Réseaux Locaux Sans Fil : IEEE 802.11

Pr. : Essaid SABIR
Contact : e.sabir@ensem.ac.ma
Ecole d'ingénierie : GI2
Année : 2018/2019

Plan

- Les systèmes de communication sans fil
- La norme IEEE 802.11
- Mode Ad-hoc
- Sécurité de la norme IEEE 802.11
- Déploiement d'un réseaux WIFI

Les systèmes de communication sans fil

Introduction

- Avec l'essor des débits, les réseaux sans fil sont aussi bien utilisés comme réseaux locaux dans le cadre des réseaux privés d'entreprise que dans celui des réseaux d'accès.
- Produits sont construits autour de la norme 802.11
- le plus répondu d'entre eux est le Wi-Fi issu de la norme 802.11b qui fournit un débit de 11Mbit/s
- Vers 11millions de cartes radio IEEE 802.11b auraient été vendues (2012).

Le WIFI

- Wireless Fidelity c'est une marque délivré par le WECA (wireless Ethernet compatipility alliance) pour la norme IEEE 802.11 b

- WiFi-5 : la norme 802.11a

Pourquoi déployer un réseau sans fil ?

- Pour faciliter la connexion des utilisateurs itinérants, en particulier dans les espaces collectifs
- Pour connecter des locaux impossibles ou trop coûteux à câbler (monument historique)
- Pour mettre en place une connexion provisoire (travaux)
- Pour occuper l'espace : offrir le service pour éviter les installations pirates
- Le sans fil n'est pas destiné à remplacer intégralement le câblage filaire (fiabilité, débit)
- *Il n'est pas fait pour connecter des serveurs !*

Les différents types de réseau sans fil

	WPAN	WLAN	WMAN	WWAN
Nom commun	Bluetooth et autres	WiFi	WiMax	GSM, GPRS, UMTS
Bande de fréquence	2,4 GHz	2,4 / 5 GHz	2 – 11 GHz	900 / 1800 MHz 1900 / 2200 MHz
Portée	qq m	100 m	50 km	35 km
Débit théorique	3 Mb/s	54 Mb/s	70 Mb/s	9600 Kb/s -> 2 Mb/s
Applications	Connexion périphériques	Réseau local	Accès	Téléphonie et données
Norme	IEEE 802.15	IEEE 802.11	IEEE 802.16	ITU

La norme IEEE 802.11

La norme IEEE 802.11

- « Wi-Fi » est un label d'interopérabilité délivré par la Wi-Fi alliance :
- groupement de constructeurs qui publie des listes de produits certifiés (http://www.wi-fi.org/)
- 802.11 (1997) : jusqu'à 2 Mb/s
- 802.11 (1999) : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- 802.11b (1999) : 11 Mb/s dans la bande des 2,4 GHz
- 802.11a (1999) : 54 Mb/s dans la bande des 5 GHz
- 802.11g (2003) : 54 Mb/s dans la bande des 2,4 GHz (compatible avec 802.11b)

La norme IEEE 802.11

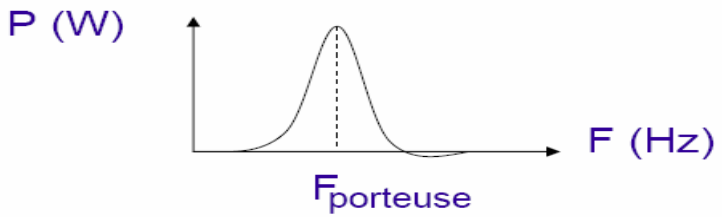
- 802.11f (2003) : Inter Access Point Protocol (IAPP) gestion de la mobilité (roaming)
- 802.11h (2003) : pour l'utilisation de 802.11a en Europe sélection dynamique de canal et gestion de la puissance d'émission
- 802.11i (2004) : sécurité
- 802.11j : Normalisation Japonaise
- 802.11r : Utilisation de l'infra-rouge
- 802.11e (2005) : qualité de service
- Travaux en cours :
  - IEEE 802.11k : mesure de la qualité de la liaison radio
  - IEEE 802.11n : débit > 100 Mbps
  - IEEE 802.11r : transfert rapide de connexion entre bornes
  - IEEE 802.11s : réseaux maillés
  - IEEE 802.11ac : norme (débit > 1 Gbps)

La norme IEEE 802.11

Norme	Date de normalisation	Fréquences	Débit moyen	Débit max	Portée intérieure	Portée extérieure
Norme initiale	1997	2,4-2,5 GHz	1 Mbit/s	2 Mbit/s	?	?
802.11a	1999	5,15-5,35 GHz 5,47-5,725 / 5,725-5,875	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11b	1999	2,4-2,5 GHz	6,5 Mbit/s	11 Mbit/s	~35 m	~100 m
802.11g	2003	2,4-2,5 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11n	2009	2,4 GHz et/ou 5 GHz	200 Mbit/s	450 Mbit/s	~50 m	~125 m
802.11ac	jan. 2014	5,15-5,35 GHz 5,47-5,875 GHz	433 Mbit/s	1300 Mbit/s	~20 m	~50 m
802.11ad	2016	2.4, 60 GHz		7 Gbit/s	~15 m	~30 m

Emission / réception radio

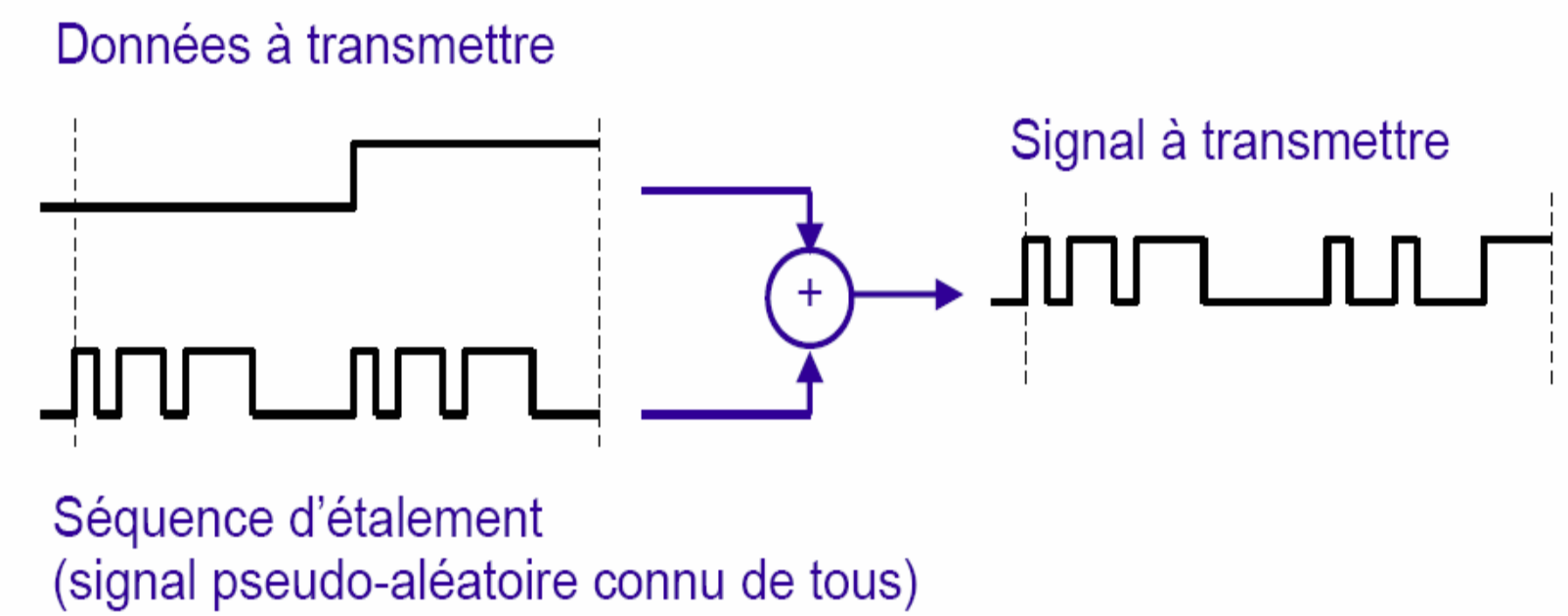
- Principe : transmission de l'information par modulation d'une porteuse
- Le signal transmis est caractérisé par son spectre



