

IEEE 802.11

Plan

- Introduction
- Architecture de 802.11
- Couche physique
- Couche liaison de données

Introduction 802.11 (1)

- L'IEEE (Institute of Electrical and Electronics Engineers) a normalisé plusieurs catégories de réseaux locaux
 - Ethernet (IEEE 802.3)
 - Token Bus (IEEE 802.4)
 - Token Ring (IEEE 802.5)

Introduction 802.11 (2)

- 1990 : lancement du projet de création d'un réseau local sans fil ou WLAN (Wireless Local Area Network)
 - But : offrir une connectivité sans fil à des stations fixes ou mobiles qui demandent un déploiement rapide au sein d'une zone locale en utilisant différentes bandes de fréquences
 - 2001 : le premier standard international pour les réseaux locaux sans fil, l'IEEE 802.11, est publié

Introduction 802.11 (3)

- Fréquences choisies dans la gamme des 2,4 GHz (comme pour Bluetooth)
 - Pas de licence d'exploitation
 - Bande pas complètement libre dans de nombreux pays
- Communications
 - Directes : de terminal à terminal (impossible pour un terminal de relayer les paquets)
 - En passant par une station de base
- Débits variables selon la technique de codage utilisée et la bande spectrale du réseau

Introduction 802.11 (4)

- Technique d'accès au support physique (protocole MAC ou Medium Access Control)
 - Assez complexe, mais s'adapte à tous les supports physiques des Ethernet hertziens
 - Nombreuses options disponibles sur l'interface radio
 - Technique d'accès provenant du CSMA/CD
 - Carrier Sense Multiple Access/Collision Detection, utilisée pour l'accès au support physique dans les réseaux Ethernet
 - Détection de collision impossible en environnement hertzien: algorithme CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

Le standard 802.11

- **802.11** - Standard d' origine (juin 1997)
 - Le groupe de travail concentre maintenant ses efforts pour produire des standards pour des WLAN à grande vitesse
- **802.11x** - Amendements
 - **802.11b** - Vitesse de 11 Mbits/s (bande ISM)
 - **802.11a** - Vitesse de 54 Mbits/s (bande UN-II)
 - **802.11g** - Vitesse de 20 Mbits/s (bande ISM)
 - **802.11e** - Qualité de service
 - **802.11i** - Amélioration de la sécurité
 - **802.11f** - Roaming

Famille des standards 802.11

	IEEE 802.11	IEEE 802.11a	IEEE 802.11b
Application	Wireless Ethernet (LAN)	Wireless ATM	Wireless Ethernet (LAN)
Fréquences	2,4 GHz	5 GHz	2,4 GHz
Débit	1-2 Mbps	20-25 Mbps	5,5 Mbps, 11 Mbps

Plan

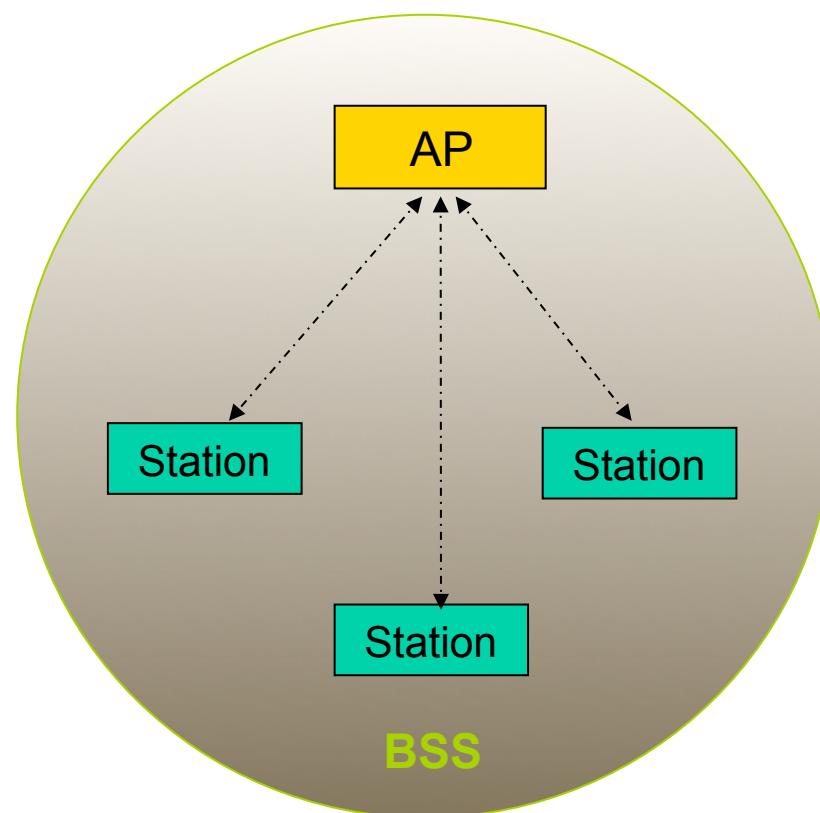
- Introduction
- Architecture de 802.11
- Couche physique
- Couche liaison de données

Architecture d' un réseau 802.11

Architecture (1)

- Architecture cellulaire
 - Association de terminaux pour établir des communications directes
 - Constitue un BSS (Basic Set Service)
 - Équipements terminaux munis d'une carte d'interface réseau 802.11
 - Zone occupée par les terminaux d'un BSS = BSA (Basic Set Area) ou cellule

Basic Service Set (BSS)



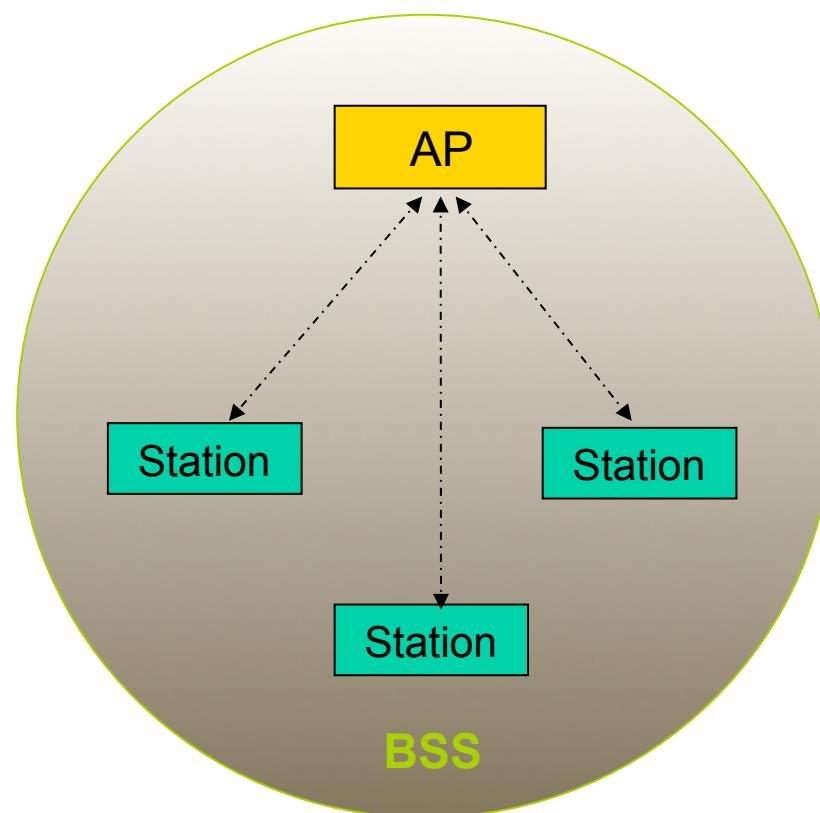
Architecture (2)

- 2 modes de fonctionnement
 - Mode infrastructure
 - Mode peer-to-peer (ou ad-hoc)

Mode infrastructure (1)

- Fournit aux différentes stations des services spécifiques sur une zone de couverture déterminée par la taille du réseau
- Réseaux d'infrastructure établis en utilisant des points d'accès ou Access Points (AP), qui jouent le rôle de station de base pour un BSS

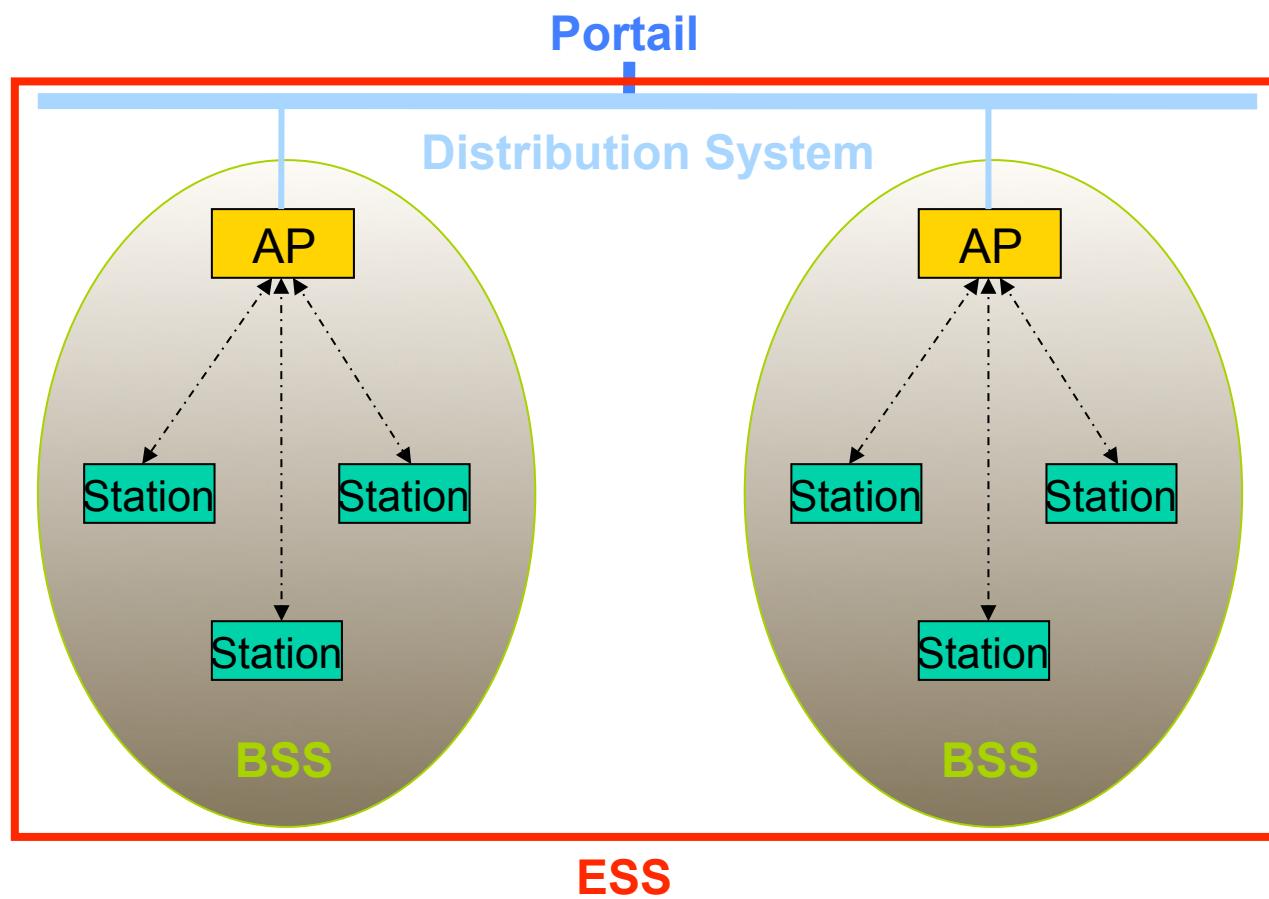
Basic Service Set (BSS)



Mode infrastructure (2)

- Chaque BSS est relié à un système de distribution ou DS (Distribution System) par l'intermédiaire de leur point d'accès (AP) respectif
- Système de distribution : en général un réseau Ethernet utilisant du câble métallique
- Groupe de BSS interconnectés par un DS = ESS (Extended Set Service)

Réseau d'infrastructure



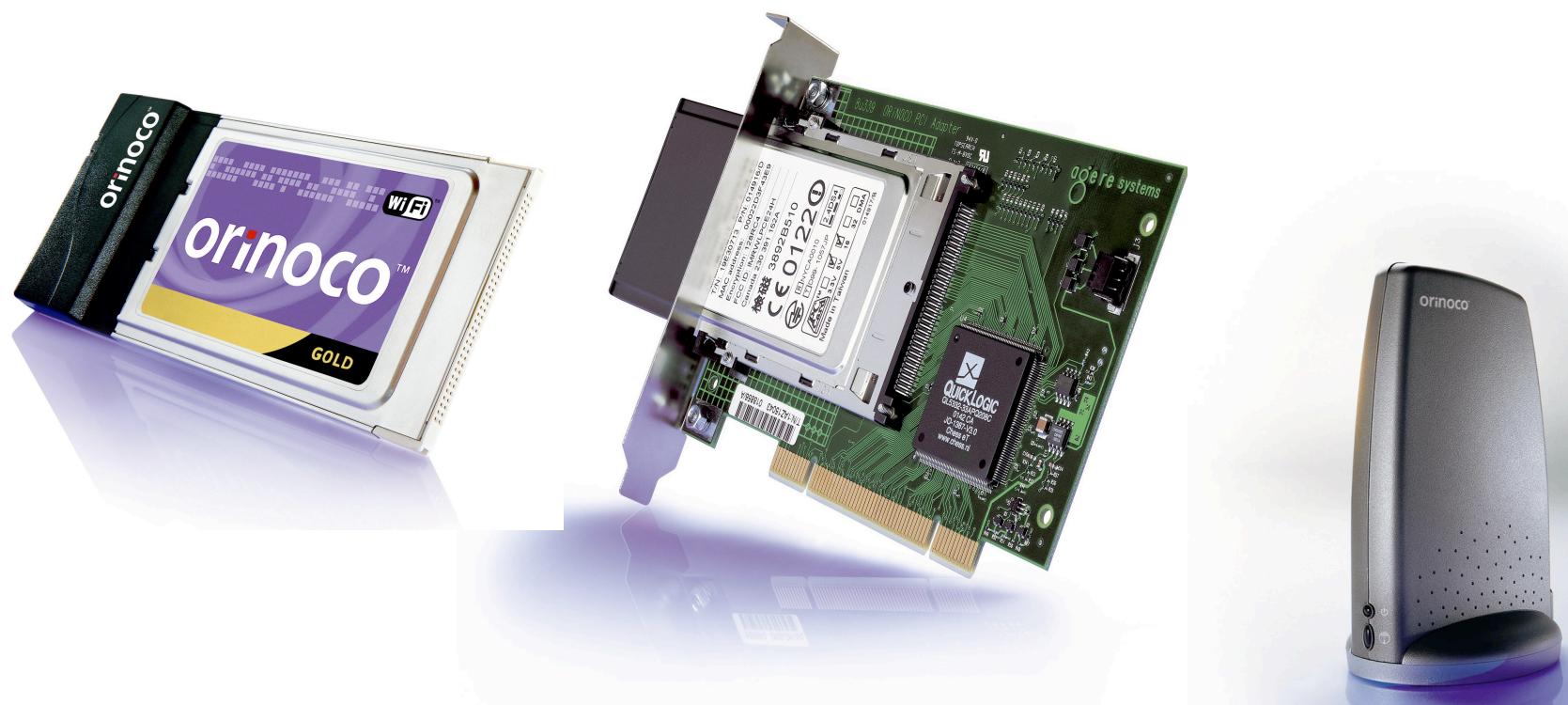
Mode infrastructure (3)

- Rôle du DS
 - Le système de distribution (DS) est responsable du transfert des paquets entre différents BSS d'un même ESS
 - DS implémenté de manière indépendante de la structure hertzienne de la partie sans fil
 - Le DS peut correspondre à un réseau Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface) ou un autre IEEE 802.11

Mode infrastructure (4)

- Rôle de l'ESS
 - L'ESS peut aussi fournir aux différentes stations mobiles une passerelle d'accès vers un réseau fixe, tel qu'Internet
 - Passerelle : connexion du réseau 802.11 à un autre réseau

