Académie Cisco
Reims
Champagne-Ardenne

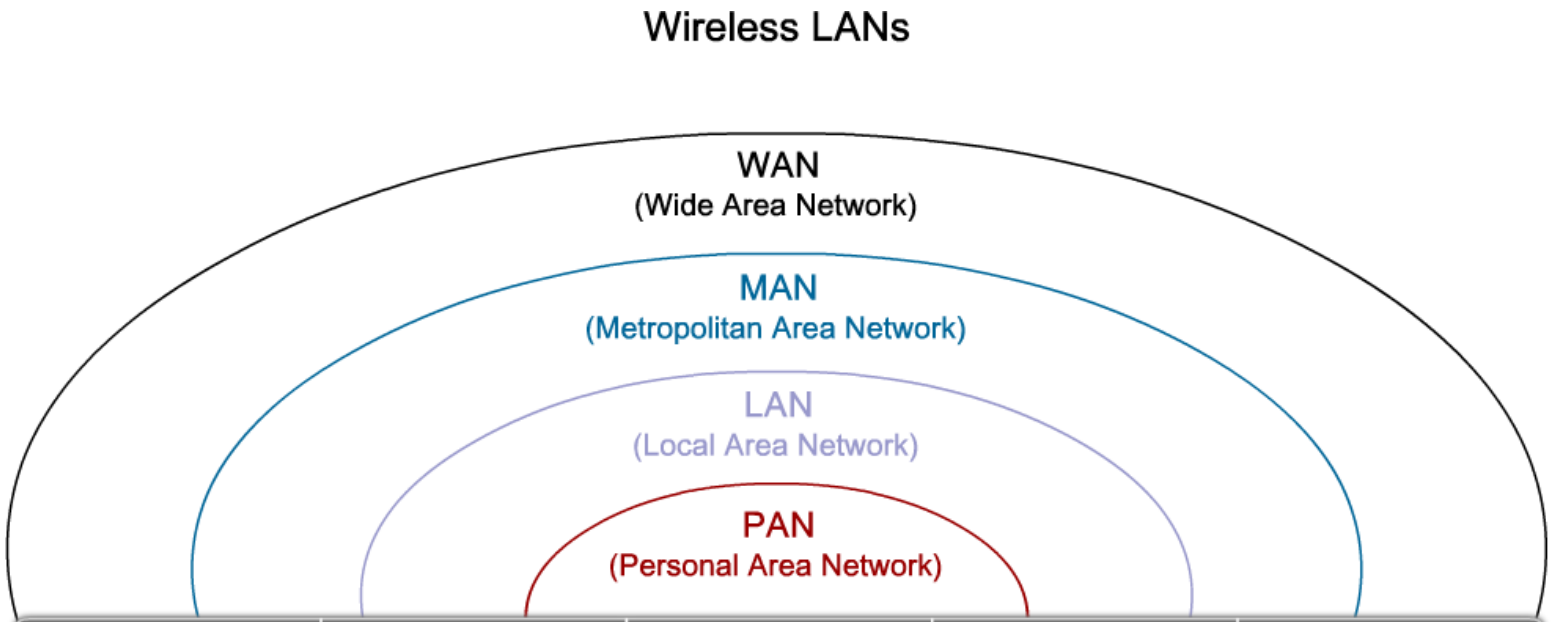
UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

Le Wireless

Le Wireless

Introduction

Les réseaux Wireless ?



	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

Les différentes normes (1)

- 802.11a (ou WiFi 5)
  - Bande de fréquences utilisées : 5 Ghz
  - Débit max. théorique : 54 Mb/s
  - Porté max. théorique : 100 m
- 802.11b (ou WiFi)
  - Bande de fréquences utilisées : 2,4 Ghz
  - Débit max. théorique : 11 Mb/s (débits supportés : 1, 2, 5.5 et 11 Mb/s)
  - Portée max. théorique : 300 m
- 802.11c : Bridge Operations Procedures
- 802.11d : Global Harmonization
  - Adresse les problèmes légaux

Les différentes normes (2)

