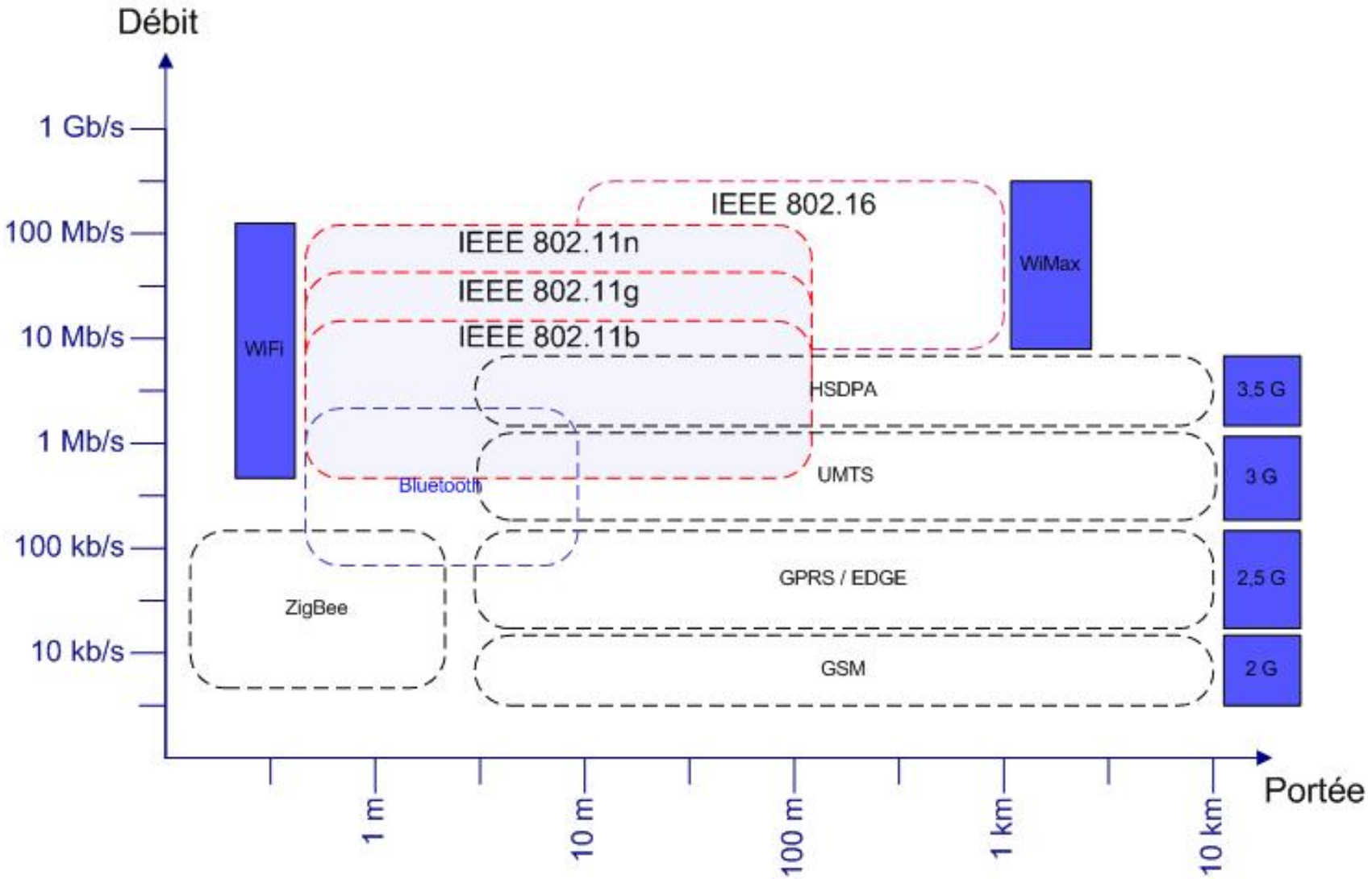
Panorama des réseaux sans fils



Intérêts des réseaux sans fils

Développement pour 2 raisons principales :

- Coût du cablâge
  - Lieux publiques (gares, aéroport, . . .) ;
  - Transmission entre deux bâtiments ;
  - Monuments historiques ;
  - . . .
- Applications mobiles
  - unité de maintenances ;
  - entrepôt et gestion de stocks ;
  - . . .

Domaines d'application

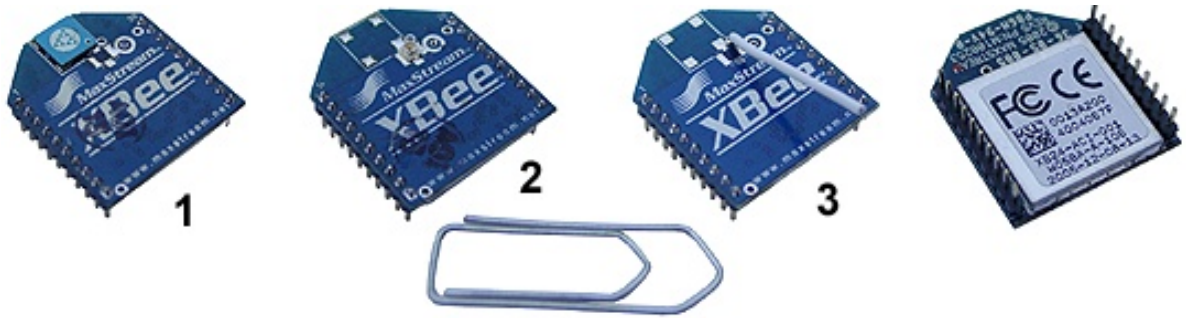
- gare, aéroport, . . . (*hotspot*) ;
- usines ;
- entrepôts ;
- grandes surfaces ;
- hôpitaux ;
- . . .

Bluetooth

- Principale technologie pour les WPAN
  - première spécification en 1999
  - Lien avec le IEEE 802.15 (WPAN)
  - bande de fréquence des 2.4 GHz (2400 à 2483.5 MHz), possible interférences avec 802.11b/g
- Avantages :
  - mécanisme de détection automatique (configuration facile)
  - faible consommation, taille réduite, prix
- Inconvénients :
  - faible débit (1Mb/S)
  - faible distance
- Complémentaire aux réseaux 802.11

ZigBee

- Défini par the ZigBee Alliance
- Technologie similaire à Bluetooth
  - 2.4 GHz ou 868 MHz ou 915 MHz
  - faible distance
  - très faible débit (20 ou 250 kb/s)
- Avantages :
  - grande simplicité
  - faible coût
  - très faible consommation



IEEE 802.11

Wi-Fi

- Wi-Fi = Wireless Fidelity
- Terme commercial défini par la Wireless Ethernet Compatibility Alliance (WECA)
  - WECA "a pour objectif de promouvoir l'usage de WLAN basés sur le standard IEEE 802.11"
- Réalisation d'un label de certification
- Wi-Fi n'est ni un protocole réseau, ni un standard réseau ni une technique réseau, ni une architecture de réseau, c'est juste une marque déposée

Différentes normes 802.11

Norme	Nom	Description
802.11a	WiFi	54 Mbps - 5 GHz
802.11b	WiFi	11 Mbps - 2.4 GHz
802.11e	QoS	Priorité des flux (ex : vidéo/audio)
802.11f	Roaming	Gestion des déplacements
802.11g	WiFi	54 Mbps - 2.4 GHz
802.11h	HiperLan2	54 Mbps - 5GHz
802.11i	802.11i	Sécurité (AES - clés dynamique)
802.11n	WiFi	540 Mbps - 2.4 GHz ou 5 GHz

Comparaison des différentes normes Wi-Fi

- 802.11a
  - 5 GHz, modulation OFDM
  - débit maximal : 54 Mb/s
- 802.11b
  - 2.4 GHz, modulation DSSS ou HR-DSSS
  - débit maximal : 11 Mb/s
- 802.11g
  - 2.4 GHz, modulation DSSS, HR-DSSS ou OFDM
  - débit maximal : 54 Mb/s
- 802.11n
  - MIMO
  - débit maximal : 540 Mb/s

Comparaison des débits

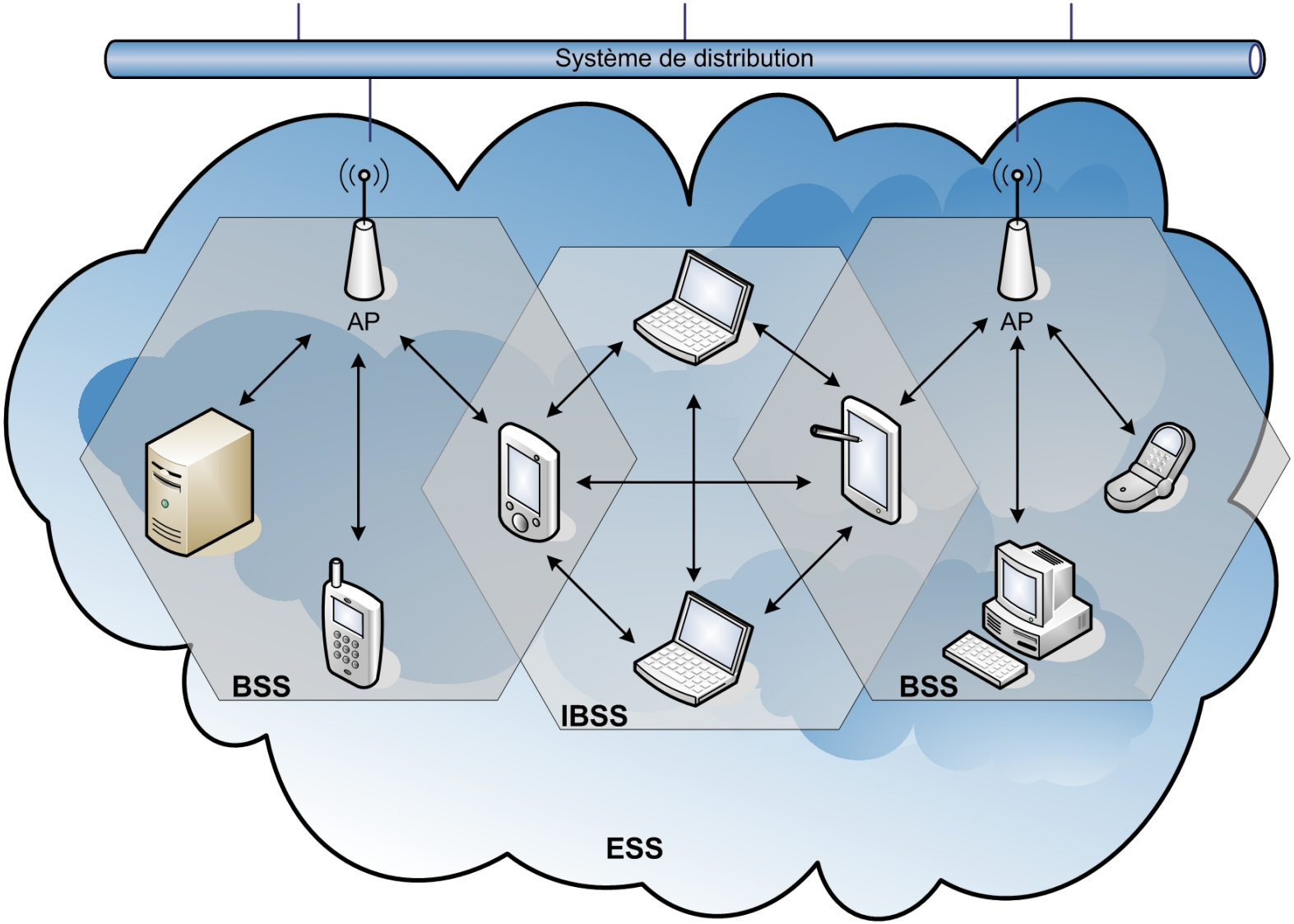
	Débit nominal (Mbps)	Débit approximatif (Mbps)
802.11b	11	6 (750 Ko/s)
802.11g avec client 802.11b associé	54	8 (1000 Ko/s)
802.11g sans client 802.11b associé	54	22 (2750 Ko/s)
802.11a	54	25 (3125 Ko/s)

