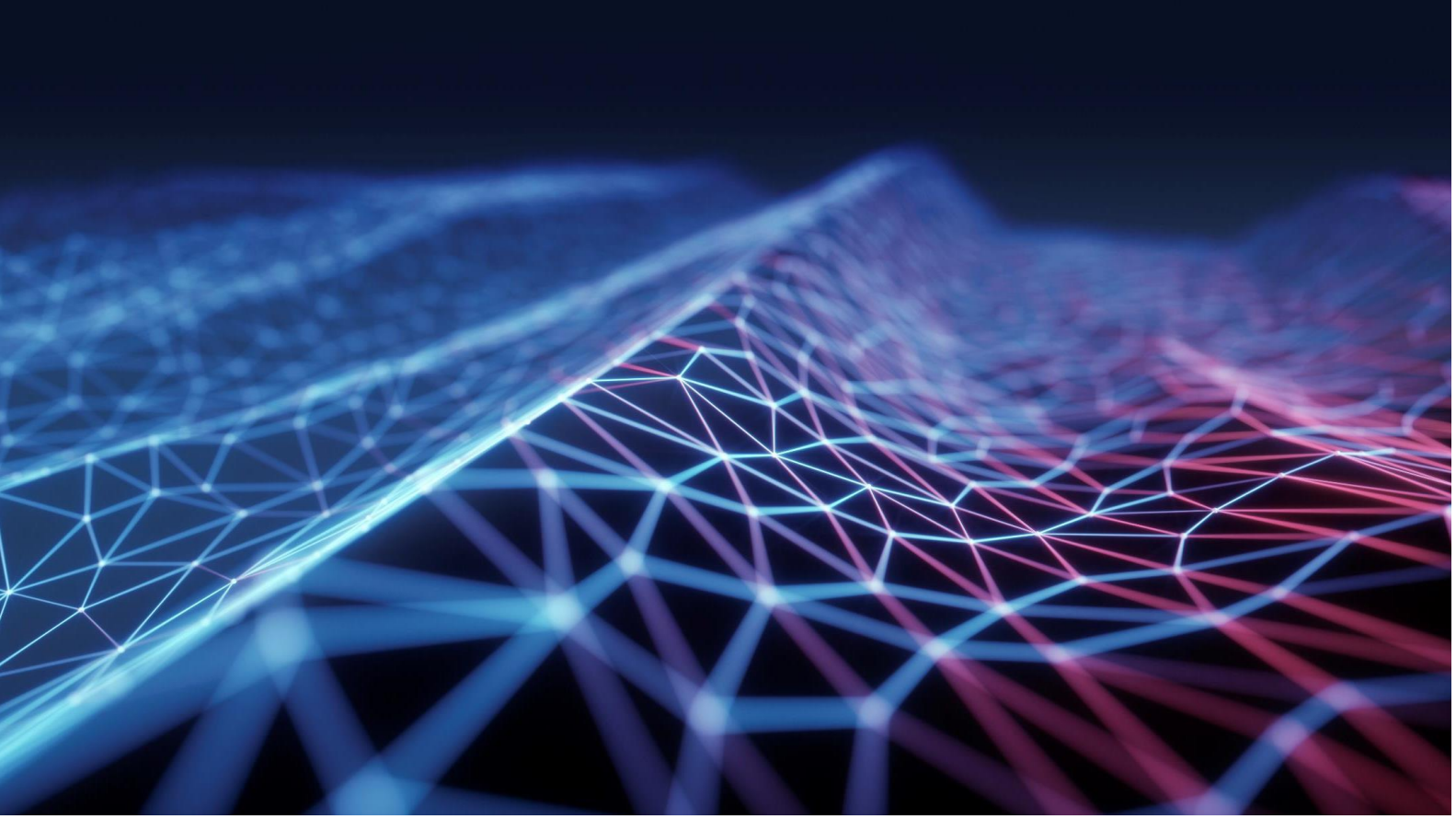


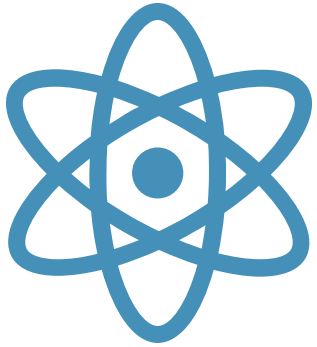
LE WI-FI
CONCEPTS ET SÉCURITÉ

UN TUTO POUR LES BRISER TOUS

UTILITÉ DE CE SOIR

- Le Wi-Fi regroupe des technlogies et concepts utilisés partout
- Comprendre le Wi-Fi
- Observer des trames 802.11
- Observer et exploiter les failles de certains protocoles
- Observer les dangers d'un CA non protégé
- Introduction aux outils comme Aircrack-ng, WireShark, OpenSSL et Scapy

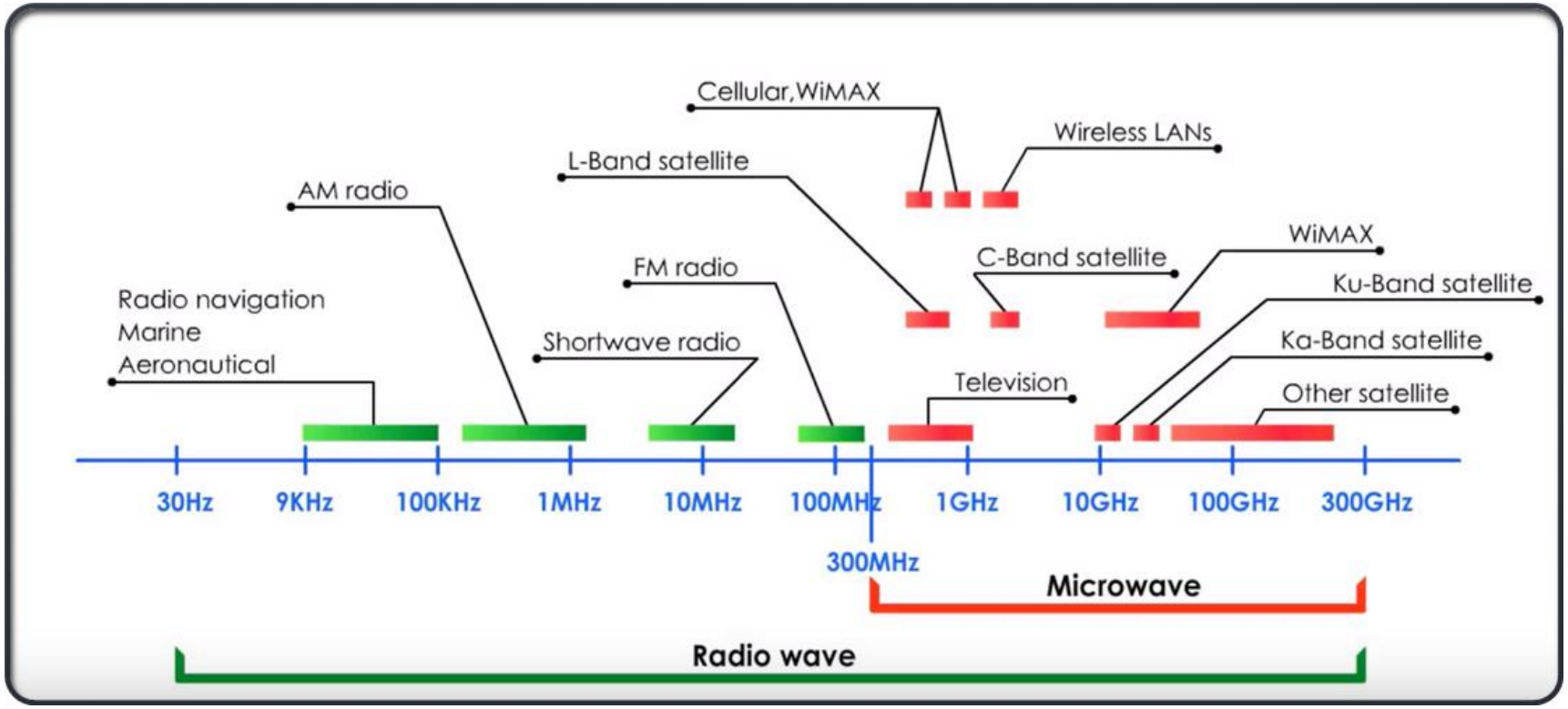
ORGANISME DE STANDARDIATION ET DE CERTIFICATION



Institute of Electrical and Electronics Engineers : (IEEE)