- En radio, la puissance est souvent exprimée en dBm (décibels)
- dBm = 10*log_{10}(P/ 0.001)
- 0 dBm = 1mW

IEEE 802.11b : Modulation

- DSSS : *Direct Sequence Spread Spectrum* étalement de spectre, séquence directe



- Selon la vitesse de transmission et du codage de 1, 4 ou 8 bits simultanément puis modulation de phase à 2 ou 4 états

Réglementation (ARCEP ex-ART)

- Puissances autorisées depuis juillet 2003 (exprimées en PIRE : Puissance Isotrope Rayonnée Equivalente)

Fréquences (MHz)	Canaux	Intérieur	Extérieur
2400 - 2454	1-8	100 mW	100 mW
2454 -2483,5	9-13	100 mW	10 mW

- Les usages privés (réseaux indépendants, usages particuliers) ne nécessitent pas de démarche auprès de l'ART.

Caractéristiques induites par le support

- Support partagé par tous
- Pas de limite franche ni visible au delà de laquelle la réception est impossible
- Le signal peut être brouillé par une source extérieure
- Le support de transmission est beaucoup moins fiable qu'en réseau filaire, et non maîtrisé
- Les stations ne sont pas fixes, mais portables, voire mobiles
- Certaines stations peuvent être cachées les unes aux autres
- Les vitesses de propagation peuvent varier dans le temps et être asymétriques

La norme IEEE 802.11

Couche MAC (IEEE 802.11)		
IEEE 802.11 DS 1,2 Mbit/s FH 1,2 Mbit/s IR	IEEE 802.11b 11Mbit/s	IEEE 802.11 a

La norme 802.11 propose :

- Une couche MAC unifiée (couche liaison), utilisée aussi bien par 802.11b que par 802.11a
- Une couche physique la ou il y a trois systèmes de niveaux physique différents et incompatibles entre eux.

Modes de fonctionnement

- La norme IEEE 802.11 dispose de deux modes de fonctionnement distincts qui correspondent à des architectures différentes
- Mode infrastructure avec point d'accès
- Mode ad-hoc

Modes de fonctionnement

- Mode avec infrastructure :
  - Existence d'un Point d'Accès (PA)
  - Des stations sans fil
  - Communication entre stations sans fil et réseau filaire
  - La norme désigne par BSS (basic service set) l'ensemble des stations radio à portée radio du PA
  - La zone de couverture est donc restreinte à la zone de portée radio autour de ce point d'accès.

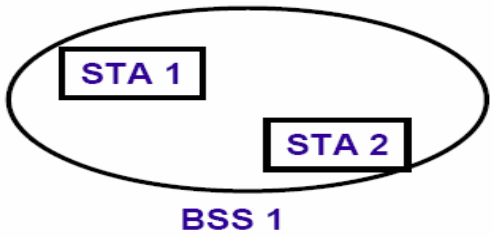
Modes de fonctionnement

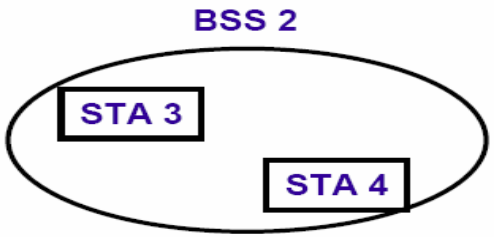
- Mode Ad-hoc
- Pas de station particulière , le réseau fonctionnant de façon totalement distribuée
- La norme désigne par IBSS (independent basic service set) l'ensemble des stations radio à portée radio mutuelle
- Le fonctionnement est totalement distribué, et la communication ne peut dépasser la portée de la transmission radio

Université Internationale de Casablanca
LAUREATE INTERNATIONAL UNIVERSITIES

Architecture 802.11

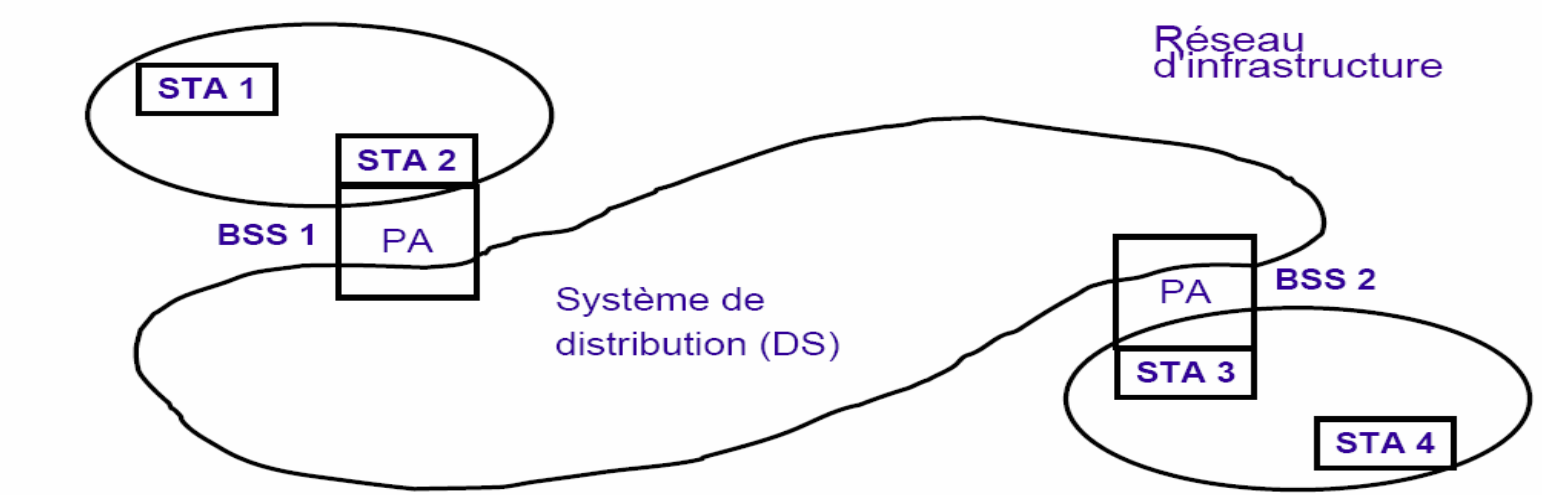
- Station : toute machine équipée d'une interface 802.11
- BSS (*Basic Service Set) : zone à l'intérieur de laquelle les stations* restent en communication
- BSS indépendants = réseaux « ad hoc »