Mode de fonctionnement

La norme IEEE 802.11 dispose de deux modes de fonctionnement :

- **Mode infrastructure** :
  - les clients se connectent sur les points d'accès (AP) grâce au **SSID** (**S**ervice **S**et **ID**entifier, 32 caractères maxi)
  - chaque AP émets et reçois les données sur un canal radio particulier. Deux balises proches doivent utiliser des canaux différents afin que les ondes radio ne perturbent pas (chevauchement des zones d'émissions) (voir tableau des fréquences plus loin dans ce cours)
  - permet le roaming, i.e., le passage d'une balise à l'autre sans que l'utilisateur s'en rende compte
  - Il n'y a pas de communication directe entre les clients, ils sont obligés de passer par l'AP
- **Mode ad-hoc** : IBSS (Independant Basic Service Set)
  - connexion pair à pair entre les clients
  - notion de SSID (groupe de pairs)
  - Portée limitée

Architecture générale d'un réseau 802.11



Architecture générale d'un réseau 802.11

- AP (**A**cess **P**oint) : point d'accès
- BSS (**B**asic **S**et **S**ervice) : cellule de base
- ESS (**E**xtended **S**et **S**ervice) : ensemble des cellules de base
- IBSS (**I**ndependent **B**asic **S**et **S**ervice) : cellule de base en mode ad-hoc

La couche physique

802.11 - Infrarouge

- Deux débits acceptés : 1 et 2 Mb/s
- Transmission :
  - Longueur d'ondes : 850 - 950 nm
  - Lumière diffuse (pas un "rayon laser")
  - Utilise des diodes IR
  - Réflexion possibles
  - Distance limitée à 10 m entre les dispositifs de transmission
- Avantages :
  - Simple
  - Bon marché
  - Disponibles dans de nombreux appareils
  - Pas de licence pour utiliser la fréquence de transmission
  - Facile à isoler
- Inconvénients :
  - Interférence avec la lumière solaire et la chaleur
  - Faible largeur de bande

Modulations utilisées en Wi-Fi

Aperçu des types de modulation

Trois types de modulation sont utilisés pour les réseaux 802.11

- Frequency Hopping Spread Spectrum (FHSS)
  - version originale pour 802.11
- Direct Sequence Spread Spectrum (DSSS)
  - 802.11b et 802.11g
- Orthogonal Frequency Division Multiplexing (OFDM)
  - 802.11a et 802.11g

Frequency Hopping Spread Spectrum

- La bande de fréquence est séparée en plusiseurs canaux
- Communication par saut de fréquence d'un canal à l'autre
  - Séquence et rythme prédéfini
- Avantages :
  - difficulté d'intercepter les communications
  - utilisé pour les communications militaire
- Résistance aux interférences
  - évite le brouillage des canaux
  - inutilisé par le Wi-Fi, utilisé par Bluetooth
- Possibilité de partager la bande de fréquence en utilisant différentes séquences
- 802.11
  - bande : 2400 MHz à 2483 MHz, canaux de 1 MHz

Direct Sequence Spread Spectrum

- Séquencement
  - envoi d'une séquence de bits ("chip") pour chaque bit d'information
  - transition d'état à un taux plus élevé ("spread spectrum")
- intérêt :
  - l'utilisation d'un spectre large permet un débit plus élevé et une meilleure résistance au bruit
  - redondance pour autoriser la correction d'erreur
- Wi-Fi
  - 14 canaux de largeur 22 MHz dans la bande de fréquence des 2.4 GHz
  - nécessite de choisir un canal
  - possibilité d'interférences

Orthogonal Frequency Division Multiplexing

- Basé sur le multiplexage :
  - multiplexage par division de fréquence (FDM : *Frequency Division Multplexing*)
  - Spectre large divisé en plusieurs sous-porteuse
  - émission simultanée sur les sous-porteuses
- Wi-Fi
  - 52 porteuses de 312,5 kHz chacune (canaux de 16,66 MHz)
  - modulation de porteuse : 2PSK, 4PSK, 16 QAM ou 64 QAM
  - 48 symboles envoyés simultanément
- Adaptation du débit

Canaux de communications

Canaux 802.11 DSSS (802.11b et 802.11g)

- Utiliation de la bande des 2.4 GHz
- 14 canaux de 22 MHz
- Le centre de chaque canal est espacé de 5 MHz cela implique donc un chevauchement des canaux
- Canaux utilisables :
  - canaux 1 à 13 en Europe ;
  - canaux 1 à 11 aux USA ;
  - canal 14 aux japon ;
- Recommandation : utilisation de canaux sans chevauchement. Les plus courant sont les canaux 1, 6 et 11

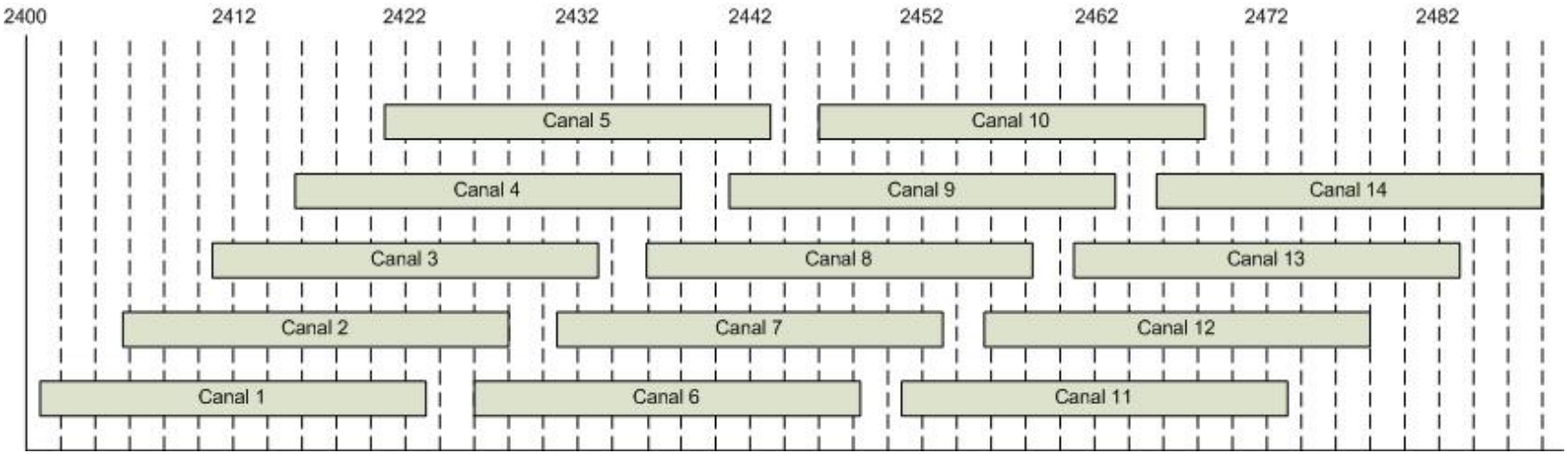
Fréquences WiFi (802.11b et 802.11g)

Le tableau ci-dessous indique la fréquence du milieu du canal ainsi que les puissances d'émissions intérieures et extérieures autorisées en France.

Canal	Fréquence	Intérieur	Extérieur
1	2,412 GHz	100 mW	100 mW
2	2,417 GHz	100 mW	100 mW
3	2,422 GHz	100 mW	100 mW
4	2,427 GHz	100 mW	100 mW
5	2,432 GHz	100 mW	100 mW
6	2,437 GHz	100 mW	100 mW
7	2,442 GHz	100 mW	100 mW
8	2,447 GHz	100 mW	100 mW
9	2,452 GHz	100 mW	100 mW
10	2,457 GHz	100 mW	10 mW
11	2,462 GHz	100 mW	10 mW
12	2,467 GHz	100 mW	10 mW
13	2,472 GHz	100 mW	10 mW
14	2,477 GHz	100 mW	10 mW

Fréquences WiFi (802.11b et 802.11g)

La figure montre les chevauchements des différents canaux.