- 802.11e : MAC Enhancements for QoS
- 802.11f : Inter Access Point Protocol
  - Améliore la qualité de service (QoS) pour les utilisateurs itinérants
- 802.11g : Physical Layer Update
  - Débit max. de 54 Mb/s sur du 802.11b
  - Débits supportés : 54, 48, 36, 24, 18, 12, 9 et 6 Mb/s
- 802.11h : Spectrum Managed 802.11a
  - Dédié aux problèmes légaux européens liés à l'utilisation de la bande des 5 Ghz
- 802.11i : MAC Enhancements for Enhanced Security
  - Amélioration de la sécurité des protocoles utilisés en 802.11b
- 802.11n : Débit annoncé supérieur à 100 Mb/s (voir 600 Mb/s ?)
  - Actuellement version Draft 2

Les normes

	802.11a	802.11b	802.11g		802.11n
Band	5.7 GHz	2.4 GHz	2.4 GHz		Unconfirmed Possibly 2.4 and 5 GHz bands
Channels*	Up to 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Data Rates	Up to 54 Mbps	Up to 11 Mbps	Up to 11 Mbps	Up to 54 Mbps	Speculated to be 248 Mbps for two MIMO streams
Pros	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters		~230 feet or 70 meters
Cons	October 1999	October 1999	June 2003		Expected in 2008
Pros	Fast, less prone to interference	Low cost, good range	Fast, good range, not easily obstructed		Very good data rates, improved range
Cons	Higher cost, shorter range	Slow, prone to interference	Prone to interference from appliances operating on 2.4 GHz band		

- Pour le 802.11n, incompatibilité avec le 802.11b/g, version draft 3.0 en cours et certaines personnes annoncent une finalisation pour 2009 !

Avantages du WiFi

- Norme internationale maintenue par l'IEEE et indépendante d'un constructeur en particulier
- Fonctionnement similaire à Ethernet
  - Évite le développement de nouvelles couches réseaux spécifiques
- Rayon d'action important (jusque 300m, en champ libre)
- Débit acceptable
- Mise en oeuvre facile
  - Pas de travaux, pas de nouveau câblage
  - Pas de déclaration préalable dans la plupart des pays
  - Pas de licence radio à acheter
  - Coût d'une installation faible : environ 30 € pour une carte wifi et 100 € pour une borne.

Quelques inconvénients

- Les plus gros constructeurs proposent des normes propriétaire
  - 802.11b+ (Dlink) ou Turbo (3Com/US Robotics) : Extension à 22Mb/s dans la bande des 2,4Ghz
  - 802.11g Turbo à 100Mbps (annoncé en Mai 2003)
  - 802.11 Pre-n ou 802.11 Draft-n, ...
    - Seront-ils compatibles avec la version finale du 802.11n ?
  - Intégration de nouvelles extensions, incompatibles avec les normes actuelles

WLAN et LAN ?

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

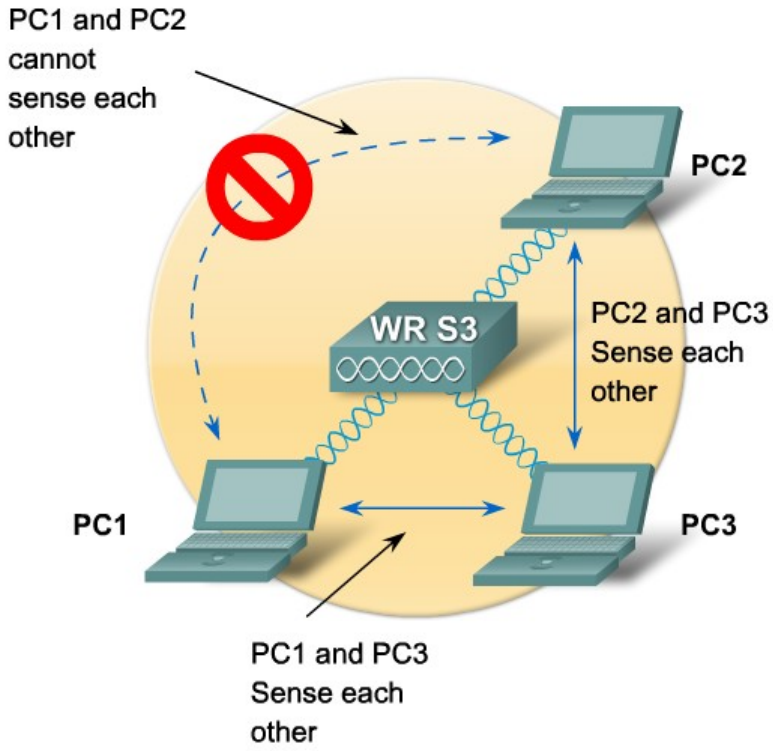
CSMA/CA ?

