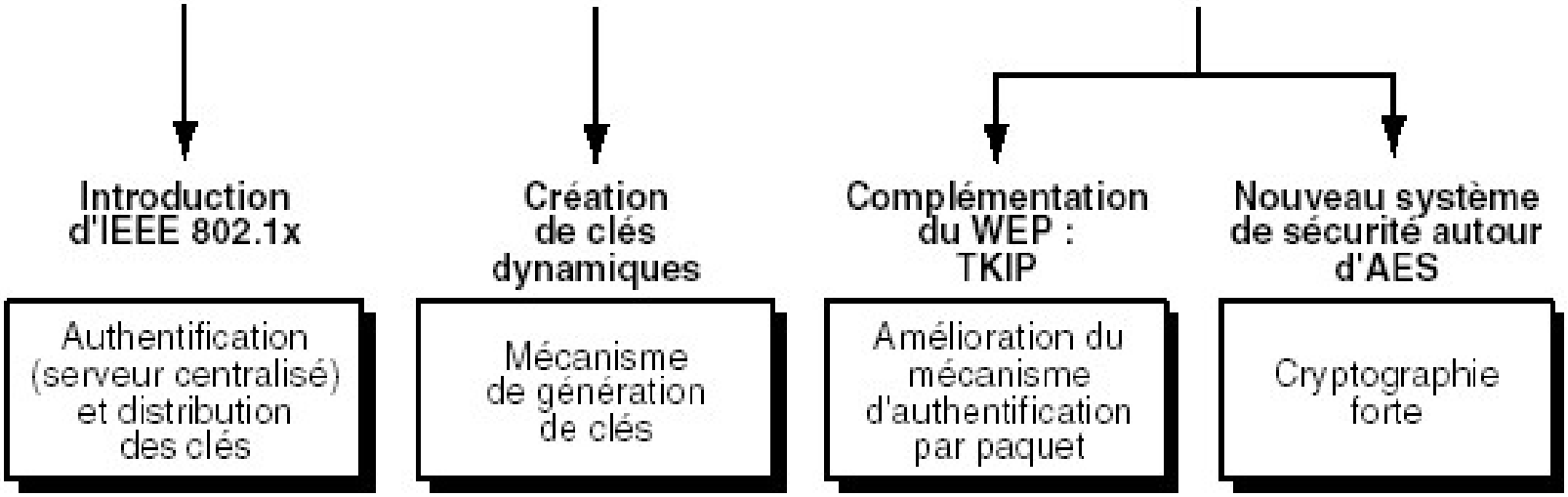
- Intégration de la norme IEEE 802.11x, qui permet la mise en place de procédures d'authentification dans un réseau avec ou sans fil.
  - Un serveur d'authentification identifie les stations souhaitant se raccorder au réseau. Il peut de plus assurer la distribution de clés dynamiques.

La station envoie les informations d'authentification au point d'accès, qui les relaie par le système de distribution vers le serveur d'authentification AS. Ce dernier authentifie la station IEEE 802.11.



La norme IEEE 802.11i

❑Résumé :



❑ Cependant, peu de recul sur ces algorithmes. On conseille l'utilisation d'IPSEC pour garantir la confidentialité des échanges.

La norme IEEE 802.11n

- Elle vise à remplacer la norme IEEE 802.11g en restant compatible avec 802.11a et 802.11g
- Etait censée être ratifiée par la Wi-Fi Alliance en octobre 2004. En juin 2007, ratification d'un draft (brouillon) de la norme...
- Débit : 300 Mbit/s

- Comme 802.11a et 802.11g, repose sur la modulation OFDM, mais utilise 54 sous-porteuses de données par canal, au lieu de 48.
- Utilise plusieurs antennes par poste pour une même communication (diversité spatio-temporelle ou technique MIMO – *Multiple Input Multiple Output*).