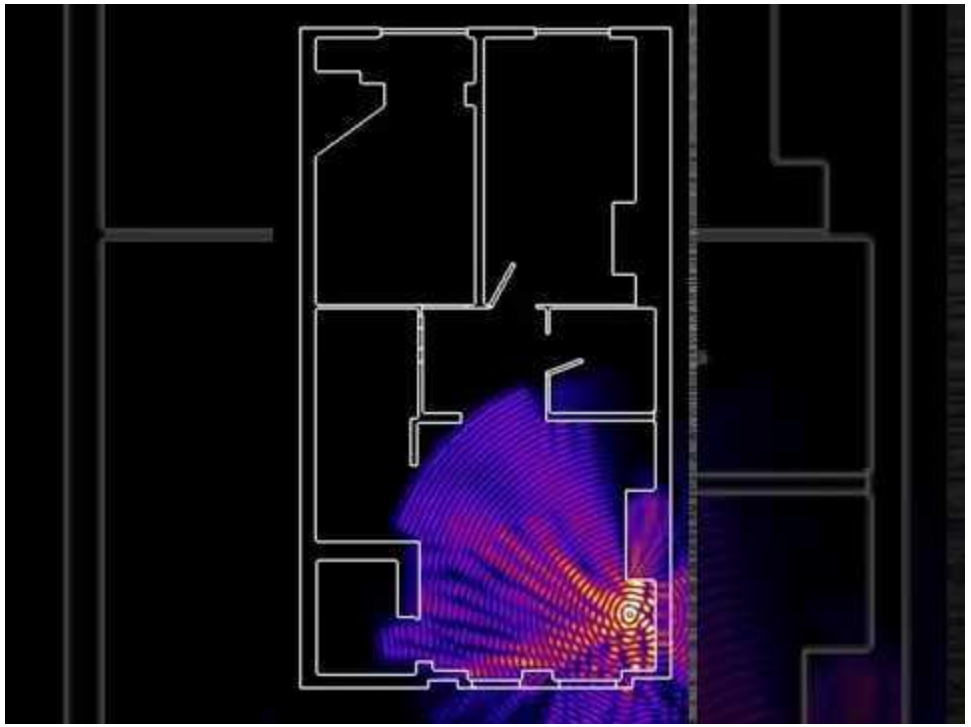
Wi-Fi Alliance

PRÉSENTATION DU SPECTRE DES FRÉQUENCES



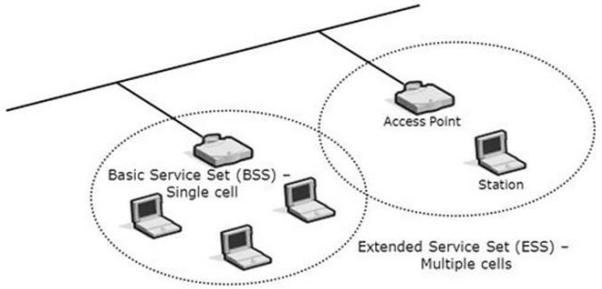
LES VERSIONS DU WI-FI

	Débit Théorique	Débit atteint	Année
802.11 - Wi-Fi 1	11 Mb/s	5-7 Mb/s	1997
802.11a/b - Wi-Fi 2	1.5 - 54 Mb/s	20 Mb/s	1999
802.11g - Wi-Fi 3	54 Mb/s	31 Mb/s	2003
802.11n - Wi-Fi 4	54 - 600 Mb/s	150 – 200 Mb/s	2009
802.11ac - Wi-Fi 5	3.5 Gb/s	1.3 Gb/s	2013
802.11ax - Wi-Fi 6	10.53 Gb/s	6 Gb/s	2019



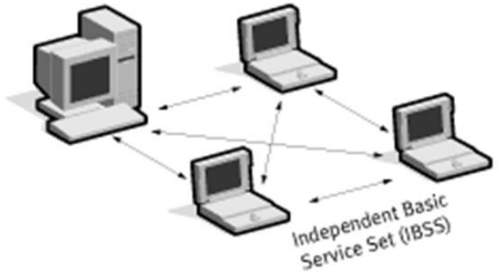
TOPOLOGIES

- SSID: nom du Wi-Fi
- BSSID: adresse MAC du point d'accès
- ESSID.. Et autre petit trucs



BSS : Basic Service Set
ESS : Extended Service Set

- Point d'accès



IBSS : Independant Basic Service Set

- Sans point d'accès
- Fonctionne pour une salle donnée
- Client ⇔ Point d'accès
- Connu sous le nom de "ad-hoc"

LA CARTE WIFI

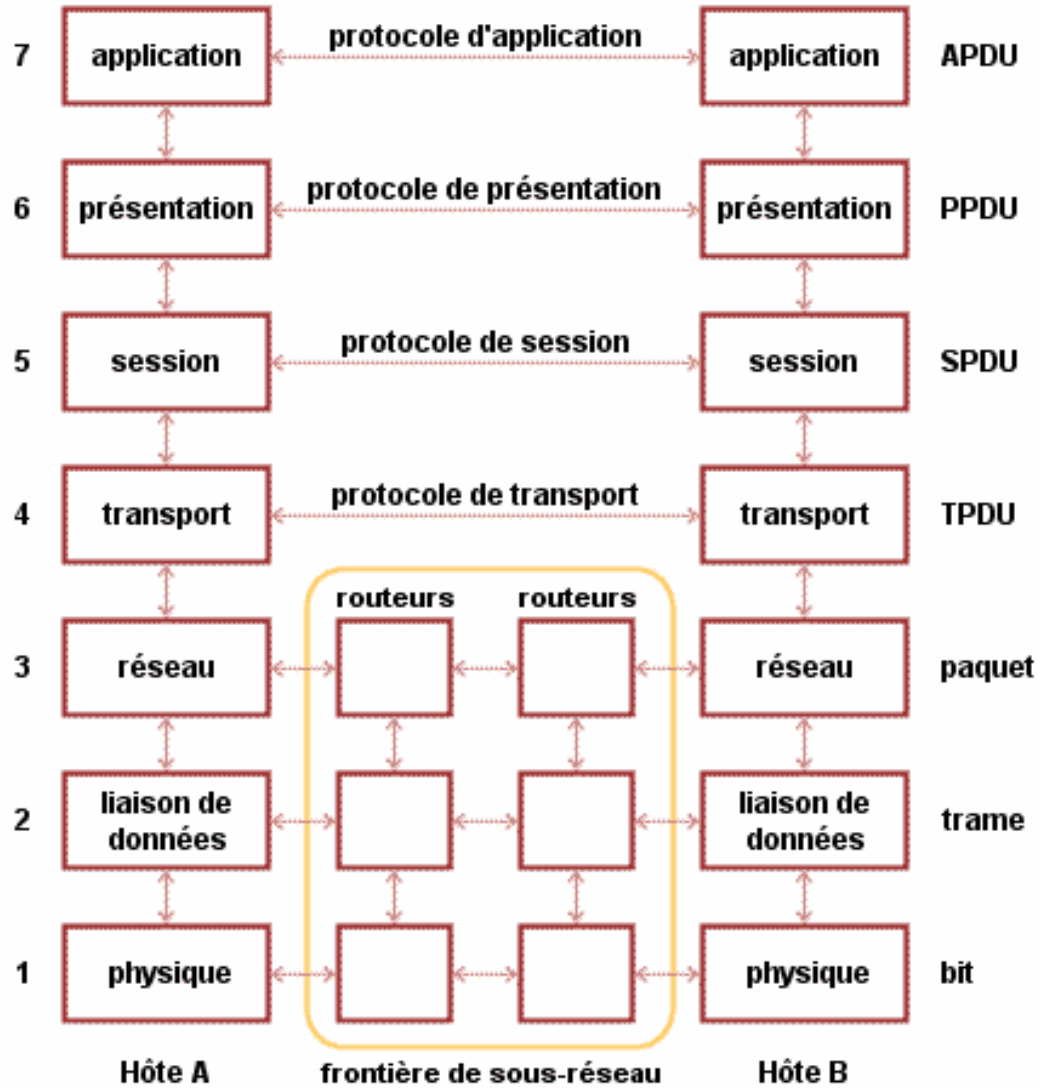
- Différents modes:
  - Station
  - Monitoring

- Outils:
  - Ifconfig
  - Iwconfig
  - ip

EXO AD HOC

- Utiliser ifconfig et iwconfig pour créer ou se connecter à un réseau ad-hoc
- Trouver vos adresses IP/MAC et les passer a votre groupe
- Utiliser les scripts server.py et client.py pour échanger des informations sur votre réseau

LE MODÈLE OSI


7
application
protocole d'application
application
APDU
6
présentation
protocole de présentation
présentation
PPDU
5
session
protocole de session
session
SPDU
4
transport
protocole de transport
transport
TPDU
routeurs
routeurs
3
réseau
réseau
paquet
2
liaison de données
liaison de données
trame
1
physique
physique
bit
Hôte A
frontière de sous-réseau
Hôte B

NORME IEEE 802.11

OSI Layer 2 ***Data Link Layer***	802.11 Logical Link Control (LLC)					
	802.11 Medium Access Control (MAC)					
OSI Layer 1 ***Physical Layer (PHY)***	FHSS	DSSS	IR	Wi-Fi 802.11b	Wi-Fi 802.11g	Wi-Fi5 802.11a

802.11 : LA COUCHE L1

Contraintes

Modulations des porteuses

FHSS
DSSS
OFDM

Modulations des signaux

Modulations "classiques"
Modulations QAM

UN MILIEU À FORTES CONTRAINTES

Effets d'atténuation

Distance

Pénétration

Interférences

Avec soit même

Avec les autres

MODULATIONS DES PORTEUSES

FHSS : Une bande de départ fixée

DSSS : Répartition sur une large plage

OFDM: Superposition des plages de fréquences

AVANTAGES

FHSS

- Très résistant aux interférences
- Difficulté d'espionnage

DSSS

- Résilient aux perturbations
- Sécurité supplémentaire dû à la redondance

OFDM

- Haute efficacité spectrale
- Robuste aux interférences
- Peu de sensibilité aux problèmes d'horloge

INCONVÉNIENTS

FHSS

- Mauvais usage de la bande passante
- Mauvais usage de l'énergie

DSSS

- Forte redondance
- Pas d'optimisation de la bande passante
- Peu de multiples sources

OFDM

- Effet doppler
- Sensible aux problèmes de synchronisation de fréquence
- Peu d'optimisation énergétique