- Carrier Sense Multiple Access with Collision Avoidance
- Fonction du Request To Send/Clear To Send pour résoudre le problème de la station cachée

The Hidden Node Problem:

- PC1 and PC2 reach WRS3
- PC1 and PC2 cannot reach each other
- PC1 does not detect PC2 activity on the channel
- PC1 sends data while PC2 is transmitting
- A collision occurs

PC3 is sensed by both PC1 and PC2, so there are no collisions involving PC3.



La connexion ?

- En Wifi, 3 étapes
  - La recherche du point d'accès
  - L'authentification
    - En clair
    - Avec clé partagé
  - L'association

Trouver un point d'accès

- En 802.11b, 14 canaux sont disponibles dans la bande des 2.4Ghz, différence de 5 Mhz entre chaque canal
  - Canal 1 : 2,412 Ghz
  - Canal 2 : 2,417 Ghz
  - Canal 3 : 2,422 Ghz
  - Canal 4 : 2,427 Ghz
  - Canal 5 : 2,432 Ghz
  - ...
  - Canal 13 : 2,472 Ghz
  - Canal 14 : 2,484 Ghz (!! pas à 5 Mhz du canal 13)

Les limites légales

- Jusqu'en 2003
  - USA : Canal 1 à 11, puissance max. 1000 mW
  - Europe (hors France) : Canal 1 à 13, puissance max 100mW
  - Japon : Canal 1 à 14, puissance max 10mW
  - France : Canal 10 à 13, puissance max 100mW
- Depuis fin 2003, en France Canal 1 à 13
- Historiquement, certains portables Wifi en importation US ne pouvaient pas fonctionner en France
  - Canaux 12 et 13 non utilisable !

Les interférences

- Chaque fréquence pour un canal est la fréquence médiane d'un canal de 22 Mhz
- Donc seuls 3 canaux sont utilisables simultanément, par des réseaux proches, afin d'avoir les performances optimales
- Si deux réseaux utilisent des canaux avec des fréquences qui se superposent
  - L'un va détecter que les signaux de l'autre sont des interférences, et réciproquement

Les BSS

- Les stations qui communiquent sur les réseaux 802.11 sont regroupés dans des Basic Service Set
- Existence de 2 types de Basic Service Set (BSS)
  - Independent BSS (IBSS) ou mode ad-hoc : chaque station communique avec d'autres stations
  - Infrastructure BSS (abrégé en BSS) ou mode infrastucture : chaque station communique avec un point d'accès
- Les stations doivent être dans le même Basic Service Set pour pouvoir communiquer ensemble
- Processus de communication
  - Les stations doivent s'associer au IBSS ou au BSS
  - Objectif : éviter que quiconque, proche d'une station, puisse directement communiquer avec elle

Les SSID

- Un BSS est identifié par une valeur de 48 bit, appelé BSS Identifier
  - En mode infrastructure : le BSS est souvent l'adresse MAC du point d'accès
  - En mode ad-hoc : nombre aléatoire généré par la première station
- En wifi, il est possible de se déplacer d'un BSS à un autre, sans perdre la connexion : le roaming
  - Attention : le wifi n'est pas fait pour assurer une communication lors de déplacement comme les réseaux cellulaires
- Le regroupement de plusieurs BSS se fait dans un Extended Service Set (ESS)
- Chaque BSS dans un ESS sont identifiés par le même Service Set Identifier (SSID)
- Le SSID est unique sur un réseau, sensible à la casse, de longueur comprise entre 2 et 32 caractères

Usage des SSID

- Les SSID servent à contrôler les accès aux points d'accès
- Les stations et les points d'accès doivent avoir le même SSID pour pouvoir communiquer
- Comment connaître le SSID d'un point d'accès ?

