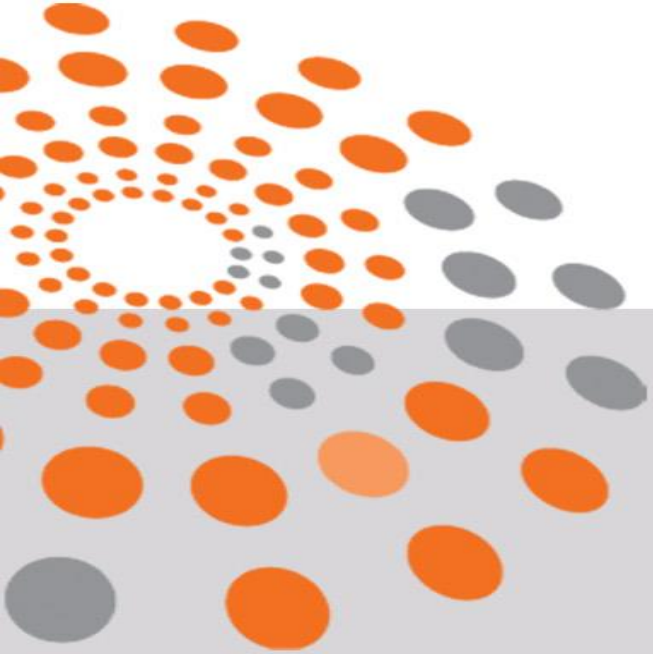


WIFI
Chapitre 4

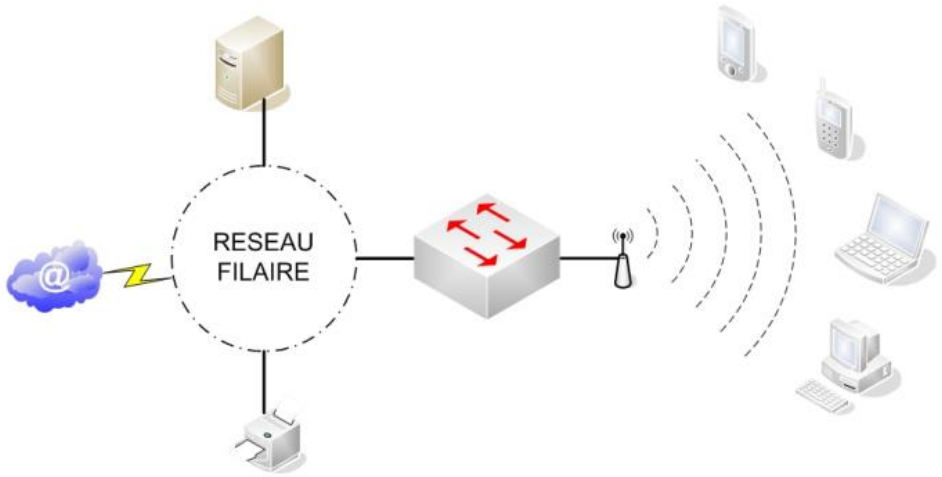
1. WLAN

- Un WLAN est un réseau partagé
- Un point d’accès (AP) permet l’accès au réseau
- Un AP fonctionne comme un hub
- Les accès sont en half duplex, partage de bande passante
- Utilisation de la même fréquence en émission et en réception
- Un répéteur peut amplifier un signal radio affaibli

2. WLAN vs LAN

- Avantages des réseaux sans fils :
  - Moins contraignant (mobilité)
  - Accès plus simple et moins contraignant (mobilité)
  - Déploiement
  - Couverture des sites et mutualisation
- Inconvénients :
  - Débits souvent moins importants
  - Sécurité
  - Fiabilité
  - Couverture faible

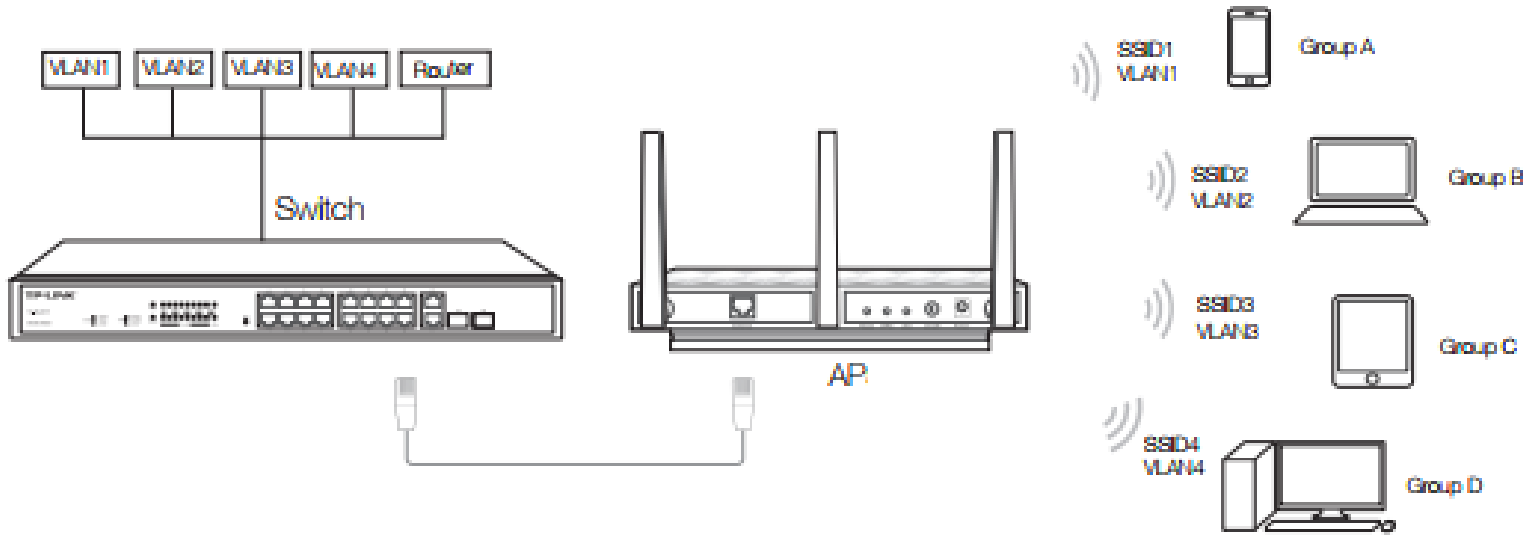
3. Fonctionnement d'un AP



- Un WLAN (Wireless LAN) est un réseau partagé
- Un point d'accès (AP, Access Point) permet l'accès au réseau
- Un AP fonctionne comme un hub Ethernet partagé
- Les accès se font en Half duplex
- Même fréquence pour émission-réception
- Méthode d'accès CSMA/CA