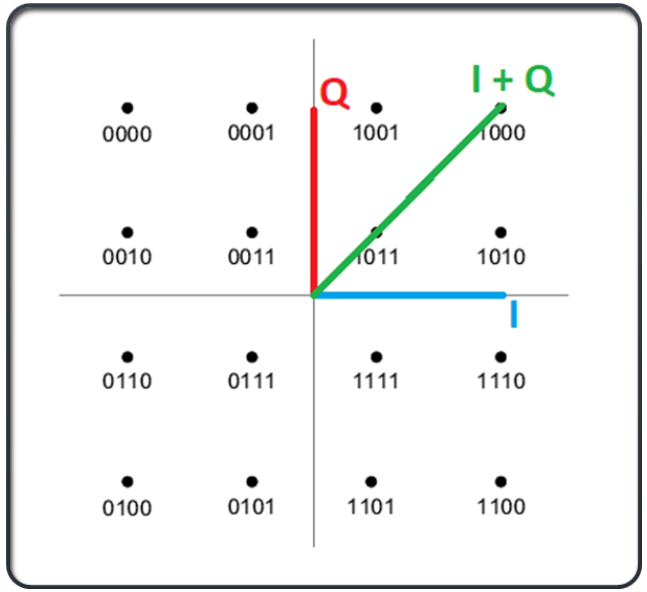
MODULATIONS DES SIGNAUX

Théorème de Shannon

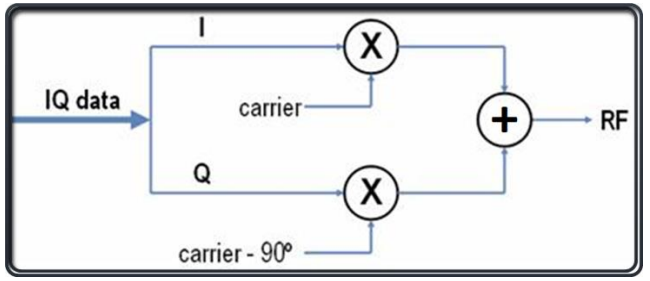
Fréquence de mesure

Contraintes du milieu

MODULATION 16-QAM

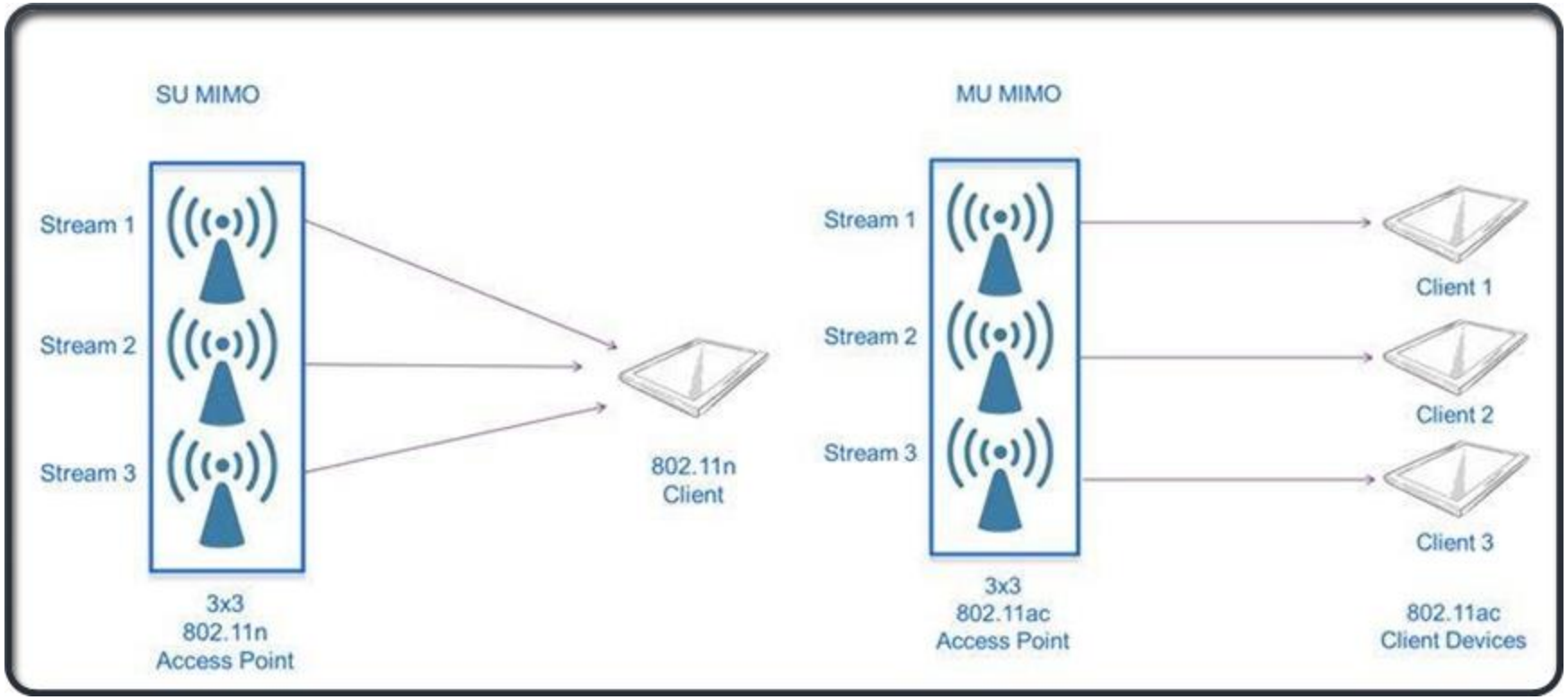


Représentation graphique



Implémentation physique

MIMO


SU MIMO
Stream 1
Stream 2
Stream 3
3x3
802.11n
Access Point
802.11n
Client
MU MIMO
Stream 1
Stream 2
Stream 3
3x3
802.11ac
Access Point
Client 1
Client 2
Client 3
802.11ac
Client Devices

NORME IEEE 802.11

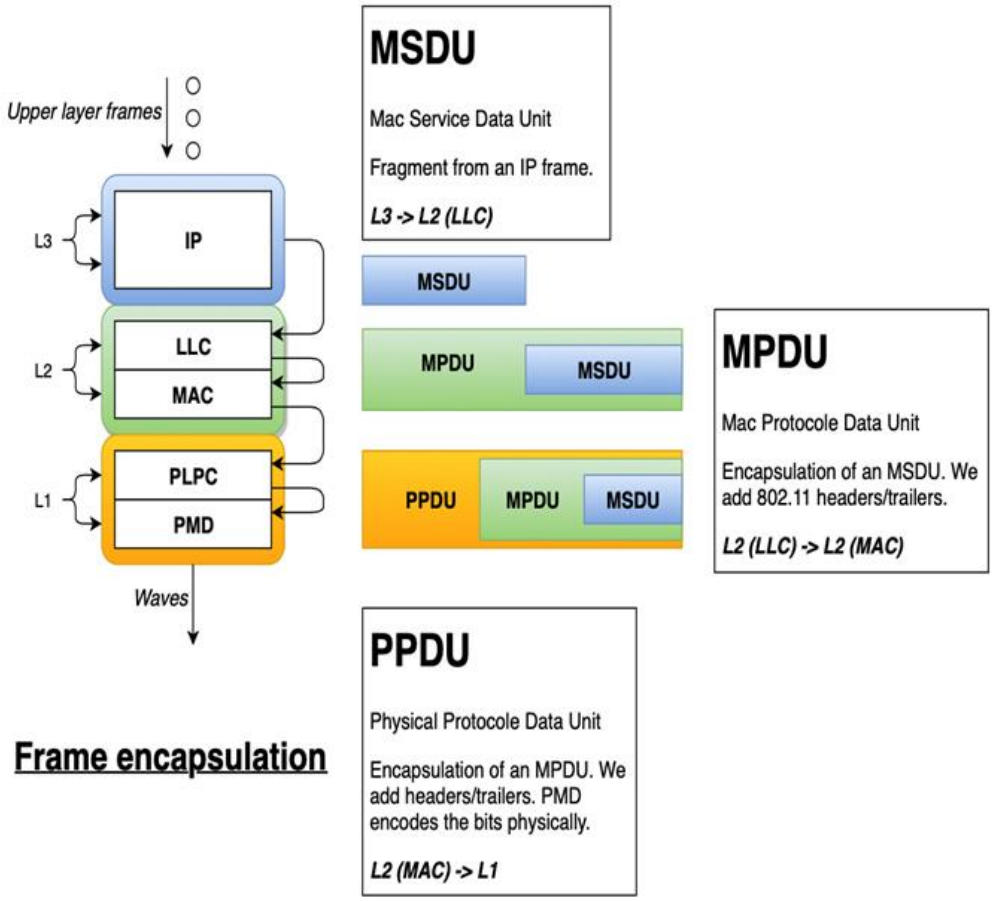
OSI Layer 2 ***Data Link Layer***	802.11 Logical Link Control (LLC)					
	802.11 Medium Access Control (MAC)					
OSI Layer 1 ***Physical Layer (PHY)***	FHSS	DSSS	IR	Wi-Fi 802.11b	Wi-Fi 802.11g	Wi-Fi5 802.11a

FONCTIONNALITÉ MAC

- Fragmentation:
  - Dans le cas où une MSDU est trop grosse, celle-ci sera fragmenté en plusieurs MPDU

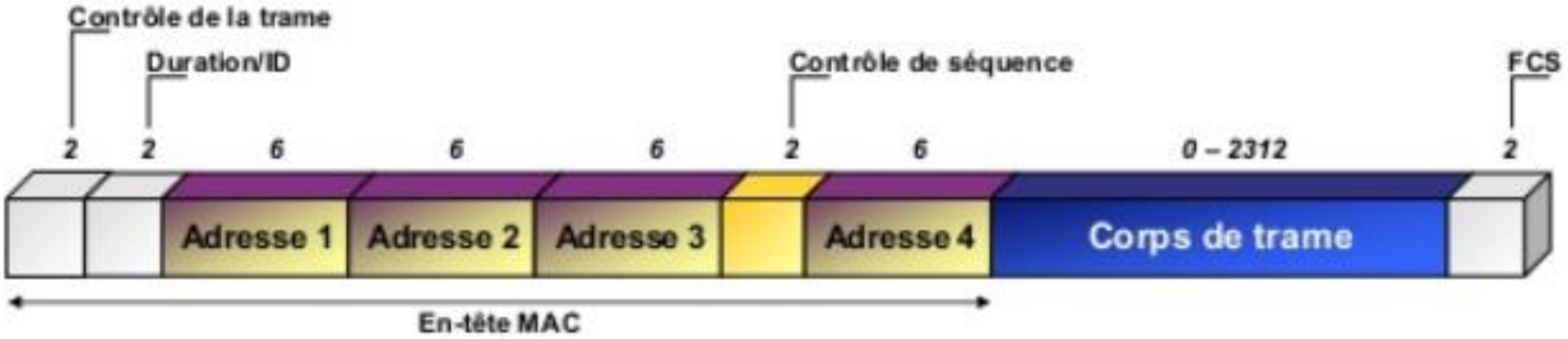
- Aggrégation
  - Afin d'optimiser le débit sur les réseaux, on peut aggréger plusieurs MSDU dans une MPDU et plusieurs MPDU dans une PPDU.
  - Cela limite l'overhead en réduisant le nombre de header et trailer 802.11 transmis.