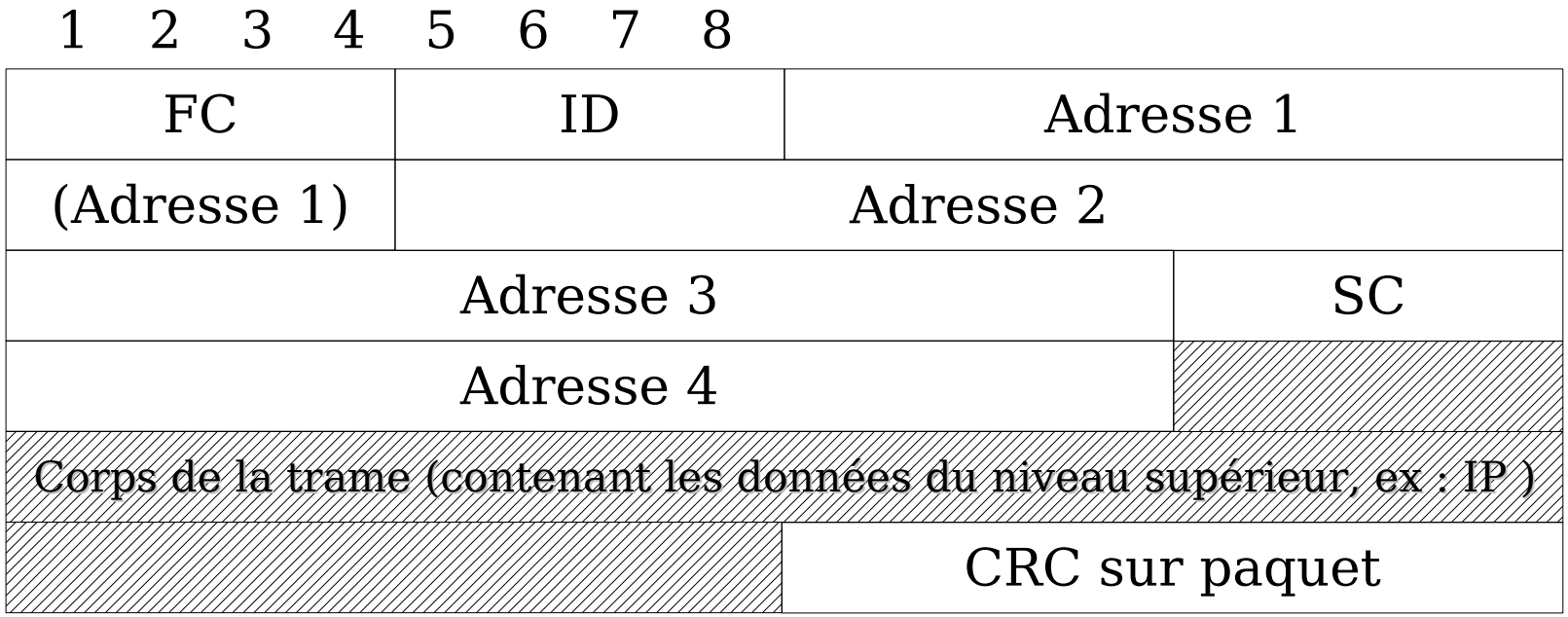
Beacon frames

- Les trames de type beacon sont expédiées régulièrement sur le réseau (en infrastructure) ou entre station (en ad-hoc)
- Ils transportent de nombreuses informations
  - Synchronisation temporelle entre la station et le point d'accès afin d'être sûr que toutes les fonctions sensibles aux temps soient correctement exécutées (saut de fréquences en FHSS, pa exemple). Attention : indépendant de l'horloge du système d'exploitation
  - Paramètres spécifiques aux bons fonctionnements du FHSS ou du DSSS
  - Le SSID du réseau est inclus dans les beacon trames. Attention : la désactivation du broadcast du SSID ne stoppe pas l'émission des beacon trames.
  - Traffic Indication Map : permet de gérer les paquets en file d'attente à destination de station en veille
  - Débit supporté par le point d'accès