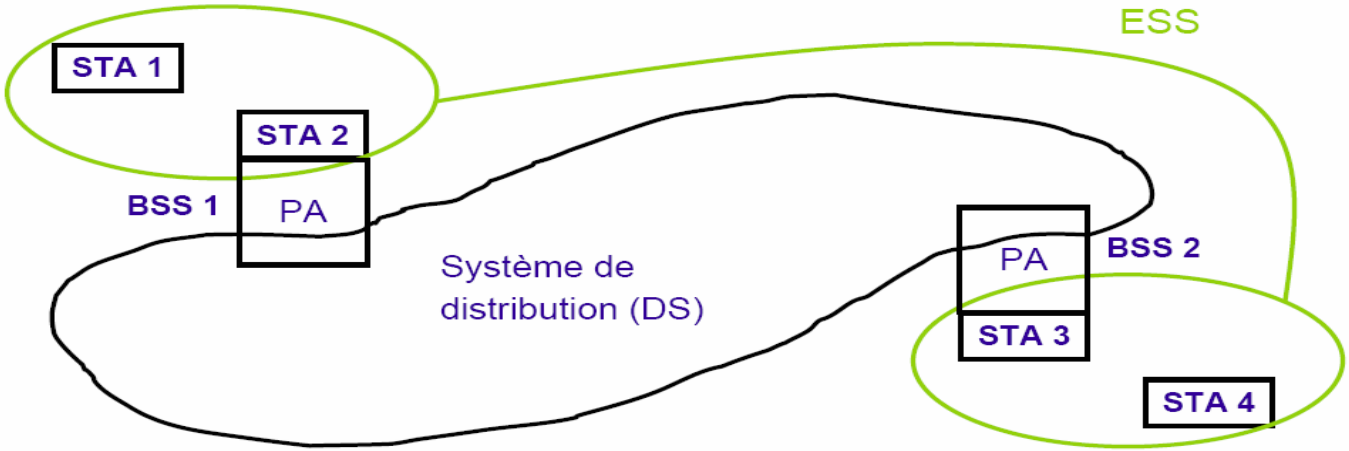
Architecture 802.11

- Les BSS peuvent être interconnectés par un « système de distribution » (DS, *Distribution System) : le plus souvent un réseau Ethernet*
- Un point d'accès est une station qui fournit l'accès au DS



Architecture 802.11

- ESS (*Extended Service Set) : ensemble de BSS interconnectés par un* système de distribution
- Les stations peuvent communiquer entre elles et passer d'un BSS à l'autre à l'intérieur d'un même ESS



Services de base

- Authentification/dés-authentification
  - Doit permettre à une station de s'authentifier , ce service peut être vide si aucune authentification n'est requise.
- Acheminement des trames
  - Il permet de transmettre une trame d'une station source vers une station destination
- Sécurité
  - Permet de chiffrer les trames de données transmises

Services complémentaires

- Mode infrastructure
  - Association/détachement
  - Distribution
  - Intégration

Services complémentaires

- Association/dés-association
  - Permet de fédérer les stations autour d'un point d'accès. Une station qui souhaite s'insérer dans le réseau doit s'associer avec le oint d'accès. Fait parti alors du BSS du PA
  - La station peut faire appel au service du point d'accès pour l'acheminement des trames qu'elle souhaite envoyer
  - La dés-association est le service qui permet de rompre cet attachement

Services complémentaires

- Distribution

  - Permet d'aiguiller les trames dans le système de distribution pour que celles-ci puissent rejoindre leur destination finale

  - Le point d'accès est point de passage obligé pour la transmission en mode infrastructure, même pour l'échange d'une trame entre deux stations d'un même BSS.

Services complémentaires

- Intégration
  - Le service d'intégration fait communiquer deux points d'accès par un canal de communication différent de celui fourni par le médium d'IEEE 802.11 au travers du système de distribution
  - Ce service est le plus rendu par un réseau local

Les services MAC

- Service MAC de base: service d'échange sans connexion de trames de données MAC de type best-effort
- Service de livraison de trame MAC de données de type temps réel c'est un service optionnel du standard
- Service de confidentialité: service fourni par l'algorithme WEP (wired equivalent privacy), la confidentialité, l'authentification, le contrôle d'accès et la gestion de couche
- Service de reséquencement, permet si nécessaire de remettre en ordre les trames MAC reçues.
- Adresses BSS et IBSS

Protocole : types de trames

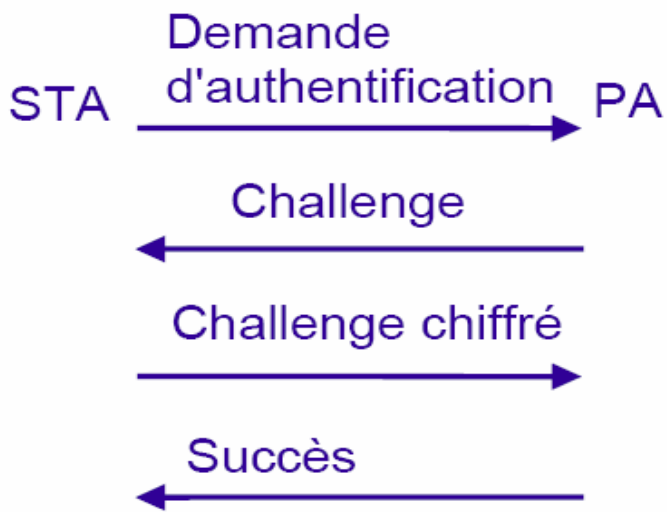
- Trames de gestion
  - balise (*beacon*)
  - *Probe Request / Response*
  - Authentification
  - association
- Trames de contrôle
  - contribuent au bon acheminement des trames de données
  - exemple : ACK, RTS/CTS
- Trames de données

Protocole : découverte des réseaux

- Le point d'accès émet à intervalles réguliers (~ 100 ms) des trames balise (*beacon) qui contiennent :*
  - SSID Service Set Identifier : chaîne de caractères identifiant le réseau sans fil. Les points d'accès d'un même ESS émettent le même SSID
  - Débits supportés
- La station peut émettre des trames Probe Request pour identifier les réseaux sans fil disponibles sur différents canaux
- Le point d'accès lui renvoie une trame Probe Response (mêmes infos que dans la balise)
- Pour utiliser le réseau sans fil, la station doit s'authentifier et s'associer

Authentification

- Deux modes d'authentification :
  - ouvert (*open system)*
  - partagé *(shared key)*

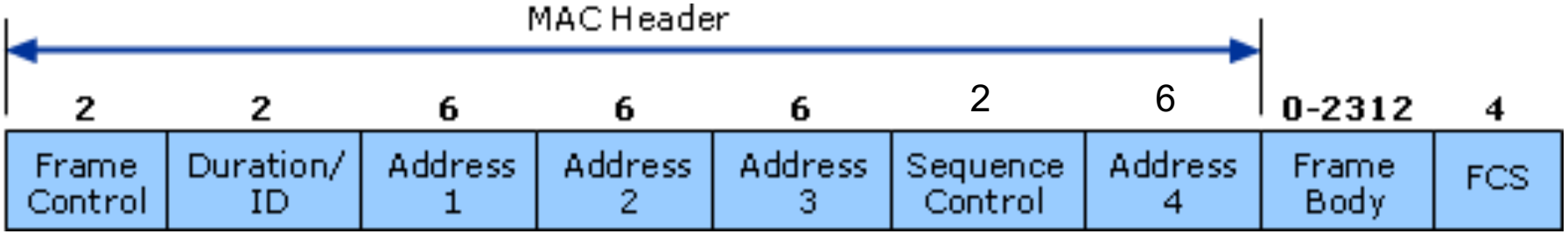


Association – réassociation

- La station envoie au PA une demande d'association
- Si la station est déjà authentifiée le PA accepte la demande et retourne un identificateur d'association (*Association ID)*
- La station peut alors échanger des trames de données avec les autres stations de l'ESS
- Réassociation : lorsqu'une station se déplace d'un BSS à l'autre