- Encapsulation:
  - Voir schema à coté



3 TYPES DE DE TRAMES MAC DIFFÉRENTES

Trames de données	Trames de contrôle	Trames de gestion
• Transmission de données	• Contrôle de l'accès au support	• Association,réassociation, synchronisation, authentification



TRAMES MAC

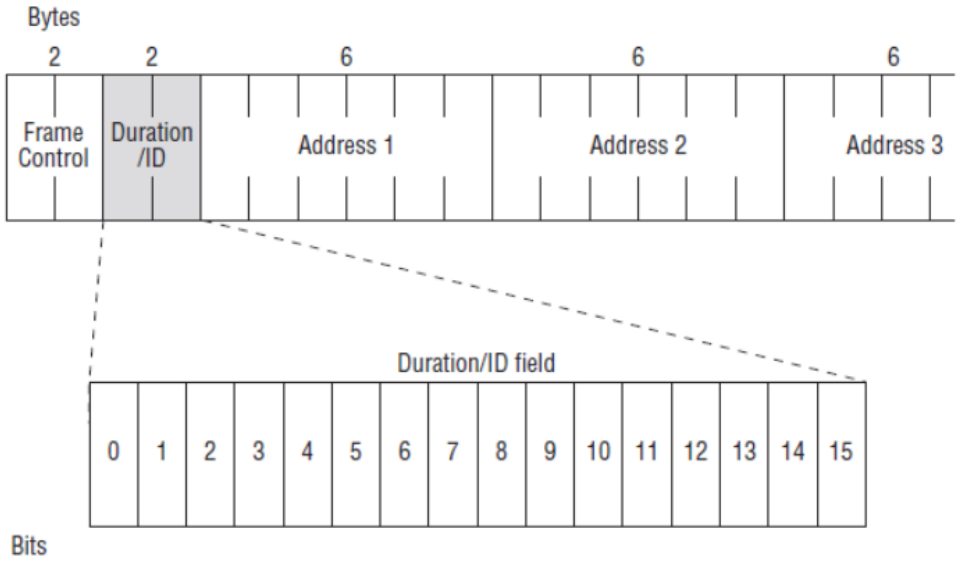
❖ Contrôle de trame

- Version de protocole: fixé à 0
- Type et sous-type : 3 types de trames, plusieurs sous-types
- To DS et FromDS : trame envoyée vers le ou provient du destinataire
- More fragments =1 si trame fragmentée et ce n'est pas le dernier fragment=0 si trame non fragmentée ou dernier fragment
- Retry=1 si retransmission
- Power management : mode économie d'énergie (=1) ou actif (=0)
- More data : trames présentes en mémoire tampon
- WEP : trame chiffrée ou non (trame donnée ou gestion/authentification)
- Order: classe de service strictement ordonnée (Strictly Ordered Service Class)

TRAMES MAC

❖ Duration/ID

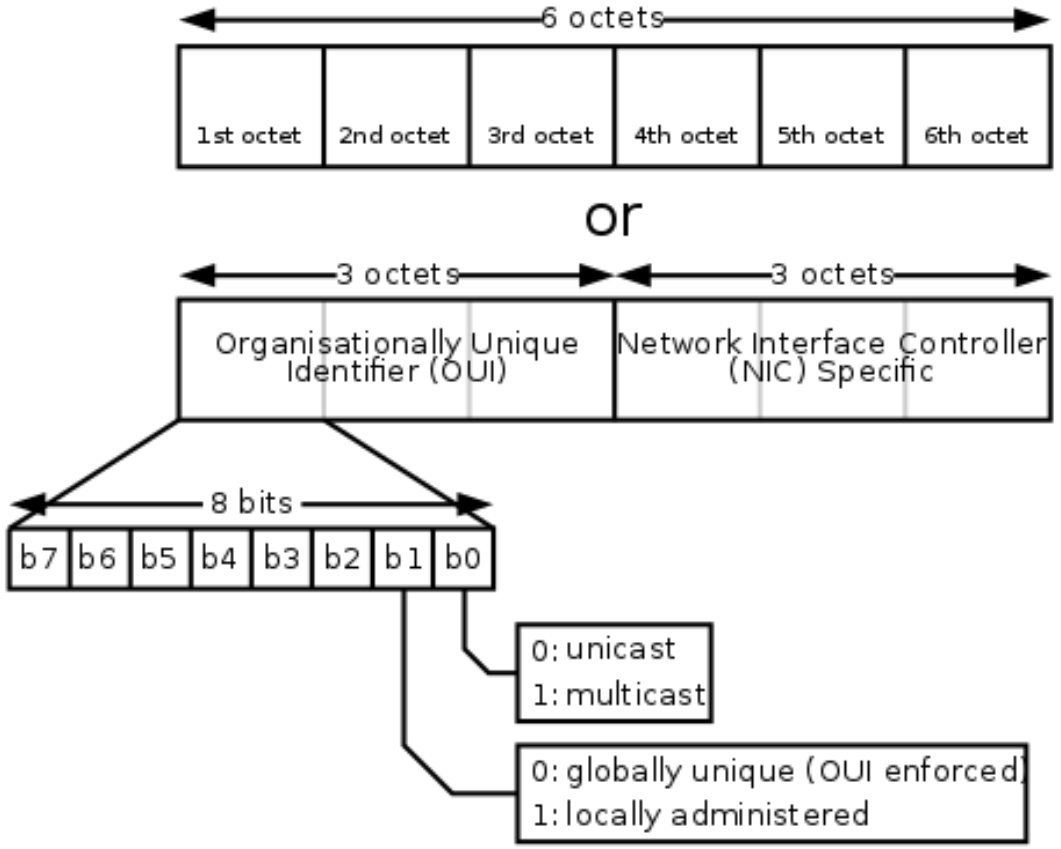
- Utiliser pour reset le timer NAV des stations
- NAV : Network allocation vector
  Il est une durée pendant laquelle une
  station ne doit pas accéder au medium de communication



TRAMES MAC

❖ Adresse

- Même format que les addresses IEEE 802 MAC



- 1er bit : adresse individuelle ou de groupe
- 2ème bit : adresse locale ou universelle
- 22 bits : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur
- 24 bits : adresse unique (défini par le constructeur)

TRAMES MAC

❖ Contrôle de séquence

- Numéro de séquence (12 bits)
  - Attribué à chaque trame
  - Initialisé à 0 puis incrémenté pour chaque nouvelle trame
- Numéro de fragment (4 bits)
  - Initialisé à 0 puis incrémenté pour chaque nouveau fragment

TRAMES MAC

❖ Corps de la trame

- Taille minimale : 0 octets (trame de gestion ou de contrôle)
- Taille maximale : 1500 octets (taille plus importante si elle est chiffrée par WEP)

❖ FCS (Frame Check Sequence)

- CRC (Cyclic Redundancy Check) sur 32 bits pour contrôler l'intéggrité des trames