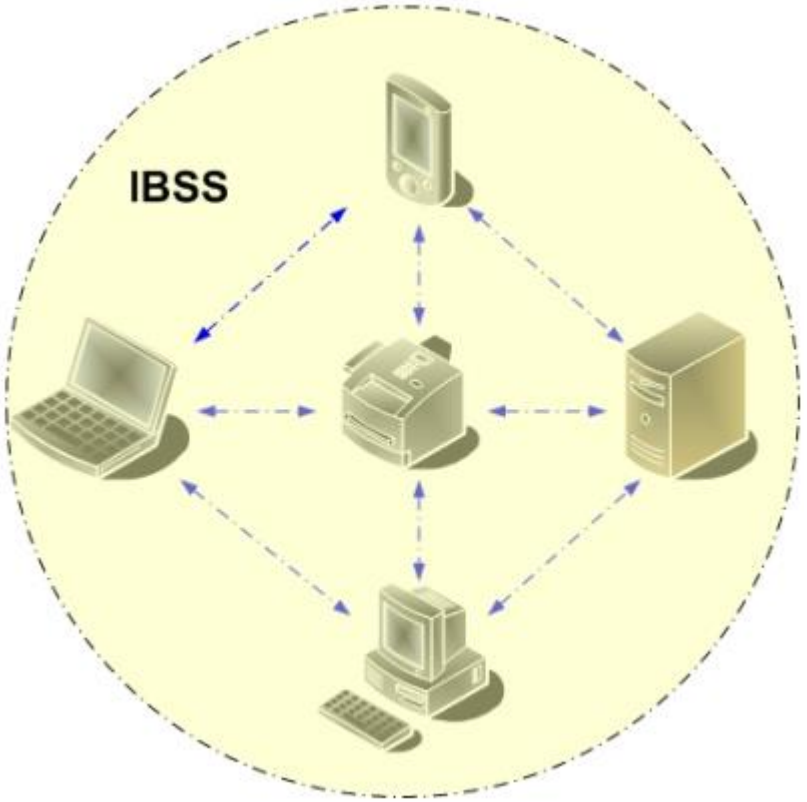
4. SSID

- Le Service Set IDentifier permet de différentier les réseaux logiques WLAN
- Un client doit connaitre le SSID du réseau WLAN auquel il veut se connecter
- Ce sont les AP qui annoncent eux-mêmes le SSID sauf SSID non difusé
- Pour accéder de manière univoque à une borne, il faut que le couple (SSID, canal) soit unique



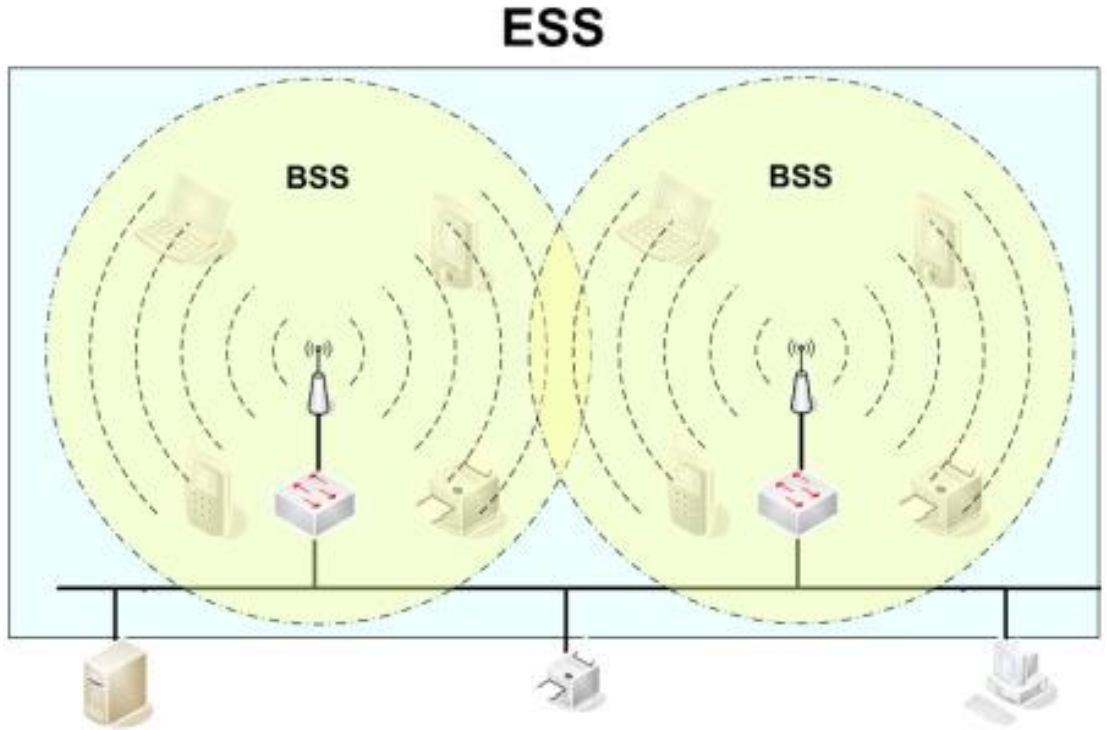
5. Modes de fonctionnement

- Mode Ad-Hoc :
  - Relation directe entre homologues en point-à-point (Peer to Peer)
  - Simple à mettre en place, mais limite, de facto, l'étendue des échange
  - Pas de possibilité d'interconnexion avec un réseau filaire
  - Utilisée pour les communications directes entre deux machines : les homologues doivent être à portée radio