Canaux (802.11a)

- Utilisation de la bande des 5 GHz
- Canaux de 20 MHz
- Le centre de chaque canal est espacé de 5 MHz cela implique donc un chevauchement des canaux
- 12 canaux utilisés par 802.11a dans le monde
  - 34, 36, ..., 48
  - 52, 56, ..., 64
- En France :
  - La bande des 5 GHz est interdit à l'extérieur
  - 8 canaux sans chevauchement :
    - 36, 40, 44, 48, 52, 56, 60 et 64

Transmission radio

- Étalement de spectre :
  - augmente la résistance au brouillage ;
  - permet la cohabitation de transmissions ;
  - étalement par séquence directe :
    - une suite aléatoire de **n** chips ;
    - un bit est remplacé par la suite.
  - étalement par saut de fréquence :
    - une séquence aléatoire de fréquences ;
    - la porteuse se décale sur la séquence.

La norme IEEE 802.11

- Une méthode d'accès commune
- Diverses couches physiques :
  - la norme de base IEEE 802.11 :
    - une version infra-rouge jamais commercialisé ;
    - une version à saut de fréquences (bande des 2,4 GHz) ;
    - une version à séquence directe (bande des 2.4 GHz) ;
    - débit théorique de 1 et 2 Mbit/s
  - une extension IEEE 802.11b :
    - modulation de type CCK (bande des 2.4-2.5 Ghz) ;
    - débits théoriques de 5.5 et 11 Mbit/s ;
    - débit réels de 4 et 6.5 Mbit/s.
  - une extension IEEE 802.11a :
    - modulation OFDM (bande des 5 Ghz) ;
    - débits théoriques jusqu'à 54 Mbit/s ;
    - débit réel de 20 Mbit/s.
  - une extension IEEE 802.11g :
    - modulation mixte CCK/OFDM (bande des 2.4-2.5 Ghz) ;
    - débit théorique jusqu'à 54 Mbit/s ;
    - débit réel de 25 Mbit/s.
  - une extension 802.11n :

Différentes configurations

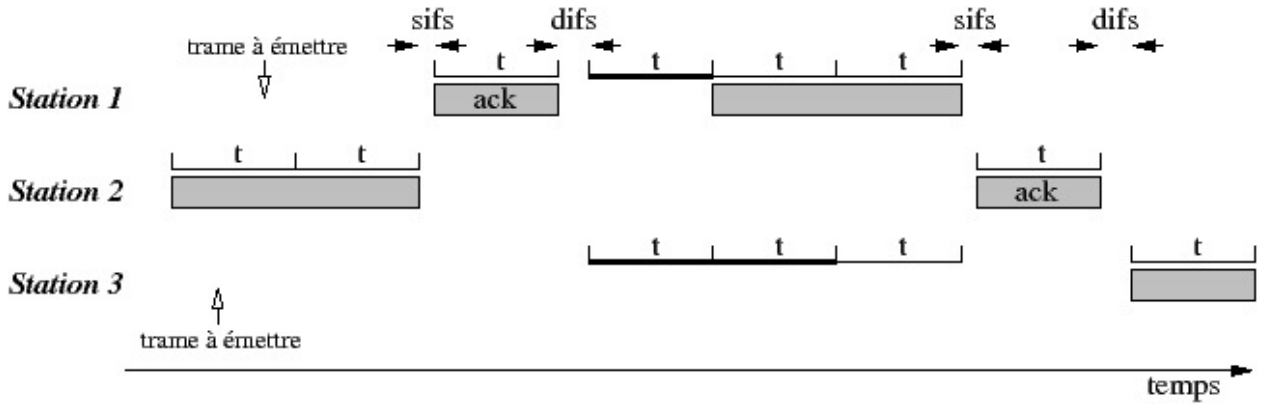
- Les modes de fonctionnement :
  - infrastructure avec point d'accès :
    - une station raccordée à un réseau filaire ;
    - communication uniquement via la station ;
  - réseau ad-hoc :
    - fonctionnement distribué ;
    - communication entre stations à porté.
- Les techniques d'accès :
  - un mode d'accès à compétition :
    - Distribution Coordination Function (DCF) ;
    - mode obligatoire dans la norme 802.11 ;
    - une méthode à base de CSMA
  - un mode d'accès contrôlé :
    - Point Coordination Function (PCF) ;
    - mode optionnel dans la norme 802.11 ;
    - une station gère les temps de parole ;
    - mode quasiment jamais implémenté (peu efficace)

Accès à compétition : le principe

- Accès basé sur une méthode CSMA :
  - attente comme dans le CSMA-1 persistant ;
  - attente durant un intervalle de temps fixe DIFS plus . . .
  - . . . un multiple aléatoire d'intervalle de collision (20 μs) ;
  - émission si le canal est encore libre
- Contrôle des collisions par accusés de réception
- Priorité des accusés de réceptions :
  - des inter-trames de tailles différentes :
  - les Short Inter-Frame Spacing (10 μs, accusé) ;
  - les Distributed Inter-Frame Spacing (50 μs, mode DCF) ;
  - Les Point Coordination Inter-Frame Spacing (30 μs, mode PCF)

Accès à compétition : le principe

- Un exemple de fonctionnement :

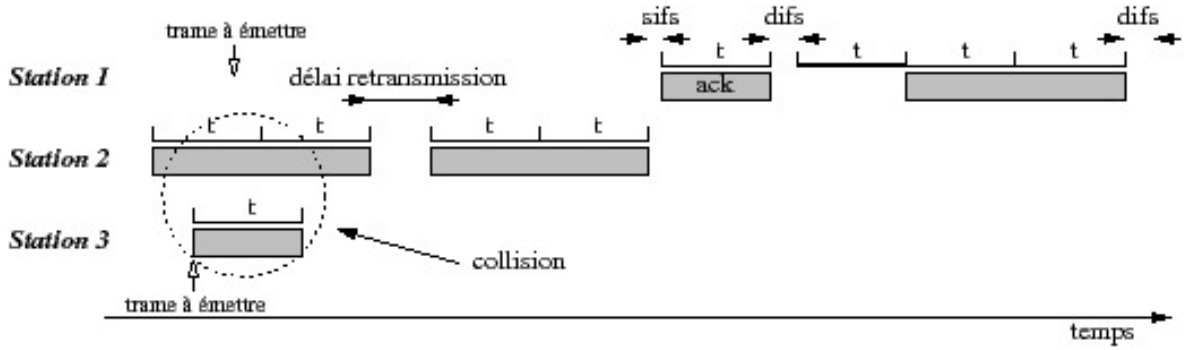


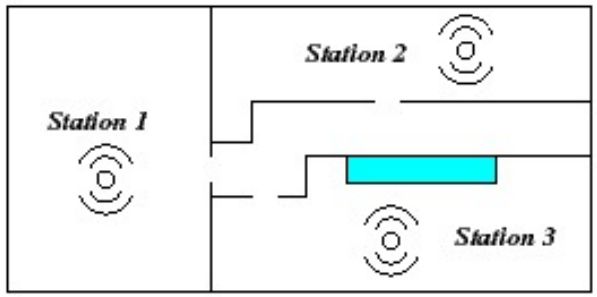
Accès à compétition : stations cachées

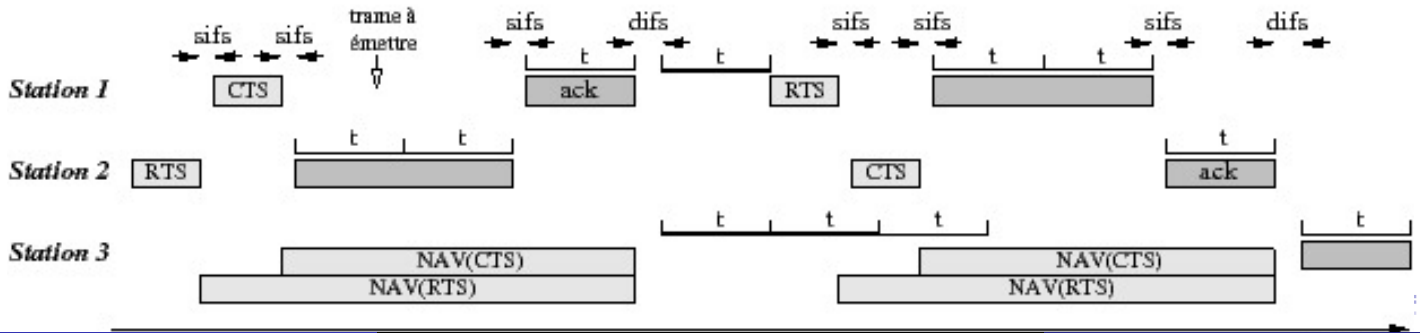
- Comment prendre en compte les stations cachées ?
- Un vecteur d'allocation (Network Allocation Vector)
  - la source prévient de sa transmission (Request To Send)
  - la cible autorise la transmission (Clear To Send)
  - la durée de transmission est annoncée

Accès à compétition : stations cachées

- Un exemple de fonctionnement :

