



# Segurització d'una xarxa SenseFils

**Atac Sensefils**

**Novembre 2004**

**Frederic Monpeat**

**<http://www.matarowireless.net>**

# Índex

1. Introducció al Wireless (802.11)
2. Segurització / Vulnerabilitats

# 1. Introducció al Wireless (802.11)

1.1 Què és Wireless?

1.2 Per què 802.11?

1.3 Equips

1.4 Funcionament

- Ad-hoc
- Infraestructura

1.5 Configuració

# 1.1 Qué es Wireless?

- Literalmente Wireless significa Sin Cables.
- Wireless como sistema de comunicación es un modo en el cual intervienen un *emisor* y un *receptor* en un contexto dado, en el cual el aire es el medio y las ondas electromagnéticas las encargadas de transportar la información.
- Según los estándares existen diferentes tipos de comunicaciones wireless: Bluetooth, Irda (infrarrojos), LMDS, GSM, UMTS, HomeRF... En definitiva cualquiera que utilice el aire como medio.
- Nosotros nos centraremos en las basadas en el protocolo **802.11 (Wi-Fi) en 2,4 GHz**

## 1.2 Por qué 802.11 ?

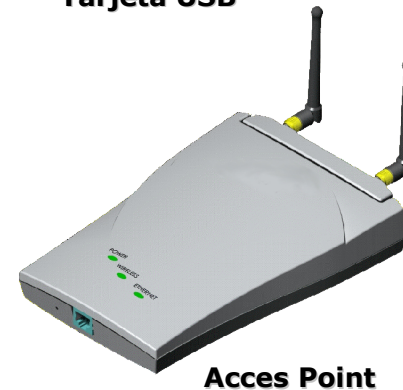
- Trabaja en la Banda de frecuencia de los 2,4 GHz → Banda Libre → no se necesita licencia para emitir.
- LA U.E. Dispone de 13 canales en esta frecuencia → podemos evitar el solapamiento → permite crear infraestructuras más estables y robustas.
- Actualmente se consiguen velocidades **reales** de 2,2 MB/s de transmisión.
- Un equipo básico consigue distancias de 400 metros, llegando a enlaces de varios Km con antenas externas.
- Los equipos no són excesivamente caros <100 euros podemos montar una red doméstica.

# 1.3 Equipos

Encontramos 2 equipos básicos:

- **Targetas de Red:** serian el equivalente de la targetas ethernet. Su función és la de dotar al equipo de interficie wireless. Según el tipo de connector las podremos utilizar en un u otro equipo (USB, PCI, PCMCIA, mini-PCI).

- **Punto de Acceso (Access Point):** lo podemos definir como un HUB inalámbrico. Se utiliza para concentrar a varios equipos.



# 1.4 Funcionamiento

- Podemos trabajar como en una red normal TCP/IP
- Evidentemente funcionan los mismos protocolos y servicios: ftp, http, chat, correo, juegos online ...
- Los equipos deben cumplir **WI-FI** (Wireless Fidelity): asegura la compatibilidad entre equipos de distintos fabricantes.
- Diferenciamos 2 protocolos dentro del 802.11 que funcionan en los 2,4 GHz:
  - **802.11b**: permite velocidades de 11 Mbs (+/- 800 KBs reales). Con equipos del mismo fabricante puedes llegar a los 22 Mbs.
  - **802.11g**: llega a los 54 Mbs (+/- 2.000 KBs). También duplica velocidad con equipos de mismo fabricante.