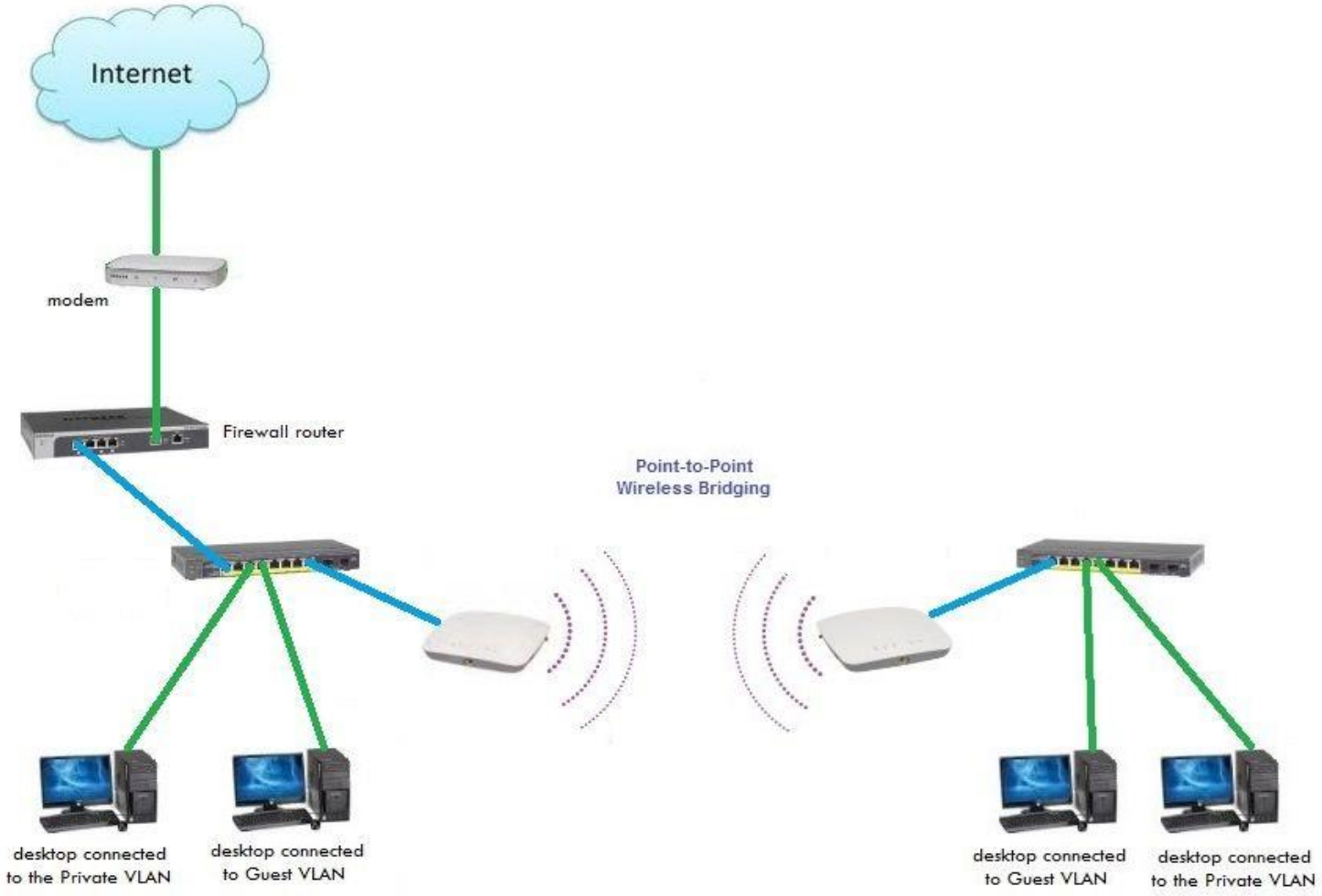
5. Modes de fonctionnement

- Infrastructure :
  - Un pont permet aux machines munies d'un émetteur sans fil d'accéder aux réseaux filaires
  - Plus complexe à mettre en place
  - Etendue et couverture beaucoup plus importantes
  - On désigne par BSS, Basic Service Set, l'ensemble constitué du point d'accès et des stations à portée radio
  - On désigne par ESS, Extended Services Set, l'ensemble des BSS reliés entre eux



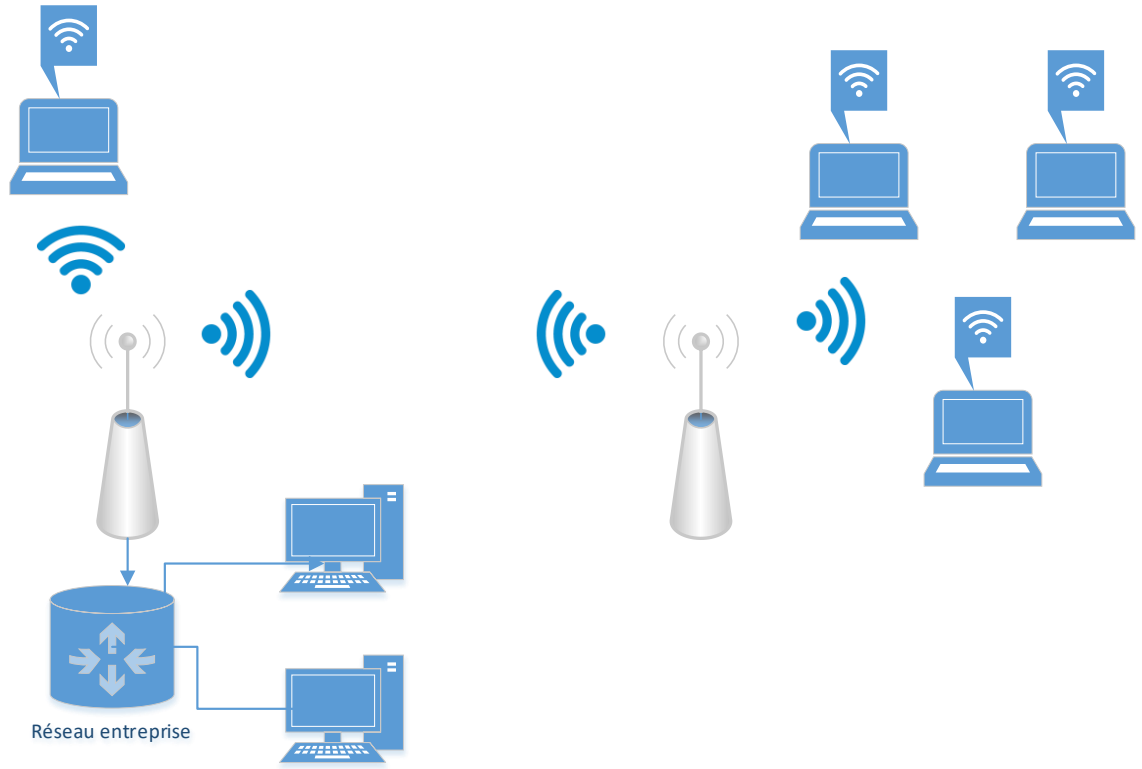
5. Modes de fonctionnement

- Pont (« bridge »)
  - Permet d'interconnecter des réseaux filaires entre eux
  - Un root bridge (diffuse le SSID) et des bridge (clients)
  - Distances faibles
  - Un seul SSID

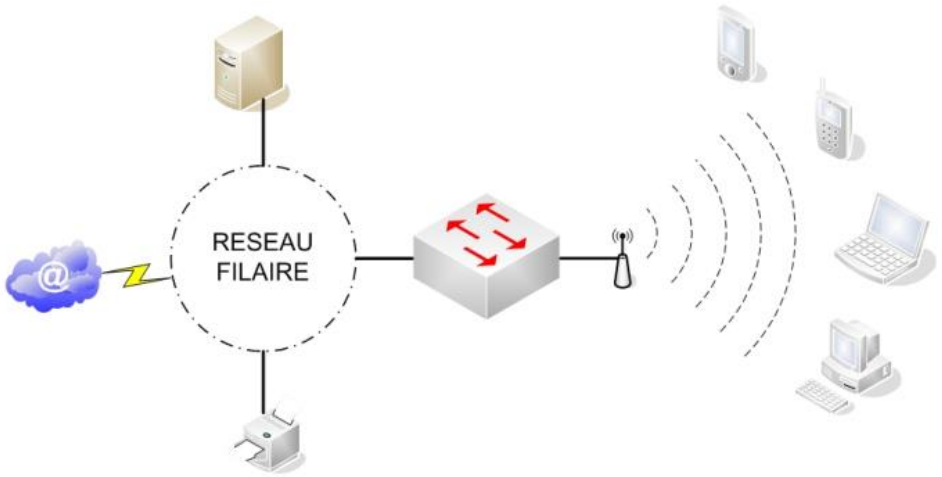


5. Modes de fonctionnement

- Répéteur :
  - Permet de répéter le signal (extension de portée
  - Interface Ethernet inactive
  - Débit partagé vers l'AP principale
  - Latence



6. Utilisation



- **Connectivité mobile :**
  - Permet aux utilisateurs d'accéder aux ressources des réseaux filaires
  - Utilisation la plus répandue
  - Utilise des antennes omnidirectionnelles
- **Connectivité LAN-to-LAN**
  - Utilisée pour connecter entre eux des réseaux éloignés
  - Utilise des antennes unidirectionnelles

7. Historique

- 1992, début des travaux de l'IEEE sur les réseaux sans fils
- 1997, première norme : 802.11
- WECA a défini la certification Wi-Fi (Wi-Fi pour Wireless Fidelity). Cette certification a deux buts :
  - Promotion du 802.11 sous un nom moins technique
  - Assurer l'interopérabilité des constructeurs
  - Wi-Fi alliance (nouveau nom)
- 1999, extensions :
  - 802.11a : 54 Mb/s, 5-6 GHz
  - 802.11b : 11 Mb/s, 2,4-2.5 GHz
- 2003 : 802.11g : 54 Mb/s, 2,4-2.5 GHz