Equipements : Cartes 802.11(1/2)



Equipements : Cartes 802.11(2/2)



Equipements : Point d'accès



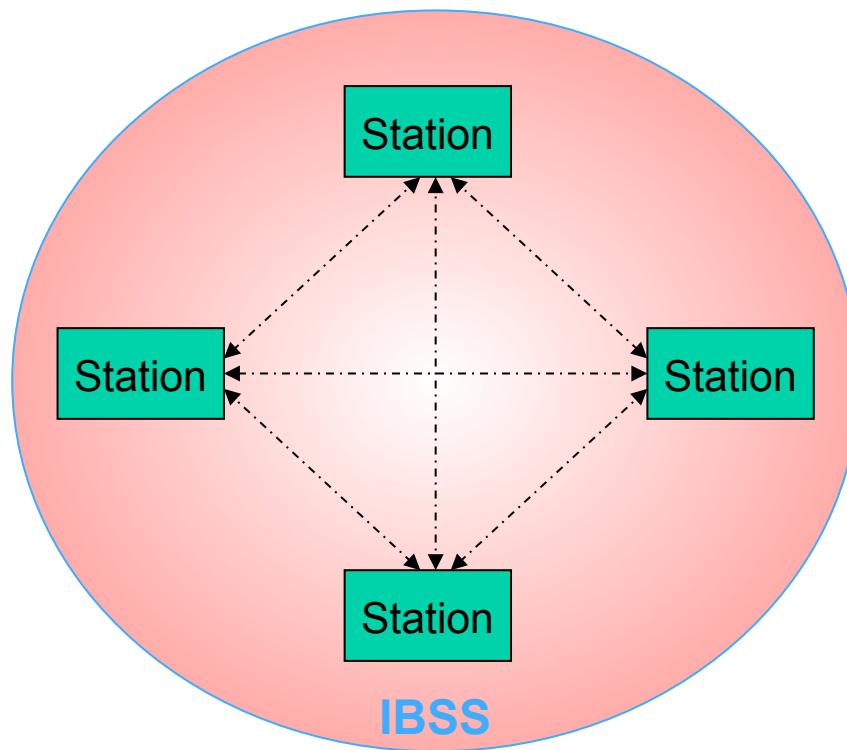
Equipements : Antenne



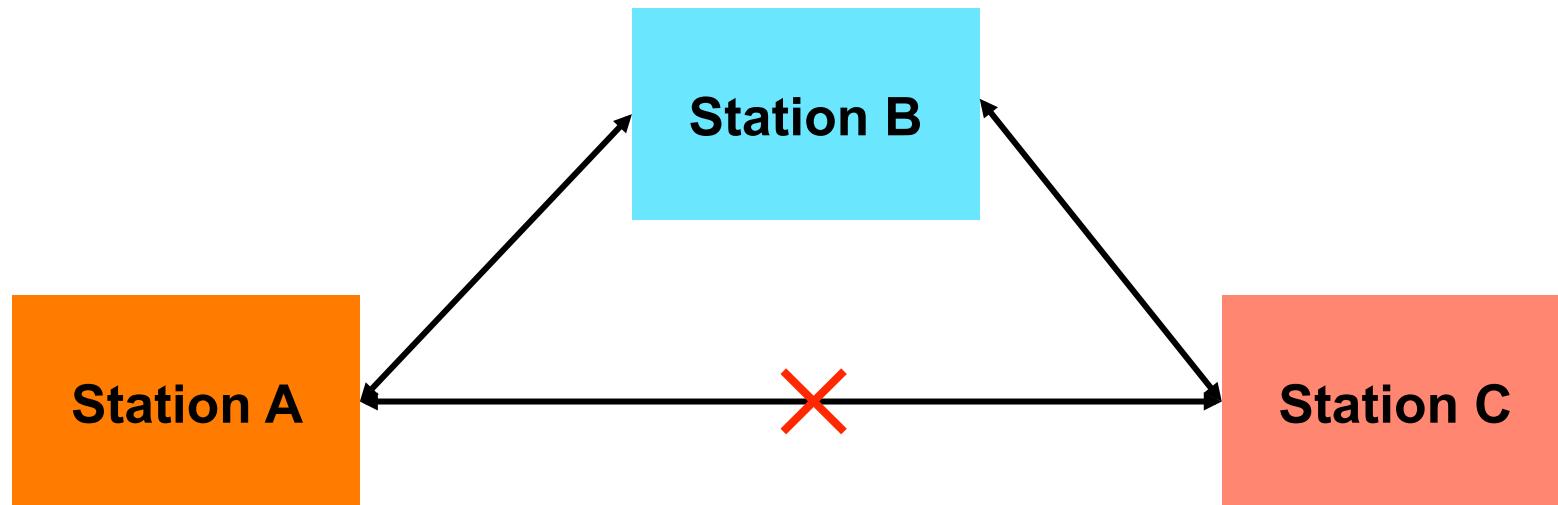
Mode peer-to-peer (ou ad-hoc)

- Groupe de terminaux formant un IBSS (Independent Basic Set Service)
- Rôle : permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure telle qu'un point d'accès ou une connexion au système de distribution
- Chaque station peut établir une communication avec n'importe quelle autre station dans l'IBSS
- Pas de point d'accès : les stations n'intègrent qu'un certain nombre de fonctionnalités
- Mode très utile pour mettre en place facilement un réseau sans fil lorsqu'une infrastructure sans fil ou fixe fait défaut

Réseau en mode peer-to-peer (ad hoc)



Ad hoc vs. Mode ad hoc (peer-to-peer-)



Modèle en couches

OSI Layer 2 <i>Data Link Layer</i>	802.11 Logical Link Control (LLC)					
	802.11 Medium Access Control (MAC)					
OSI Layer 1 <i>Physical Layer (PHY)</i>	FHSS	DSSS	IR	Wi-Fi 802.11b	Wi-Fi5 802.11a	...

Plan

- Introduction
- Architecture de 802.11
- Couche physique
- Couche liaison de données

La couche physique

Bandes de fréquences dans 802.11x

- Pour 802.11, Wi-Fi (802.11b) et 802.11g
 - Bande sans licence ISM (Instrumentation, Scientific, Medical) dans les 2,4 GHz
 - Largeur de bande : 83 MHz
- Pour Wi-Fi5 (802.11a)
 - Bande sans licence UN-II dans les 5,2 GHz
 - Largeur de bande : 300 MHz

Réglementation de la bande ISM

Pays	Bandes de fréquences
Etats-Unis <i>FCC</i>	2,400 – 2,485 GHz
Europe <i>ETSI</i>	2,400 – 2,4835 GHz
Japon <i>MKK</i>	2,471 – 2,497 GHz
France <i>ART</i>	2,4465 – 2,4835 GHz

La réglementation française

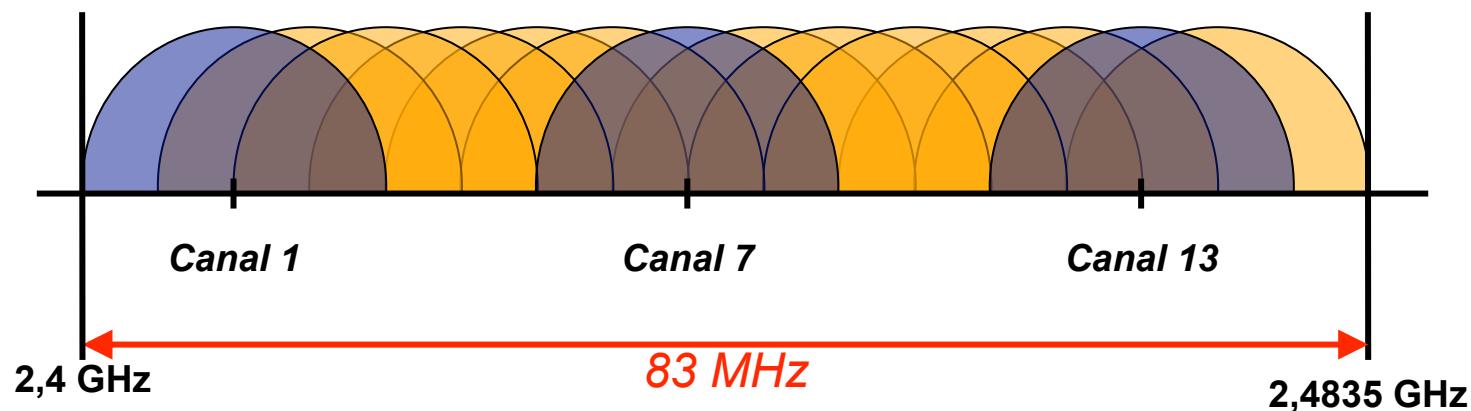
- A l'intérieur des bâtiments
 - Aucune demande d'autorisation
 - Bande 2,4465 – 2,4835 GHz, puissance 100 mW
 - Bande 2,400 – 2,4835 GHz, puissance 10 mW
- A l'extérieur des bâtiments sur un domaine privé
 - Demande d'autorisation obligatoire auprès de l'ART
 - Bande 2,4465 – 2,4835 GHz, puissance 100 mW
- A l'extérieur des bâtiments sur le domaine public
 - réglementé

Wi-Fi ou 802.11b

- Bande ISM
- Basé sur le DSSS
étalement de spectre à séquence directe
- Débits compris entre 1 et 11 Mbits/s
- Mécanisme de variation de débit selon la qualité de l'environnement radio

DSSS : Séquence directe

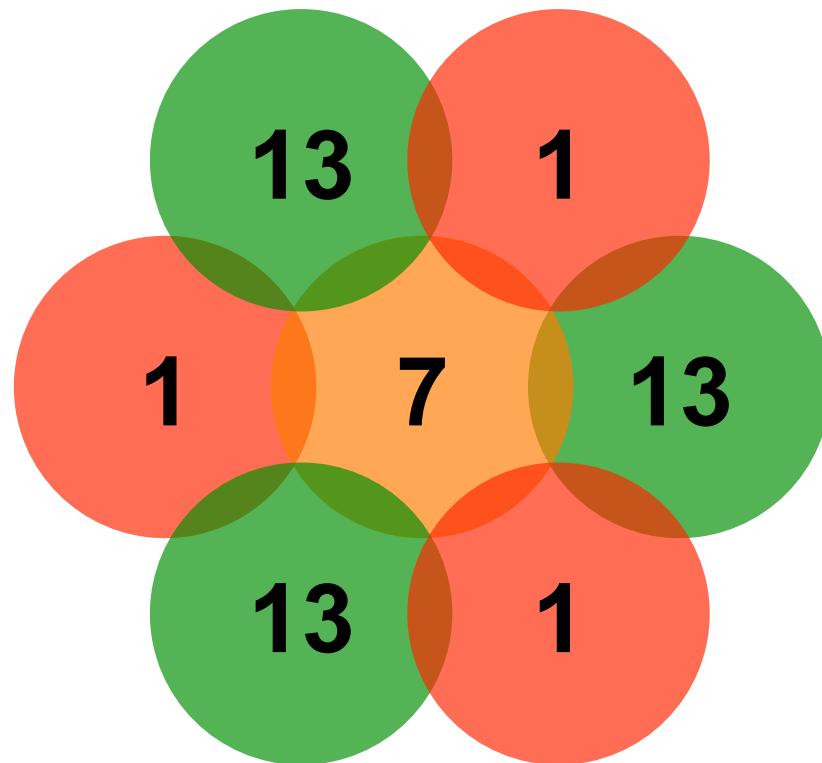
- Bande ISM
- Bande divisée en 14 canaux de 20 MHz
- La transmission ne se fait que sur un seul canal
- Co-localisation de 3 réseaux au sein d'un même espace



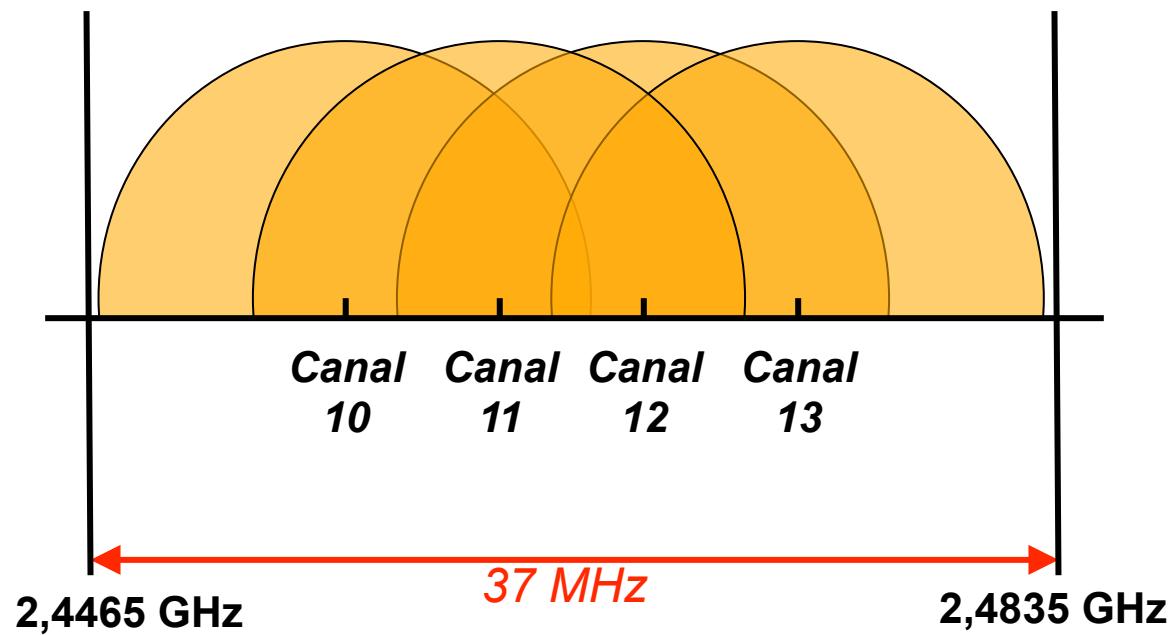
Affectation des canaux (1/3)

Pays	Etats-Unis	Europe	Japon	France
Nombres de sous canaux utilisés	1 à 11	1 à 13	14	10 à 13

Affectation des canaux (2/3)



Affectation des canaux (3/3)



Zone de couverture

- A l' intérieur des bâtiments

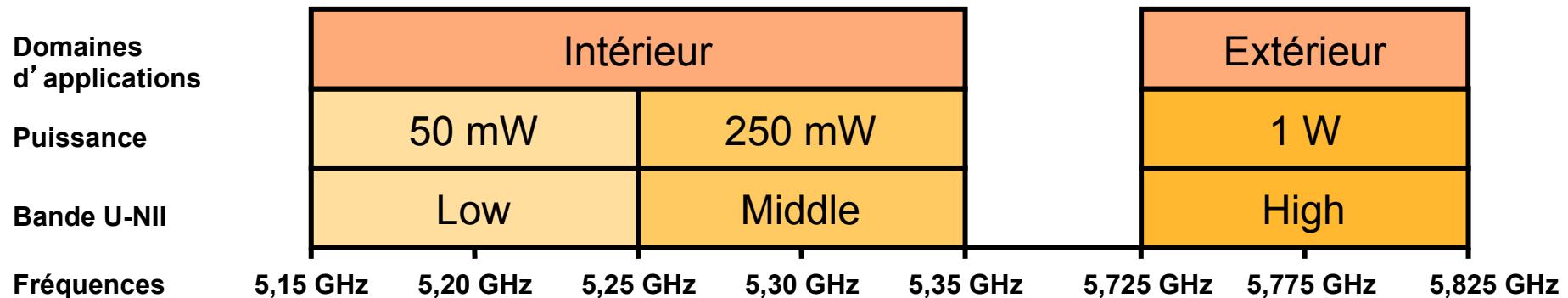
Vitesses (Mbits/s)	Portée (Mètres)
11	50
5	75
2	100
1	150