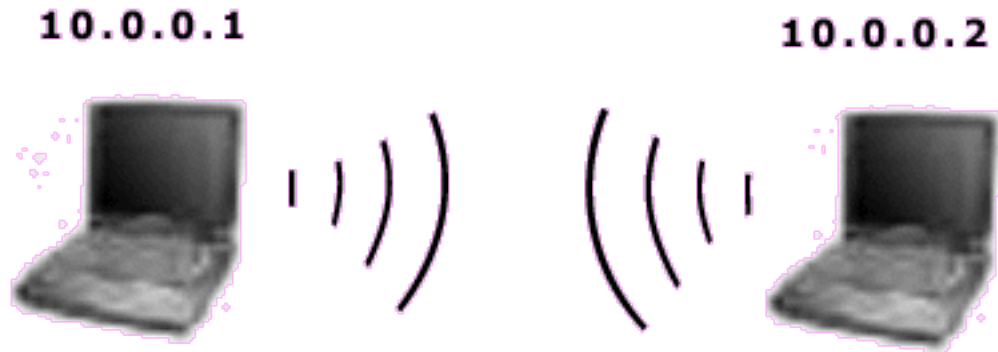
# 1.4 Funcionamiento

- Hay equipos de 802.11b, de 802.11g y duales. En principio cualquier equipo 802.11g puede operar también en 802.11b, pero sólo de una forma a la vez.
- En función de cómo conectemos los equipos trabajaremos en 2 topologías diferenciadas:
  - **Modo Ad-hoc:** conexión punto a punto → no necesitamos AP. Podemos conectar más de 2 equipos de esta forma. *Ej: similar a la conexión con cable cruzado entre 2 pc's.*
  - **Modo Infraestructura:** 1 Ap al cual se le conectan varios equipos wireless con targeta. Para conectar un equipo a otro se ha de pasar por el AP.

# 1.4 Funcionamiento

## Modo Ad-hoc:

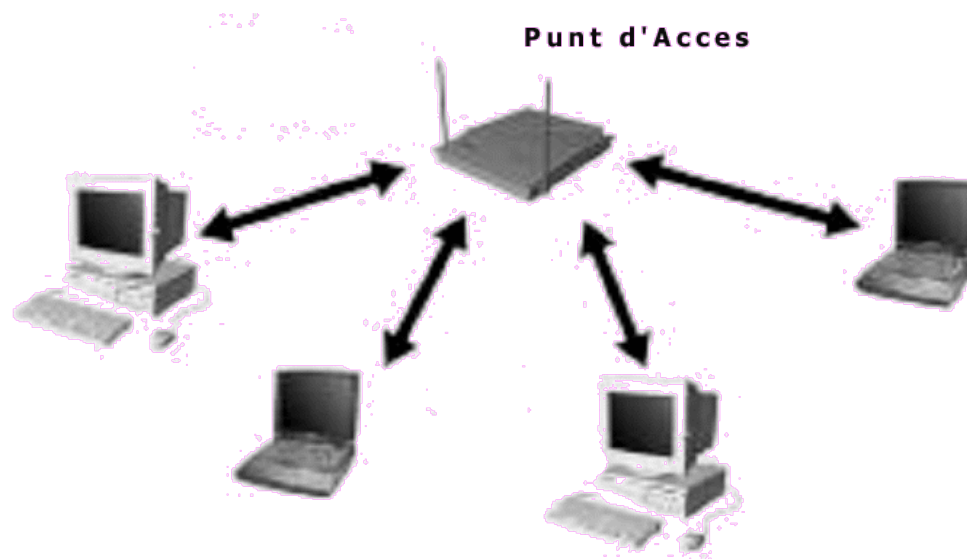
- Conexión directa de los equipos (P2P)
- Solución económica.
- +Equipos -- Rendimiento



# 1.4 Funcionamiento

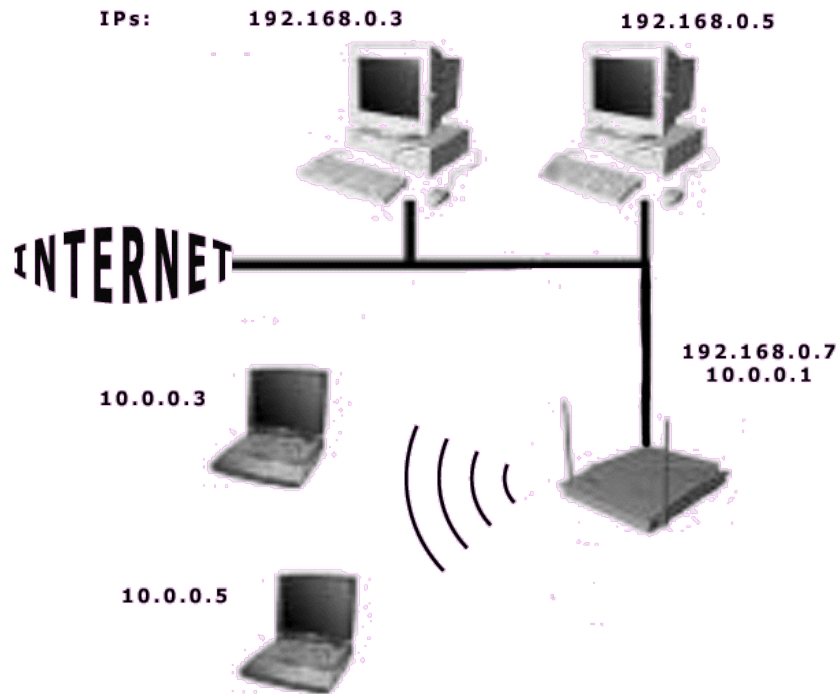
## Modo Infraestructura:

- Unión con las Redes cableadas:
  - Subred Wireless → función de Router.
  - Extensión de la red cablejada → función de Bridge



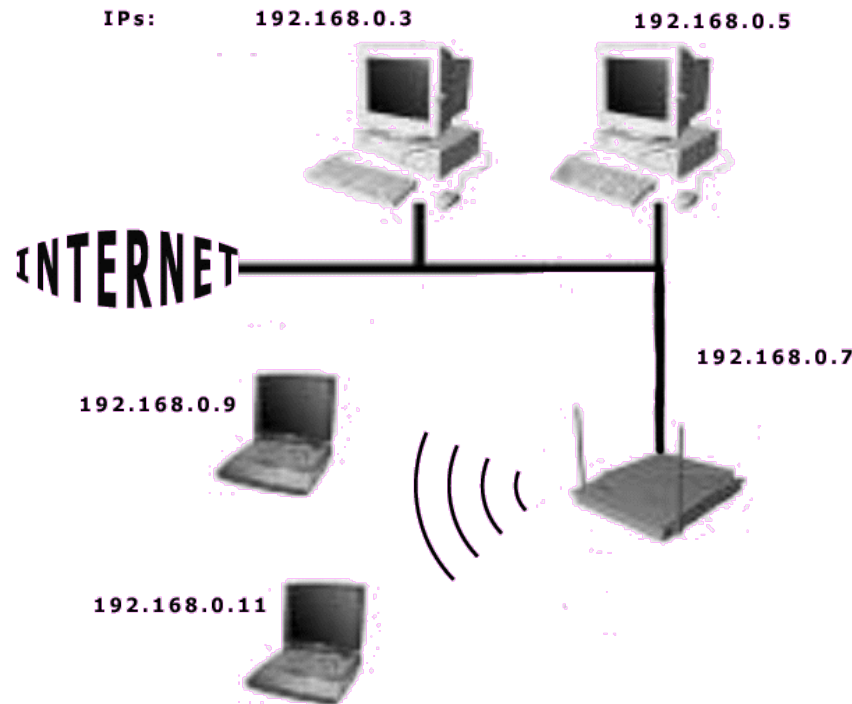
# 1.4 Funcionamiento

## Modo Infraestructura: (Router)



# 1.4 Funcionamiento

## Modo Infraestructura: (Bridge)



# 1.5 Configuración

- Se configura el Punto de Acceso :
  - **ESSID**: nombre de la RED (no és password!!)
  - **Canal**: por defecto escogerá el más óptimo (menos saturado).
  - **WEP**: és la encriptación de los datos (128, 64 ... Bits)
  - Existen **otros parámetros** en función del equipo: Listado de MAC (ACL), WPA (alternativa WEP), función de router, DHCP, modo repetidor...
- Se configura la Tarjeta Wireless: sólo el ESSID.
- Si el AP acepta el equipo → equipo **Linkado** a la Red Wireless (Asociado)
- Configuramos el TCP/IP → Equipo en la Red.



# 2. Segurització/Vulnerabilitats

2.1 ACL

2.2 WEP

2.3 Autenticació

2.4 WPA

## 2.1 ACL

- **Access Control List:** mecanisme que controla els equips que es poden connectar al AP
- Es disposa d'una llista de MAC's en l'AP les quals podran associar-se.

### **Vulnerabilitats:**

- Podem esnifar connexions actives i suplantar l'adreça MAC del client (en una connexió wireless l'AP no distingiria que es comunica amb 2 equips).
- Podem fer-nos passar per l'AP: desconnectem a tots els clients, rebem la informació que ens enviïn...