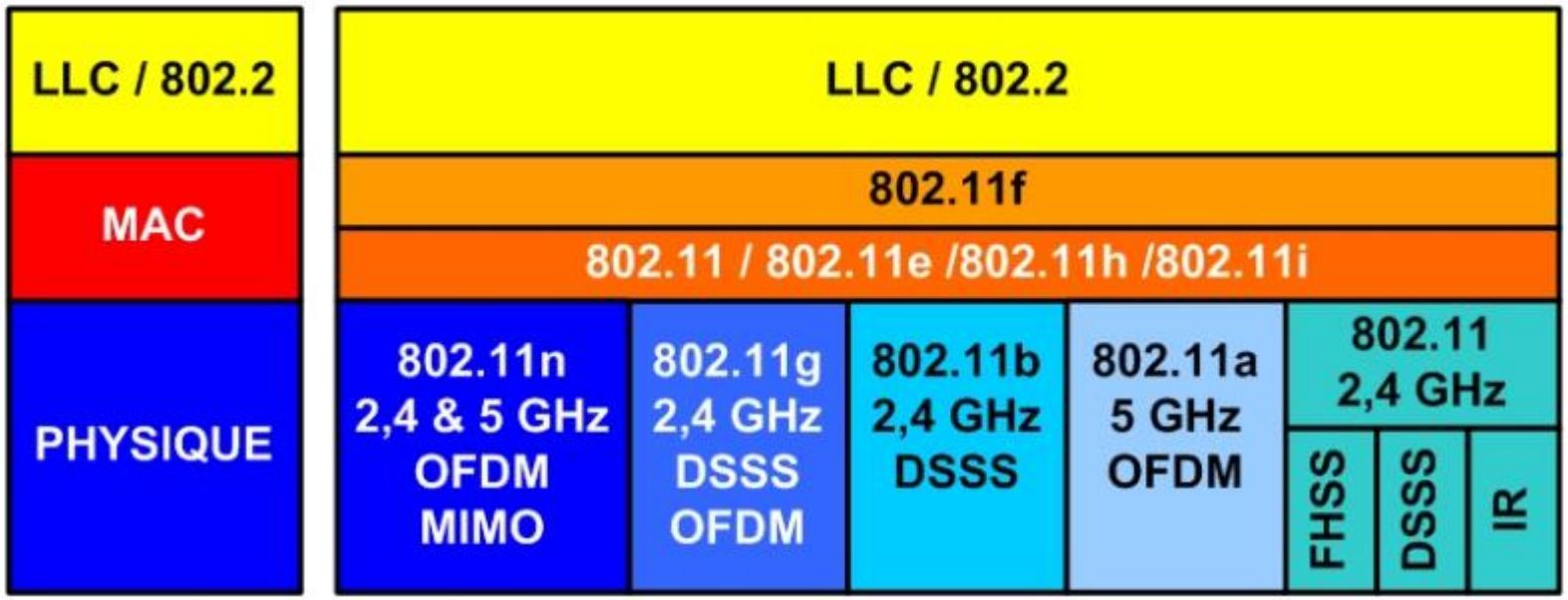
7. Historique

- 2009 : 802.11n : 288Mb/s (2.4GHz) 600Mb/s (5Ghz) => Wi-Fi « 4 »
  - MiMo (Multiples input Multiples Output)
  - OFDM
- 2013 : 802.11ac : 2.6Gb/s => Wi-Fi « 5 », 5GHz
- 2021 : 802.11ax : 10Gb/s => Wi-Fi « 6 », 5GHz
- A venir : WiFi 6E (en cours), 6GHz

8. Norme 802.11

- 802.11 définit, à l'origine :
  - Une couche MAC unique
  - Trois couches physiques principales, incompatibles entre-elles
  - Support des modes ad-hoc et infrastructure
  - Sécurité : authentification et cryptage des données
  - Fréquences utilisables :
    - 2.4 à 2.5 GHz
    - 5 GHz à 6GHz
  - Deux modes de transmission radio :
    - DSSS et FHSS en étalement de spectre (ancien)
    - Le multiplexage OFDM (Orthogonal Frequency-Division Multiplexing)

8. Norme 802.11



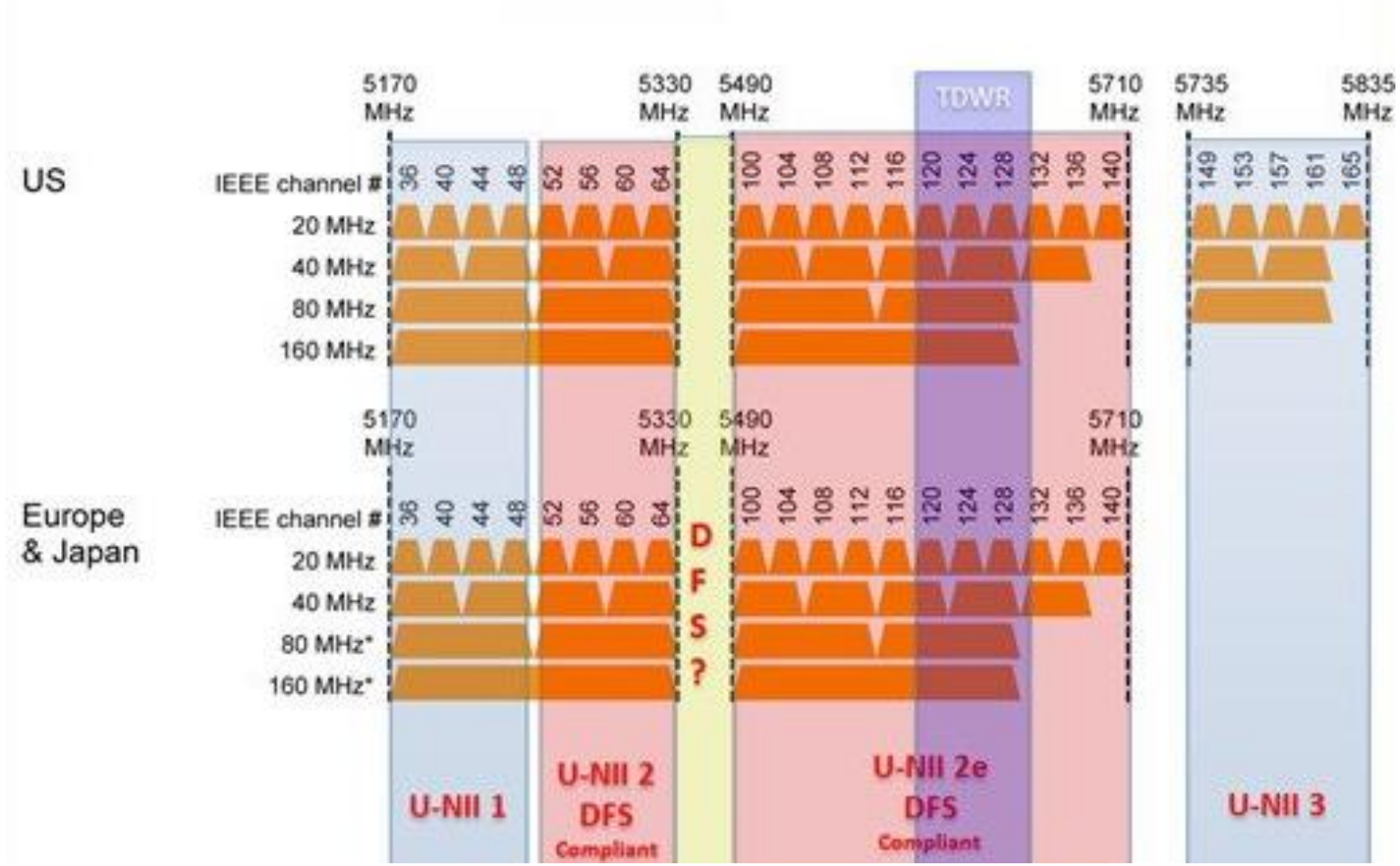
8. Norme 802.11

- 802.11i définit l'amélioration des fonctionnalités de sécurité
  - Définition d'un standard 802.1x spécifique à la gestion de l'authentification et de l'échange des clés dans les réseaux 802.11 :
    - Serveurs d'authentification
    - Authentifications EAP-MD5 et EAP-TLS
  - Génération et gestion de clés dynamiques
  - Amélioration de WEP via le protocole TKIP, ne nécessitant qu'une mise à jour logicielle.
  - Utilisation de AES en lieu et place de RC4 pour le cryptage des données