- A l' extérieur des bâtiments

Vitesses (Mbits/s)	Portée (Mètres)
11	200
5	300
2	400
1	500

Wi-Fi5 ou 802.11a

- Bande UN-II (5GHz)
- Largeur de la bande : 300 MHz
- Basé sur OFDM
- Débits compris entre 6 et 54 Mbits/s

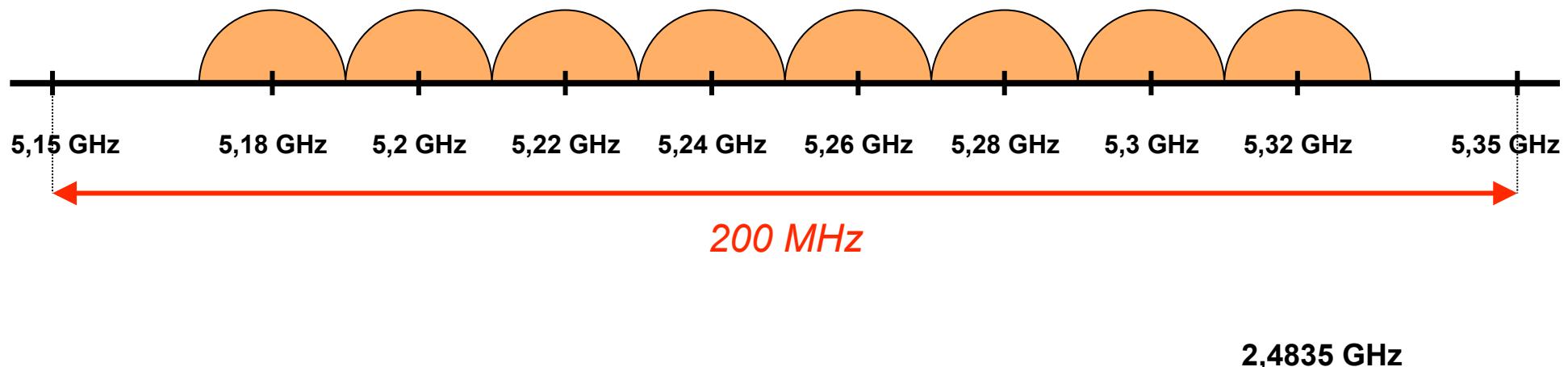


IEEE 802.11 a

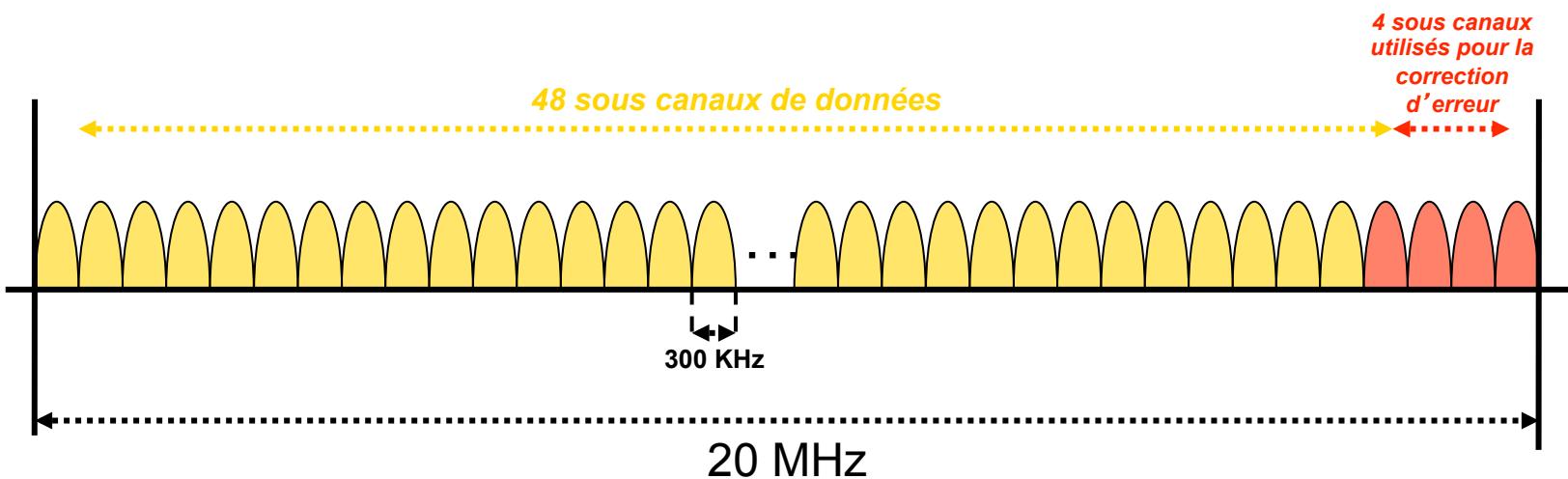
- La proposition IEEE contient la définition du support physique ainsi que des couches qui se trouvent au-dessus
- Partie physique
 - Fréquence de 5 GHz dans la bande UNII
 - Unlicensed National Information Infrastructure : pas besoin de licence d'utilisation
 - Modulation OFDM
 - Orthogonal Frequency Division Multiplexing
 - 52 porteuses
 - Excellentes performances en cas de chemins multiples
 - 8 vitesses de 6 à 54 Mbit/s
- Devrait permettre à de très nombreuses stations de travail et portables de se connecter automatiquement dans les entreprises
 - Couches supérieures : correspondent à celles des réseaux Ethernet

OFDM (1/2)

- 8 canaux de 20 MHz
- Co-localisation de 8 réseaux au sein du même espace



OFDM (2/2)



Un canal dans OFDM

IEEE 802.11e

- Amélioration de 802.11a en introduisant
 - De la qualité de service
 - Des fonctionnalités de sécurité et d'authentification
- But : faire transiter la parole téléphonique et les données multimédias sur ces réseaux partagés
 - Définition de classes de service
 - Les terminaux choisissent la bonne priorité en fonction de la nature de l'application transportée

IEEE 802.11e

- Gestion des priorités
 - Au niveau du terminal
 - Technique d'accès modifiée par rapport à 802.11
 - Les stations prioritaires ont des temporiseurs d'émission beaucoup + courts que ceux des stations non prioritaires : avantage pour l'accès au support
- Mécanismes de sécurité améliorés
 - Authentification mutuelle entre les terminaux et les stations de base
 - Trafic protégé par un chiffrement
 - Authentification de la source disponible
 - Technique de distribution des clés : elle-même sécurisée
- Extensions prévues pour permettre la communication vers des terminaux qui ne sont pas en contact direct avec la station de base
 - Cheminements multisauts

Wi-Fi vs. Wi-Fi5

- La bande ISM devient de plus en plus saturée (802.11b, 802.11g, Bluetooth, etc.)
- Co-localisation plus importante dans Wi-Fi5
- Débits plus importants pour Wi-Fi5 mais zone de couverture plus petite
- En France, les produits Wi-Fi5 ne sont pas encore disponibles

Plan

- Introduction
- Architecture de 802.11
- Couche physique
- Couche liaison de données

La couche liaison de données

Couche liaison de données de 802.11

- Composée de 2 sous-couches
 - LLC : Logical Link Control
 - Utilise les mêmes propriétés que la couche LLC 802.2
 - Possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE
 - MAC : Medium Access Control
 - Spécifique à l'IEEE 802.11
 - Assez similaire à la couche MAC 802.3 du réseau Ethernet terrestre

Couche Mac 802.11

- Principe :
 - Les terminaux écoutent la porteuse avant d'émettre
 - Si la porteuse est libre, le terminal émet, sinon il se met en attente
- La couche MAC 802.11 intègre beaucoup de fonctionnalités que l'on ne trouve pas dans la version terrestre
- Particularité du standard : définition de 2 méthodes d'accès fondamentalement différentes au niveau de ma couche MAC
 - DCF : Distributed Coordination Function
 - PCF : Point Coordination Function

Méthodes d'accès dans 802.11

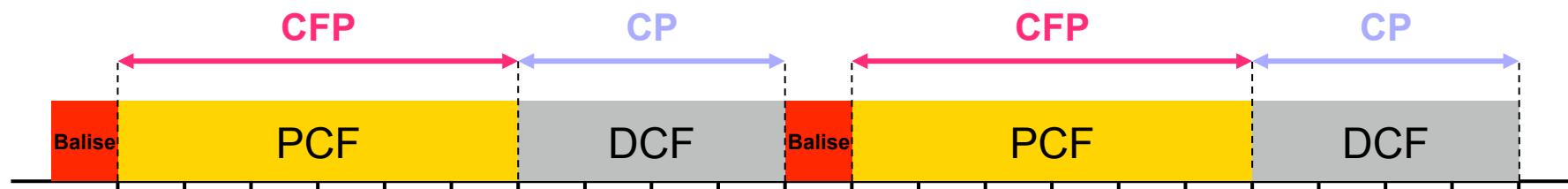
- DCF : Distributed Coordination Function
 - Assez similaire au réseau traditionnel supportant le Best Effort
 - Conçue pour prendre en charge le transport de données asynchrones
 - Tous les utilisateurs qui veulent transmettre ont une chance égale d'accéder au support
- PCF : Point Coordination Function
 - Interrogation à tour de rôle des terminaux (polling)
 - Contrôle par le point d'accès
 - Conçue pour la transmission de données sensibles
 - Gestion du délai
 - Applications de type temps réel : voix, vidéo

Méthodes d'accès dans 802.11

- Réseau ad-hoc
 - Uniquement DCF
- Réseau classique IEEE 802.11, avec des points d'accès
 - À la fois DCF et PCF

Méthodes d' accès dans 802.11

- *Distributed Coordination Function (DCF)*
 - méthode d' accès avec contention
- *Point Coordination Function (PCF)*
 - méthode d' accès sans contention



DCF

- Basé sur le CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
- Ethernet : CSMA/CD (Collision Detection)
 - CSMA/CD ne peut pas être utilisé dans les environnements sans fil
 - La détection des collisions n'est pas possible pour les réseaux locaux 802.11
 - Pour détecter une collision, une station doit être capable d'écouter et de transmettre en même temps
 - Dans les systèmes radio, la transmission couvre la capacité de la station à entendre la collision
 - Si une collision se produit, la station continue à transmettre la trame complète : perte de performance du réseau

Protocole CSMA/CA

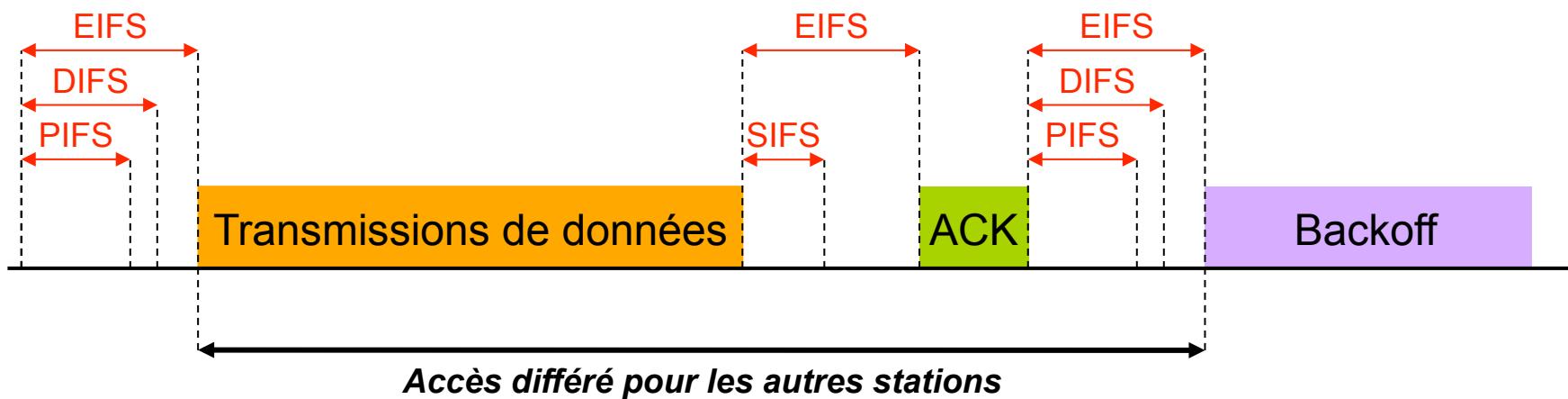
- Le CSMA/CA est basé sur :
 - L' utilisation d' acquittements positifs
 - Les temporiseurs IFS
 - L' écoute du support
 - L' algorithme de Backoff

Protocole CSMA/CA

- Évite les collisions en utilisant des trames d'acquittement
 - ACK envoyé par la station destination pour confirmer que les données sont reçues de manière intacte
- Accès au support contrôlé par l'utilisation d'espace inter-trame ou IFS (Inter-Frame Spacing)
 - Intervalle de temps entre la transmission de 2 trames
 - Intervalles IFS = périodes d'inactivité sur le support de transmission
 - Il existe différents types d'IFS

Temporiseurs

- 4 types de temporiseurs
 - **SIFS**
 - **DIFS**
 - **PIFS**
 - **EIFS**
- Permet d' instaurer un système de priorités



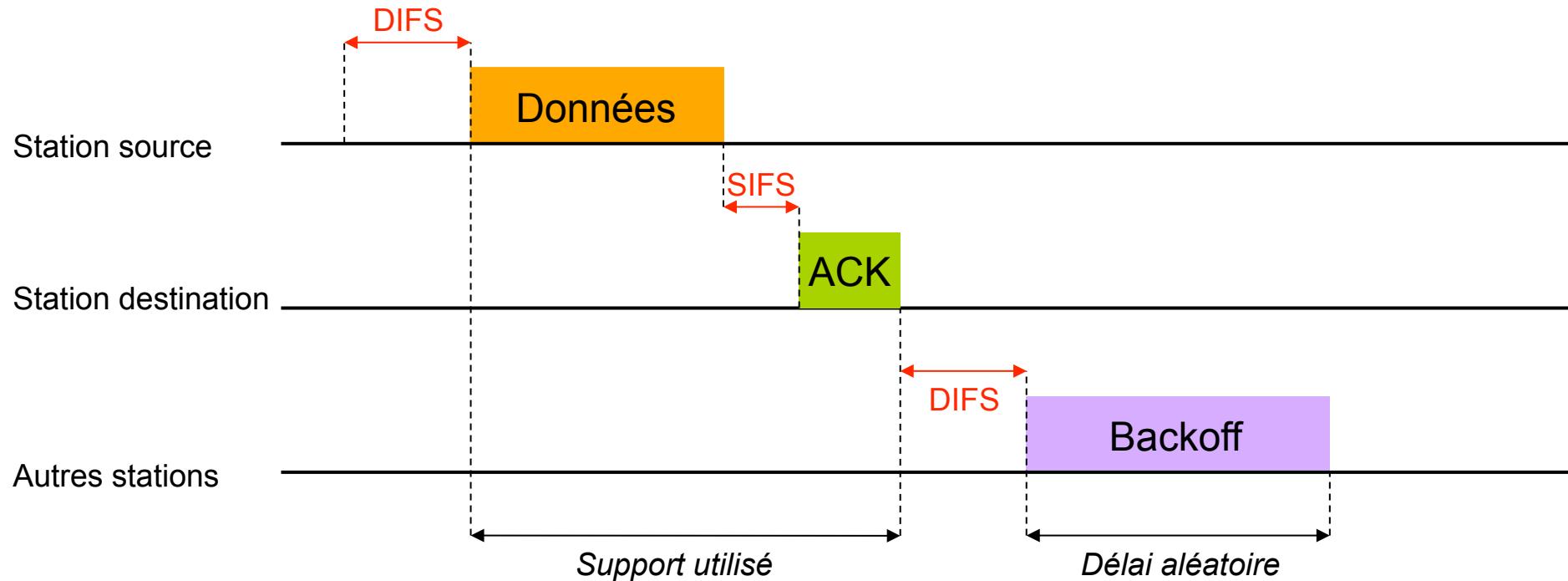
Écoute du support

- Les terminaux d'un même BSS peuvent écouter l'activité de toute les stations se trouvant dans le même BSS
- Lorsqu'une station envoie une trame
 - les autres stations mettent à jour un timer appelée NAV (Network Allocation Vector)
 - Le NAV permet de retarder toutes les transmissions prévues
 - NAV calculé par rapport à l'information située dans le champ durée de vie ou TTL contenu dans les trames envoyées