Protocole : adressage

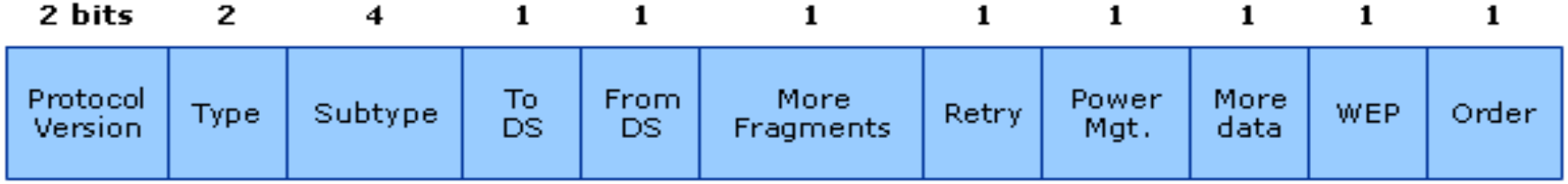
- Adresses sur 48 bits, même format qu'une adresse Ethernet
- Une trame 802.11 contient 4 champs adresse, dont la signification varie en fonction du type de trame



Champs Contrôle de Séquence

Numéro de Séquence (12bits) + Numéro de Fragment (4bits)

Champs Contrôle de Trame



Protocole : adressage

Frame Control Field

- Protocol Version provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported.
- Type and Subtype determines the function of the frame. There are three different frame type fields: control, data, and management. There are multiple subtype fields for each frame type . Each subtype determines the specific function to perform for its associated frame type.
- To DS and From DS indicates whether the frame is going to or exiting from the DS (distributed system), and is only used in data type frames of STAs associated with an AP.
- More Fragments indicates whether more fragments of the frame, either data or management type, are to follow.
- Retry indicates whether or not the frame, for either data or management frame types, is being retransmitted.
- Power Management indicates whether the sending STA is in active mode or sleep mode.
- More Data indicates to a STA in power-save mode that the AP has more frames to send. It is also used for APs to indicate that additional broadcast/multicast frames are to follow.
- WEP indicates whether or not encryption and authentication are used in the frame. It can be set for all data frames and management frames, which have the subtype set to auth.
- Order indicates that all received data frames must be processed in order.

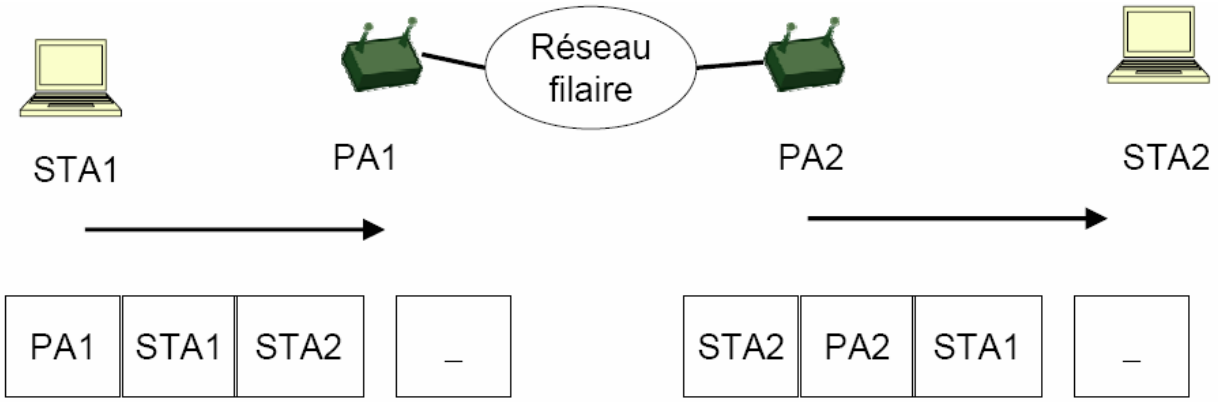
Protocole : adressage

Selon le type de la trame, Les 4 champs adresse indiquent

- Le BSSID : il identifie de manière unique un BSS
  - mode infrastructure : adresse MAC du point d'accès
  - mode ad hoc : choisie de manière à être unique
  - à ne pas confondre avec le SSID (aussi appelé ESSID)
- L'adresse de destination : adresse du destinataire final
- L'adresse source : adresse de la station qui a initialement émis la trame
- L'adresse du récepteur : adresse du destinataire immédiat
- L'adresse de l'émetteur : adresse de la station qui émet la trame