Les réseaux sans-fil : IEEE 802.11

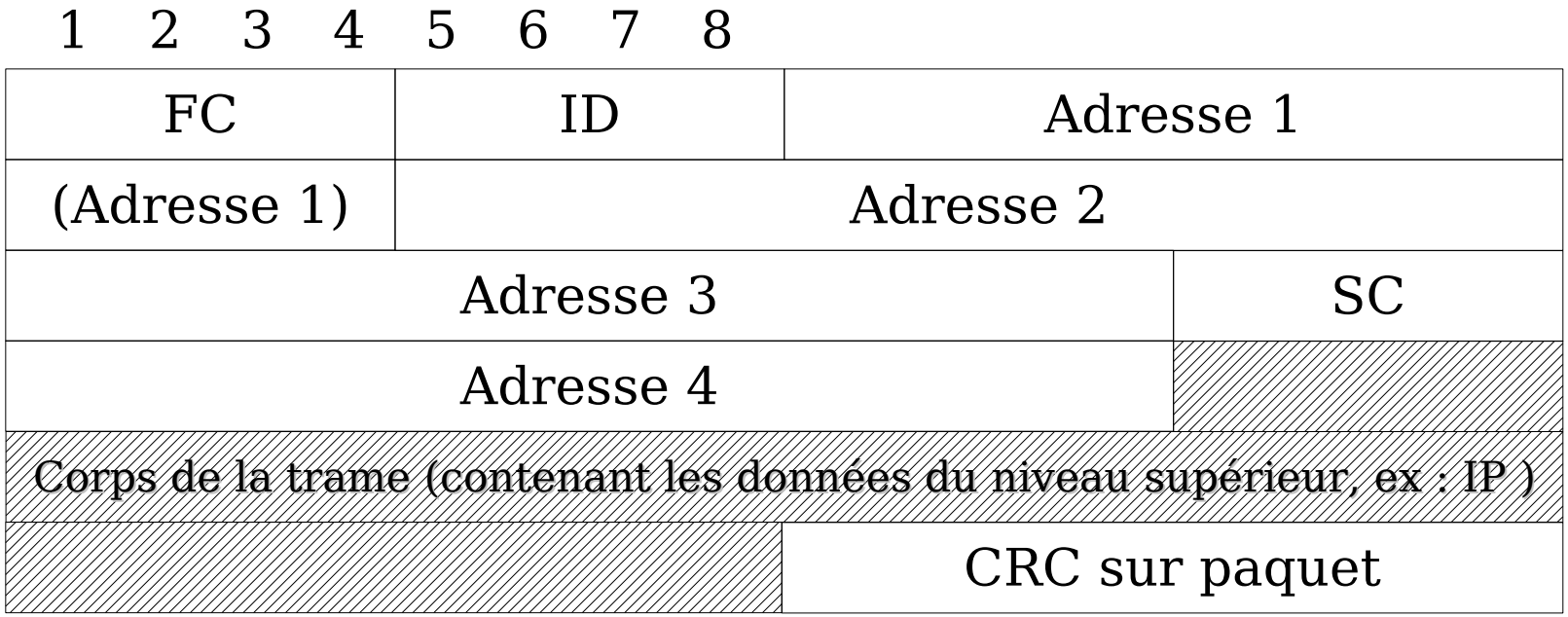
Format des trames

Format des trames 802.11 (1)



- FC (*Frame Control*) sur 2 octets : version du protocole et type de trame
  - Gestion, données ou contrôle
- ID (*Duration/ID*) : utilisées pour l'envoi de certains messages et le calcul du *Network Allocation Vector*

Format des trames 802.11 (2)



- Adresses : en fonction du FC, Chacune peut correspondre à l'un des cinq types : adresse source, destination, de l'émetteur, du récepteur, du point d'accès
- SC (*Sequence Control*) : indique un numéro de fragment et un numéro de séquence, permettant de réordonner des fragments et de repérer les paquets dupliqués

La Frame Control (1)

1	2	3	4	5	6	7	8
Prococole				Type		Sous-Type	
To DS	From DS	Frag ?	Retry	Pw Mgt	Data ?	Wep	Ordre

- Protocole : version du standard 802.11
- Type : gestion, contrôle ou données
  - gestion : demande d'association, annonce de point d'accès
  - contrôle : accès au média (ex : demandes d'autorisation d'émission)
  - données : concerne les communications normales
- Sous-type : dépend du type

La Frame Control (1)

1	2	3	4	5	6	7	8
Prococole				Type		Sous-Type	
To DS	From DS	Frag ?	Retry	Pw Mgt	Data ?	Wep	Ordre

- To DS (*To Distribution System*) : positionné à 1 si le message est à destination du système de distribution, 0 sinon
- From DS : positionné à 1 si la trame provient du système de distribution
- Frag ? : positionné à 1 s'il reste des fragments appartenant à la même trame après le fragment courant

Le Frame Control (2)

1	2	3	4	5	6	7	8
Protocole				Type		Sous-Type	
To DS	From DS	Frag ?	Retry	Pw Mgt	Data ?	Wep	Ordre

- Retry : positionné à 1 s'il s'agit d'une réemission du fragment courant
- Pw Mgt : indique le mode de gestion de l'énergie que la station utilisera après avoir transmis le fragment courant
- Data ? : indique que la station a encore un certain nombre de trames dans son tampon
- WEP : indique ou non l'utilisation de l'algorithme de chiffrement WEP
- Ordre : indique si la trame est émise en utilisant une classe spéciale

Les réseaux sans-fil : IEEE 802.11

La sécurité

La sécurité ?