Écoute du support

- La station voulant émettre écoute le support
 - Si aucune activité n'est détectée pendant un DIFS, transmission immédiate des données
 - Si le support est occupé, la station écoute jusqu'à ce qu'il soit libre
 - Quand le support est disponible, la station retarde sa transmission en utilisant l'algorithme de backoff avant de transmettre
- Si les données ont été reçues de manière intacte (vérification du CRC de la trame), la station destination attend pendant un SIFS et émet un ACK
 - Si l'ACK n'est pas détecté par la source ou si les données ne sont pas reçues correctement, on suppose qu'une collision s'est produite et le trame est retransmise

Exemple de transmission



Algorithme de backoff

- Permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps
- Temps découpé en tranches (timeslots)
- Timeslot de 802.11 un peu plus petit que la durée de transmission minimale d'une trame ; utilisé pour définir les intervalles IFS

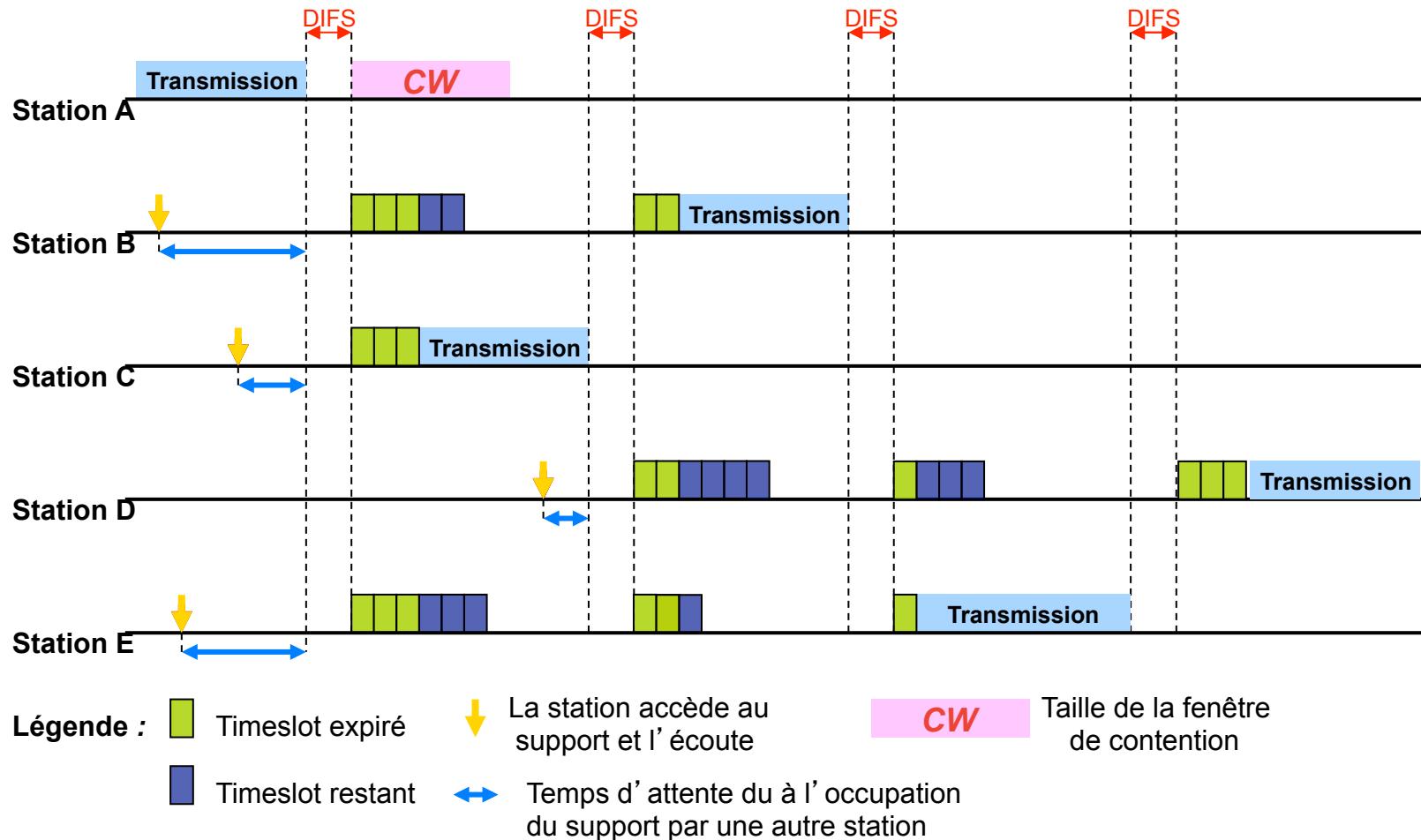
Algorithme de backoff

- Initialement, une station calcule la valeur d'un temporisateur = timer backoff, compris entre 0 et 7
- Lorsque le support est libre, les stations décrémentent leur temporisateur jusqu'à ce que le support soit occupé ou que le temporisateur atteigne la valeur 0
 - Si le temporisateur n'a pas atteint la valeur 0 et que le support est de nouveau occupé, la station bloque le temporisateur
 - Dès que le temporisateur atteint 0, la station transmet sa trame
 - Si 2 ou plusieurs stations atteignent la valeur 0 au même instant, une collision se produit et chaque station doit regénérer un nouveau temporisateur, compris entre 0 et 15
 - Pour chaque tentative de retransmission, le temporisateur croît de la façon suivante : $[2^{2+1} * \text{randf}()] * \text{timeslot}$

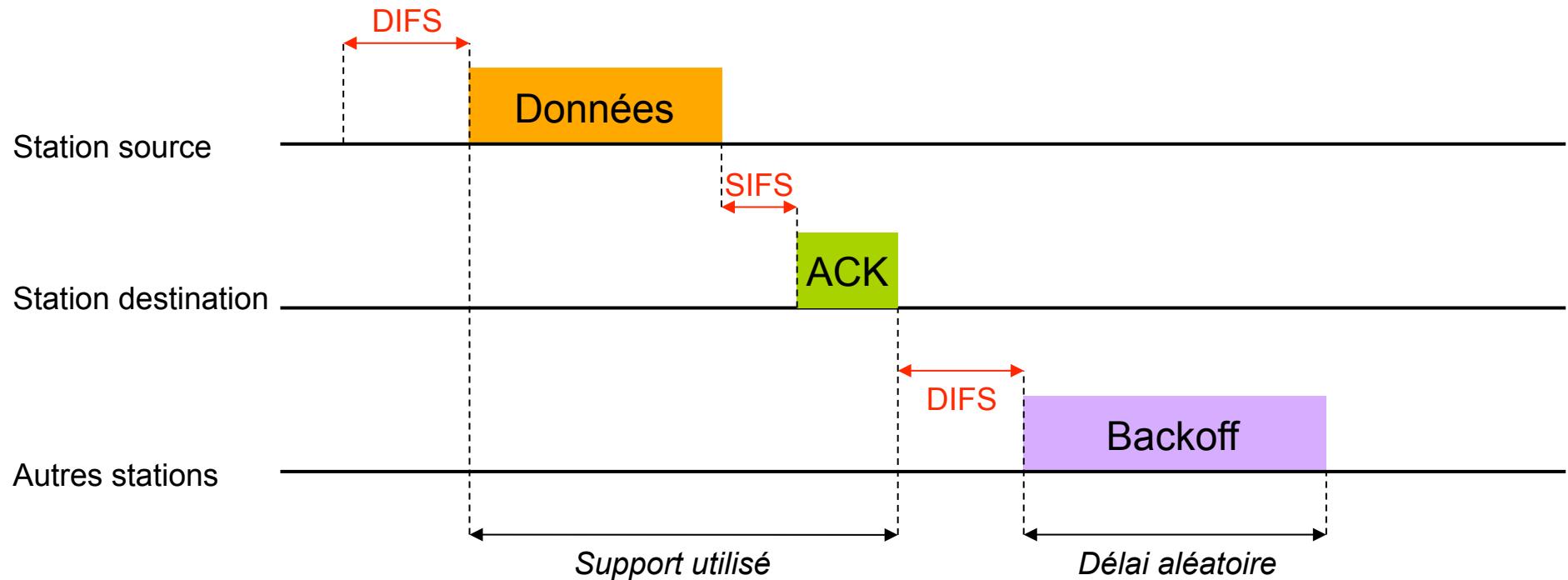
Algorithme de backoff

- Les stations ont la même probabilité d'accéder au support car chaque station doit, après chaque retransmission, réutiliser le même algorithme
- Inconvénient : pas de garantie de délai minimal
 - Complique la prise en charge d'applications temps réel telles que la voix ou la vidéo

Algorithme de Backoff



Exemple de transmission



Ecoute du support

- Couche physique avec PCS
 - Physical Carrier Sense
- Couche MAC avec VCS
 - Virtual Carrier Sense

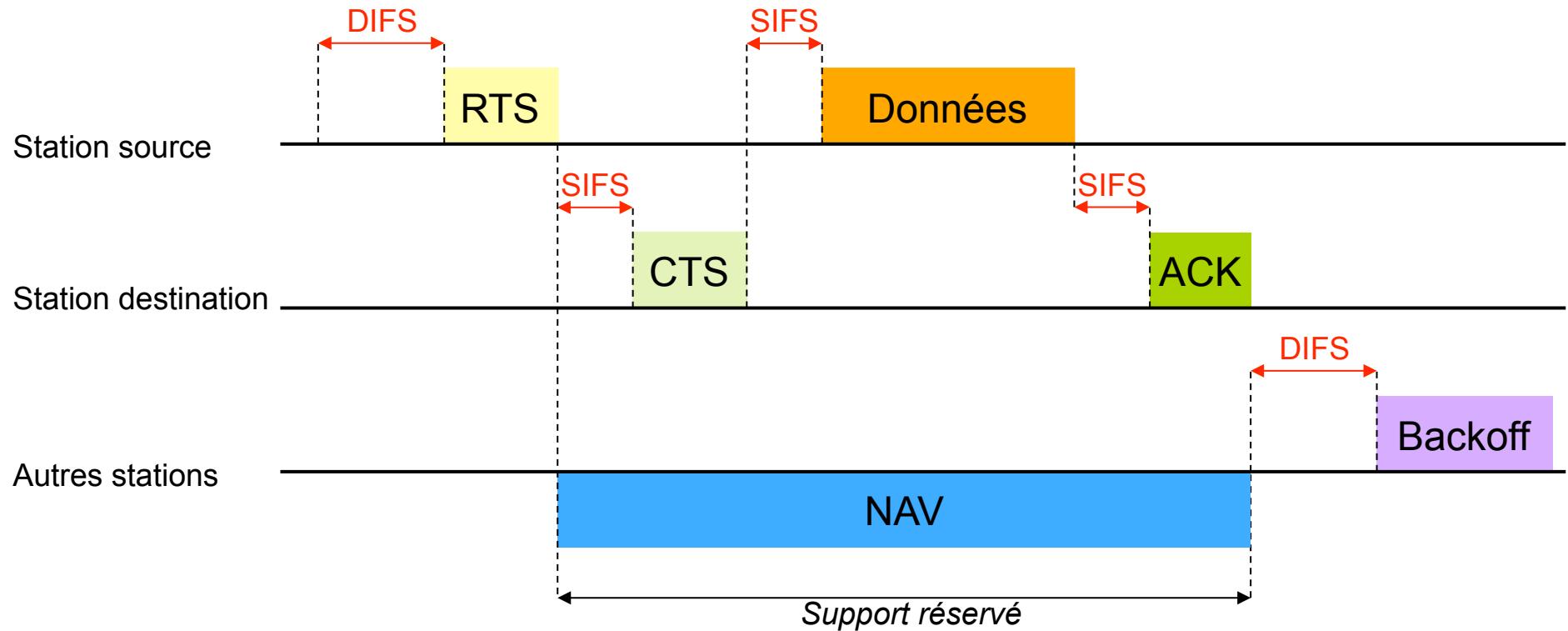
PCS : Physical Carrier Sense

- Le PCS détecte la présence d'autres stations 802.11
 - en analysant toutes les trames passant sur le support hertzien
 - en détectant l'activité sur le support grâce à la puissance relative du signal des autres stations

VCS : Virtual Carrier Sense

- Mécanisme de réservation
 - envoi de trames RTS/CTS (Request To Send/Clear To Send) entre une station source et une station destination avant tout envoi de données
 - Station qui veut émettre envoie un RTS
 - Toutes les stations du BSS entendent le RTS, lisent le champ de durée du RTS et mettent à jour leur NAV
 - Station destination répond après un SIFS, en envoyant un CTS
 - Les autres stations lisent le champ de durée du CTS et mettent de nouveau à jour leur NAV
 - Après réception du CTS par la source, celle-ci est assurée que le support est stable et réservé pour la transmission de données

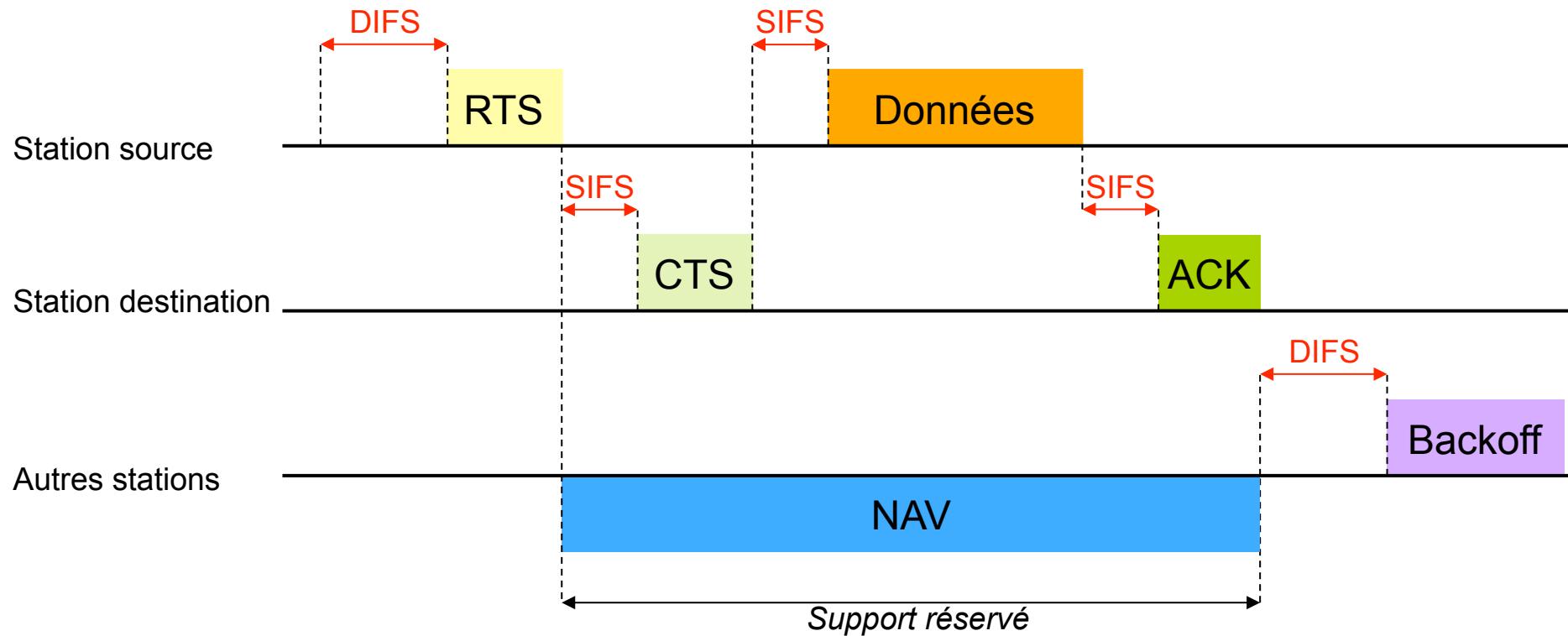
Transmission avec mécanisme de réservation