Protocole : adressage

- Exemple : station 1 émettant une trame de données vers station 2

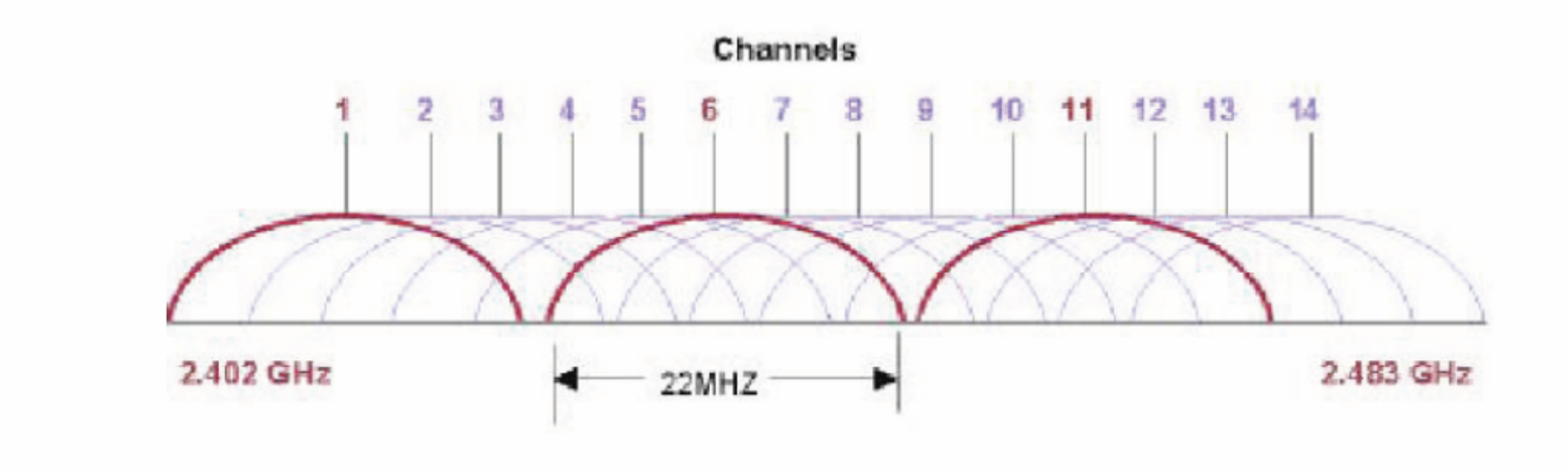


- La station lit le champ Adr1 pour savoir si une trame lui est ou non Adressée

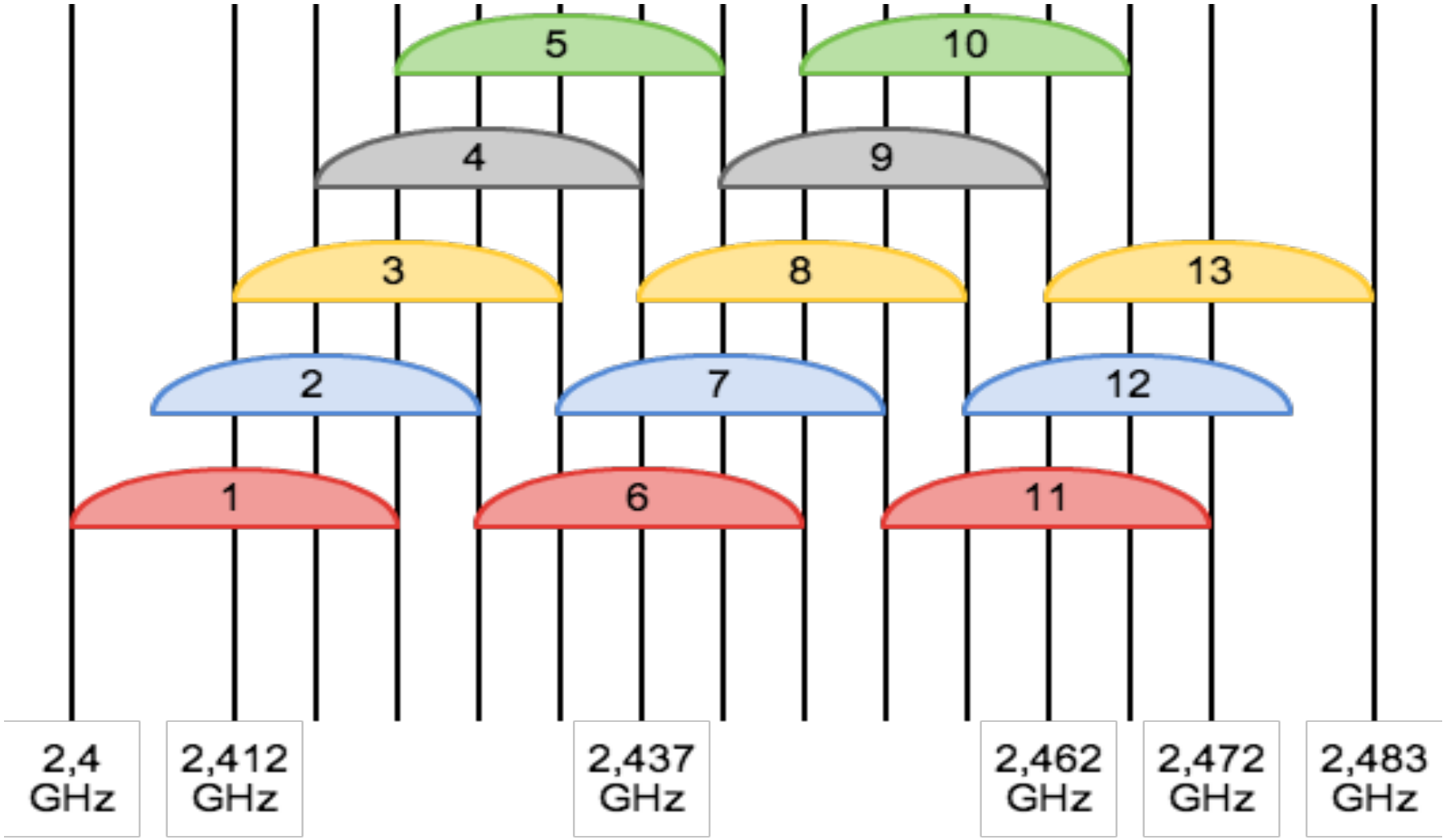
- Si Adr1 est une adresse de groupe (broadcast/multicast), elle vérifie de plus que le BSSID est celui du PA auquel elle est associée

Les canaux physiques

- 14 canaux disponibles de 22 MHz
- 3 canaux disjoints



Les canaux physiques



Techniques d'accès au canal

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 la couche MAC

Techniques d'accès au canal

Média partagé => 802.11 définit deux méthodes d'accès

- Mode d'accès à compétition (par défaut)
  - DCF (distribution coordination function)
- Mode d'accès contrôlé (optionnel)
  - PCF (point coordination function)

Techniques d'accès au canal

PCF : Point Coordination Function

- Uniquement dans les points d'accès, peu implémentée
- Interrogation à tour de rôle des terminaux (polling)
- L'AP prendre le contrôle du support et choisit les stations qui peuvent transmettre
- Conçue pour la transmission de données sensibles
  - Gestion du délai
  - Applications de type temps réel : voix, vidéo

Techniques d'accès au canal

DCF : Distributed Coordination Function

- Conçue pour prendre en charge le transport de données asynchrones
- Dans toutes les stations, sur réseau ad hoc et d'infrastructure
- Tous les utilisateurs qui veulent transmettre ont une chance égale d'accéder au support

Techniques d'accès au canal

DCF (Distributed Coordination Function)

- Dans toutes les stations, sur réseau ad hoc et d'infrastructure
- CSMA/CA *Carrier Sense Multiple Access Collision Avoidance*
- Principe : la station écoute le média pour vérifier qu'il est libre avant d'émettre (idem CSMA/CD)
- Mais elle ne peut pas détecter les collisions
  - parce qu'elle n'entend pas nécessairement toutes les stations
  - parce que la liaison radio est half duplex
- *Avoidance => la station réceptrice émet un ACK qui indique que la trame a* été correctement reçue et qu'il n'y a pas eu de collision
- Si une collision se produit, la station continue à transmettre la trame complète : perte de performance du réseau
- Mécanisme supplémentaire : émetteur et récepteur échangent un RTS/CTS avant d'émettre les données contrôlé par le paramètre RTS threshold

Protocole CSMA/CA

Le CSMA/CA est basé sur :

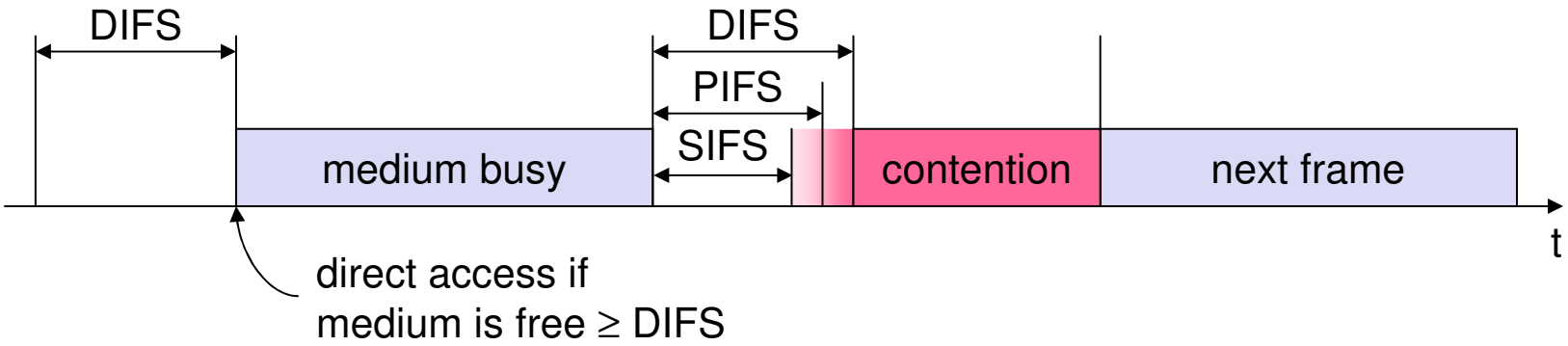
- L'utilisation d'acquittements positifs
- Les temporisateurs IFS
- L'écoute du support
- L'algorithme de Backoff

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

Temporisateurs

- Plusieurs types de temporisateurs
  - **SIFS (Shortest IFS)**
  - **DIFS (Distributed IFS)**
  - **PIFS (PCF IFS)**



- Permettent d'instaurer un système de priorités.
  - SIFS (Priorité maximale): RTS, CTS, Polling reponse
  - PIFS (Priorité moyenne): PCF
  - DIFS (Priorité minimale): traffic asynchrone, données

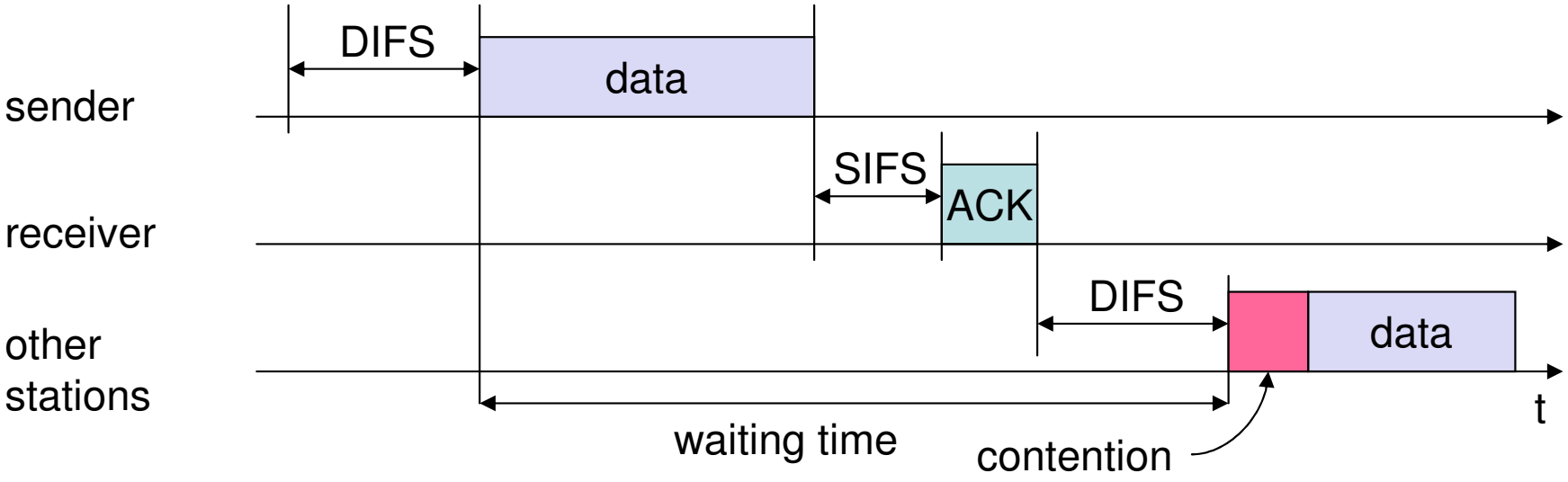
Écoute du support

- Les terminaux d'un même BSS peuvent écouter l'activité de toute les stations se trouvant dans le même BSS grâce à la puissance relative du signal des autres stations.
- 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. SIFS correspond au temps nécessaire pour le traitement d'une trame reçue et pour répondre avec une trame de réponse
  - Si l'ACK n'est pas détecté ou si les données ne sont pas reçues correctement → émulation d'une collision→ retransmission.

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 (un certain nombre de timeslot)
- 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 régénérer un nouveau temporisateur, compris entre 0 et 15
- Pour chaque tentative de retransmission, le temporisateur croît de d'une manière exponentielle.

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

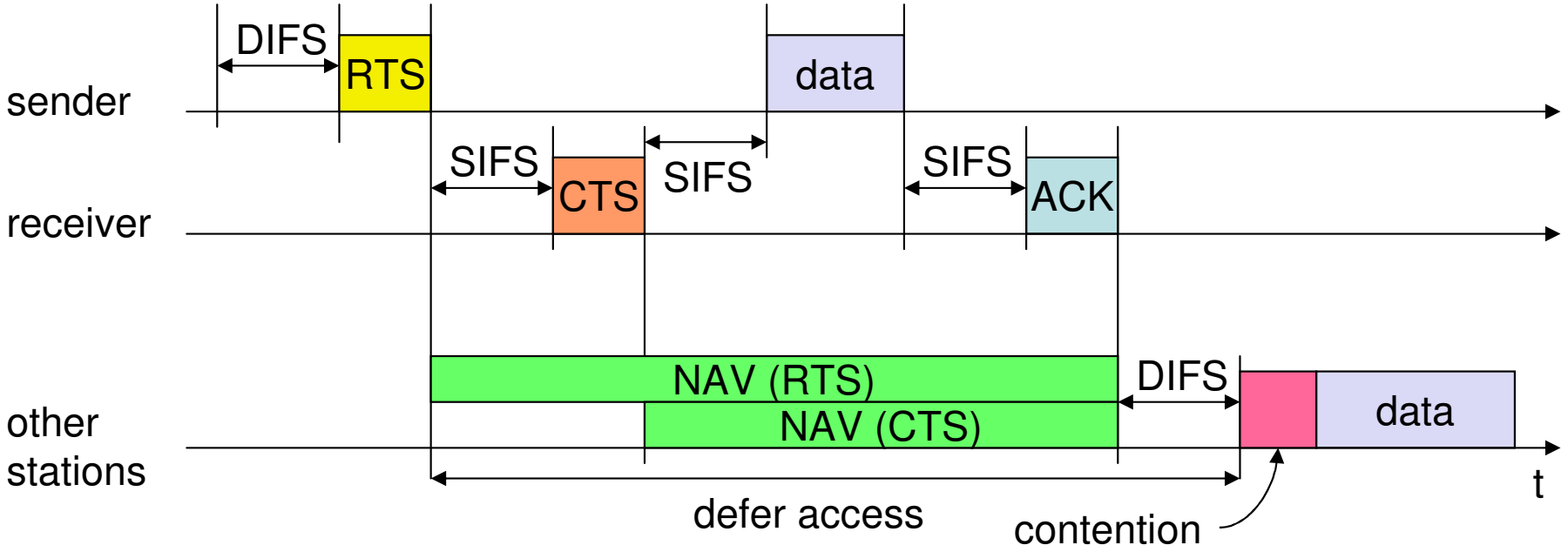
Mécanisme RTS/CTS

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

Mécanisme RTS/CTS



Mécanisme RTS/CTS

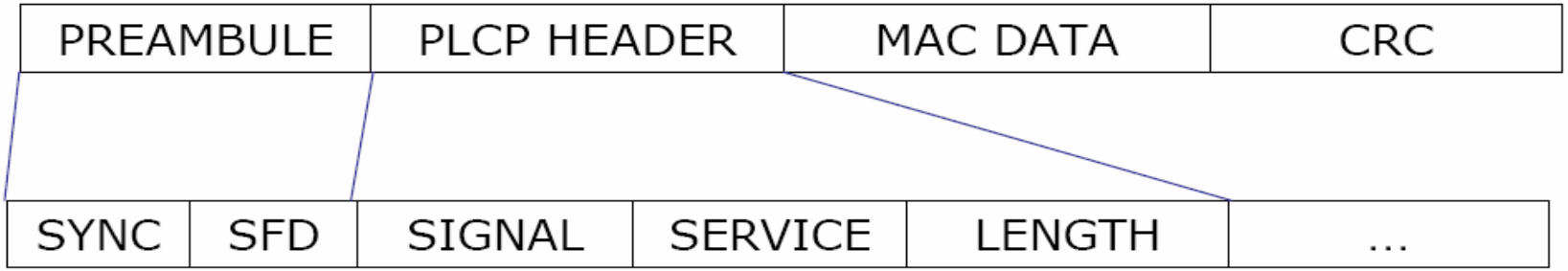
- Transmission des données et réception de l'ACK sans collision
- Trames RTS / CTS réservent le support pour la transmission d'une station
  - Mécanisme habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante
- Les stations 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