## 2.2 WEP

- **Wired Equivalent Privacy:** Sistema que intenta procurar la mateixa seguretat que trobem en una xarxa cablejada.
- Basat en un algoritme d'enciptació **RC4**: genera claus de 64 i 128 bits .
- **IV** (Vector d'Inicialització): s'inclou en la capçalera de cada trama, ocupant 24 bits (0-16.000.000)
- Enciptem a partir d'una **Passphrase** introduïda com a clau (transformada en Hexadecimal).
- La clau ha de ser coneguda per TOTS els equips que formen la xarxa sensefils: *Passphrase* elemental.

## 2.2 WEP

### Generem les claus:

- A partir de la *Passphrase* se'ns generaran 4 claus.
- Com que en tots els equips hem introduït la mateixa *Passphrase*, en tots tindrem les mateixes 4 claus.
- Realment només s'utilitza una per l'encryptació: l'equip que envia la informació encryptada ha d'informar a l'equip receptor la clau que necessita.
- Realment només utilitzem 40 i 108 bits per l'encryptació (24 bits són del IV)

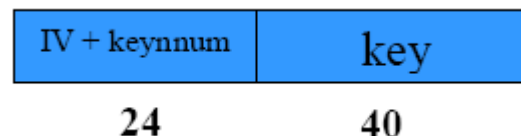
## 2.2 WEP

### Encriptem:

- Una trama la forma una Capçalera i un Payload (informació que volem enviar).
- Mitjançant un algorisme CRC, generem un ICV (Valor que Comprova l'Integritat) i l'afegim al Payload.

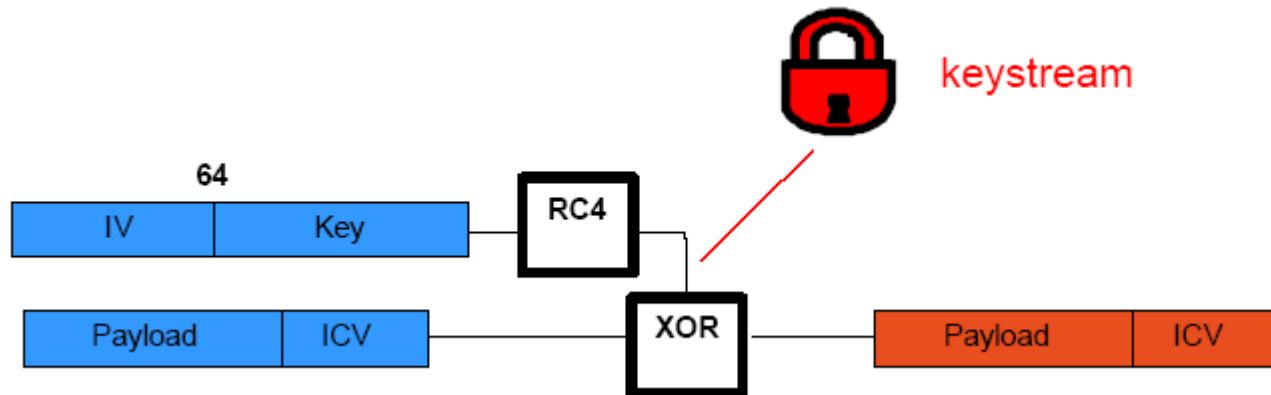


- Triem una de les 4 claus generades.
- Li afegim el IV amb el número de clau: tenim la clau per encriptar.