RTS / CTS

- Transmission des données et réception de l'ACK sans collision
- Trames RTS / CTS réservent le support pour la transmission d'une station
 - Mécanisme habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante
- Les stations peuvent choisir
 - D'utiliser le mécanisme RTS / CTS
 - De ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold
 - De ne jamais l'utiliser

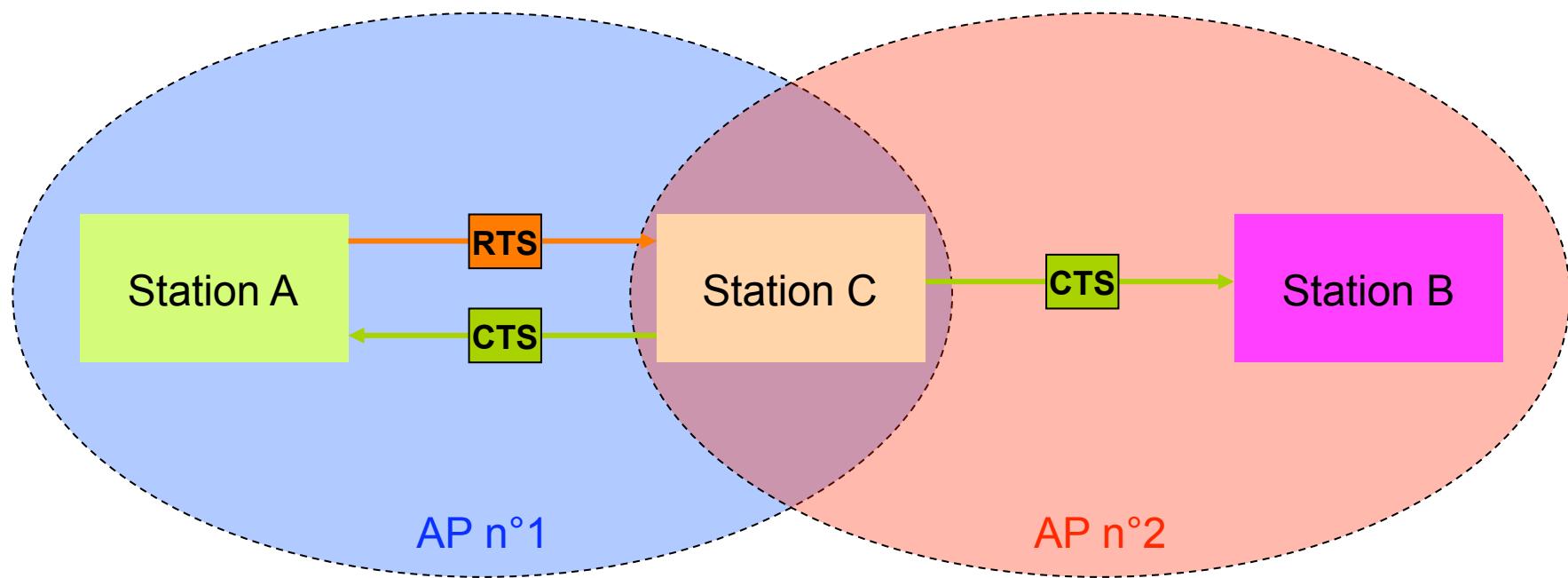
Transmission avec mécanisme de réservation



Problème de la station cachée

- 2 stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station
 - peuvent entendre l'activité de cet AP
 - ne peuvent pas s'entendre l'une l'autre du fait que la distance entre les 2 est trop grande ou qu'un obstacle les empêche de communiquer entre elles
- Le mécanisme de RTS / CTS permet de résoudre ce problème

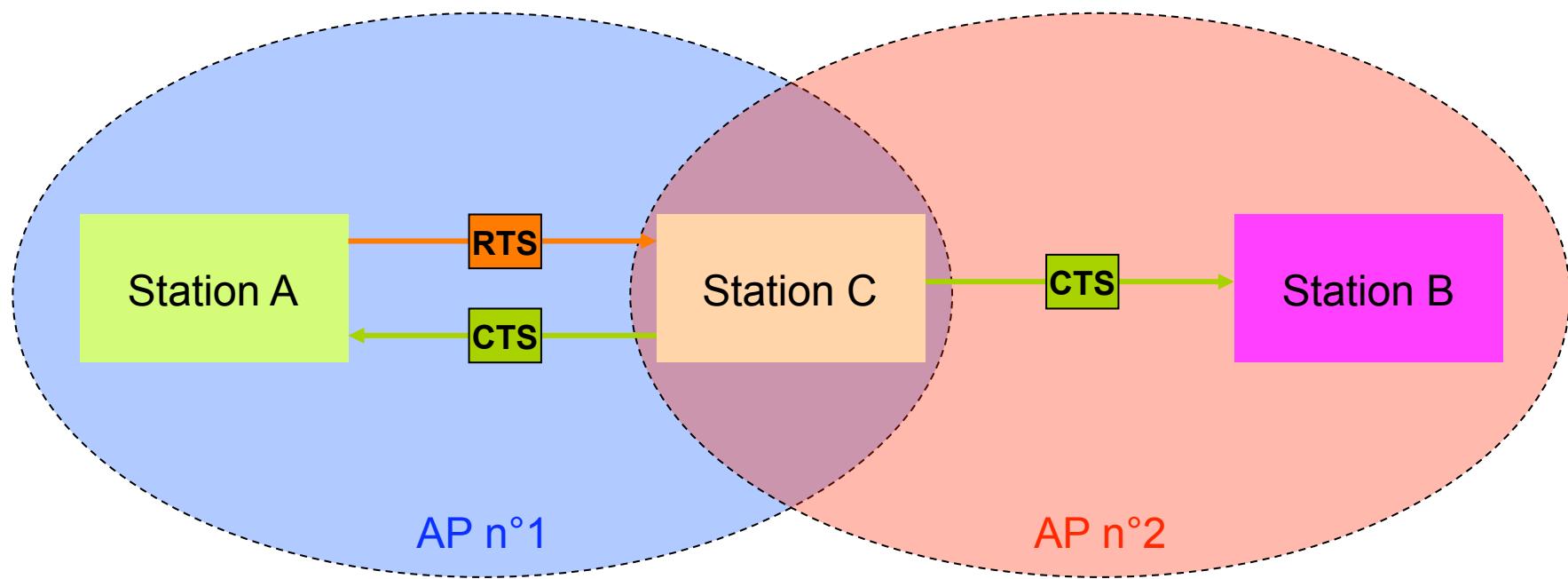
Station cachée



Station cachée

- Station B cachée de la station A mais pas de la station C
- La station A transmet des données à la station C, mais la station B ne détecte pas d'activité de la station A
 - Dans ce cas, la station B peut transmettre librement sans interférer avec la transmission de la station A
 - Si A et C échangent des RTS / CTS, la station B, bien que n'écoulant pas directement la station A, est informée par l'envoi par la station C d'un CTS que le support est occupé
 - B n'essaie donc pas de transmettre durant la transmission entre A et C
 - Ce mécanisme ne permet pas d'éviter les collisions, mais une collision de RTS / CTS ne gaspille pas autant de bande passante qu'une collision de données

Station cachée

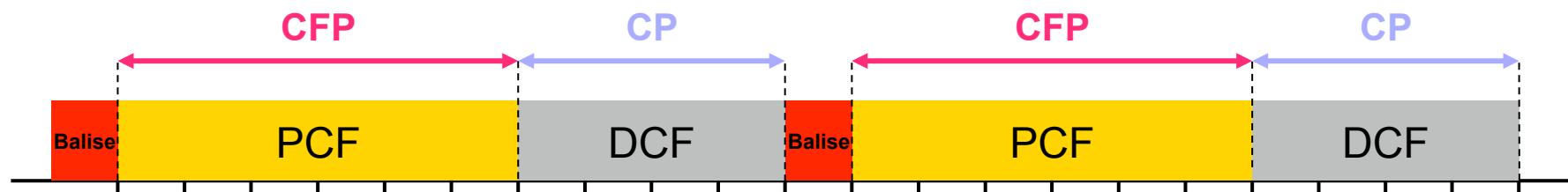


Conclusion CSMA/CA

- Permet de partager l'accès
- Mécanisme d'acquittement supporte les problèmes liés aux interférences et à tous les problèmes de l'environnement radio
- Mécanisme de réservation RTS / CTS évite les problèmes de la station cachée
- Inconvénient : ajout d'en-têtes aux trames 802.11
 - Performances + faibles que les réseaux locaux Ethernet

Méthodes d' accès dans 802.11

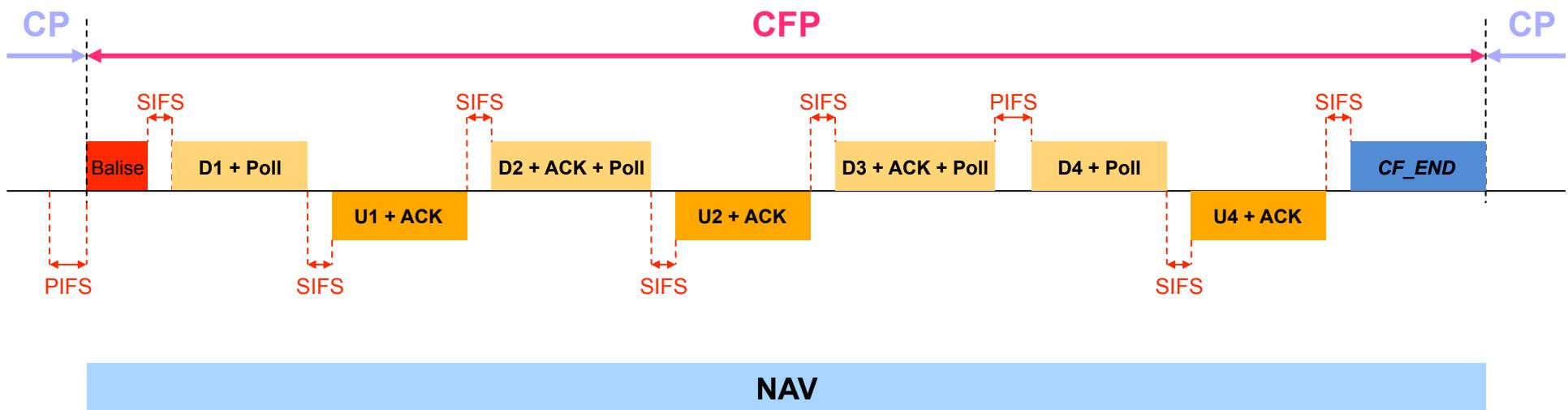
- *Distributed Coordination Function (DCF)*
 - méthode d' accès avec collision
- *Point Coordination Function (PCF)*
 - méthode d' accès sans collision



PCF (1/2)

- PCF permet le transfert de données isochrones
- Méthode d' accès basée sur le polling
- Inconvénient : Méthode jamais implémentée au niveau des points d' accès

PCF (2/2)



Couche liaison

- Fragmentation – réassemblage
- Handovers
- Sécurité
- Économie d' énergie
- Trames 802.11

Fragmentation - réassemblage

- La fragmentation accroît la fiabilité de la transmission en permettant à des trames de taille importante d'être divisées en petits fragments
 - Réduit le besoin de retransmettre des données dans de nombreux cas
 - Augmente les performances globales du réseau
- Fragmentation utilisée dans les liaisons radio, dans lesquelles le taux d'erreur est important
 - + la taille de la trame est grande et + elle a de chances d'être corrompue
 - Lorsqu'une trame est corrompue, + sa taille est petite, + le débit nécessaire à sa retransmission est faible

Fragmentation - réassemblage

- IEEE 802.11 utilise un système à saut de fréquence (frequency hopping)
 - Le support s'interrompt toutes les 20 ms pour changer de fréquence
- Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil, appelée Fragmentation_Threshold
- Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle
 - Le support n'est libéré qu'une fois tous les fragments transmis avec succès
 - Si un ACK n'est pas correctement reçu, la station arrête de transmettre et essaie d'accéder de nouveau au support et commence à transmettre à partir du dernier fragment non acquitté
 - Si les stations utilisent le mécanisme RTS / CTS, seul le premier fragment envoyé utilise les trames RTS / CTS

Fonctionnement d'IEEE 802.11

- Handover
 - passage d'une cellule à une autre sans interruption de la communication
 - Handover non prévu dans les premières versions, introduit dans les nouvelles versions
- Sécurité renforcée pour éviter :
 - qu'un client ne prenne la place d'un autre
 - Qu'il n'écoute les communications d'autres utilisateurs

Handovers

- Lorsqu'un terminal se déplace d'une cellule à une autre sans interrompre la communication
 - À peu près de la même manière que dans la téléphonie mobile
 - Dans les réseaux sans fil, le handover se fait entre 2 transmissions de données et non au milieu d'un dialogue
- Le standard ne fournit pas un mécanisme de handover à part entière, mais définit quelques règles
 - Synchronisation
 - Écoute active et passive
 - Mécanismes d'association et de réassociation, qui permettent aux stations de choisir l'AP auquel elles veulent s'associer

Handover et synchronisation

- Lorsque les terminaux se déplacent, ils doivent rester synchronisés pour pouvoir communiquer
- Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès
 - Pour garder la synchronisation, le point d'accès envoie périodiquement des trames balisées appelées Beacon Frames, qui contiennent la valeur de l'horloge du point d'accès
 - Lors de la réception de ces trames, les stations mettent à jour leurs horloges pour rester synchronisées avec le point d'accès

Écoute passive et active

- Quand un terminal veut accéder à un BSS ou à un ESS contrôlé par 1 ou plusieurs points d'accès
 - Après allumage, retour d'un mode veille ou d'un handover
 - Choisit un point d'accès auquel il s'associe selon un certain nombre de critères
 - Puissance du signal
 - Taux d'erreur des paquets
 - Charge du réseau
 - Si la puissance d'émission du point d'accès est trop faible, la station cherche un autre point d'accès approprié
 - 2 manières différentes : écoute passive ou active

Écoute passive et active

- Selon des critères tels que les performances ou la consommation d'énergie
- Écoute passive
 - La station attend de recevoir une trame balise provenant du point d'accès
- Écoute active
 - Une fois que la station a trouvé le point d'accès le plus approprié, il lui envoie directement une requête d'association par l'intermédiaire d'une trame Probe Request Frame et attend que l'AP lui réponde pour s'associer

Écoute passive et active

- Lorsque le terminal est accepté par le point d'accès, il se règle sur son canal radio le + approprié
- Périodiquement, le terminal surveille tous les canaux du réseau pour évaluer si un AP ne possède pas de meilleures performances

Réassociations

- Lorsqu'une station se déplace physiquement par rapport à son point d'accès d'origine
 - Diminution de la puissance du signal
- Changement des caractéristiques de l'environnement radio
- Trafic réseau trop élevé sur le point d'accès d'origine
 - Fonction d'équilibrage de charge fournie par le standard : Load Balancing
 - Répartition de la charge de manière efficace au sein du BSS ou de l'ESS

Handover dans 802.11

- Le standard ne définit pas de handovers ni de roaming dans les réseaux 802.11
- Solution : 802.11f en cours de développement

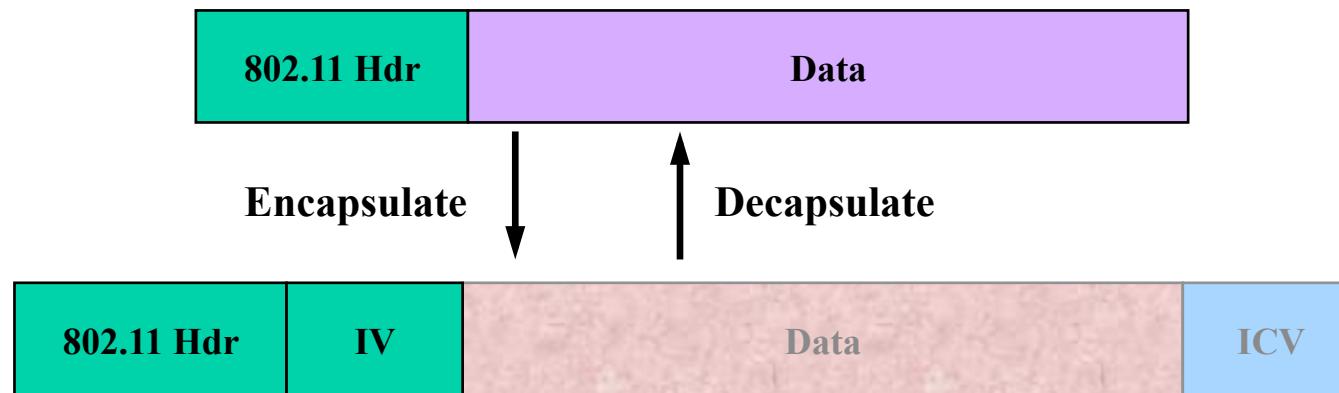
Sécurité dans 802.11

- Accès au réseau
 - Service Set ID (SSID)
 - Access Control List (ACL)
- Wired Encryption Privacy (WEP) : Mécanisme de chiffrement basé sur le RC4
- Authentification
 - Open System Authentication
 - Shared Key Authentication

WEP

- WEP(Wired Equivalent Privacy).
- Une partie du standard 802.11.
- Ses objectifs:
 - Confidentialité.
 - Contrôle d' accès.
 - Intégrité.
- L' utilisation de WEP est une option du 802.11.