CSMA/CA avec RTS/CTS

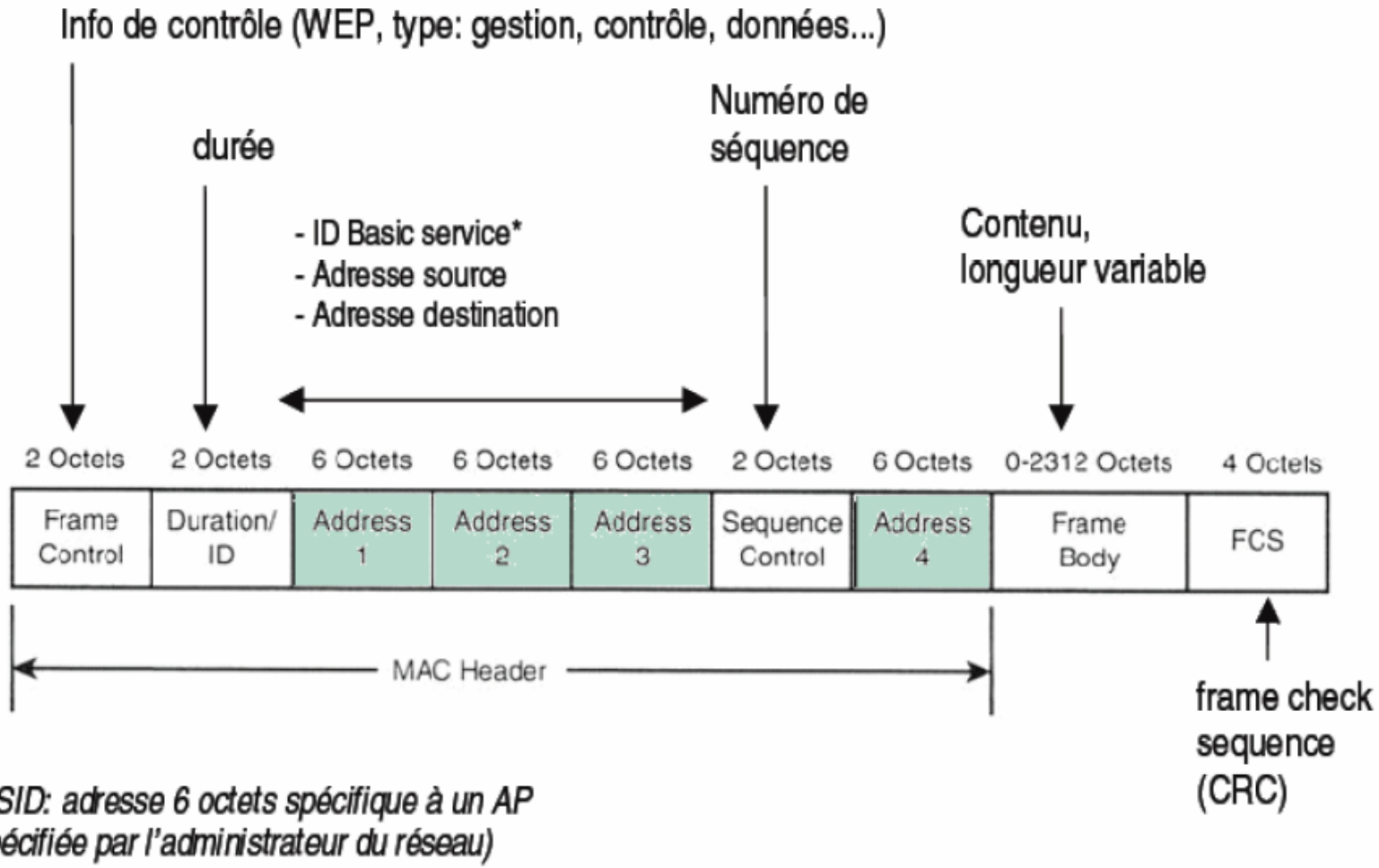
- Permet de partager l'accès
- Mécanisme d'acquittement supporte les problèmes liés aux interférences et à tous les problèmes de l'environnement radio
- Mécanisme de réservation RTS / CTS évite les problèmes de la station cachée
- Inconvénient :
  - Ajout d'en-têtes aux trames 802.11
  - Performances + faibles que les réseaux locaux Ethernet
  - L'équité d'accès au support influe sur le débit réel de transmission

Trames IEEE 802.11 : Couche physique

- Préambule : dépend de la couche physique
  - Séquence Synch pour sélectionner l'antenne à laquelle se raccorder : 80 bits.
  - Séquence SFD (Start Frame Delimiter) pour définir le début de la trame : 16 bits : 0000 1100 1011 1101
- PLCP : infos logiques utilisées par la couche physique pour décoder la trame
- Données MAC et CRC



Trames IEEE 802.11 : Couche MAC



*BSSID: adresse 6 octets spécifique à un AP (spécifiée par l'administrateur du réseau)

Mode Ad-hoc

Le routage

- L'algorithme de routage doit être implémenté sur chaque nœud
- Solution la plus simple: routage directe : toute stations peuvent se voir sans passer par un nœud intermédiaire
- Cas le plus classique : nœuds intermédiaires dotés de table de routage optimisées
- Les grandes familles de routages
  - Routage réactif
  - Routage proactif

Routage réactif

- Travaillent par inondation : détermination de la meilleure route lorsque les paquets sont prêts à être émis
- Pas d'échange de paquets de contrôle, sauf paquets de supervision (détermination de chemin)
- Le paquet de supervision diffusé vers les nœuds voisins est transmis par ceux-ci vers le nœud destination : plusieurs routes possible si problème sur la route principale

Routage proactif

- Émission ininterrompu de paquets de supervision
- Maintien de la table de routage : rafraîchissement dynamique
- Chaque information de supervision influençant le comportement du réseau entraine la modification des tables
- Difficulté : calcul des tables de routage pour qu'elles soient cohérentes

Exemples

- AODV (réactif)
- OLSR (proactif)
- TBRPF (proactif)

Sécurité de la norme IEEE 802.11

Les principales attaques

- Interception des données
- Intrusion dans le système
- Usurpation d'identité
- Attaque de l'homme au milieu
- Porte dissimulée

Les principales attaques

Interception des données

- Attaque la plus classique
- Absence de système de chiffrement efficace
- Le caractère ouvert des équipements de réseaux sans fil
- Interception par une station espion dans le domaine normal de couverture ou bien à distance (antenne directive)

Les principales attaques

Intrusion dans le système

- Un élément étranger peut se connecter au point d'accès radio puis à pénétrer dans le réseaux local derrière le point d'accès.
- Écoute passive (antenne directive)
- Les points d'accès servent à l'attaquant de point d'entrée dans le réseau puis il peut pénétrer les équipements reliés au réseau.

Les principales attaques

Intrusion dans le système

- Adresse MAC
- Adresse IP
- Adresses MAC and IP en même temps

Modifier ses paramètres d'adressage, le tour est joué ! On peu aussi le désassocier et prendre sa place !!

Les principales attaques

Attaque de l'homme au milieu

- L'attaque est classique dans les réseaux mais plus facile dans les réseaux sans fil
- Disposer d'un point d'accès étranger **de même SSID** comme cheval de Troie
- Une station cherche à s'y connecter, livrant ainsi les clés du processus de connexion.
- Ces clés ayant été collectées, elles servent à un futur intrus pour pénétrer dans le réseau

Les principales attaques

Porte dissimulée

- Cette attaque consiste à raccorder un accès félon à un réseau, via un point d'accès contrôlé par un espion.

- Pénétration dans le réseau

Sécurisation d'un réseaux sans fil

Comment rendre un réseau sans fil sûr?

- Intervention au niveau des protocoles IEEE 802.11, dans les nœuds sans fil eux-mêmes.
- Adaptation des techniques générales de sécurité aux réseaux sans fil
- Sécurisation des applications utilisées au niveau transport ou au niveau application.

Sécurisation d'un réseaux sans fil

- Solutions minimales dans les produits IEEE 802.11
- L'identificateur de réseau
- Les mots de passe
- La protection par adresse MAC IEEE

Sécurisation d'un réseaux sans fil

- L'identificateur de réseau : permet de filtrer le trafic. Un trafic ne portant pas le même identificateur que le réseau qu'on souhaite pénétrer est ignoré par ce dernier.

- Cette protection est en fait très sommaire, car le point d'accès envoie périodiquement en clair dans les trames balise l'identité du réseau

Sécurisation d'un réseaux sans fil

- Les mots de passe
- Accès au réseau la station doit envoyer un mot de passe.
- Cette protection est également extrêmement simpliste, car il est facile de capturer le mot de passe et de le réutiliser par la suite

Sécurisation d'un réseaux sans fil

La protection par adresse MAC IEEE

- Cette protection consiste à n'autoriser l'accès au réseau qu'à des stations présentant une adresse MAC IEEE prédéfinie et connue du réseau.
- Cette protection n'est pas non plus très difficile à contourner. (écoute passive permet de récupérer ces adresses)
- De nombreuses carte radio permettent de modifier par logiciel leur propre adresse MAC IEEE

Sécurisation d'un réseaux sans fil

Si l'on souhaite offrir une meilleur sécurité vis-à-vis de l'écoute passive mais aussi pour l'authentification et le contrôle d'accès, l'utilisation du chiffrement est essentielle.

Le WEP (Wired Equivalent Privacy)

- Le WEP utilise un chiffrement qui applique aux données en clair "ou exclusif" avec une séquence pseudo aléatoire pour les crypter.
- pas de protocole de gestion des clés : une unique clé partagée entre tous les utilisateurs.
- La séquence pseudo-aléatoire est obtenue en utilisant la fonction RC4 (1987 par Ron Rivest pour RSA Company) à partir de la concaténation de la clé de cryptage K et du vecteur d'initialisation VI.
- Système à clé symétrique de longueur 40

Le WEP (Wired Equivalent Privacy)

Le principales failles du WEP

- Baisse des performances en terme de débit en utilisant WEP : de 5 à 50%, selon l'implémentation matérielle ou logiciel du protocole
- Contournement de l'algorithme d'intégrité ICV (la bonne clé)
- Possibilité de construire des dictionnaires fournissant en fonction d'un vecteur d'initialisation, la séquence pseudo-aléatoire de déchiffrement.
- Faille du chiffrement RC4
- L'algorithme de contrôle d'intégrité est linéaire
- Déjà cracké !

Autres protocole de sécurité

- Wi-Fi Access Protocol (WAP)
- Wi-Fi Access Protocol 2 (WAP2)
- Extensive Authentication Protocol (EAP)

Access Control List (ACL)

Restreint l'accès au point d'accès à des adresses MAC bien déterminées

- Adresse MAC unique pour toute carte Wifi ou réseau
- Liste des cartes autorisées ou interdites
- Peu fiable, mais conseillé par défaut

Service Set ID (SSID)

Nom du réseau

- Il est nécessaire de modifier le nom donné par le constructeur
- Masquage du SSID
- Faille : diffusée en clair à intervalles de temps constants

Bilan sur la sécurité

- Sécurité peu forte
- Travaux en cours pour corriger ce point
- Par défaut, il est plus que conseillé d'utiliser tout de même les fonctionnalités offertes (WEP, ACL, modification de SSID)
- Logiciel intéressant : netstumbler
  - Permet d'identifier et de qualifier les réseaux Wifi environnants.
  - Chaque réseau est détaillé avec un numéro du canal, un SSID, un débit, le type de périphérique Wifi (point d'accès, routeur…), le SNR, l'adresse IP (si elle est disponible), la force du signal et le bruit. Un graphe mesure en temps réel la force du signal.

Cracker un réseau WIFI

Les logiciles suivants sont capables de craquer le système de chiffrement WEP

- Airsnort: permet de calculer directement la clé de chiffrement après l'interception d'un nombre suffisant de paquets (disponible sous Linux)
- WepCrack : fonctionne sur le même principe (téléchargeable dur e web)
- Sniffer Wireless: permet de rechercher la clé secrète en utilisant des attaques de type texte en clair et les clés faibles de RC4

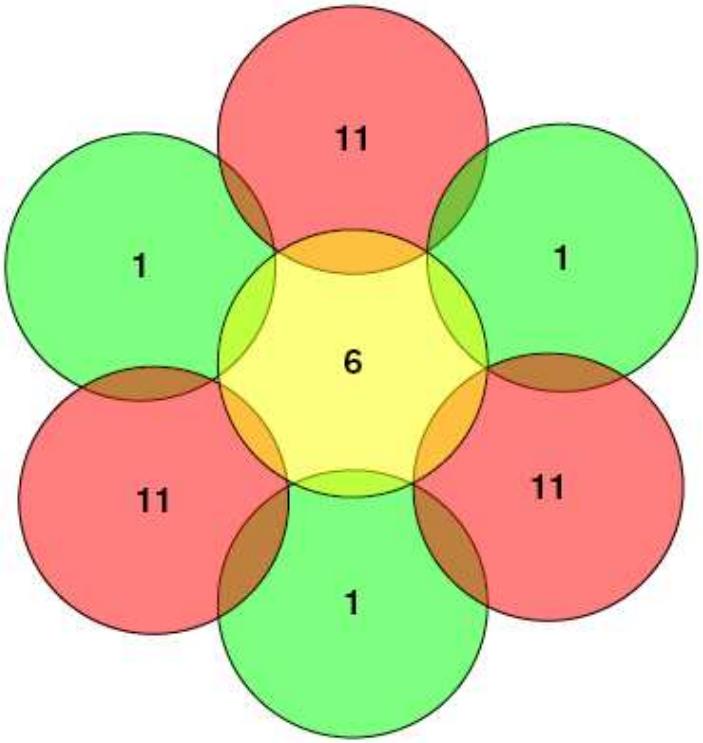
Déploiement d'un réseaux WIFI

Mise en pratique

- Choix du standard
  - Privilégier IEEE 802.11g au détriment de 802.11.b (même matériel, peu coûteux)
  - IEEE 802.11a plus intéressant en raison des fréquences utilisées mais plus cher (pas conseillé pour un usage domestique)
- Choix du point d'accès
  - Point d'accès relié à Internet
  - Placement géographique important (obstacles radio)
  - Choix des canaux

Mise en pratique

3 canaux ne se recouvrant pas pour envisager une occupation efficace de l'espace géographique



Mise en pratique

- Choix du mode : Infrastructure ou ad hoc ?
- Plan d'adressage
- Sécurité
- NAT (Network Adress Translation)
  - permet au point d'accès de partager une connexion Internet
  - impossibilité de se connecter de l'extérieur à une machine du réseau (qui héberge par exemple un serveur Web)

Mise en pratique

Hotspot

- Bornes d'accès Wifi installées dans les lieux publiques et de passage
  - Aéroport, gares, hôtels, restaurant
  - En plein essor

Merci pour votre attention !