## 2.2 WEP

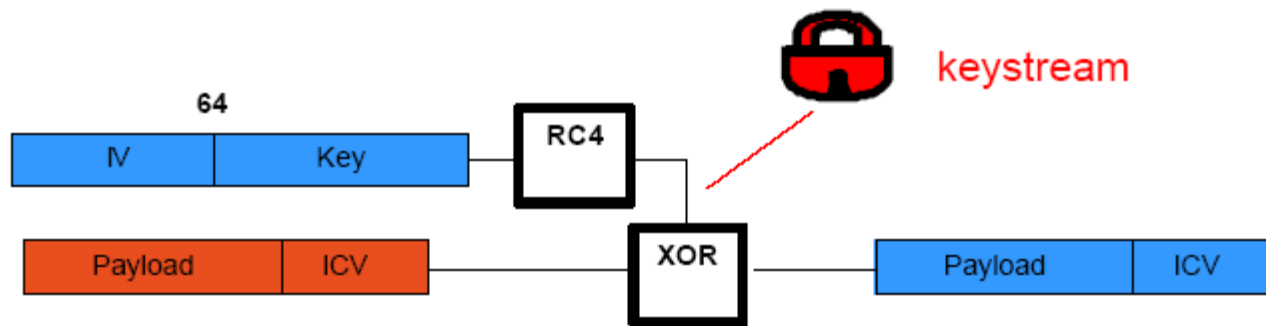
- Apliquem un algorisme RC4 a la clau i realitzem una XOR amb la informació que volem encriptar: informació encriptada!!!



## 2.2 WEP

### Desencriptem:

- Triem la clau que ens el **KeyNumber** i li afegim el **IV** (coneguts)
- Tornem a fer la metixa operació amb la part encriptada i ens la retornarà desencriptada.
- Comprovem que el **ICV** sigui el correcte: **Trama desencriptada!**



## 2.2 WEP

### Vulnerabilitats:

- **Linialitat del CRC** : podem generar ICV vàlids.
- **MIC (Check Integrity Message)** independent de la clau: podem injectar paquets.
- **IV**: no és obligatori, tamany massa curt (màxim 16.777.216) i **es poden repetir**.
  - Si generem tràfic suficient en poca estona es reinicialitza el contador de IV's i si disposem de Plaintext encriptats amb el mateix IV, matemàticament podem descobrir la clau.
  - Per generar tràfic podem injectar paquets a la xarxa.
  - Rebotar la màquina implica reinicialitzar el contador de IV's.

## 2.3 Autenticació

- Serveix per validar que l'equip amb el qual et pretens comunicar realment és qui diu ser.
- Existeixen 3 estats en un procés d'autenticació (**NO Autenticat/NO Associat, Autenticat/NO Associat, Autenticat/Associat**) que varien mitjançant l'enviament de trames (**Autenticació/Desautenticació, Associació/Desassociació**)
- Hi ha 2 mètodes en l'estàndard:
  - **Open System Authentication**: és el que ve per defecte. Qualsevol equip que desitja ser autenticat automàticament és autenticat. NO és segur!!!
  - **Shared Key Authentication**: és un mètode per clau secreta compartida (WEP).