Encapsulation WEP



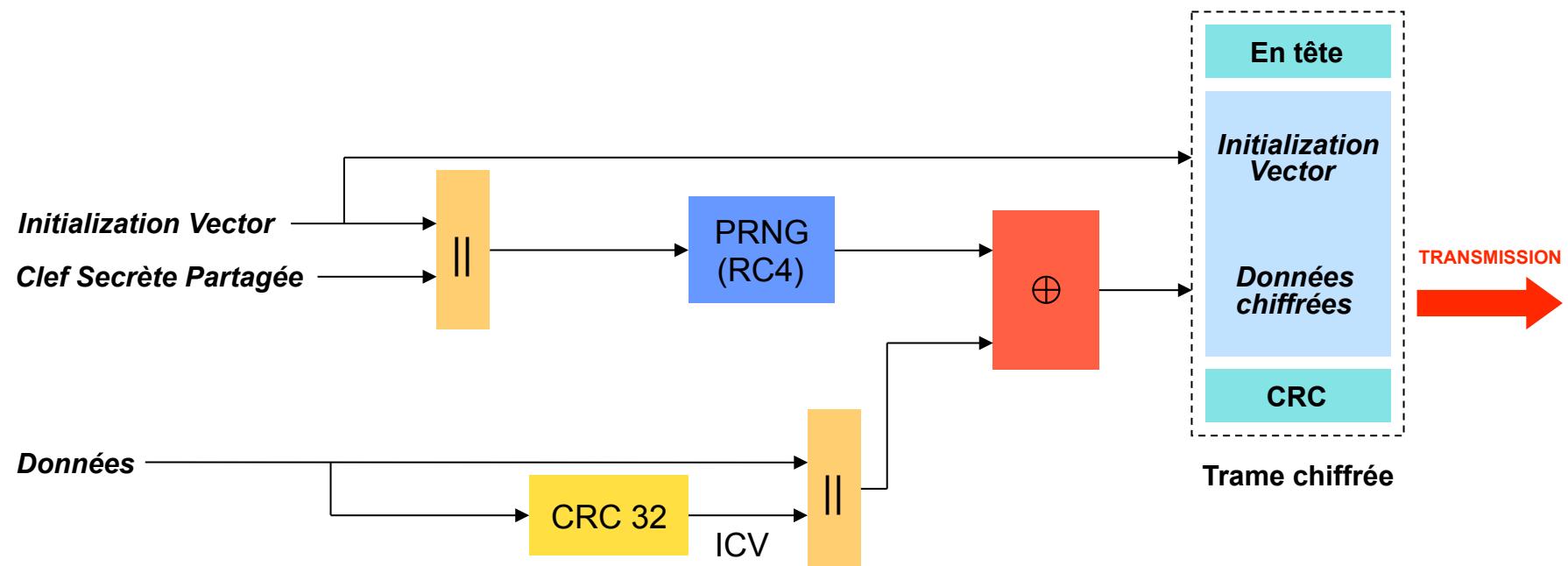
ICV : Integrity Check Value

IV : Initialisation Vector : 1 pour chaque paquet

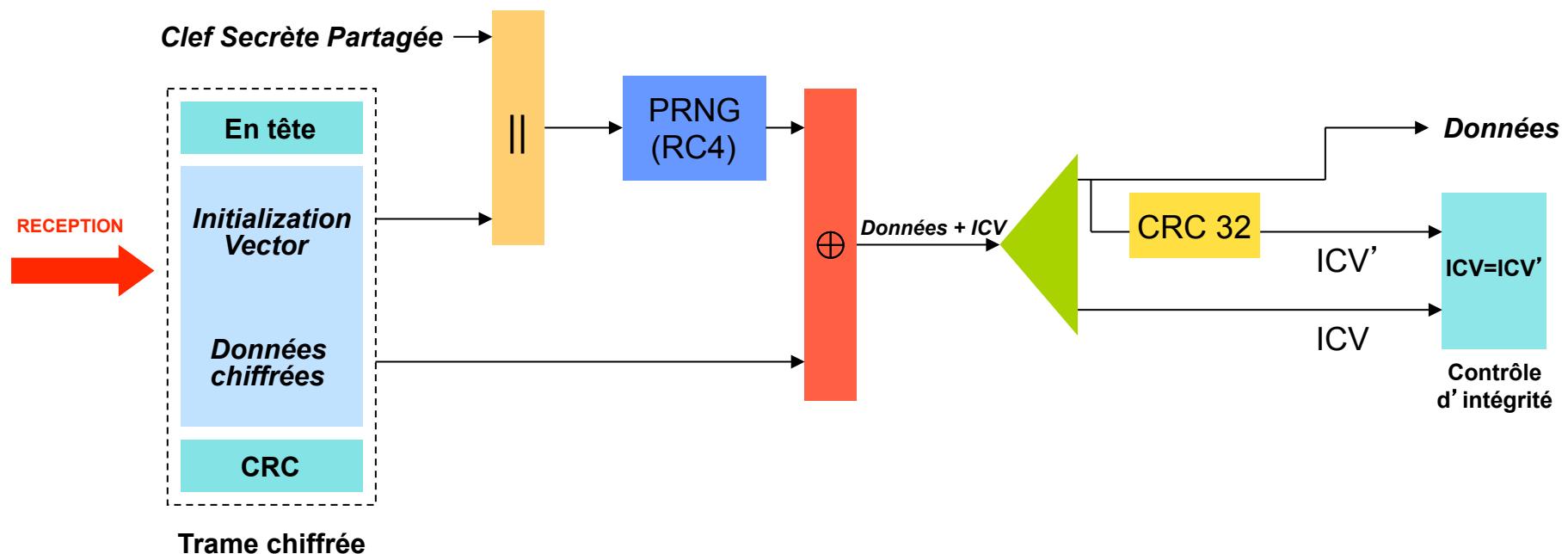
Le fonctionnement de WEP

- Algorithmes utilisés : RC4 et CRC-32bit.
- Paramètres:
 - Plaintext : P.
 - Ciphertext : C.
 - Clé partagée: k (40 bits)
 - Un vecteur d' initialisation IV (généré pour chaque paquet): v (24bits)
- Processus :
 - Calculer CRC(P): $c(P)$
 - Lier P et $c(P)$
 - Calculer $RC4(v, k)$
 - Résultat : $C = (P, c(P)) \oplus RC4(v, k)$.

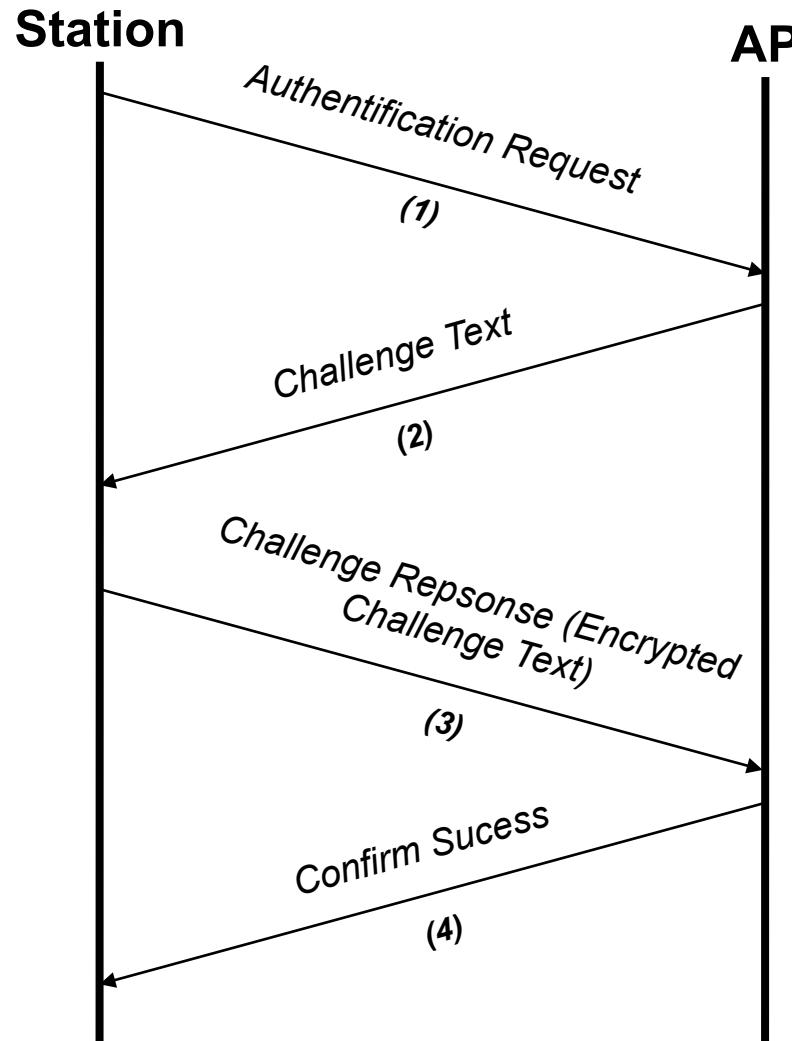
WEP : Chiffrement



WEP : Déchiffrement



Shared Key Authentication



Failles dans 802.11

- Tous les mécanismes de sécurité peuvent être déjoués
- Solutions :
 - A court terme
 - WEP +
 - 802.1x avec EAP (Extended Authentication Protocol)
 - A long terme
 - 802.11i basé sur AES (Advanced Encryption Standard)

Problèmes avec WEP

- Plusieurs attaques possibles :
 - Accès non autorisé.
 - Modification des messages.
 - Attaque par dictionnaire.
 - Etc.
- 15 minutes pour casser une clé de 40 bits en attaque passive, pas beaucoup plus long pour une clé de 128 bits !

Chiffrement symétrique

- Chiffrement par flot : (RC4)
 - Le cryptage est effectué bit-à-bit sans attendre la réception complète des données.
 - Le but d'un stream cipher est de générer une chaîne aléatoire à partir d'une clé de longueur courte.
 - Nécessité de changer de clé à chaque message ou d' introduire un IV.
- Chiffrement par bloc: (DES, AES)
 - Chiffrer les blocs de taille fixe(habituellement 64 bits).
 - Le plus souvent entrée et sortie de même taille.

Confidentialité : Les attaques passives

- Les ondes peuvent traverser les murs.
- Avec une antenne, un attaquant peut espionner les trafics dans un périmètre de 100 mètres.
- Ces attaques sont difficiles à détecter.

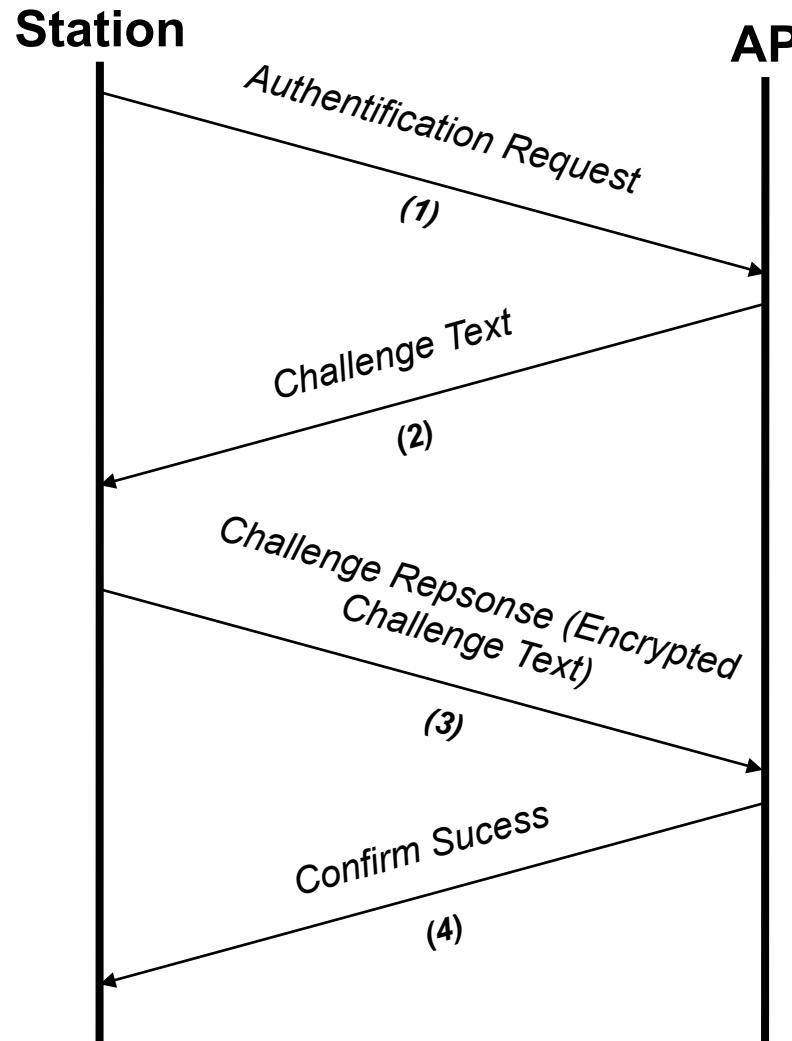
Confidentialité : Problèmes de la réutilisation de v et k

- Il faut changer k après que tous les 2^{24} IVs aient été utilisés (5 heures pour un débit de 11Mbps).
 - IV est trop court (24 bits), donc il a beaucoup de chances d’être réutilisé.
 - IV est souvent réinitialisé par la carte PCMCIA, mais non aléatoirement.
 - Pas de mécanisme pour éviter la réutilisation du v.
 - Pas de mécanisme pour renouveler k.
- Un attaquant peut établir un tableau pour toutes les possibilités et utiliser les parties connues (L’en-tête IP, ICMP etc...) pour retrouver les parties non connues.

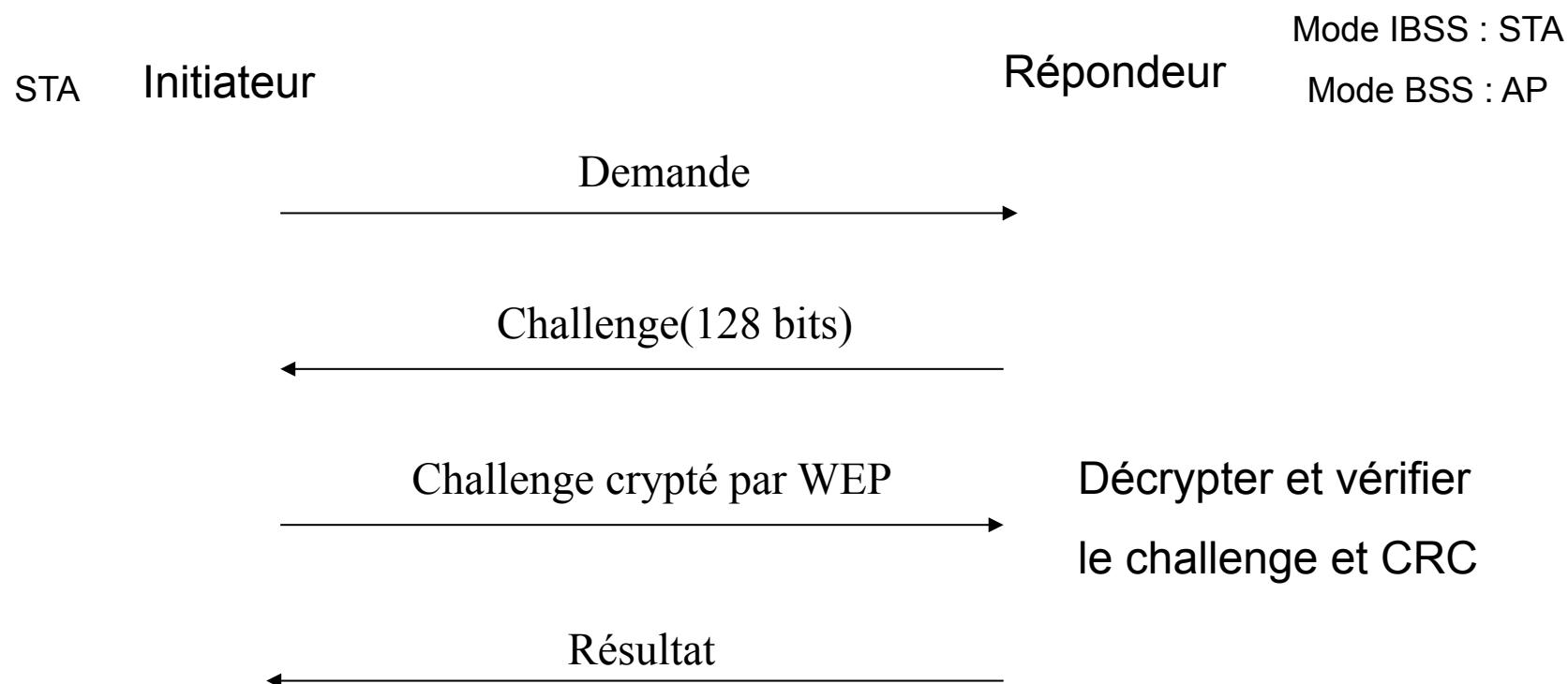
Les méthodes du contrôle d' accès

- Dans le standard:
 - Authentification ouverte(OPEN system authentication)
 - Pas de clé, les messages d' authentification sont en clair.
 - Authentification avec clé partagée(Shared key authentication).
- MAC ACL (Access-Control Lists).

Shared Key Authentication



Authentification avec clé partagée



Problème du processus

- Un attaquant peut découvrir le challenge ch et sa version cryptée C_{ch} en espionnant.
- Donc il peut calculer $RC4(v, k)$ par $C_{ch} \oplus ch$.
- Il y a aussi v dans le paquet en clair.
- Donc il peut s'authentifier avec v et $RC4(v, k)$ quand il veut, autant qu'il veut! Pas la peine de savoir k !

Filtrage de l'adresse MAC

- Une adresse MAC est obligatoirement transmise en clair.
- Les cartes sans fils permettent de changer leurs adresses MAC par logiciel.
- La liste des adresses MAC ne peut pas être très longue. (1000 nœuds maxi.)
- Quand il y a plusieurs APs (Access Point), il faut maintenir la cohérence.
- Il faut traiter les pertes et les vols.

Autres problèmes d'authentification

- Pas d'authentification pour les messages d'administration :
 - Réauthentification.
 - Désauthentification.
 - Association.
 - Réassociation.
 - Déassociation.
 - Beacon et probe.
- Les attaques par DoS sont possibles.

Intégrité : Problèmes avec CRC

- L'objectif de CRC (un checksum) est de corriger les erreurs générées pendant les transmissions.
 - Il est linéaire.
 - Il n'utilise pas de clé.
- Il ne peut pas garantir l'intégrité contre les modifications(Ajouter/Modifier).

Les logiciels d' attaque

- NetStumbler : Retrouver les APs, les cartes et l' infrastructure du réseau, et espionner les trafics <http://www.NetStumbler.com>
- Espionner les trafics, casser la clé:
 - Airsnort <http://airsnort.sourceforge.net/>
 - WEPCrack <http://sourceforge.net/projects/wepcrack>
- THC-RUT (Brute force WLAN)
<http://www.thehackerschoice.com/releases.php>.
- IBM's wireless LAN security analyzer:
 - réalisé sur un PDA linux, permet de retrouver les APs, le nom du réseau (SSID), les nœuds, les adresses, les locations et les états de la sécurité du réseau.
- ISS Internet Scanner a rajouté, l' année précédente, une partie pour scanner la vulnérabilité de WLAN, qui peut être utilisé par un attaquant aussi.
- Sous Unix et Linux, Ethereal a aussi rajouté la possibilité de sniffer les WLANs.

Résumé

- WEP n' atteint pas ses objectifs initiaux à cause de:
 - Manque de protection contre la réutilisation du IV et k.
 - Court IV.
 - Vulnérabilité du RC4 à cause de l' implémentation de WEP.
 - La linéarité de CRC.
 - Manque d' un MIC avec clé.
 - Une clé partagée trop courte.
 - Etc.
- C' est difficile de l' améliorer, il vaut mieux le changer.

Solutions proposées

- Augmenter la longueur de clé.
 - 128 bits(104 bits clé + 24 bits IV) pour WEP2.
- Changer fréquemment la clé.
- Utiliser les mots de passe pour les APs et les terminaux.
- Contrôler l' utilisation des ressources, ne pas faire «tout ou rien ».
- Ne pas utiliser « open system authentication », choisir un mécanisme de contrôle d' accès.
- Introduire plus de clés, par exemple, une clé par station.
- Authentification par paquet.
- Utiliser SSH à la couche 7, SSL/TLS à la couche 4, IPSec à la couche 3.
- Ajouter les mécanismes pour éviter la réutilisation du IV.
- VPN.
- 802.1X.

802.1x

- Boîte à outils générique pour les LANs :
 - L'authentification à base de ports.
 - La gestion des clés.
- Port = un point d'attachement d'un système à LAN :
- Ne plus authentifier les terminaux, mais authentifier les utilisateurs.
- Changer les clés fréquemment et dynamiquement par les APs ou les serveurs d'authentification.

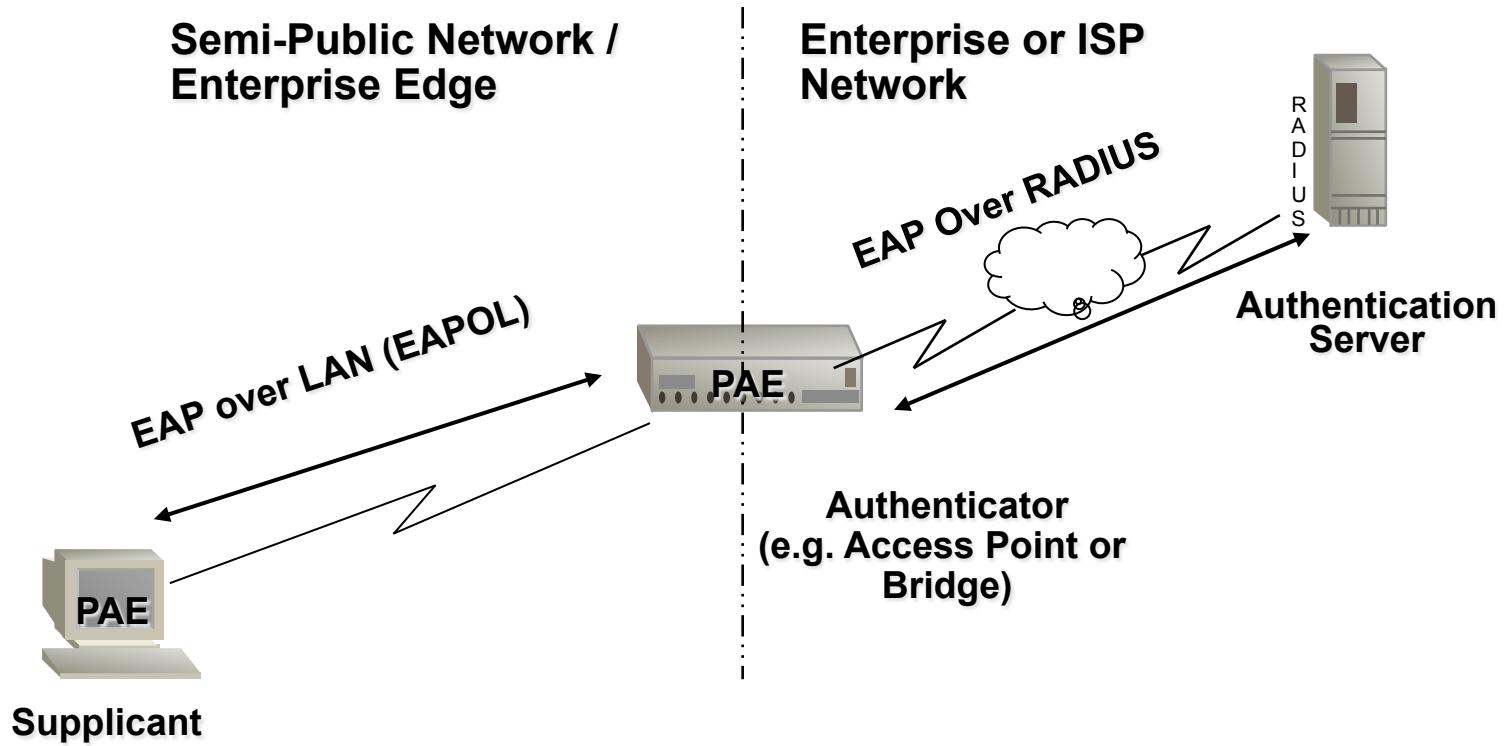
Caractéristiques de 802.1x

- Chaque station peut avoir sa propre clé dynamique par session.
- Flexible, supporte les différents types d'authentification par EAP.
- Pas de définition sur l'algorithme de cryptage.
- Pas d'encapsulation.
 - Pas d'en-tête ajouté.
 - Pas d'influence sur la performance.
 - Pas besoin d'acheter des nouveaux matériels.
 - Peut être implémenté sur NIC.
- Peut être intégré avec RADIUS et LDAP, supporte les réseaux VPN et les réseaux DialUp.
 - Remote Authentication Dial-In User Service

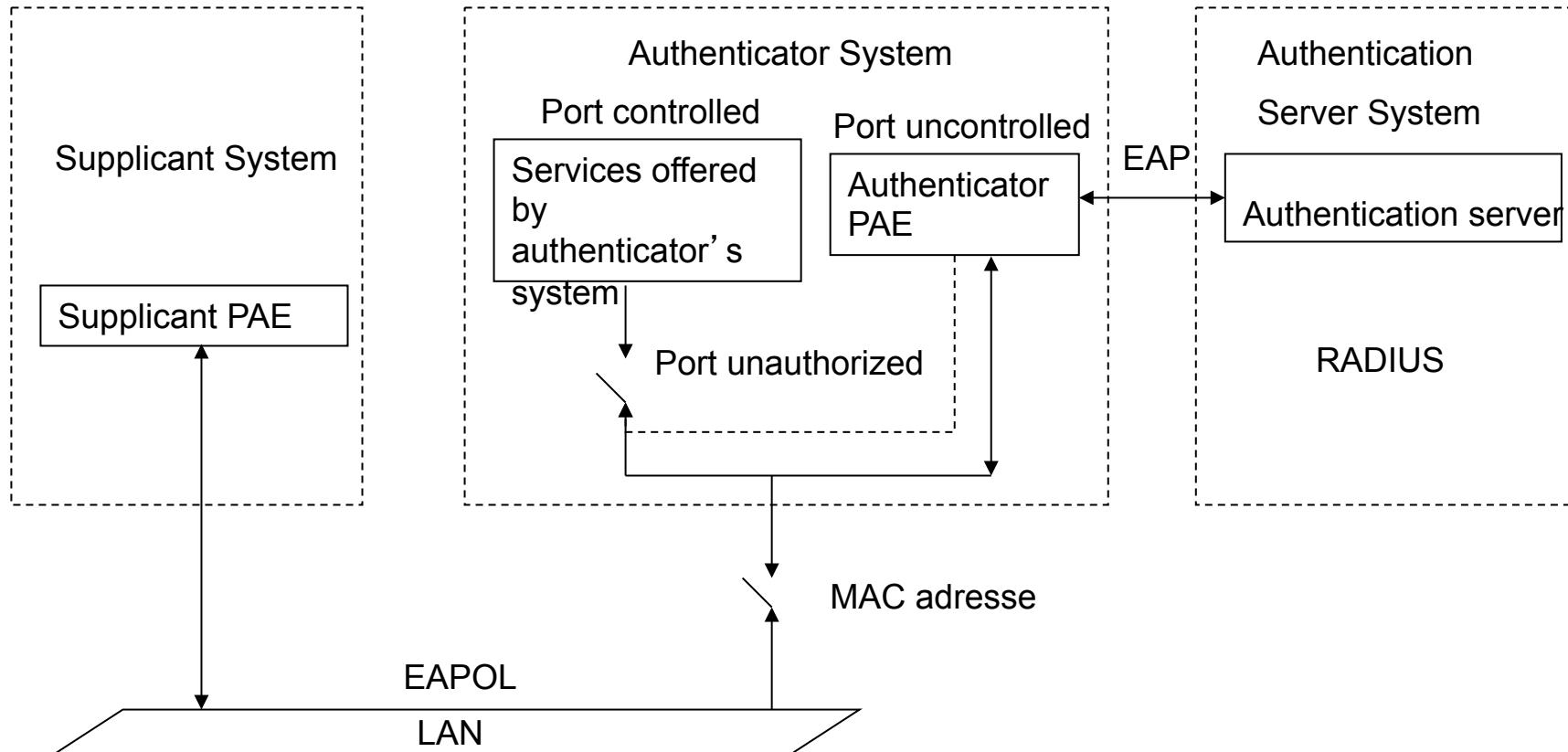
Définitions

- **Serveur d'authentification** : déterminer si un supplicant a l' autorisation d' accès aux services de l' authentificateur selon les certificats de supplicant.
 - RADIUS(Remote Authentication Dial-In User Service).
- **Authentificateur** : Un port qui veut imposer l' authentification avant les accès aux services fournis par lui-même.
- **Supplicant** : Un port qui veut accéder aux services fournis par le système de l' authentificateur.
- **PAE (Port Access Entity)** : Une entité de protocole liée avec un port.
 - **Supplicant PAE** : répondre aux demandes de l' authentificateur pour les informations qui permettent d' établir ses certificats.
 - **Authentificateur PAE** : soumettre les certificats à un serveur d' authentification pour les vérifier et ensuite déterminer et contrôler l' autorisation de ce port.