- Transmission sans fil
  - Tout le monde peut donc intercepter les informations
- Interception suivant 2 techniques
  - Ecoute passive
  - Installation d'une borne « pirate »
    - Capture sur celle-ci des adresses MAC des clients et/ou paramètres de sécurité
- Denial of service
  - Par appareil parasitant le signal
  - En diffusant
    - des trames CTS, ainsi chaque station émet des trames et donc entre en collision
    - des trames de déassociation faisant ainsi générer une réassociation des stations, ...

Les protocoles pour la sécurité

Major Stepping Stones to Secure WLAN

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i

Authentification classique

- Authentification ouverte
  - Aucune authentification n'est requise. L'association est suffisante pour communiquer avec le réseau
- Authentification par clé partagée
  - Utilisation de clés cryptographiques, basées sur le protocole WEP (*Wired Equivalent Privacy)*
  - Le client et le point d'accès partage une même information : la clé
  - Authentification fonctionne sur la technique du challenge, envoyé par le point d'accès

WEP : codage des données

- Séquence de clair (notée *M*) concaténée avec une valeur de checksum sans clé *ICV(M)* de 32 bits (CRC-32 : *Cyclical Redundancy Check*) (*M* || *ICV(M)*)
- Utilisation de l'algorithme de chiffrement RC4 (algorithme symétrique) pour générer une suite pseudo-aléatoire (initialisé avec une clé (appelée graine))
  - Clé 64 ou 128 bits en export USA
  - sinon, jusque 2048 bits
- Pour fabriquer cette clé, le WEP utilise
  - un vecteur d'initialisation (notée *IV*) de 24 bits généré pour chaque nouvelle séquence WEP
    - soit nombre aléatoire, soit issu de la simple incrémentation d'un compteur !!
  - et une clé secrète (notée *K*) de 40 ou 104 bits partagée par tous les équipements du réseau mobile
- La graine de RC4 est alors (*IV* || *K*)
- Les données cryptées C : (*M* || *ICV(M)*) XOR RC4(*IV* || *K*)
- Envoie sur le réseau : *IV* || *C*

Décrypter le WEP ?

- Données M cryptées : C = (*M* || *ICV(M)*) XOR RC4(*IV* || *K*)
- Pour décrypter
  - Extraire le vecteur d'initialisation *IV* || *K*
  - Générer la même suite pseudo-aléatoire RC4(*IV* || *K*)
  - Faire le XOR entre C et RC4(*IV* || *K*)

Le WEP est-il sûr ?

1. Fiabilité de la clé
   - Clé de 40 bits (soit 5 caractères)
     - nombre de combinaison peu important
   - Clé de 104 bits
     - La force brute n'est plus envisageable !
   - Mais ...
2. Le vecteur d'initialisation est envoyé en clair sur le réseau
3. Et entre 2 paquets codant 2 messages identiques
   - Seul le vecteur d'initialisation change
4. Or quand une collision survient, il faut ré-emettre le même message
5. Attendre les collisions permet d'avoir des informations sur la clé secrète

Temporal Key Integrity Protocol

- TKIP est la première tentative de réponse aux problèmes du WEP
- Chaque station utilise la même clé, comme pour le WEP, à laquelle elle concatène leur adresse MAC
- Utilisation d'un IV de 6 octets au lieu de 4 dans le WEP
- Changement périodique de la clé, calculée à partir de la précédente

La cryptographie dans WPA et WPA2

TKIP – Temporal Key Integrity Key	AES – Advanced Encryption Standard
• Encrypts by adding increasingly complex bit coding to each packet • Based on same cipher (RC4) as WEP	• New cipher used in 802.11i • Based on TKIP with additional features that enhances the level of provided security

- TKIP et AES sont des algorithmes cryptographiques recommandés dans la norme 802.11i
- TKIP est certifié pour WPA et AES pour WPA2
- A la place de WPA ou WPA2, il est possible de rencontrer PSK ou PSK2 pour Pre-Shared Key
  - PSK ou PSK2 avec TKIP est équivalent à WPA
  - PSK ou PSK2 avec AES est équivalent à WPA2
  - PSK2, sans cryptographie est équivalent à WPA2