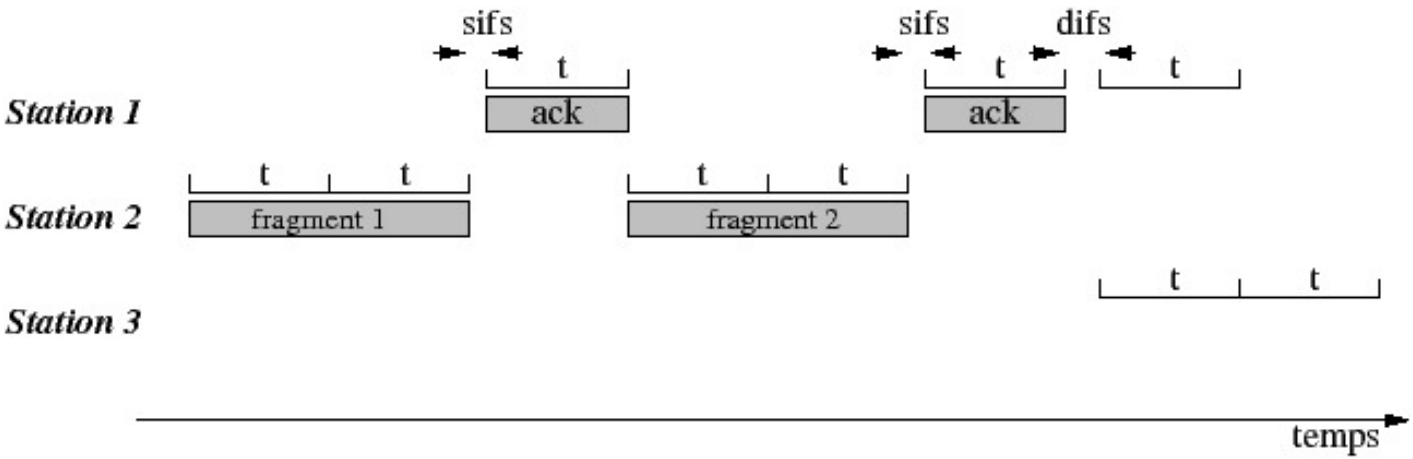




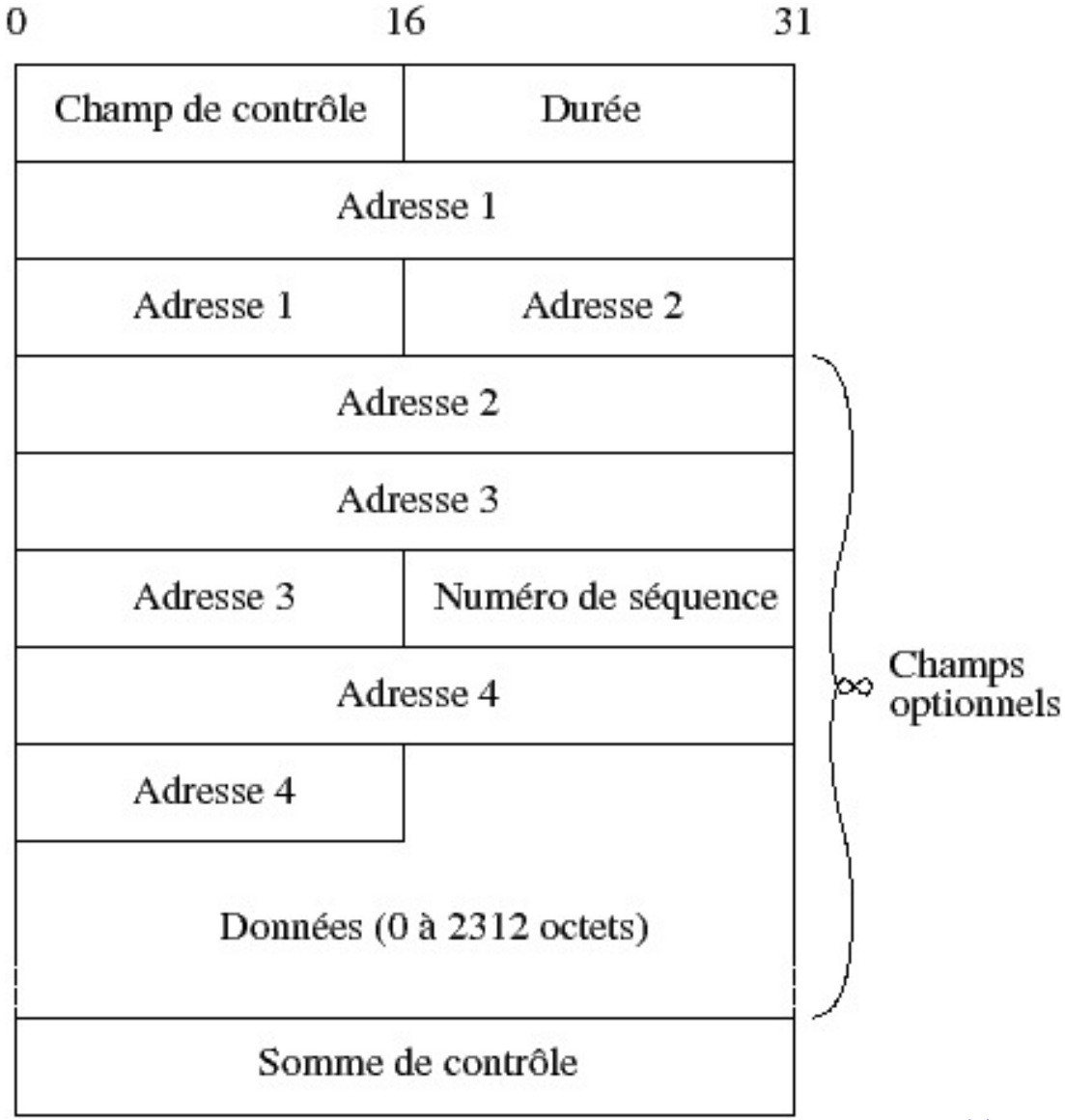


Accès à compétition : fragmentation

- Fragmenter pour améliorer la fiabilité :
  - un fragment court passe mieux qu'une grande trame
  - la station est prioritaire pour les fragments suivants
  - en cas de collision, retour à la phase de contentio
- Principe de la transmission des fragments :



Format des trames 802.11



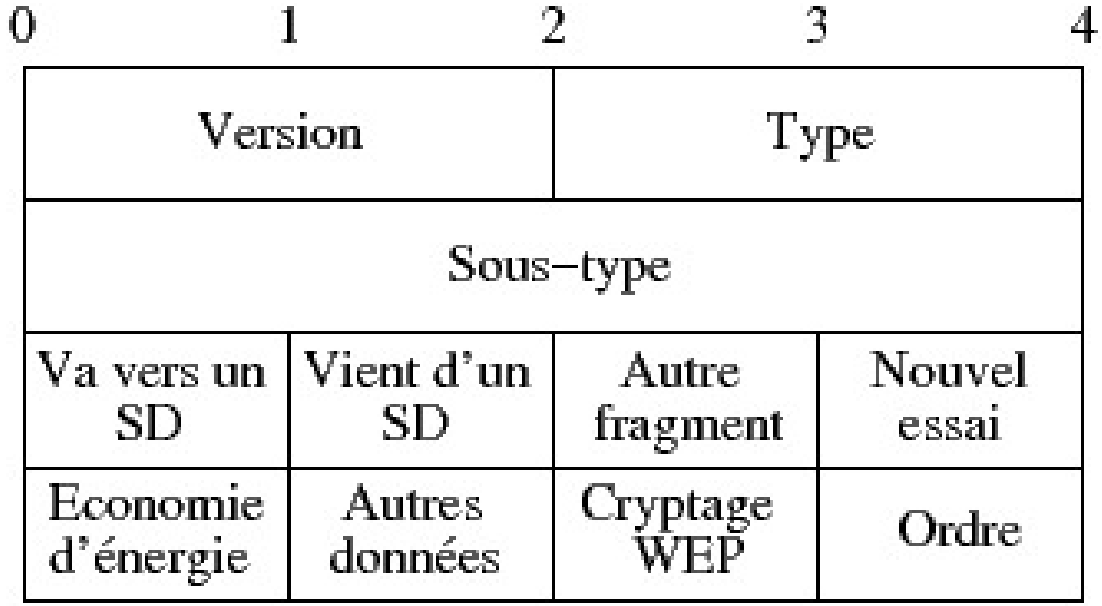
Format des trames 802.11

Signification des divers champs :

- un champ de contrôle pour la nature de la trame ;
- un champ indiquant la durée en ms de la séquence ;
- plusieurs champs d'adresse :
  - plusieurs cas de figre (mode infrastructure ou ad-hoc) ;
  - cas le plus courant du mode infrastructure :
    - adresse 1 : adresse MAC du point d'accès ;
    - adresse 2 : adresse MAC de la station source ;
    - adresse 3 : adresse MAC de la station cible :
    - adresse 4 : inutilisée
- un champ numéro de séquence utilisé pour :
  - numéroter les trames en vu de l'acquitement ;
  - numéroter les fragments si nécessaire
- un champ somme de contrôle classique (CRC 32 bits)

Types des trames 802.11

- Plusieurs types de trame :
  - les trames de gestion (dialogue avec les PA) ;
  - les trames de contrôle (implantation du protocole) ;
  - les trames de données.
- Le champ de contrôle des trames :



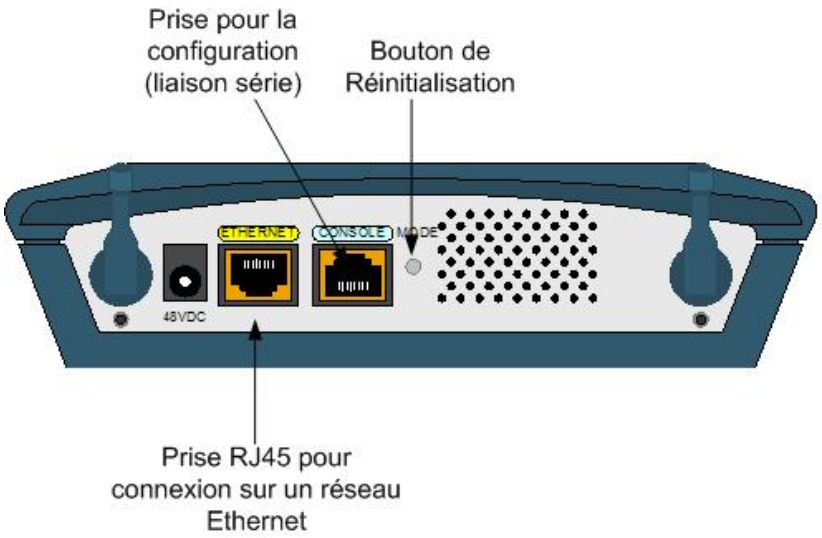
- Signification des champs :
  - le numéro de version est actuellement 0 ;
  - le type et le sous-type indiquent la nature de la trame ;
  - les deux champs suivants indiquent si la trame :
    - va vers un système de distribution (réseau filaire) ;
    - ou provient d'un système de distribution
  - le champ "autre fragment" indique une fragmentation
  - ces fragments sont en séquence si le bit "ordre" est positionné :
  - le champ "nouvel essai" indique une ré-émission de trame ;
  - le champ WEP indique si la trame est cryptée ;
  - et enfin les autres champs concernent la gestion des l'énergie
- Signification des types et sous-types :

Type	Description	Sous-type	Description sous-type
00	Gestion	0000	Requête d'association
00	Gestion	0001	Réponse d'association
00	Gestion	0010	Requête de ré-association
00	Gestion	0011	Réponse de ré-association
00	Gestion	0100	Demande d'enquête
00	Gestion	0101	Réponse d'enquête
00	Gestion	100	Balise
00	Gestion	1001	ATIM
00	Gestion	1010	Désassociation
00	Gestion	1011	Authentification
00	Gestion	1100	Désauthentification
01	Contrôle	1010	PS-Poll
01	Contrôle	1011	RTS
01	Contrôle	1100	CTS
01	Contrôle	1101	ACK