9. Canaux 2.4GHz

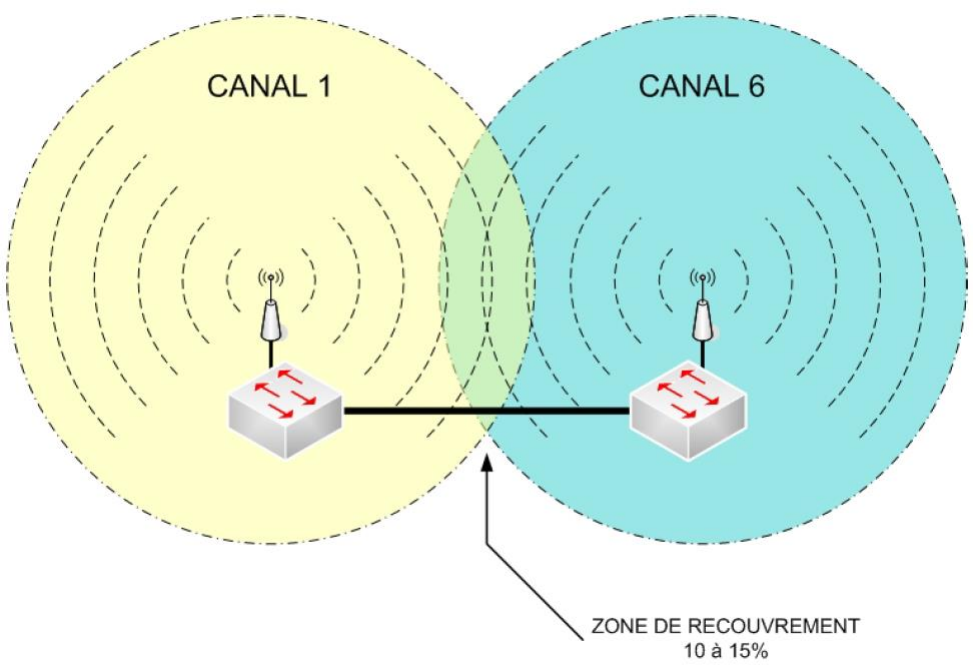
NUMERO DE CANAL	FREQUENCE « CENTRALE » (MHz)	PLAGE DE FREQUENCES (MHz)	AMERIQUES	EUROPE MOYEN-ORIENT ASIE	JAPON
1	2412	2401-2423	X	X	X
2	2417	2406-2428	X	X	X
3	2422	2411-2433	X	X	X
4	2427	2416-2438	X	X	X
5	2432	2421-2443	X	X	X
6	2437	2426-2448	X	X	X
7	2442	2431-2453	X	X	X
8	2447	2436-2458	X	X	X
9	2452	2441-2463	X	X	X
10	2457	2446-2468	X	X	X
11	2462	2451-2473	X	X	X
12	2467	2466-2478		X	X
13	2472	2471-2483		X	X
14	2484	2473-2495			X

10. Canaux 5GHz

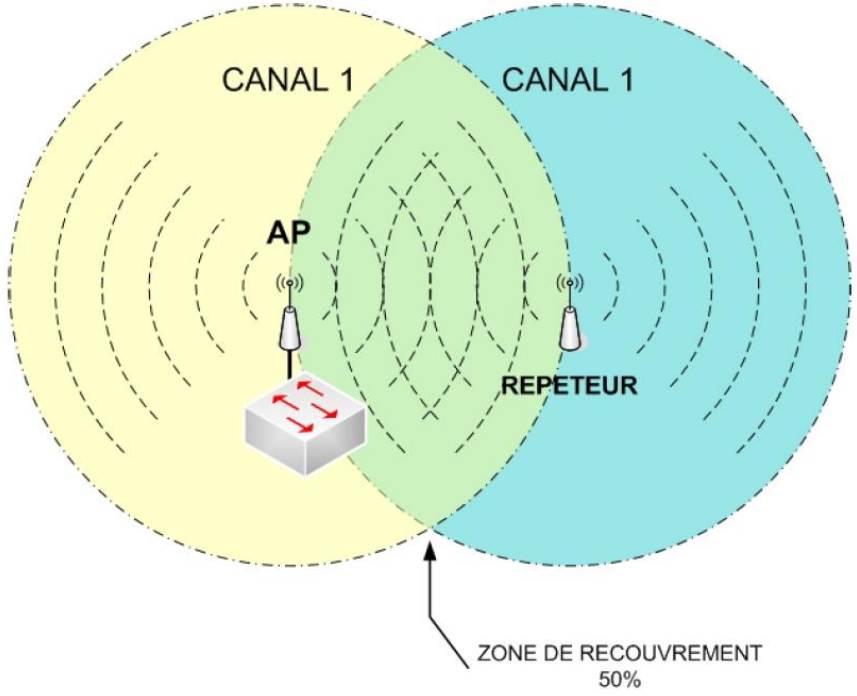


11. Recouvrement même canal

- Entre deux AP (canal identique) :

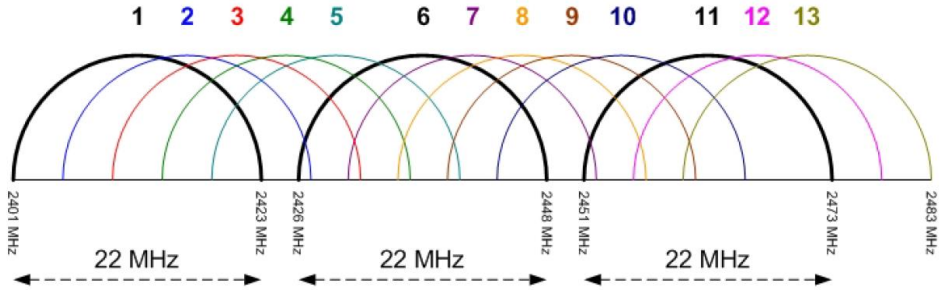


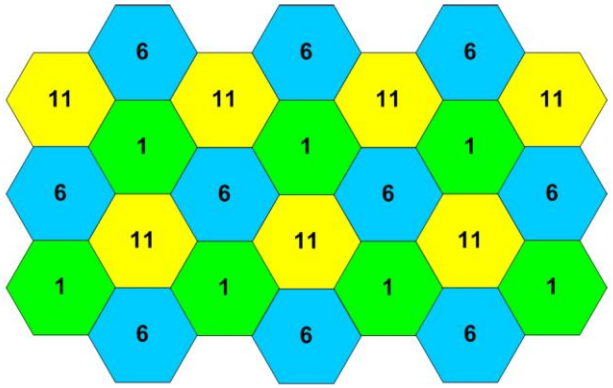
Répéteur (canal identique) :



12. Recouvrement canaux 2.4GHz

- Utilisation de 3 canaux sans chevauchement : 1, 6 et 11





- Mise en place d’un contrôleur WIFI (Essentiel pour la ToIP)
- Faire une étude de propagation dans les environnements sensibles aux Champs électromagnétiques.