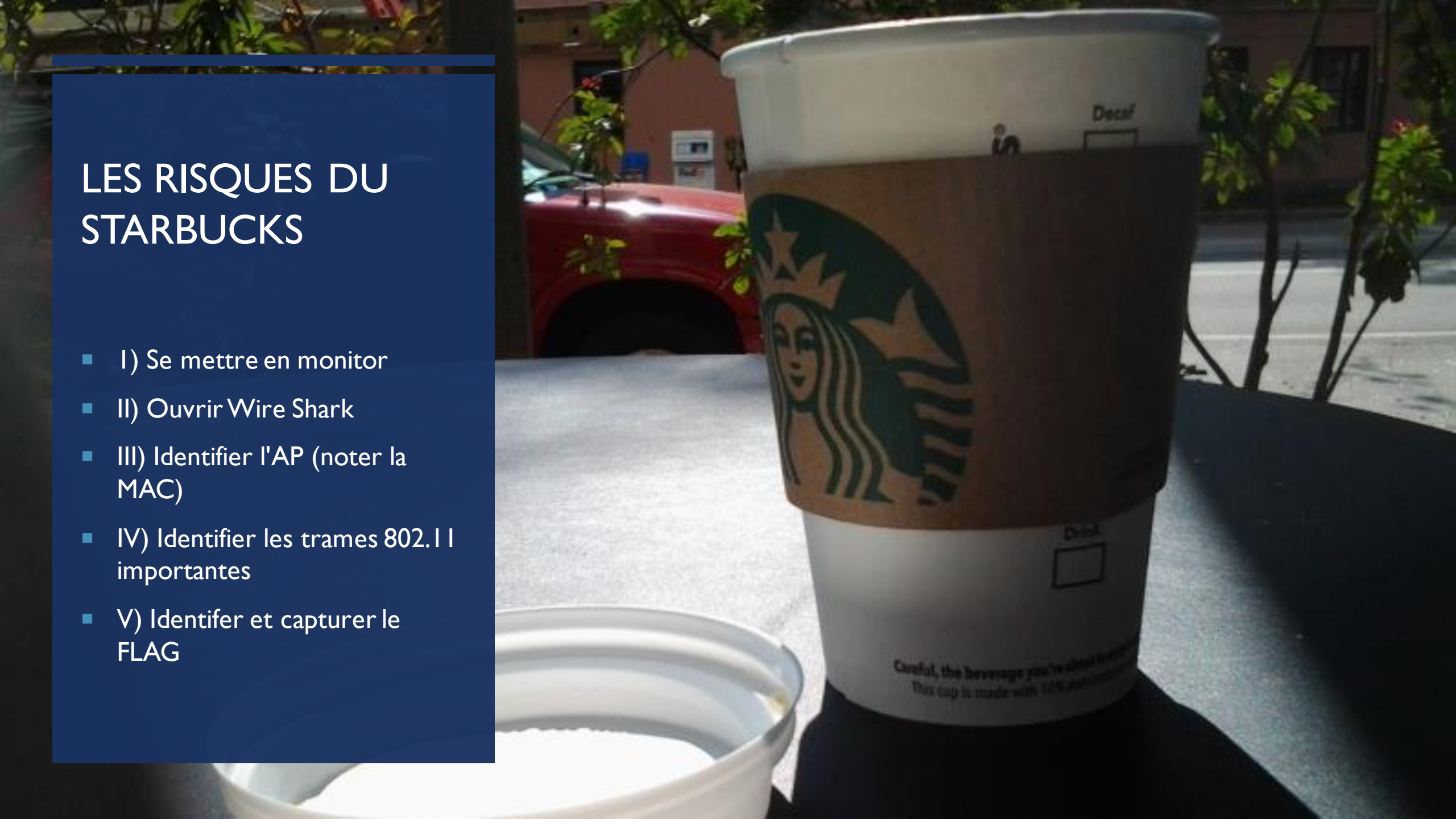
NORME IEEE 802.11 : TRAMES IMPORTANTES

- Beacons : Scanneur passif
  - Utilisé par les routeurs pour broadcast leurs informations : envoyé toutes les 102,4 ms
- Probes : Scanneur actif
  - Le client scan les canaux 1 par 1 transmettant à chaque fois en broadcast et attend un moment pour une réponse
  - Si il n'y a pas de réponse, on passe au canal suivant

- Authentification :
  - Vérifie la compatibilité entre le client et le point d'accès
- Association :
  - Génère un ID pour l'utilisateur et autorise l'accès au réseau

LES RISQUES DU STARBUCKS

- I) Se mettre en monitor
- II) Ouvrir Wire Shark
- III) Identifier l'AP (noter la MAC)
- IV) Identifier les trames 802.11 importantes
- V) Identifer et capturer le FLAG



TIME TO BECOME…A HACKERMAN!


HACKERMAN

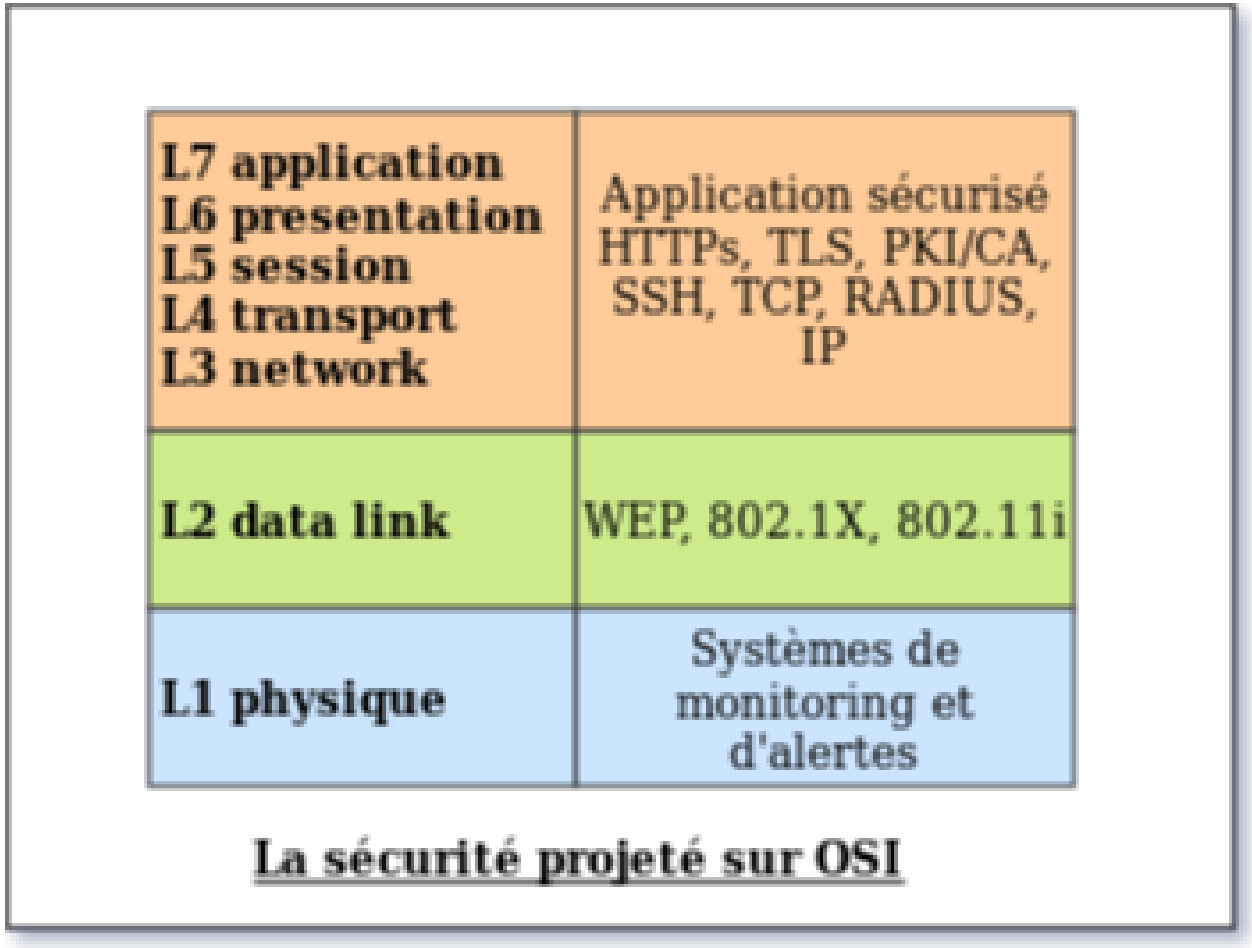
SÉCURITÉ

La sécurité est un des grands enjeux du développement des réseaux sans fil.

Ou se situe la sécurité dans le Wi-Fi?

Comment s'assurer que chacun dispose d'une clé de chiffrement?

Comment distribuer les clés de chiffrement?



La sécurité projeté sur OSI

SÉCURITÉ - VOCABULAIRE

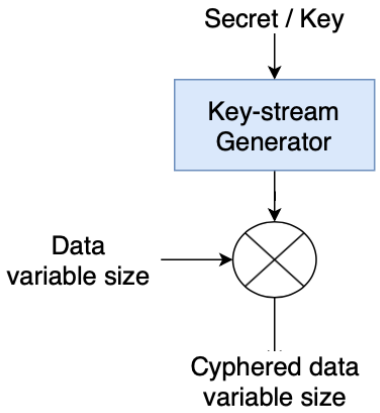
Initialization Vector **(IV)** - nonce

- Ajoute de l'aléatoire dans un process
- Utilisé dans un but précis (e.g: séquencage, génération de clés)

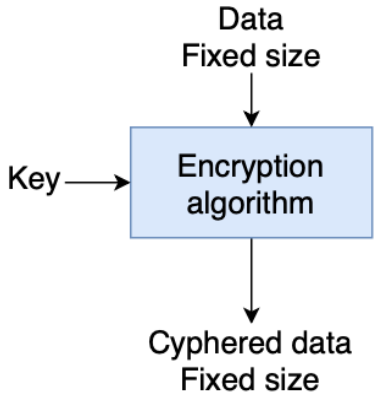
Clés:

- Générée à partir d'informations pré-définies
- Peut être dérivée pour faire une autre clés
- Durée de vie déterminée

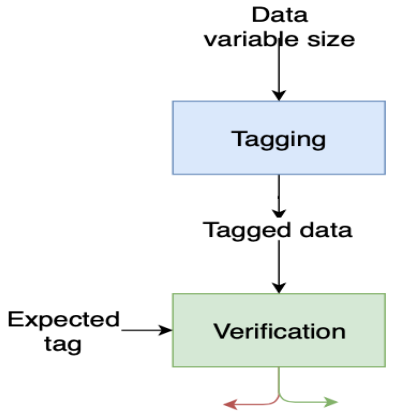
Chiffrement par flux



Chiffrement par blocs



Integrité



SÉCURITÉ - WEP

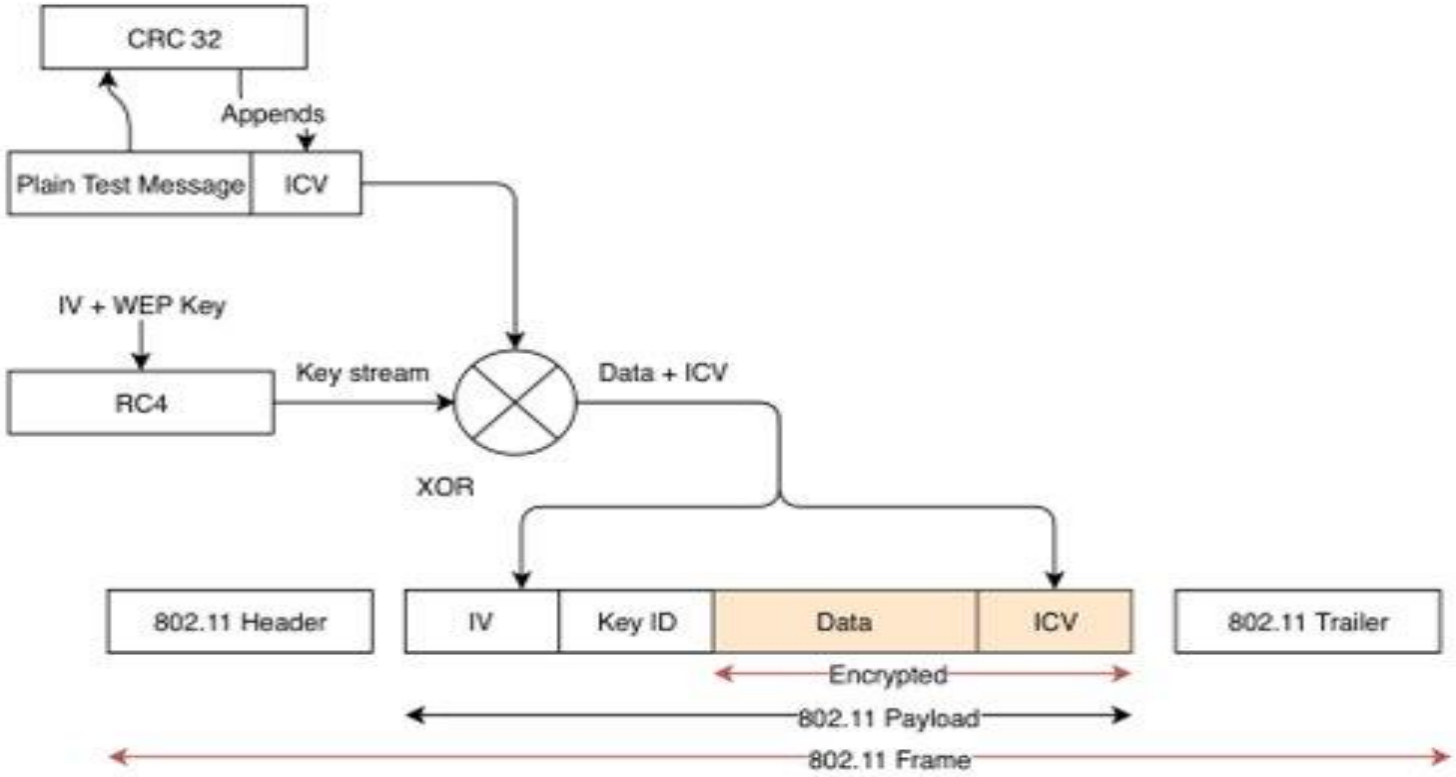
Premier standard de sécurité

Clé statique de 40 ou 104 bits
IV dynamic de 24 bits

Nombreuses **failles** de conception et d'implémentation

Valeure d'intégrité sur 32 bits (**ICV**)

Très rapide, conçu pour du vieu matériel



SÉCURITÉ - WEP FAILLES

Chiffrement:

- RC4 est faible
- **Clés faibles**:
  - Unique pour tout le réseau
  - IV: petit (17 millions de paquet force un cycle du keystream)
  - Fort lien entre l'IV et le mot de passe

Integrité:

- CRC est linéaire: CRC(A + B) = CRC(A) + CRC(B)

Gestion de trame:

- Aucune
- Replay attack

ET SI ON CASSAIT DU WEP?

TP: LA "CONFIDENTIALITÉ" DE WEP:

Outils utiles: airmon-ng, airodump-ng, aircrack-ng, Wire Shark

- Monitorer et trouver les trames chiffrées
- Obtention de la clé WEP
  - Capturer des fluxs passant par le point d'accès
  - Faire tourner aircrack pour casser la clé quand vous avez capturé 20 à 25k IV
- Déchiffrement de flux en temps réel
  - Ouvrir le script decypher_wep.py
  - Coder votre propre fonction de filtrage avec les classes Scapy pour obtenir les paquets de données circulant sur le réseau
  - Appliquer les fonctions du script rc4.py pour déchiffrer les trames en temps réel

SÉCURITÉ - 802.111

Déprecie WEP

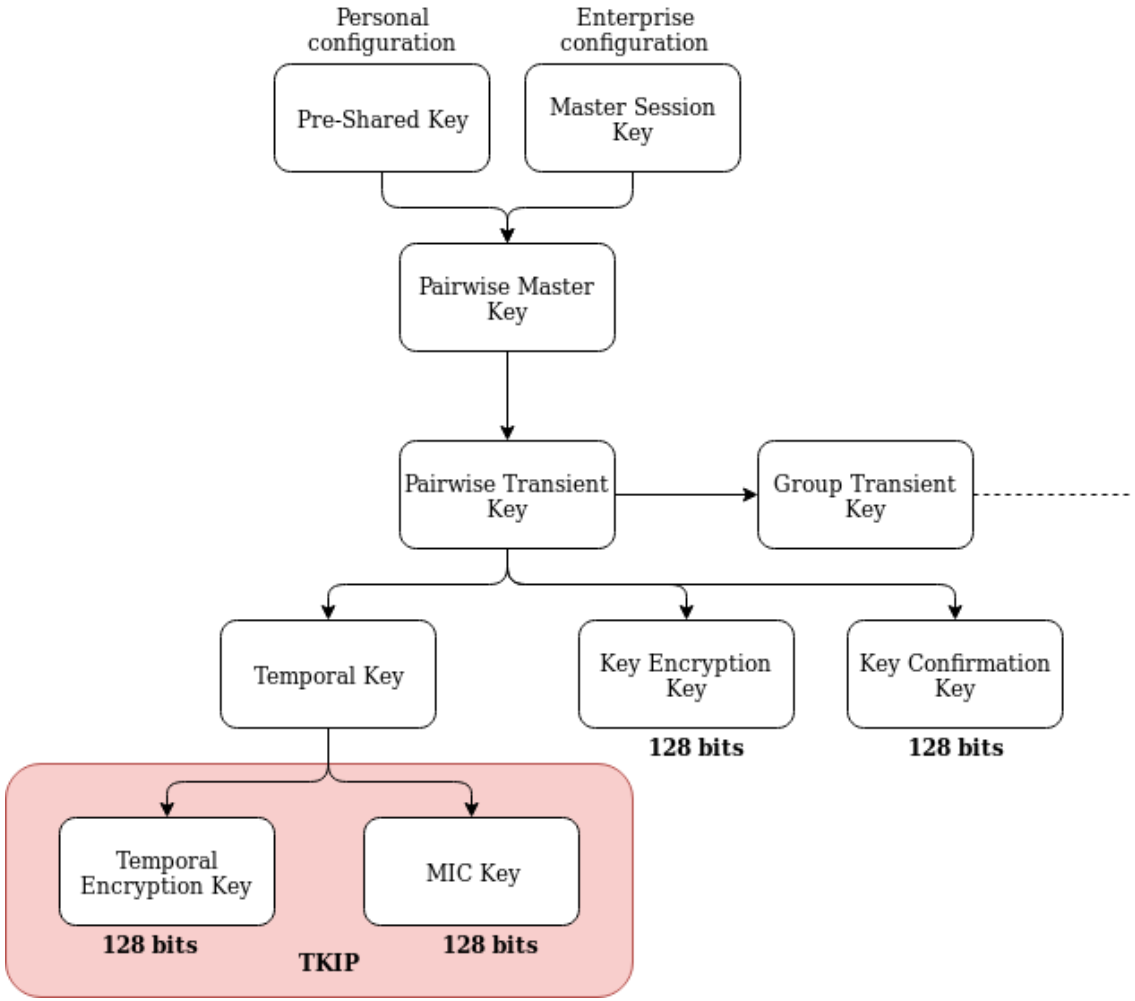
Introduit 2 certifications:

- WPA - TKIP:
  Wrapper autour de WEP
  Utilise RC4 pour le chiffrement, gère mieux les clés et construit des clés plus solides
  Remplace CRC32 par Michael
  Introduit des contre-mesures et une gestion des trames

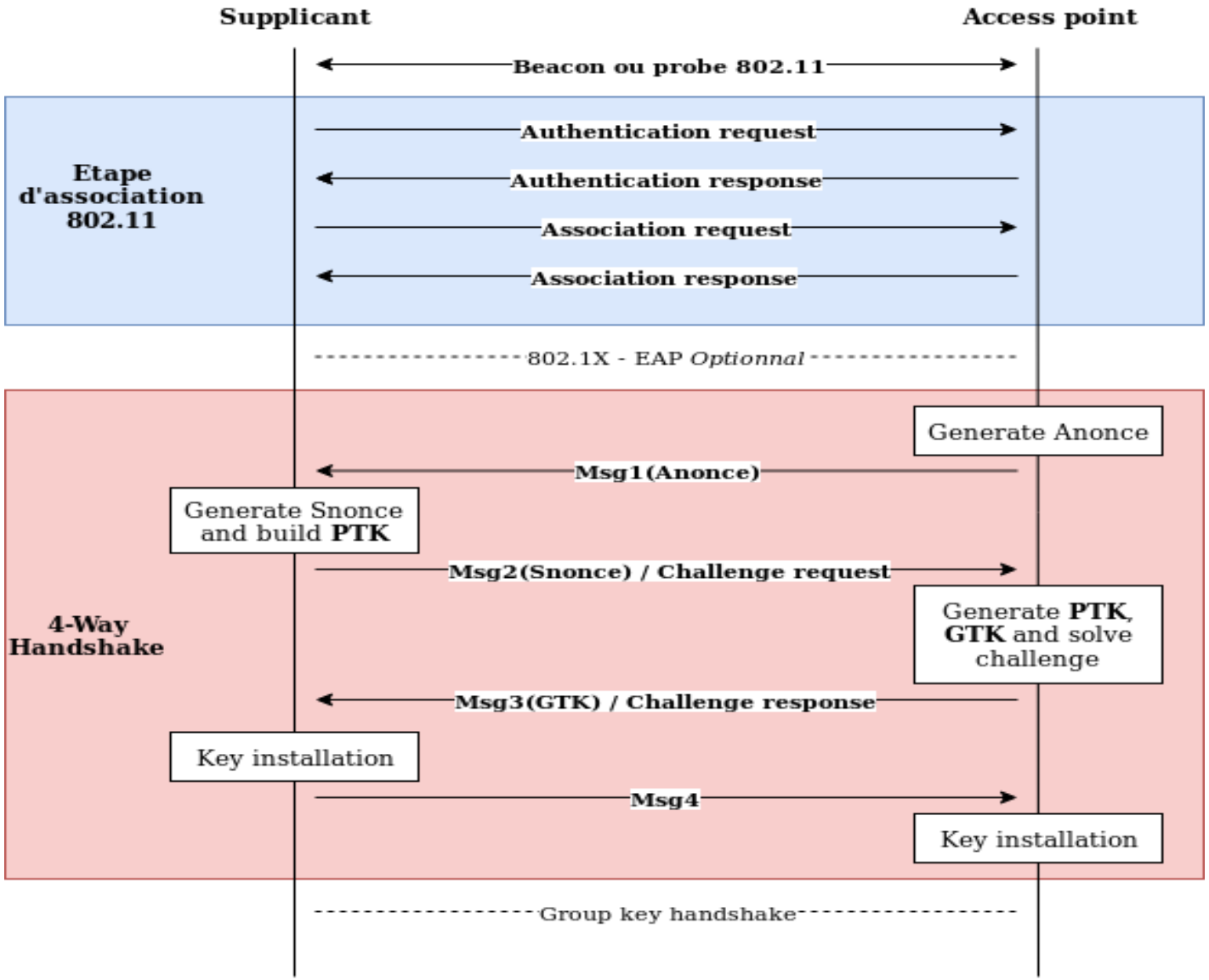
- WPA2 – CCMP:
  Chiffrement et intégrité basé sur AES-CCM
  Conçu pour du nouveau matériel
  A duré 14 ans

Introduit une nouvelle hiearchie de clés

SÉCURITÉ 802.11 CLÉS



SÉCURITÉ 802.111 AUTHENTIFICATION



SÉCURITÉ - WPA TKIP

TKIP Sequence Counter = WEP IV de 48 bits.
TKIP impose un ordre dans la réception des trames.
Les trames sont identifié par le TSC, il est incrémenté de 1 à chaque trame.

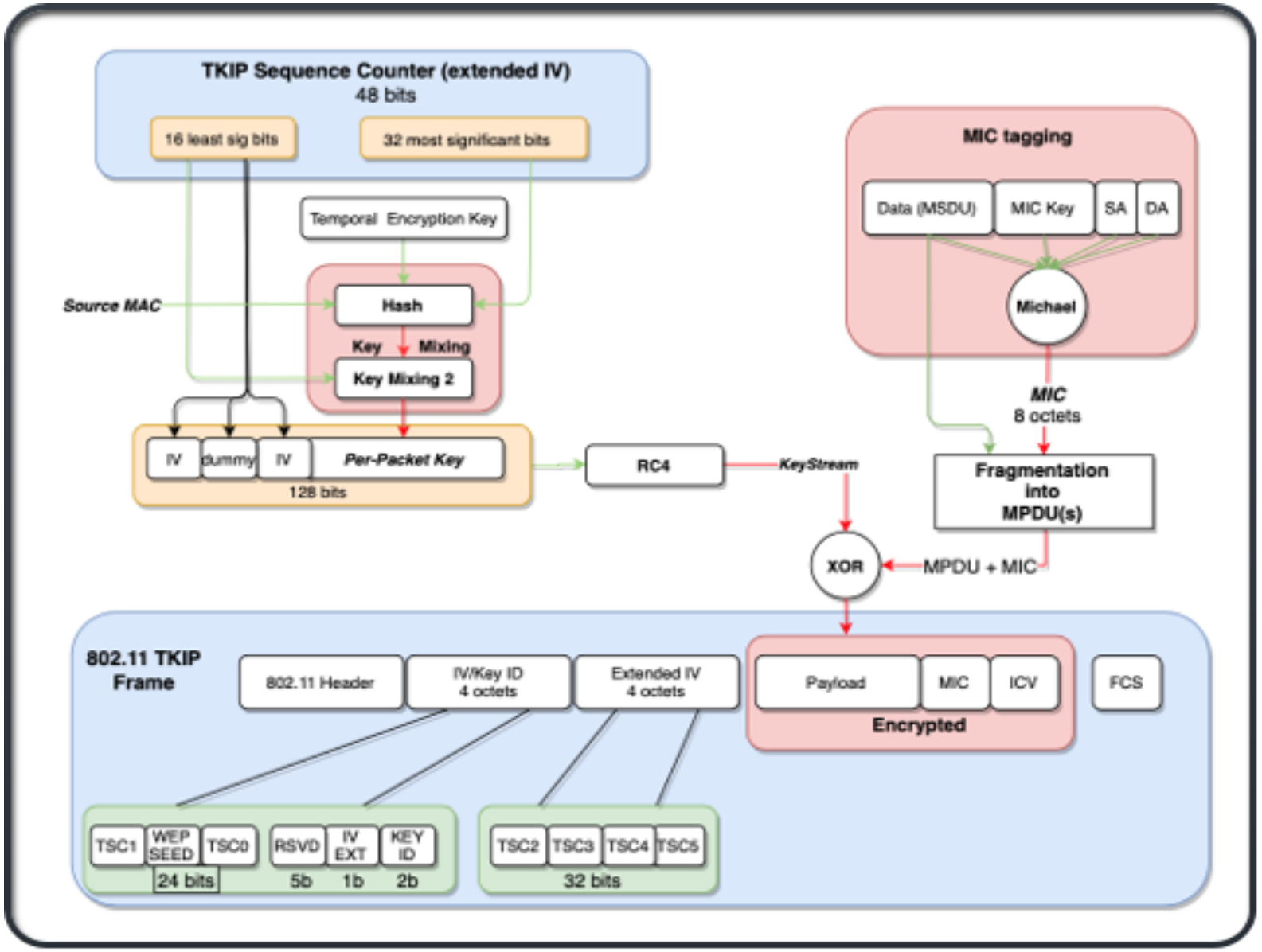
Michael répare le problème de linéarité de CRC32.
Les contre-mesures se bases sur la détection de mauvais Message Integrity Check.

Le chiffrement est plus solide car les clés sont mieux gérés:

- Introduction du key mixing
- La clé de chiffrement est "taillée" pour le poste émetteur et une trame

Vulnérabilités:

- DOS
- Replay attack via les canaux QOS
- KRACK



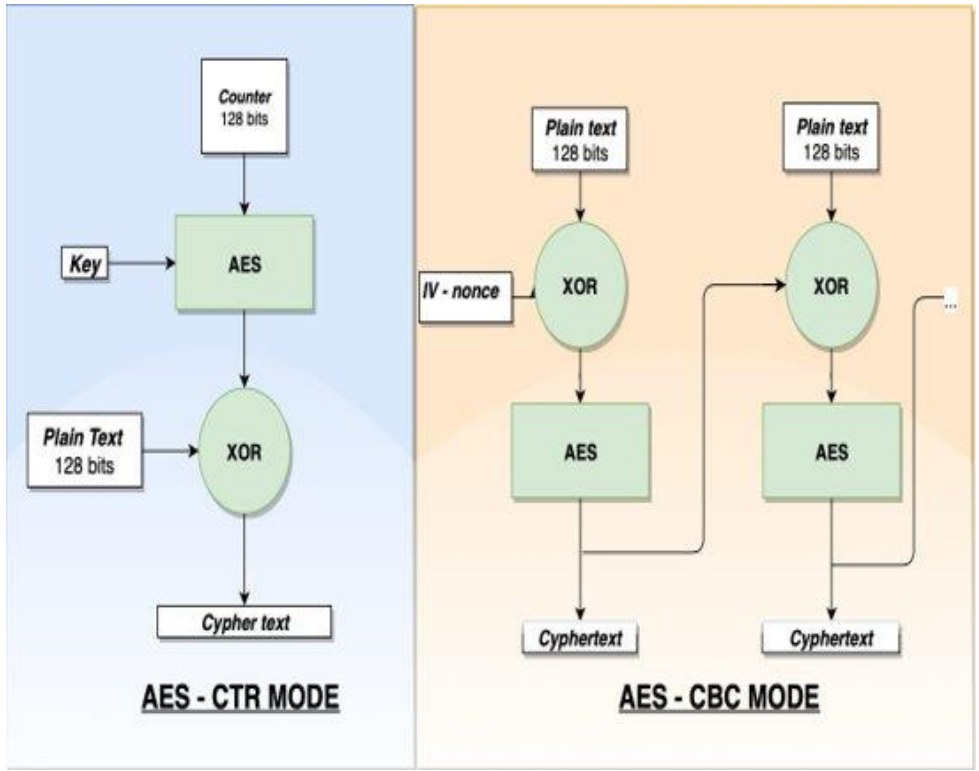
SÉCURITÉ WPA TKIP

TP: KRACK

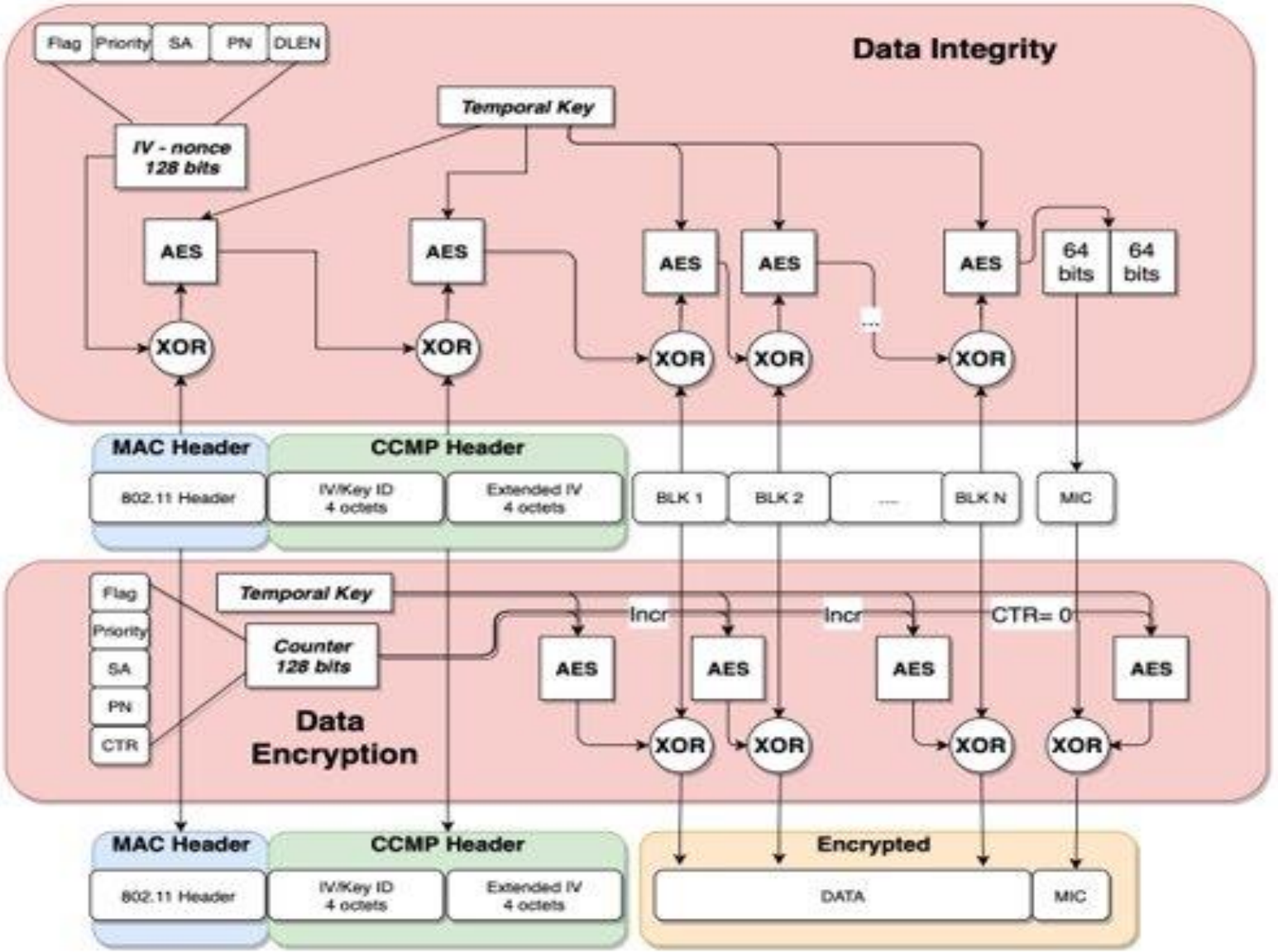
Outils utiles: airmon-ng, airodump-ng, aircrack-ng, aireplay-ng, Wire Shark

- Monitorer et lancer WireShark
- Obtention de la clé WPA
  - Capturer des fluxs passant par le point d'accès
  - Forcer des répétitions du 4-Way Handshake
  - Lancer une attaque par dictionnaire pour casser la clé (utiliser le dictionnaire fournie dans l'archi)

SÉCURITÉ - WPA2 CCMP



- CCMP simplifie l'usage des clés en utilisant qu'une seule clés pour l'encryption et l'intégrité.
- Se base sur l'algorithme de chiffrement symmétrique AES-CCM (composé de 2 modes):
  - AES-CTR: *counter mode* pour le chiffrement des données
  - AES-CBC: *cipher block chaining* pour le calcul d'intégrité
- La clé fait entre 128 et 256 bits selon la qualité du matériel utilisé.
- Vulnérabilités:
- KRACK



SÉCURITÉ WPA2 CCMP

SÉCURITÉ - TLS

Protocole de sécurité de la couche de transport (OSI 5)

Sécurité basé sur les certificats. Il y'a toujours un certificat serveur (qui authentifie le serveur).

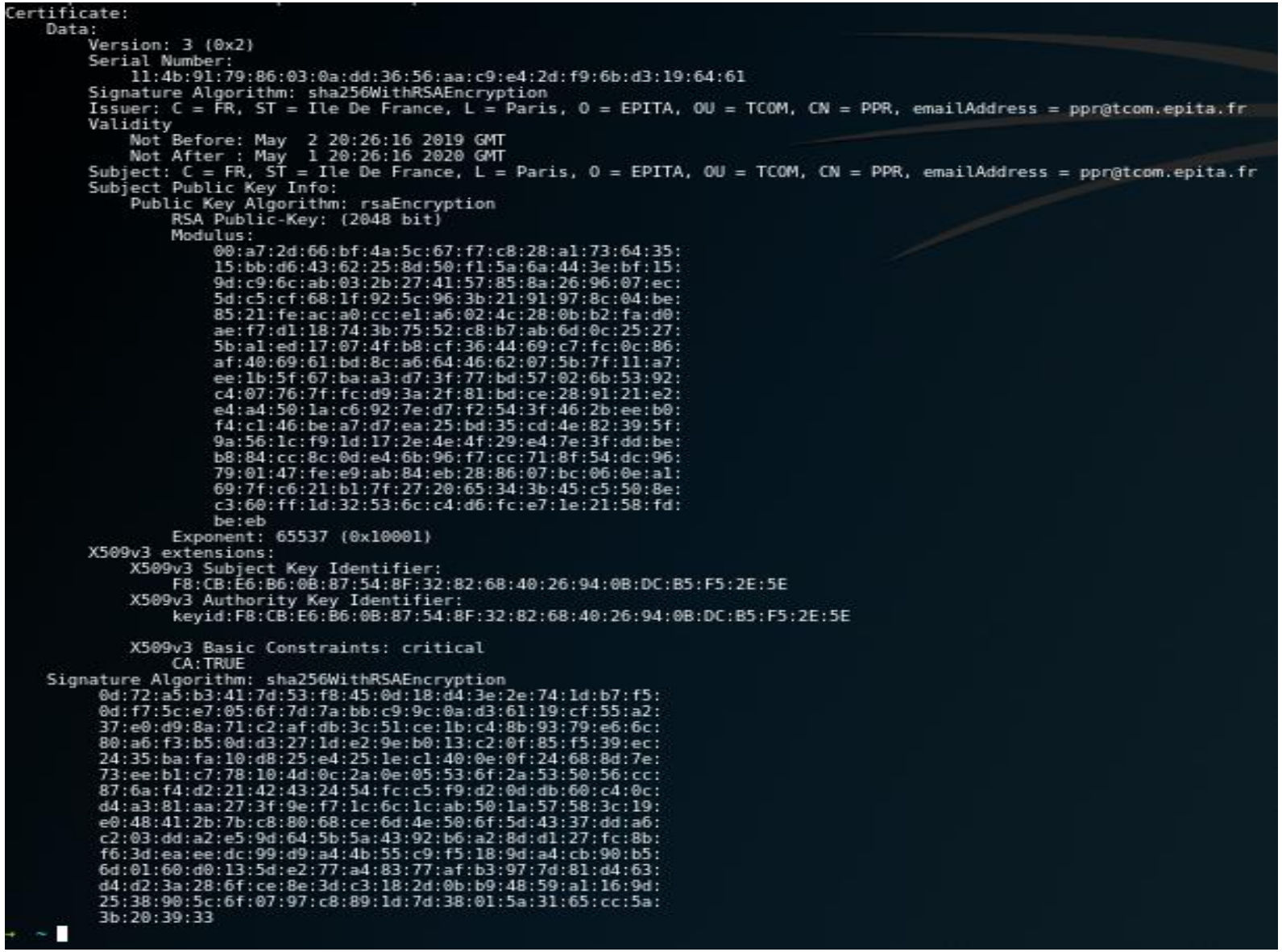
Le client génère une clé de chiffrement symétrique pour chiffrer le flux de données.

Cette clé est chiffré avec la clé publique contenu dans le certificat.

Il peut aussi y'avoir un certificat client dans les architectures qui nécessite l'authentification des utilisateurs.

SÉCURITÉ
PKI - CERTIFICATS

- **Un certificat équivaut à une carte d'identité digitale.**
- **Permet de chiffrer et d'authentifier une personne ou une entreprise.**
- **Utilise de nombreuses méthodes cryptographique.**
- **Un certificat est soit self-signed, soit signé par une root ou intermediate CA**



SÉCURITÉ - PKI CERTIFICAT / CONSTRUCTION

Pour obtenir un certificat on a besoin d'émettre une demande sous la forme d'une Certificate Signing Request.

Une CSR contient les informations de l'utilisateur du certificat, la clé publique et est signé par la clé privé de l'utilisateur.

Lorsque l'on valide le certificat on ajoute les informations de l'issuer.

Dans le cas d'un certificat self-signed:

- **L'issuer est le subject du certificat**
- **Le certificat est signé utilisant la clé privée du certificat**

Autrement:

- **L'issuer est l'authorité de certification intermédiaire ou le root CA.**
- **Le certificat est signé utilsant la clé privée du certificat parent.**

SÉCURITÉ - PKI CERTIFICAT / AUTHENTIFICATION

Lorsque l'on se connecte à un site le serveur nous envoie son certificat.

Pour un site HTTPs, son certificat sera signé par une authorité (intermédiaire ou root).

On vérifie déjà les informations contenu (subject common name, DNS lookup...).

Puis on vérifie l'intégrité du certificat:

- **On dechiffre la signature avec la clé publique du certificat parent**
- **On obtient donc le hash du certificat attendu, il suffit de recalculer localement le hash et comparer**

Si tout passe bien alors le serveur auquel on se connecte est authentifié.

SÉCURITÉ - PKI CERTIFICAT / CHAINE DE CONFIANCE

La chaine de confiance est un processus permettant de valider l'origine d'un certificat.

Un certificat de serveur peut etre signé par un intermediate CA inconnu.

Cependant si ce certificat intermédiaire est signé par un autre CA connu alors on va faire confiance a ce CA intermédiaire.

Ca permet à différentes entreprises d'avoir leur propre CA et chacune d'elles reposent sur des root CA communs à tout le monde.

On rajoute donc de la compléxité au niveau du process mais ça renforce grandement la sécurité. Ca empèche 99% des attaques de type Man In The Middle ou d'usurpation d'identité. Car chaque certifcat est identifié par une authorité supérieur.

Si jamais la clé privé d'une étape de la chaine est compromise alors tout les certificats enfants sont considérés comme compromis.

TP ENTREPRISE