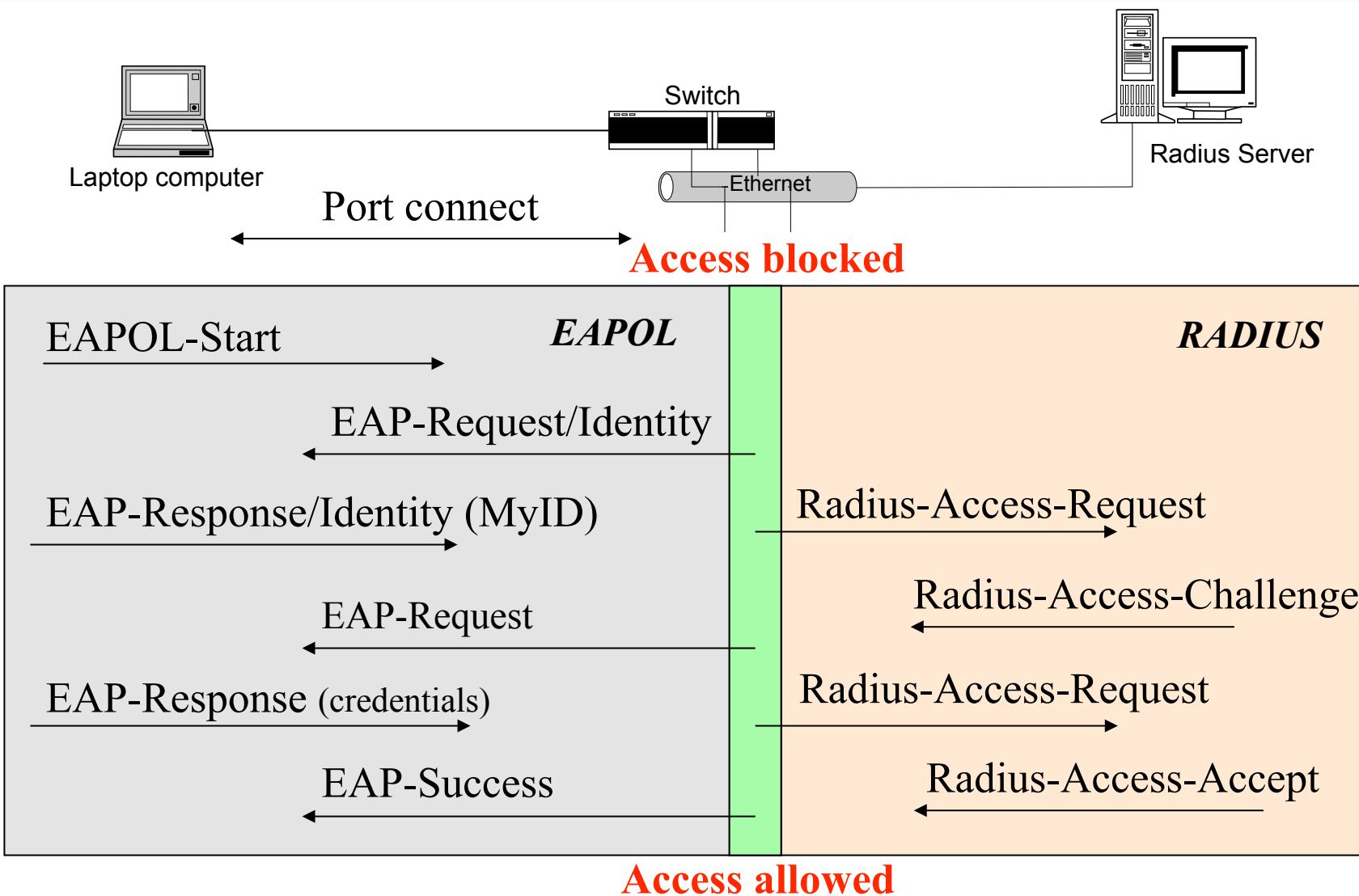
La topologie 802.1X



Rôles d' Authenticateur, Supplicant et Serveur d' authentification



IEEE 802.1x Conversation



RADIUS (RFC 2865)

- Les informations d'authentification ne sont plus dans WLAN et APs, mais dans RADIUS.
- Supporter AAA(authentication authorization, accounting).
- RADIUS utilise HMAC pour fournir l'intégrité et l'authenticité par paquet pour les paquets transmis entre AP et lui.

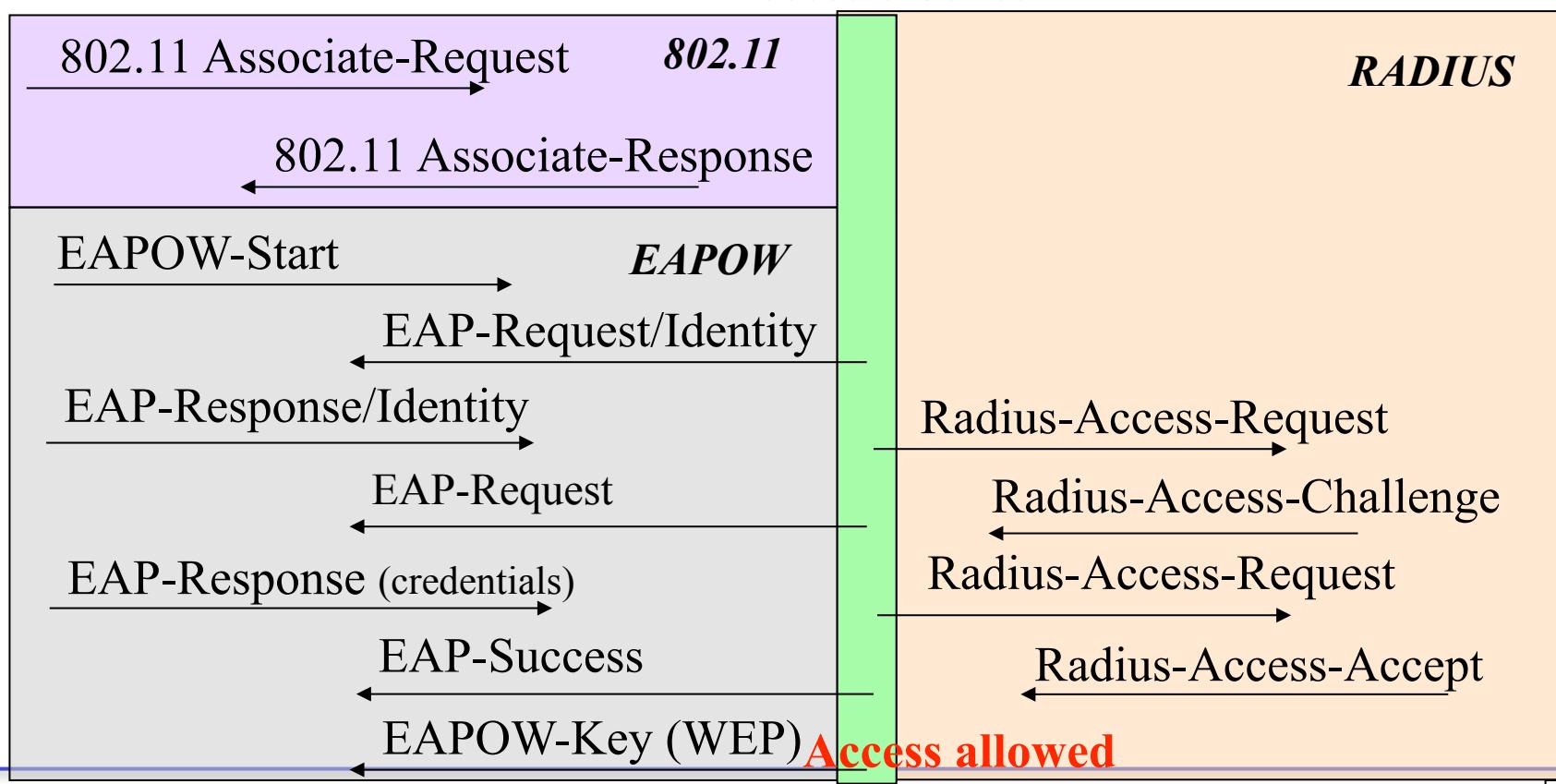
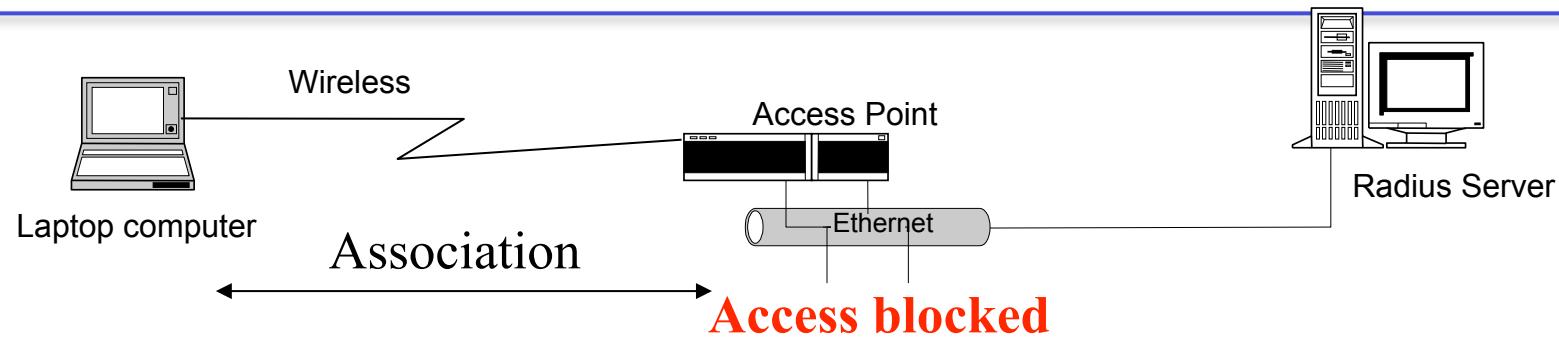
EAP (Extended Authentication Protocol) RFC 2284.

- Protocole général qui supporte de multiples méthodes (carte à puce, token cards, one-time passwords, kerberos, public key encryption, etc) d'authentification.
- EAP peut :
 - Renouveler les clés.
 - Authentifier utilisateur.
 - Faire une authentification mutuelle.

Convergence de 802.11 et 802.1x

- 802.11 Tg I (task groupe *i*).
- Utiliser 802.1x avec TKIP, AES.
- Utiliser certains EAPs pour contrer l' attaque par dictionnaire.
- Changer les clés par scripts ou SNMPv3 (Simple Network Management Protocol).
- Mise à niveau des APs.

802.1x Sur 802.11



Nouveaux algorithmes de chiffrement

- 802.11 Tg I veut introduire deux nouveaux algorithmes de chiffrement qui supportent la protection d'intégrité par paquet et la confidentialité :
 - TKIP (Temporal Key Initiation Protocol).
 - Faible protection d'intégrité
 - Mise à jour du AP.
 - Basé sur WEP, solution à court terme.
 - AES (Advanced Encryption Standard).
 - Plus forte et plus simple que 3DES.
 - Besoin de plus de 4.6 milliards d'années pour le casser.
 - Solution à long terme.

Problèmes de 802.11i (1/2)

- L'attaque par dictionnaire.
 - Utiliser les EAPs résistants: EAP TLS, SRP, TTLS et PEAP (pas kerberos).
- L'attaque sur la clé par défaut.
 - Changer la clé par session à l'aide de SNMPv3 ou un script, etc.
- L'attaque DoS sur :
 - Trame EAPOL-logoff (pas d'authenticité) :
 - Moyen d'attaque: Logoff un utilisateur depuis un AP.
 - Solution : Authentifier les trames EAPOL-logoff, ou utiliser les messages de déassociation authentifiés à la place.
 - Trame EAPOL-Start.
 - Moyen d'attaque : Bombarder les trames EAPOL-start à un AP.
 - Solution : Ne pas allouer beaucoup de ressources en acceptant une trame de ce type.

Problèmes de 802.11i (2/2)

- Consommer l’ espace du EAP Identifier. (255)
 - Moyen d’ attaque : Un AP va refuser les nouvelles connexions si l’ espace du EAP Identifier est consommé.
 - Solution : Même si l’ espace est consommée, on accepte les connexions.
- Paquet EAP-success.
 - Moyen d’ attaque : Un attaquant envoie un faux EAP-success au supplicant.
 - Solution : Authentifier les paquets EAP-success ou utiliser un EAP-key pour signifier le succès de l’ authentification.
- Paquet EAP-failure.
 - Moyen d’ attaque : Un attaquant envoie un faux EAP-failure au supplicant avec la bonne adresse MAC de l’ authenticateur.
 - Solution : Il faut un message déassociation authentifié suivi un EAP-Failure.
- La modification des paquets EAP.
 - Solution : L’ intégrité et la confidentialité de tous les paquets (données et administrations) EAP doivent être protégées. Une solution est de utiliser les EAPs TLS, TTLS et PEAP.

Conclusion sécurité

- WEP est vulnérable.
 - WLAN : hacker's playground.
- 802.1x peut renforcer la sécurité de 802.11 dans l' aspect de l' authentification et de la gestion de clé.
- 802.11 Tg I est en train de converger 802.1x et 802.11 et de introduire des nouveaux chiffrements.
- Il y a encore des problèmes de la sécurité dans 802.11i, mais on peut l' améliorer plus facilement qu' améliorer WEP.

Économie d'énergie

- Problème principal des terminaux mobiles: faible autonomie de la batterie
 - Mode d'économie d'énergie prévu par le standard
- 2 modes de travail pour le terminal
 - Continuous Aware Mode
 - Fonctionnement par défaut
 - La station est tout le temps allumée et écoute constamment le support
 - Power Save Polling Mode

Power Save Polling Mode

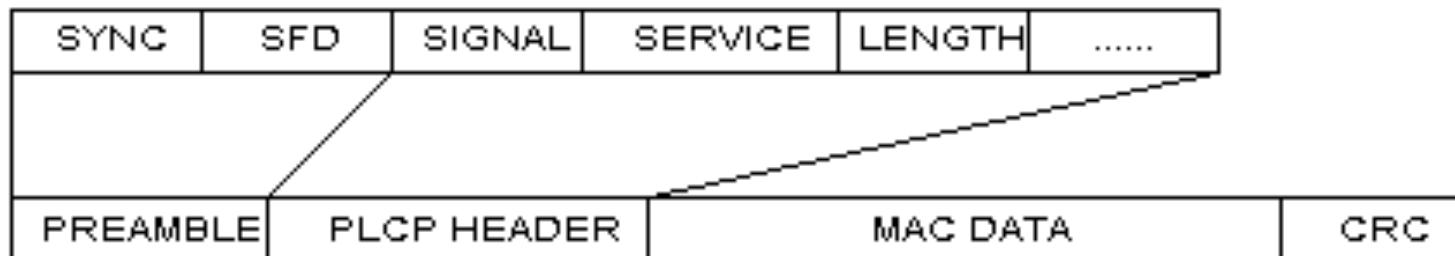
- Permet une économie d'énergie
- Géré par le point d'accès
 - L'AP tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie
 - Stocke toutes les données qui leur sont adressées
 - Les stations en veille s'activent périodiquement pour recevoir une trame TIM (Traffic Information Map), envoyée par l'AP
 - Si l'AP contient des données destinées à la station, celle-ci envoie une requête à l'AP : Polling Request Frame
- Entre les trames TIM, les terminaux retournent en mode veille
- Le point d'accès réveille périodiquement les stations en mode veille

Trames IEEE 802.11

- Les paquets IP composés dans les terminaux du réseau doivent être transmis sur le support hertzien
 - Placés dans une trame Ethernet
- 3 types de trames
 - Trames de données
 - Transmission de données utilisateur
 - Trames de contrôle
 - Pour contrôler l'accès au support
 - Trames de gestion
 - Pour les associations et désassociations
 - Pour la synchronisation
 - Pour l'authentification

Structure des trames

- Préambule : dépend de la couche physique
 - Séquence Synch pour sélectionner l'antenne à laquelle se raccorder
 - Séquence SFD (Start Frame Delimiter) pour définir le début de la trame
- PLCP : infos logiques utilisées par la couche physique pour décoder la trame
- Données MAC
- CRC



Trames de contrôle

- 3 trames de contrôle
 - RTS (Request To Send)
 - CTS (Clear To Send)
 - ACK

Conclusion et perspectives

- Version actuellement sur le marché : IEEE 802.11b
 - Mise en place de réseaux locaux sans fil pouvant atteindre un débit de 11 Mbit/s
 - Excellentes performances de IEEE 802.11, dues à l'importante bande passante disponible et à la réutilisation des fréquences
 - De nombreuses entreprises ont investi dans ce type de réseau sans fil
 - Sécurité globale assez faible
 - Facile d'écouter les porteuses depuis l'extérieur
 - Réseaux principalement utilisés dans les lieux publics, clients la recherche d'information
 - Futures générations de réseaux IEEE 802.11 bien avancées
 - Accès à l'interface réseau différent
 - Augmentation du débit (26 Mbit/s puis 52 Mbit/s, voire quelques centaines de Mbit/s)