13. Recouvrement canaux 5GHz

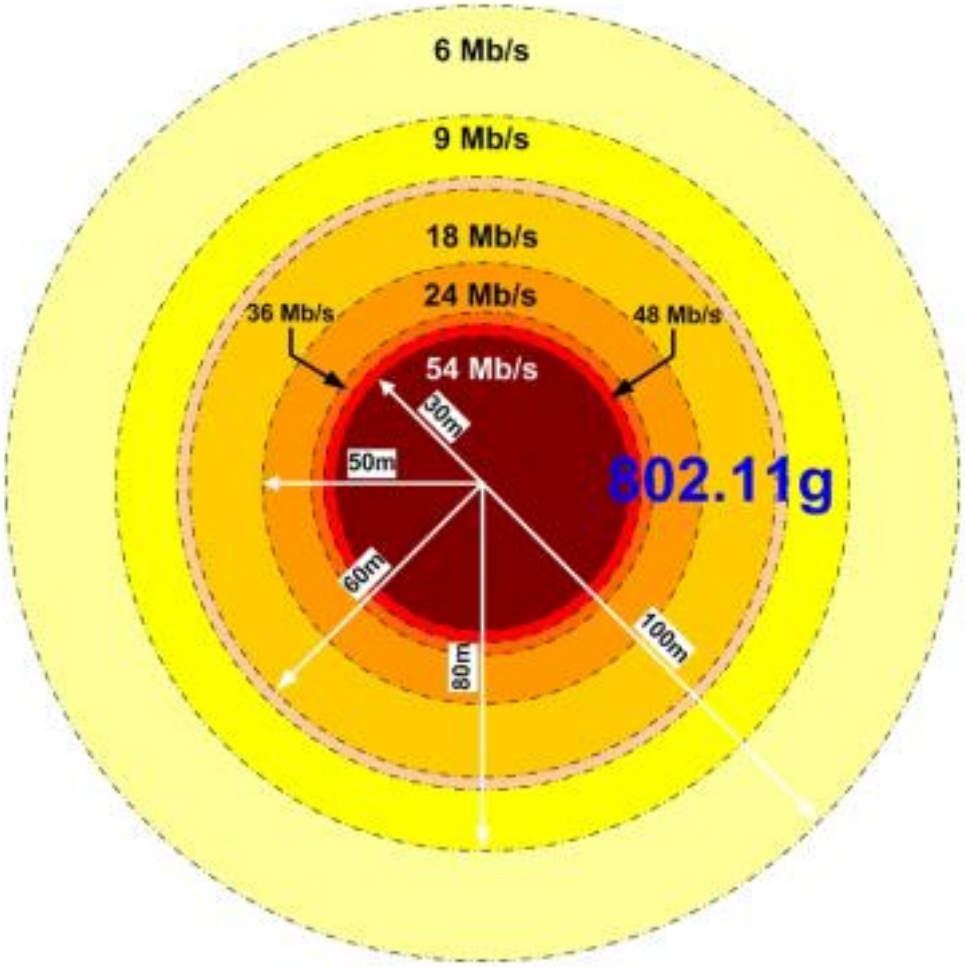
- Pas de recouvrement !
  - Attention aux canaux réservés :
    - USA (FCC) : 23 canaux possibles
    - EUROPE (ETSI) : 19 canaux possibles

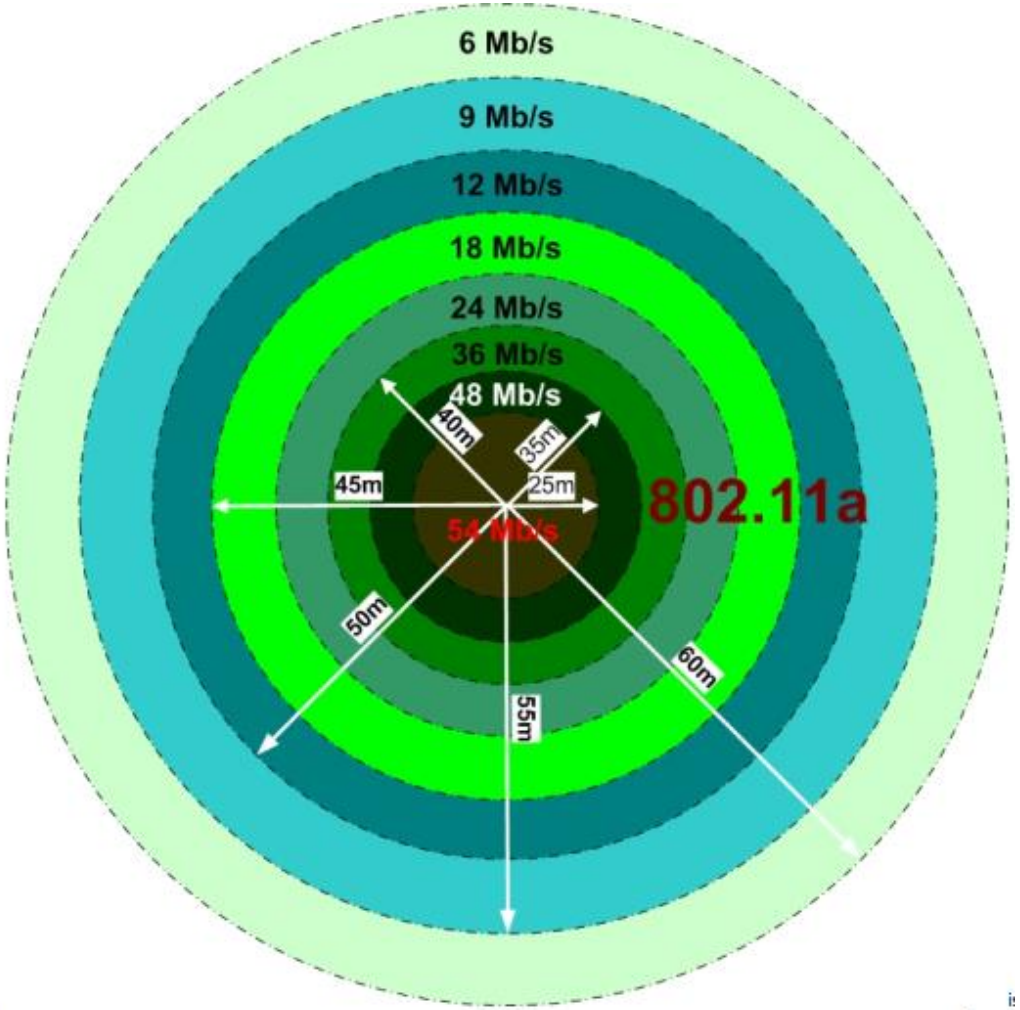
14. Débits

- Il faut différencier le débit nominal du débit maximum réel
  - Le débit nominal prend en compte le transfert total, l'intégralité de la trame
  - Le débit maximal réel ne prend en compte que le transfert de la partie utile transportée

DEBIT NOMINAL Mb/s	DEBIT REEL Mb/s	OVERHEAD %
1	0,93	7
2	1,72	14
5,5	4	27
11	6,38	42
54	26-30	52-44

14. Débits


6 Mb/s
9 Mb/s
18 Mb/s
24 Mb/s
36 Mb/s
48 Mb/s
54 Mb/s
30m
50m
60m
80m
100m
802.11g


6 Mb/s
9 Mb/s
12 Mb/s
18 Mb/s
24 Mb/s
36 Mb/s
48 Mb/s
40m
35m
45m
25m
54 Mb/s
50m
55m
60m
802.11a

15. Réglementations 2.4GHz

- **Etats-Unis :**
  - 2,400-2,483 GHz
  - FCC : documents CFR47 part 15 sec 15.205, 15.209 ,15.247 et 15.249
- **Europe :**
  - 2,400-2.483 GHz
  - ETSI : documents ETS 300 328, 300 339
  - France : ETSI SP/DGPT/ATAS/23
- **Japon :**
  - 2,471-2,497 GHz
  - ARIB : RCR STD-33A

15. Réglementations puissances

- **2,400-2,483 GHz :**
  - CEPT : CEPT/ERC/DEC/(01)07
  - ETSI : EN 300 328 et 300 339
  - France : ETSI SP/DGPT/ATAS/23
- **5 GHz :**
  - CEPT : CEPT/DEC/(96)03 et (99)23
  - ETSI : EN 300 836

FREQUENCES (GHz)	PUISSANCE (mW)	
	INTERIEUR	EXTERIEUR
2.4-2.446	<10	<2.5
2.446-2.483	<100	Autorisation
5.150-5.250	<200	non
5.250-5.350	<200	non
5.470-5.725	A l'étude	A l'étude

16. Sécurité

- Filtrage
  - Access Control List
  - Filtrage sur les adresses MAC, les adresses IP, les applications…
- Afin de sécuriser les échanges entre un point d'accès et une station, celles-ci doivent établir une association
- Une association est une relation de sécurité entre deux machines
- Protocole utilisé pour réaliser l'association en 802.11 : WEP (Wired Equivalent Pricacy)

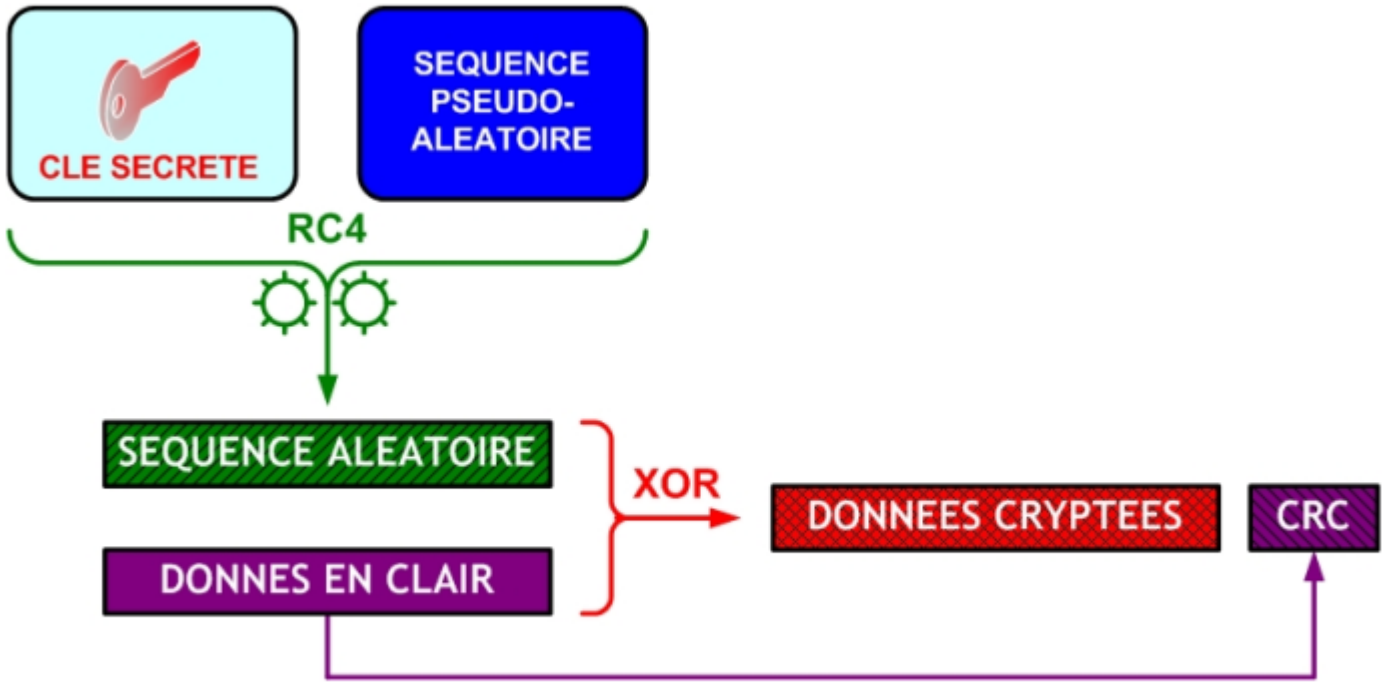
17. Sécurité - WEP

- Le standard 802.11 définit :
  - WEP comme méthode de cryptage pour la confidentialité et la vérification d'intégrité
  - Deux méthodes d'authentification :
    L'une sans authentification de fait
    L'autre permettant de vérifier la concordance de la clé secrète de cryptage
- Le cryptage s'effectue au niveau de la couche liaison de données (niveau 2), sur la trame. Ce qui signifie que tout ce qui est transporté dans les couches supérieures
  est également protégé.
- Le cryptage est à clé symétrique secrète

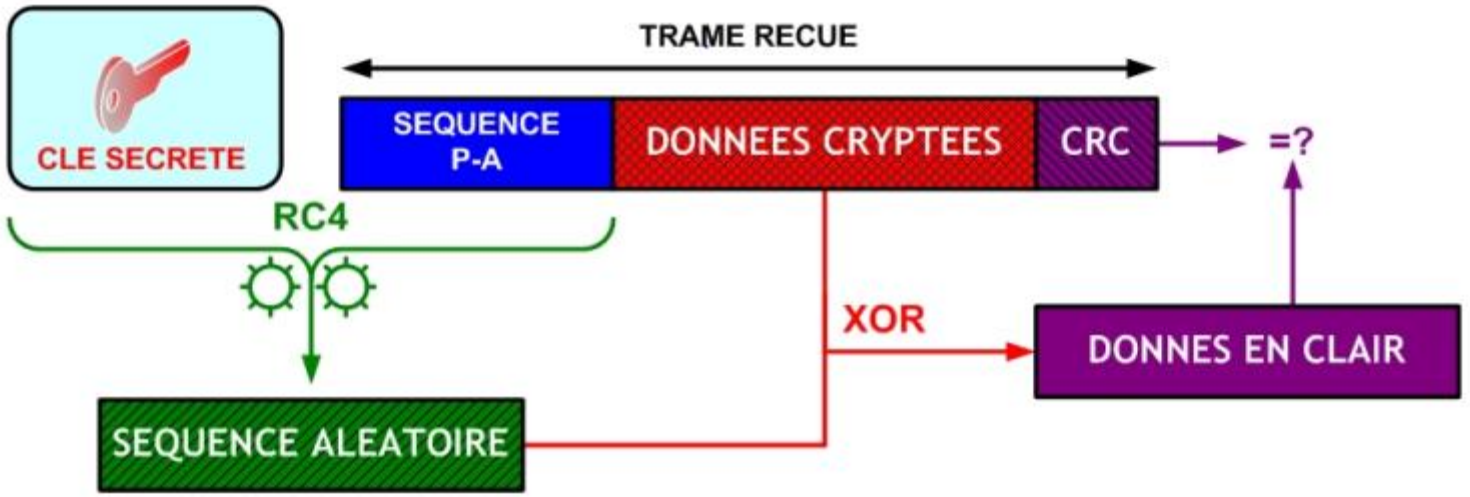
17. Sécurité - WEP

- La clé utilisée pour le cryptage est composée de deux éléments :
  - Une clé statique sur 40 bits, c'est la séquence qu'il faut configurer sur chaque station
  - Une séquence pseudo-aléatoire (ou vecteur d'initialisation), sur 24 bits, qui change à chaque trame expédiée. Elle est générée par la station émettrice
    - Algorithme publique utilisé : RC4
    - La trame envoyée contient les données cryptées, le CRC et la séquence pseudo-aléatoire

17. Sécurité - WEP



18. Sécurité - WEP



18. Sécurité - WEP

- Longueur de la clé initiale de 40 bits
- Puissance de l’algorithme de cryptage.
- Méthode d’authentification faible ou nulle.
- Méthode d’échange ou de vérification des clés.
- N’empêche pas le REPLAY
- WEP2 permet d’utiliser une clé initiale de 104 bits

18. Sécurité - WEP

- Longueur de la clé initiale de 40 bits
- Puissance de l’algorithme de cryptage.
- Méthode d’authentification faible ou nulle.
- Méthode d’échange ou de vérification des clés.
- N’empêche pas le REPLAY
- WEP2 permet d’utiliser une clé initiale de 104 bits

19. Sécurité - WPA

- 2003 :
  - WPA : WiFi Protected Access, sous ensemble de 802.11i
  - Amélioration de l'architecture de sécurité du WiFi
  - Nécessite uniquement une mise à jour du firmware
  - TKIP (Temporal Key Integrity Protocol) : amélioration de RC4, compatible avec le matériel existant (clé de 128 bits générée pour chaque paquet)
-

20. Sécurité - WPA2

- 2005 :
  - WPA2 / RSN
  - Incompatible avec la version précédente
  - CCMP (Counter-mode / CBC-MAC Protocol) qui utilise l'algorithme AES pour le cryptage des paquets (plus robuste que TKIP)
  - Robust Security Network
  - Modification de la méthode et de l'algorithme de cryptage : AES en mode OCB.
  - Mise en place d'une méthode fiable et puissante d'authentification : EAP-TLS.
  - Augmentation de la longueur des clés utilisées.
  - Individualisation des clés utilisées par session : une clé sera spécifique entre une station et un point d'accès donnés.
  - Les clés seront renouvelées à intervalles réguliers et échangées dynamiquement.

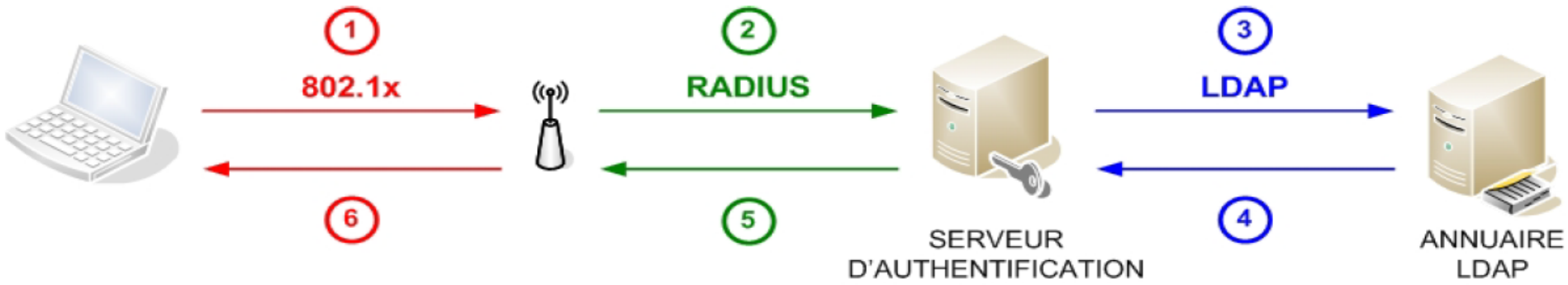
21. Sécurité - WPA2 enterprise

- Utilise 801.1x pour l'authentification en EAP
  - RADIUS pour l'authentification centralisée permettant d'être mobile et sécurisé
- EAP, Extensible Authentication Protocol est un protocole d'authentification standard et normalisé dans le TFC 3748.
  - RFC 3748
  - Il est le remplaçant de CHAP, mais beaucoup plus puissant et évolutif, EAP n'inclut pas les méthodes d'authentification, il s'appuie sur celles existantes, en autre RADIUS.
  - Utilise différentes méthodes d'authentification :
    - MD5
    - SHA-1
    - PEAP
    - TLS
    - TTLS

21. Sécurité - WPA2 enterprise

- Normalisation de l'authentification réseau réalisée par les points d'accès au réseau
- La machine utilisatrice doit s'authentifier à la première utilisation du réseau
  - Cette authentification est initiée par le point d'accès
  - Une machine ne peut accéder au réseau qu'en cas d'authentification réussie
- Le point d'accès utilise RADIUS afin de transmettre la requête d'authentification
  - Les informations d'authentification sont souvent stockées sur un serveur de type LDAP
  - De nombreux paramètres associés à l'authentification peuvent être utilisés : adresse IP, protocoles autorisés, ACL…

22. 802.1x



1. Le client lance une authentification 802.1x
2. L'AP envoie une requête d'authentification au serveur RADIUS
3. Le serveur RADIUS envoie une requête à l'annuaire LDAP
4. Le serveur LDAP répond
5. Le serveur RADIUS transmet la réponse à l'AP
6. L'AP autorise ou interdit en conséquence l'accès au réseau à la machine

23. Radius

- *Remote Authentication Dial In User Service*, protocole sécurisé d'échange d'informations d'authentification et d'autorisation
  - L'intérêt principal réside dans la centralisation de l'authentification
  - Normalisé et libre.
  - UDP 1646 & 1813
  - Seul le mot de passe est crypté, les autres informations sont transmises en clair
- Fonctionnalités :
  - Authentification des utilisateurs
  - Autorisations allouées aux utilisateurs
  - Services délivrés : PPP, Telnet, accès réseau…
  - Définition de nombreux attributs associés aux utilisateurs : standards, spécifiques, propriétaires
  - Interfaçage avec : LDAP, Unix/Linux, NDG, NDS, RDBMS, CVS, SAM, ODBC…

24. Sécurité - WPA3

- Sorti en 2018
- Reprend les grands principes de WPA2
- Chiffrement des réseaux ouverts (pas de PSK)
- Améliore la sécurité (failles WPA2-PSK sorties en 2018)

A retenir

1. Un réseau partagé WLAN avec ses AP se comportent comme des HUBS
2. Les accès sont en half duplex donc en partage de bande passante
3. Faire l'étude d'un site survey pour l'implantation de vos AP.
4. Utiliser des canaux différents pour optimiser les ondes radio, si possible en maillage.
5. La meilleure façon de sécuriser est de mettre votre réseau WIFI dans un VLAN sécurisé avec une authentification 801.X au travers un serveur radius pointant sur un annuaire LDAP.