Type	Description	Sous-type	Description sous-type
01	Contrôle	1110	CF End
01	Contrôle	1111	CF End et CF-ACK
10	Données	0000	Données
10	Données	0001	Données et CF-ACK
10	Données	0010	Données et CF-Poll
10	Données	0011	Données, CF-ACK et CF-Poll
10	Données	0100	Fonction nulle (sans données)
10	Données	0101	CF-ACK (sans données)
10	Données	0110	CF-Poll (dans données)
10	Données	0111	CF-ACK et CF-Poll (sans données)

Configuration des Access Point Cisco

Cisco Aironet 1200



Configuration WEP

```
 AP# configure terminal

AP(config)# dot11 ssid MonSSID
AP(config)# authentication open
AP(config)# guest-mode
AP(config)# exit

AP(config)# interface dot11radio 0
AP(config-if)# ssid MonSSID
AP(config-if)# encryption mode wep mandatory
AP(config-if)# encryption key 1 size 128bit 0
cafe4cac40faceb00cdeadbeef
AP(config-if)# no shutdown
AP(config-if)# exit
```

Configuration WPA

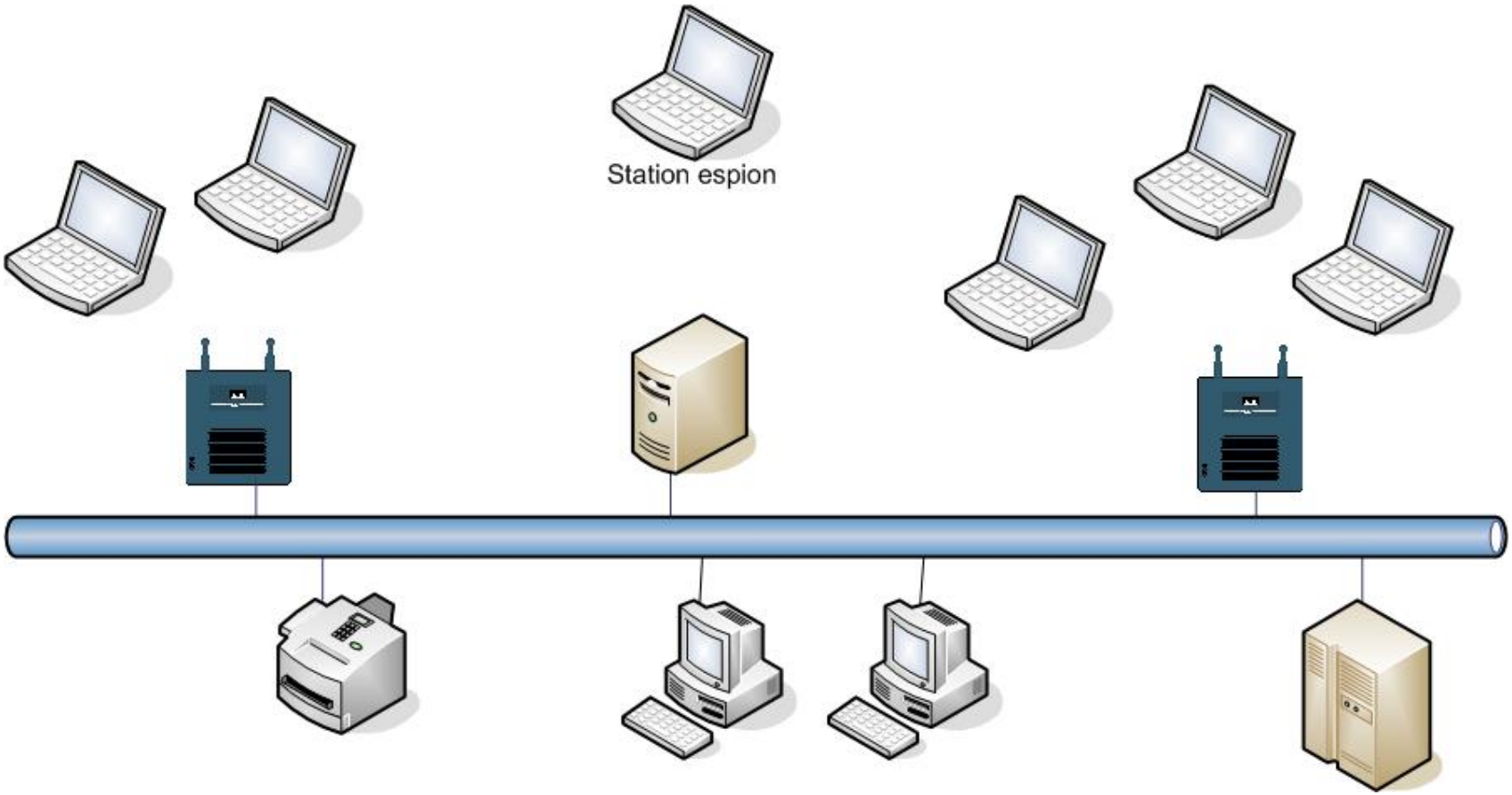
```
AP# configure terminal

AP(config)# dot11 ssid MonSSID
AP(config)# authentication open
AP(config)# authentication key-management wpa
AP(config)# wpa-psk ascii 1 mdp
AP(config)# guest-mode
AP(config)# exit

AP(config)# interface dot11radio 0
AP(config-if)# ssid MonSSID
AP(config-if)# encryption mode ciphers aes-ccm tkip
AP(config-if)# no shutdown
AP(config-if)# exit
```

Sécurité des réseaux WiFi

Types d'attaques

- interception de données ;
- intrusion dans le système ;
- attaque de l'homme au milieu (*man in the middle*) ;
- porte dissimulée (*backdoor*).

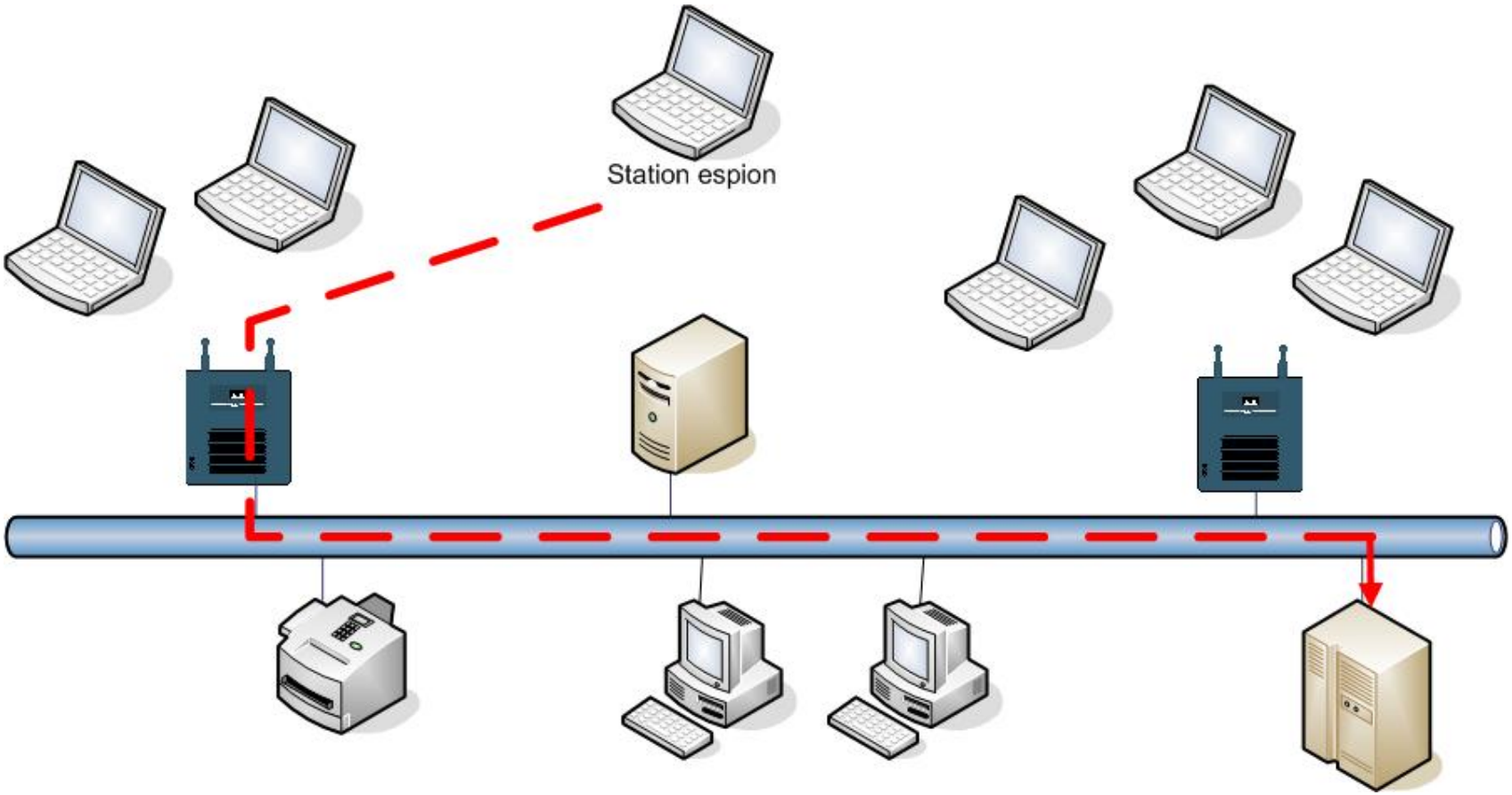
Interception des données



Interception des données

L'interception des données est l'attaque la plus facile. N'importe qui peut récupérer les trames radio qui circulent. Il suffit ensuite de réassembler les trames pour récupérer les différentes informations qui ont transité par le réseau sans fil.

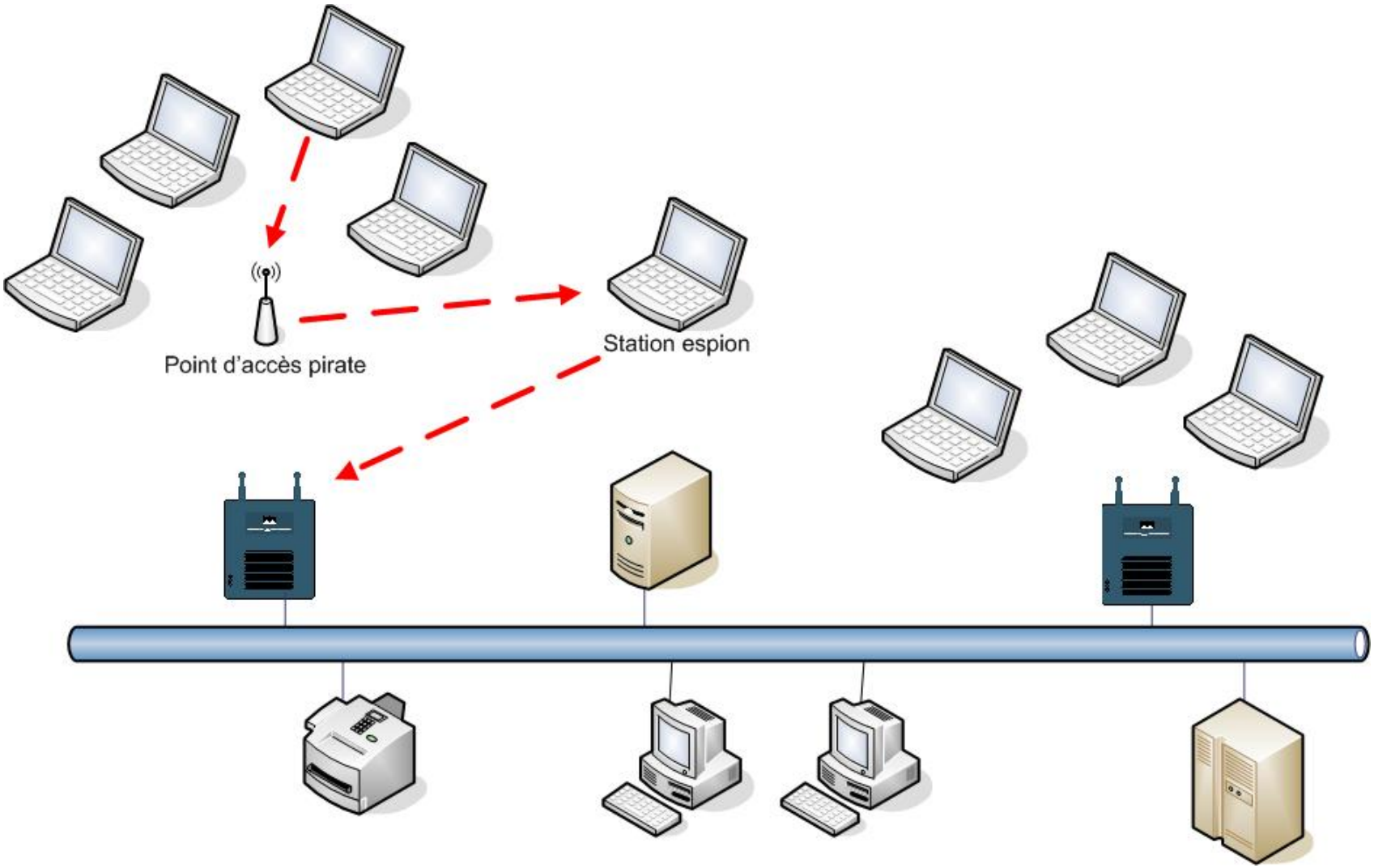
Intrusion dans le système



Intrusion dans le système

L'objectif de l'attaquant est d'accéder au résau filaire. Pour cela il va tenter de se connecter sur un AP non sécurisé. Il peut également récupérer les trames réseaux cryptés et tenter de trouver la clé de cryptage afin de s'identifier et s'authentifier auprès d'un AP.

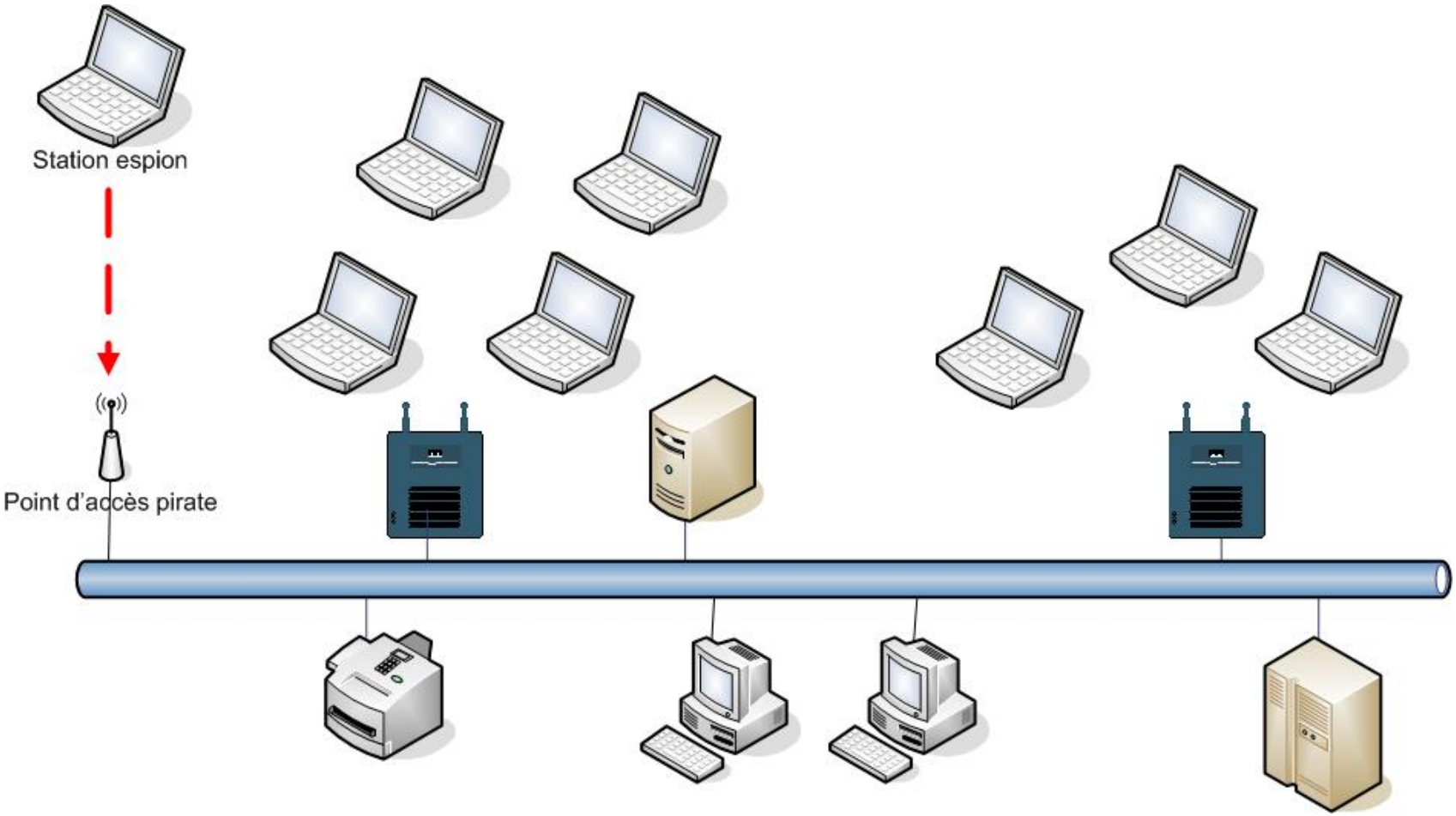
Man in the middle



Man in the middle

Man in the middle est une attaque classique de tous les systèmes informatique.

Porte dissimulée



Contre-mesures

Weak protection

- Supervision des ondes radio
- Éviter les AP pirates par une bonne couverture des locaux
- Ne pas broadcaster le SSID, mais :
  - Détection possible des AP
  - Récupération des trames possible et donc du SSID
- Filtrage par adresse MAC, mais :
  - Difficile à administrer
  - Récupération des trames possible et donc des adresses MAC autorisés
- Séparer le réseau sans-fil et le réseau filaire par utilisation par exemple de VLANs différents
- Cryptage par clé WEP
- Utilisation de VPNs

WEP

WEP : Wired Equivalent Privacy

- Clé partagée par l'ensemble des clients et invariable dans le temps
  - clé de longueur 40 ou 104 bits
  - clé en hexadecimal ou en texte
  - possibilité de générer une clé à partir d'un mot de passe
- Problème de gestion de la clé
  - beaucoup de copies de la clé (une par machine) implique un grand nombre de fuites potentielles
  - difficulté pour changer la clé. De nombreuses entreprises ne changent jamais leur clé WEP

WEP

- RC4 : Chiffrement par simple XOR de la clé avec les données (utilisation de la force brute sur le flux chiffré pour le décodage)
- authentification : AP envoie un challenge et le client répond avec le challenge chiffré avec la clé WEP (Man in the middle au moment du challenge)
- contrôle d'intégrité : CRC32 (modification des trames + nouveau CRC32 valide)

Faiblesses cryptographiques

- Répétition de la clé RC4
  - la longueur de l'IV est de 24 bits : trop court !
  - dès que deux paquets avec le même IV est reçu, le pirate peut connaître une partie des messages
  - indépendant de la longueur de la clé WEP utilisée
- Dictionnaires de décryptage
- Attaques sur les clés faibles

Conclusion sur WEP

- Il existe des outils open-source pour exploiter les faiblesses de WEP (décryptage de la clé)
- Mais WEP est mieux que rien
  - La plupart des attaques ont besoins d'écouter beaucoup de trafic
  - Les pirates doivent être à portée du réseau
  - Il existe des risques plus importants (virus, ...)
- De préférence, il faut utiliser WPA ou WPA2
  - sécurité renforcée
  - plus difficile à installer
  - une fois installé, le réseau est plus administrable

Wireless Protected Access

Vers un réseau Wi-Fi sécurisé

- Authentification forte
  - utilisation de 802.1x
  - basé sur EAP
  - nécessite un serveur d'authentification : RADIUS
- Cryptage fort
  - distribution des clés durant l'authentification
  - résoud tous les problème de cryptage de WEP
  - deux solutions :
    - WPA : cryptage TKIP (basé sur RC4)
    - WPA2 : cryptage CCMP (basé sur AES)

Mode Ad Hoc

- Communication directe
  - pas de point d'accès
  - Independent Basic Service Set (IBSS)
- Inconvénients :
  - difficulté de configuration
    - configuration WiFi
    - configuration IP manuelle
  - pas de routage
- Peut être utilisé pour connecté plusieurs points d'accès

Mode infrastructure

- Les clients se connectent au réseau via un point d'accès (AP)
  - 1 AP + clients = Basic Service Set (BSS)
  - zone de couverture : Cellule ou Basic Service Area (BSA)
  - identification par un nombre de 48 bits : BSSID
    - BSSID = AP Mac address
- Connexion de plusieurs points d'accès par un système de distribution (DS)
  - DS peut être Ethernet filaire, point-à-point, sans-fil
  - Extended Service Set / Extended Service Area
  - hand-over
    - maintien de la connexion lors d'un déplacement d'un BSS àl'autre dans le même EBSS
    - choix automatique de l'AP
    - identifié par un SSID (max 32 caractères)

Association / Reassociation

- After successful identification
- Send association request
  - list of the handled data rates
- AP
  - allocates unique ID
  - register information in allocation table
  - send acknowledge
- Hand-over : if station detects a better AP
  - send a unassociation request to former AP
  - send a reassociation request to new AP
    - contains ID of former AP
  - completely transparent to the user

Security

- SSID masking
  - weak : sniff probe packets
- MAC address filtering
  - not feasible if several AP and lots of stations
  - MAC spoofing
- WEP (Wired Equivalent Privacy)
  - shared key
  - free software allow to break WEP
- 802.1x and WEP key rotation
  - needs a RADIUS server
- 802.11i and WPA (Wireless Protected Access)
  - based on 802.1x
  - needs a RADIUS server
  - WPA : TKIP cryptography
  - 802.11i : AES cryptography (WPA2 certification)

Error Control / Fragmentation

- 32 bits CRC for each packet
  - high confidence in validated packets
  - in case of interferences : elimination of packets
- Fragmentation
  - error rate : $FER = 1 - (1 - BER)^{SIZE}$
  - it can be interesting to fragment packets
    - threshold parametrized
    - trade-off between FER and overhead
  - beacon frames, broadcast and multicast not fragmented

Dispatching and WDS

- Dispatch problem
  - where to forward receive packets ?
  - to the BSS or to the DS ?
- Mechanism : 2 bits

toDS	fromDS	signification
0	0	Ad Hoc
1	0	station → AP
0	1	AP → station
1	1	WDS : AP → AP

- Wireless Distribution Service
  - extension of a wireless network with AP not connected to wired network
  - vague specification → compatibility problems
  - discussion for mesh networks → 802.11s

Wireless Security

- Fundamental qualities
  - confidentiality
  - integrity
  - availability
  - non repudiation
- Common attacks
  - war-driving
  - spying
  - intrusion
  - denial of service
  - message modification

Solutions

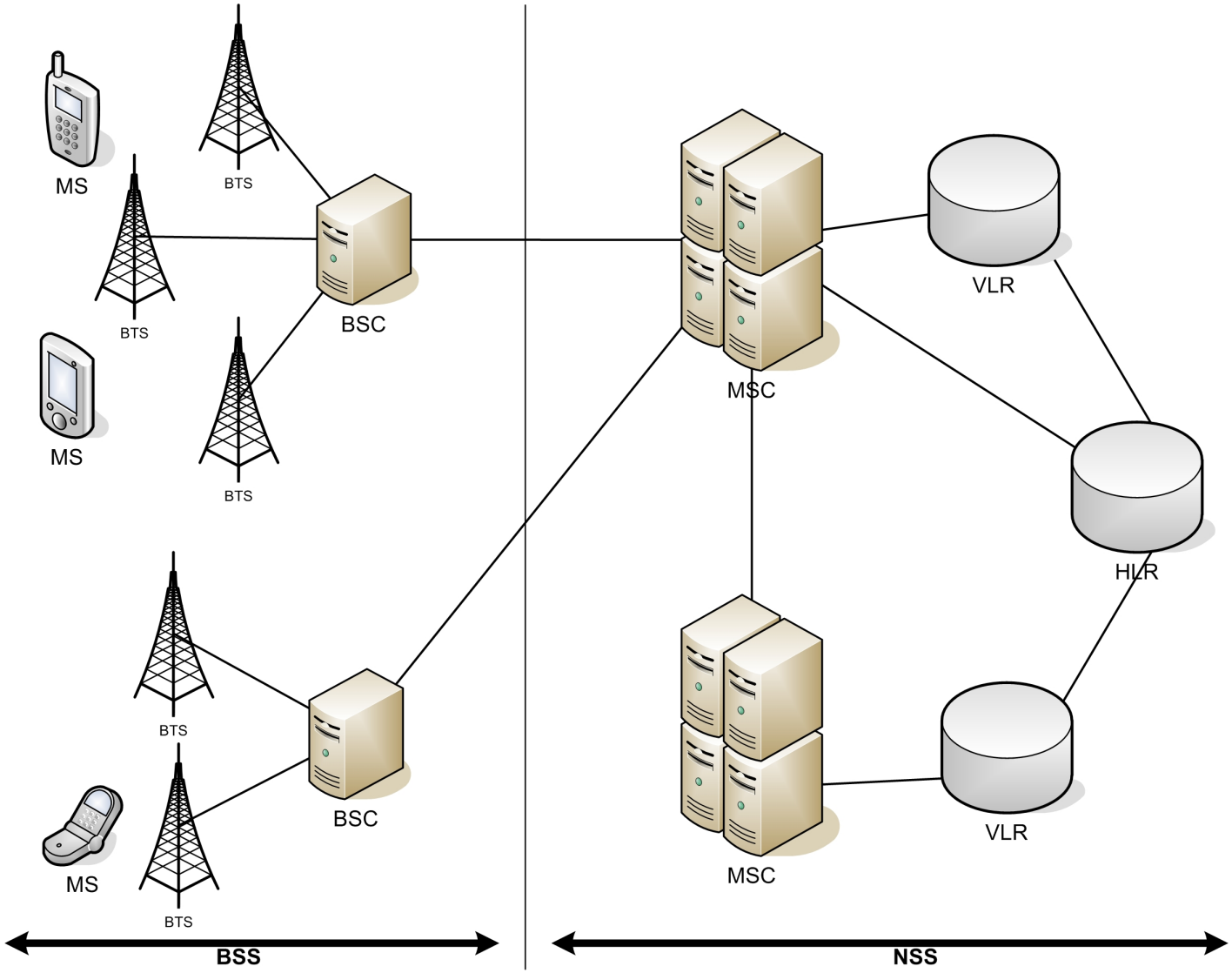
- First solutions
  - limit overflowing → deployment
  - avoid pirate access point → limit temptation by a good coverage
  - radio supervision
  - mask the SSID
  - MAC address filtering
  - VLANs
  - WEP cryptography
  - isolate the wireless network from the wired network
  - use VPNs
- Other solutions
  - LEAP (Cisco) and proprietary solutions, WPA, 802.11i
  - all based on 802.1x, itself based on EAP
  - use an authenticating server, nearly always RADIUS

Principle

- Everybody shares a common key
  - key length : 40 or 104 bits
  - key format : hexadecimal or text
  - possibility of key generation from a password
- Key handling problem
  - lots of copies of the key → lots of potential security leaks
  - difficulty of key changing → many enterprises never change their WEP key

Infrastructure d'un réseau GSM

Architecture générale d'un réseau GSM



Constituants d'un réseau GSM

MS : Mobile Station ;

BTS : Base Transceiver Station ;

BSC : Base Station Controller ;

BSS : Base Station Subsystem ;

MSC : Mobile services Switching Center ;

VLR : Visitor Location Register ;

HLR : Home Location Register ;

NSS : Network SubSystem.

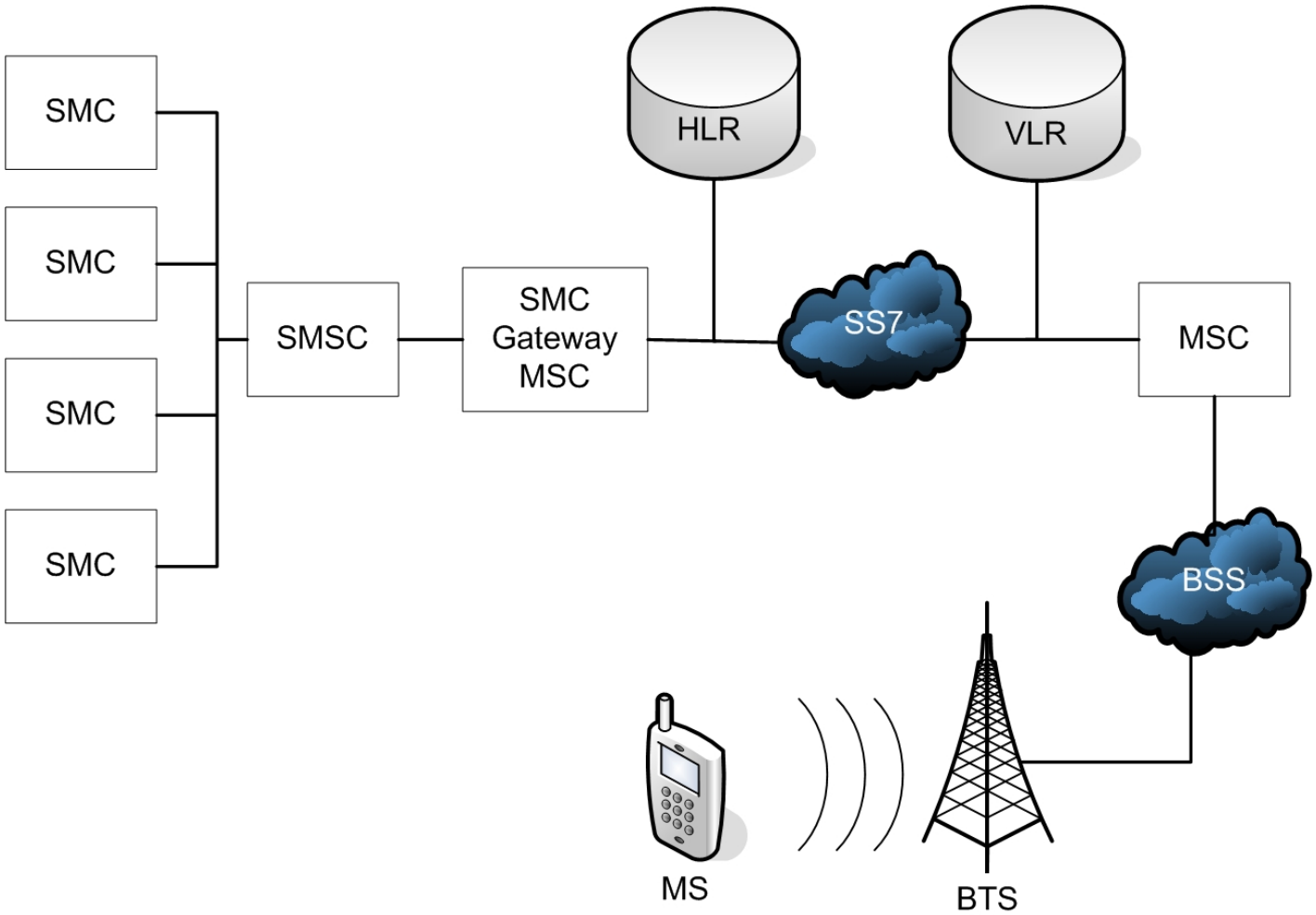
Le service des messages courts

Introduction

Définition :

- Le service des messages courts ou SMS (Short Message Service) est un service qui permet la transmission de messages alphanumériques entre des GSM, des téléphones fixes, des ordinateurs . . . ou vers des systèmes de courriers électronique, de fax, . . .
- La taille maximale du message est de 160 caractères.

Architecture du réseau SMS



Constituants du réseau SMS

SME : Short Messaging Entities est l'entité qui reçoit ou émet des SMS ;

SMC : Short Message Center

SMSC : Short Message Service Center

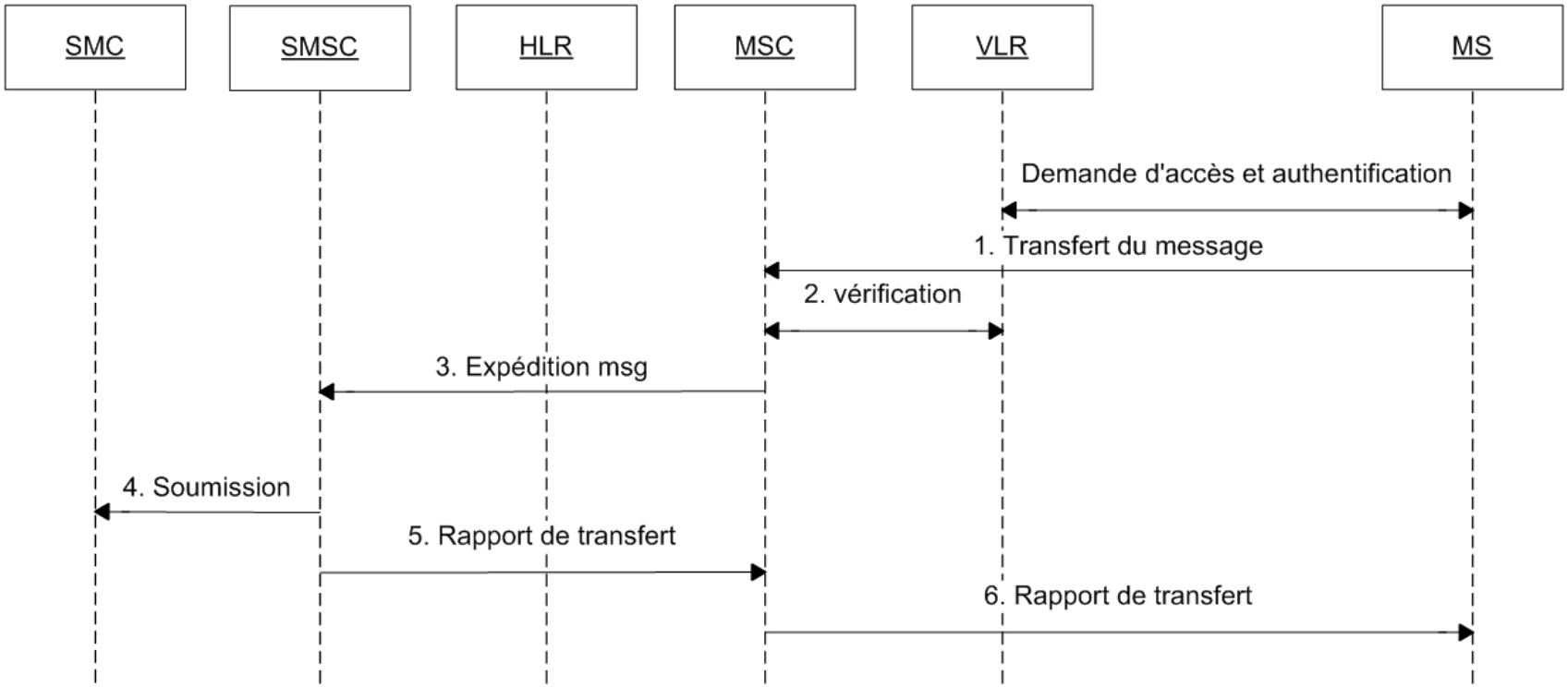
HLR : Home Location Register

MSC : Mobile services Switching Center

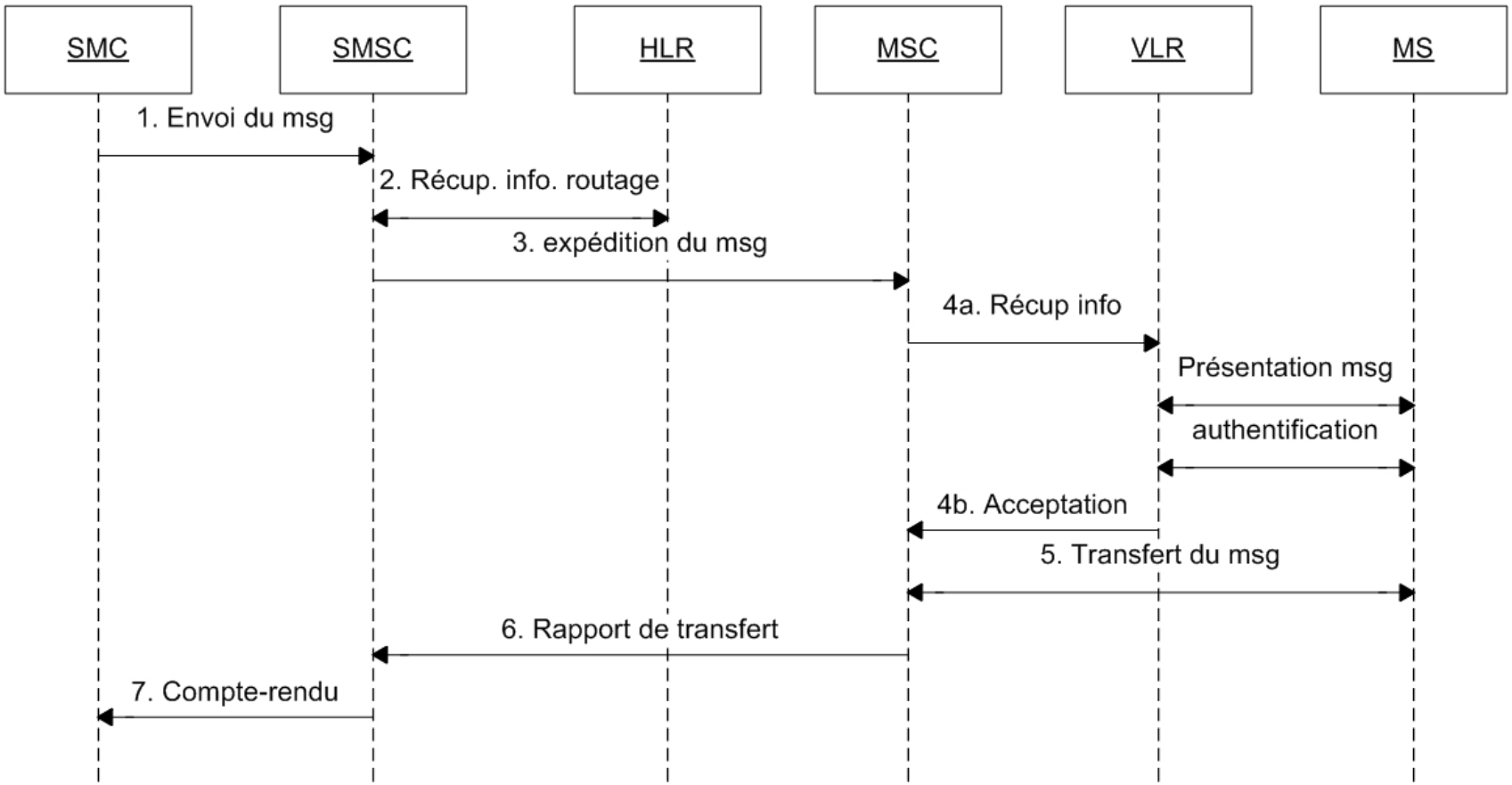
VLR : Visitor Location Register

BSS : Base Station System est le sous-système gérant les relais radio.

Émission d'un message



Réception d'un message



Glossaire

- CSMA : Carrier Sense Multiple Access
- DSSS : Direct Sequence Spread Spectrum
- GPRS : General Packet Radio Service
- GSM : Global System for Mobile Communication
- ISM : Industrial, Scientific and Medical
- OFDM : Orthogonal Frequency Division Multiplexing
- PAN : Personal Area Network
- PSTN : Public Switched Telephone Network
- QAM : Quadratic Amplitude Modulation
- RADIUS : Remote Authentication Dial-In User Service
- SSID : Service Set IDentifier
- TDMA : Time Division Multiple Access
- TKIP : Temporal Key Integrity Protocol
- UMTS : Universal Mobile Telecommunication System
- WECA : Wireless Ethernet Compatibility Alliance

Glossaire

- WEP : Wired Equivalent Privacy
- Wi-Fi : Wireless Fidelity
- WISP : Wireless Internet Service Provider
- WLAN : Wireless Local Area Network