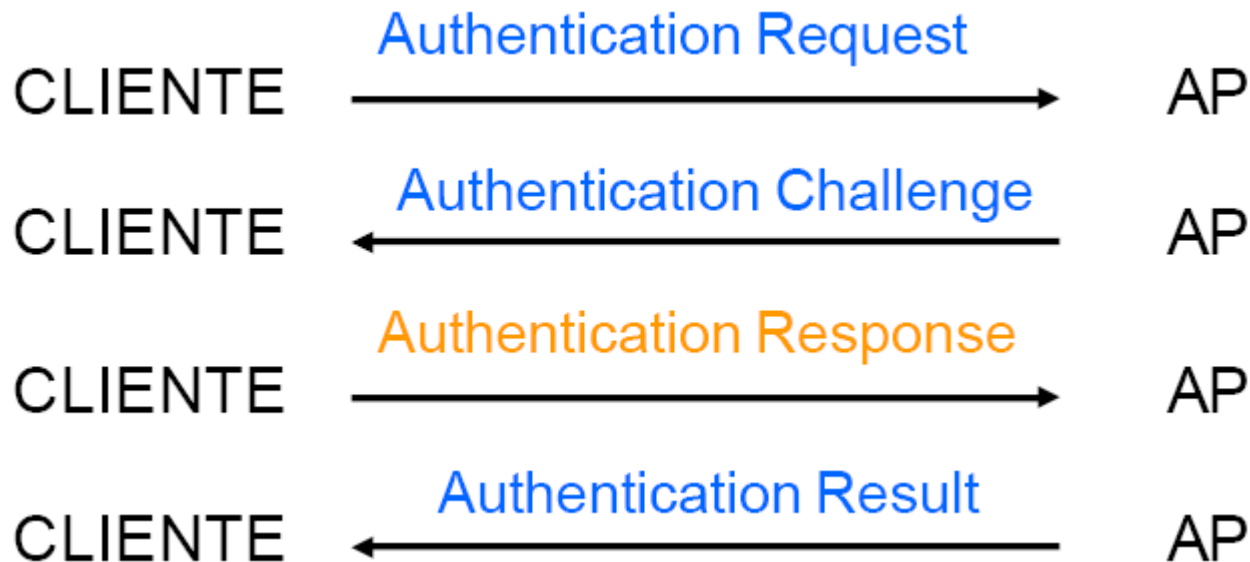
## 2.3 Autenticació

### Shared Key Authentication:

1. El client envia una petició d'autenticació al AP.
2. L'Ap respon amb un **text de desafiament**.
3. El client **encripta el desafiament** amb la Passphrase, **afegeix un IV** i **retorna la trama encriptada**.
4. L'AP desencripta la trama, comprova el desafiament i la integritat (ICV).
5. Si és tot correcte: **client autenticat**.
6. Ara s'autentica l'AP en el client: procés invers.

## 2.3 Autenticació

### Shared Key Authentication:



## 2.3 Autenticació

### Vulnerabilitats:

- **Open System:** No hi ha cap seguretat
- **Shared Key:**
  - L'atacant captura el 2on i el 3er Management Frame del Procés, disposa del text de desafiament sense encriptar i encriptat a més de la clau compartida.
  - Tots els Management Frames són de text conegut.
  - Ens podem autenticar sense conèixer la clau.

## 2.4 WPA

- **Wi-Fi Protected Acces:** solució adoptada per substituir al WEP
- Millora les deficiències en l'enciptació de les dades i l'autenticació dels usuaris.
- Diferencia dos models d'implementació:
  - **Consumer Mode:** enfocat als usuaris. Treballa amb PSK (Pre-Shared Key) i enciptació TKIP.
  - **Enterprise Model:** Enfocat a entorns empresarials, autentica als usuaris en xarxa i de forma independent (cada usuari té la seva pròpia clau). Combina 802.1x amb servidors Radius per l'autenticació, TKIP per l'enciptació, Per-Packet key mixing (encipta cada paquet amb una clau única) i millora la integritat de les dades.

## 2.4 WPA

- **Funcionament bàsic del Consumer Model:**
  1. **Associació** amb l'AP.
  2. **Autenticació** i distribució de la **PMK** (Pair-Wise Master Key) una mena de Clau Principal.
  3. Basada en la PMK es crea i s'instal·la una clau anomenada **PTK** (Pair-Wise transient Key) una mena de Clau Temporal.
  4. Es comprova la integritat
  5. Amb la clau transitòria encriptem amb **TKIP**.

## 2.4 WPA

### Vulnerabilitats:

- Per construir la **Clau Principal** PMK necessitem introduir en un algorisme la **PassPhrase**, el **SSID**, la longitud del SSID i un hashing de **4096** que generarà un valor de **256** bits.
- Per construir la **Clau temporal** PTK, necessitem introduir en un algorisme la **PMK**, **MAC** del AP/Client i unes **altres variables**.
- Si sabem les variables que s'introdueixen en els algorismes per generar les claus, **podem descriptar els paquets**.

**Només es dona en el Customer Mode!!!**

## 2.4 WPA

### Vulnerabilitats:

- Per construir la **Clau Principal** PMK necessitem introduir en un algorisme la **PassPhrase**, el **SSID**, la longitud del SSID i un hashing de **4096** que generarà un valor de **256** bits.
- Per construir la **Clau temporal** PTK, necessitem introduir en un algorisme la **PMK**, **MAC** del AP/Client i unes **altres variables**.
- Si sabem les variables que s'introdueixen en els algorismes per generar les claus, **podem descriptar els paquets**.

**Només es dona en el Customer Mode!!!**

# REFERÈNCIES

**[1] WPA Passive Dictionary Attack Overview**

TakehiroTakahashi

**[2] In-Seguridad en redes 802.11b**

Pau Oliva Fora

**[3] Documentació de Mataró Wireless**

<http://documentacion.matarowireless.net>



**<http://www.matarowireless.net>**

En col·laboració amb:



**IluroWireless**



Aquesta obra està sota llicència Creative Commons.  
<http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca>