Seguridad En Redes Inalámbricas 802.11 a/b/g

Protección y vulnerabilidades

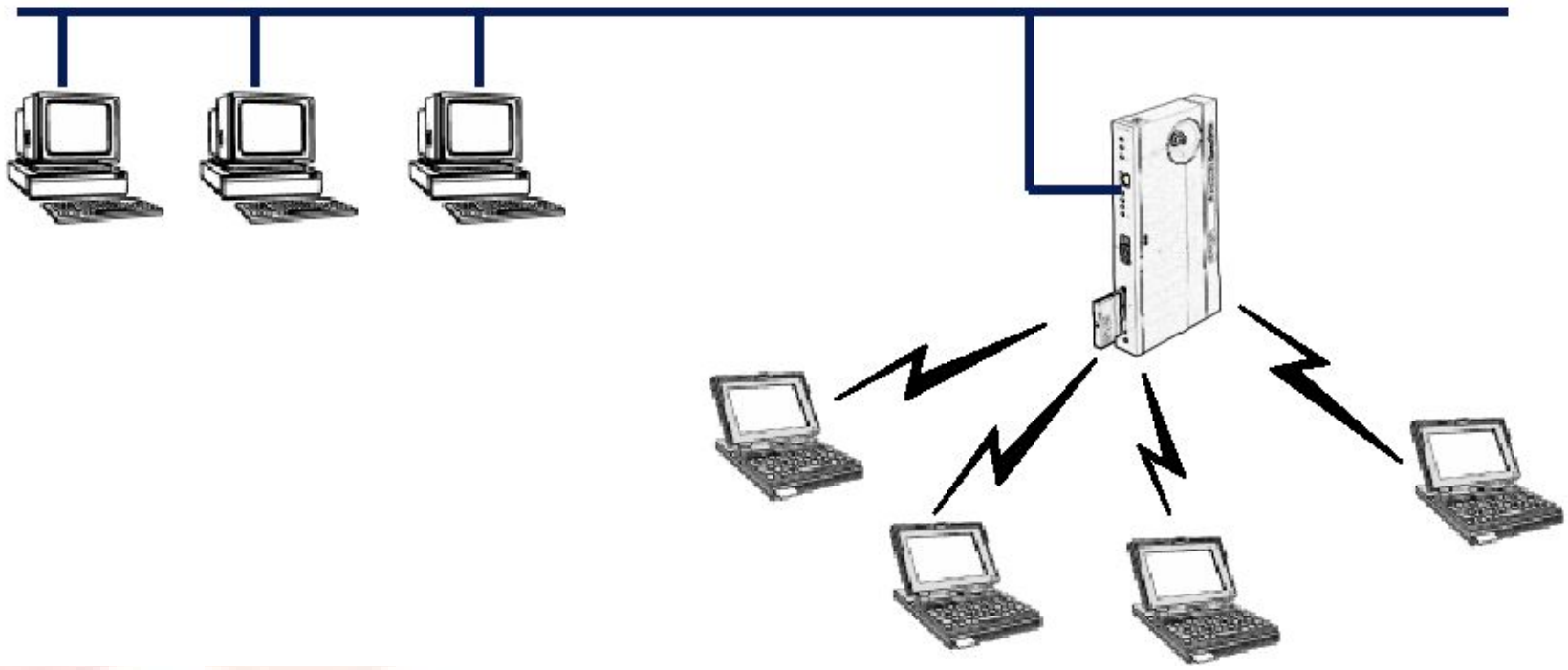
Pablo Garaizar Sagarminaga
garaizar@eside.deusto.es

Redes WiFi

- ¿Qué es una red WiFi?
  - Conjunto de equipos interconectados a través de un “bridge” inalámbrico o Punto de Acceso.
- Los principales dispositivos en una red WiFi son:
  - Tarjetas de red.
  - Puntos de Acceso o Access Points (AP).
  - Antenas.

Redes WiFi

- **Topología típica:**



Tarjetas de red WiFi

- Sustituyen a las tarjetas de red cableadas.
- Chipsets más extendidos:
  - Hermes (Lucent): Orinoco, Avaya, Compaq, Lucent, Enterasys...
  - Prism 2 / 2.5 / 3 (Intersil): D-Link, Linksys, SMC, USRobotics, Conceptronic...
  - Airo (Aironet): Cisco.
  - ATMEL: Belkin...
  - Atheros: Senao, 3com...
  - Prism GT/Duette/Indigo: Netgear, D-Link, etc.
  - Intel/Centrino.

Tarjetas de red WiFi

- Varios modos de funcionamiento:
  - Ad-hoc: interconexión sin la necesidad de un AP.
  - Managed o Infrastruture: conectada a un AP que gestiona las conexiones.
  - Master: funcionando como un AP, da servicio y gestiona las conexiones.
  - Monitor: permite capturar paquetes sin asociarse a un AP o red ad-hoc

Tarjetas de red WiFi

- **Modo ad-hoc**
  - **Es similar a la conexión punto a punto mediante cable ethernet cruzado (sin embargo, pueden estar conectados varios PCs ad-hoc).**
  - **Ningún AP gestiona el medio** → aumento de colisiones → baja el rendimiento.

Tarjetas de red WiFi

- **Modo Managed o Infrastructure:**
  - **La tarjeta deja toda la responsabilidad al AP para que gestione el tráfico.**
  - **En ocasiones es necesario saber el ESSID (Indentificativo de red) de la red que gestiona el AP para poder entrar** → detectarlo entrando en modo monitor.

Tarjetas de red WiFi

- **Modo Master:**
  - **Podemos convertir PCs en Aps.**
  - **HostAP: http://hostap.epitest.fi**
  - **Ventajas:**
    - **Un PC es mucho más potente que un AP, muchas posibilidades (filtrados, mejoras de seguridad, enrutado, DHCP...)**
    - **Reciclaje de equipos obsoletos, APs baratos.**
  - **Inconvenientes:**
    - **No todas las tarjetas pueden ponerse en modo Master (sólo las Prism y desde hace poco las Hermes)**

Tarjetas de red WiFi

- **Modo monitor:**
  - **Monitoriza un canal específico sin transmitir paquetes (de forma pasiva)**
  - **La tarjeta no mira los CRC's de los paquetes**
  - **NO es lo mismo que el modo promiscuo**
  - **Existen dificultades a la hora de poner una tarjeta en modo monitor si no es Hermes o Prism.**

Tarjetas de red WiFi

- **Utilización en GNU/Linux: wireless-tools.**
  - **iwconfig:**
    - **Identificador de red (essid).**
    - **Frecuencia o canal (freq/channel).**
    - **Modo (mode: master|managed|ad-hoc|monitor).**
    - **Velocidad (rate).**
    - **Clave de encriptación (key).**
    - **Potencia de transmisión (txpower).**
    - **...**

Tarjetas de red WiFi

- **Utilización en GNU/Linux: wireless-tools.**
  - **iwpriv:**

```
iwpriv atml0
atml0     Available private ioctl :
          set_preamble      (8BE0) : set   1 int   & get   0
          get_preamble      (8BE1) : set   0       & get   7 char
          atmlparam         (8BE3) : set   2 int   & get   0
          get_atmlparam     (8BE4) : set   1 int   & get   1 int
          wpa               (0001) : set   1 int   & get   0
          getwpa            (0001) : set   0       & get   1 int
          privacy_invoked   (0002) : set   1 int   & get   0
          getprivacy_invo   (0002) : set   0       & get   1 int
          wpa_mode          (0003) : set   1 int   & get   0
          getwpa_mode       (0003) : set   0       & get   9 char
```

Tarjetas de red WiFi

- **Utilización en GNU/Linux: wireless-tools.**
  - **iwlist:**

```
iwlist wlan0 scanning
wlan0     Scan completed :
          Cell 01 - Address: 00:11:24:22:FD:3F
                    Mode:Managed
                    Quality=255/70  Signal level=-
                     125 dBm  Noise level=-139 dBm
```

Tarjetas de red WiFi

- **Utilización en GNU/Linux: wireless-tools.**
  - **iwevent:**

```
# iwevent
Waiting for Wireless Events from
  interfaces...
09:39:05.548329    wifi0    Expired
  node:00:11:24:22:FD:3F
09:39:12.509017    wifi0    Registered
  node:00:11:24:22:FD:3F
```

Tarjetas de red WiFi

- **Utilización en GNU/Linux: wireless-tools.**
  - **iwspy: eventos WiFi de uno o varios interfaces o APs.**
  - **Similar a /proc/net/wireless**

```
# cat /proc/net/wireless
Inter-| sta-|   Quality        |   Discarded packets               | Missed | WE
 face | tus | link level noise |  nwid  crypt   frag  retry misc | beacon | 17
 atml0: 0000    0.    0.    0.       0      0      0      0    0        0
 wifi0: 0000    0     0     0        0      0      0     21   26        0
 wlan0: 0000    0     0     0        0      0      0     21   26        0
```

Puntos de Acceso WiFi

- Complementan a los hubs, switches, routers, etc.
- Gestionan el medio físico.
- Retransmiten selectivamente los datos.
- Pueden tener servicios adicionales:
  - Servidor DHCP.
  - Gestión remota (web, telnet, ssh).
  - Filtrados por IP, MAC, etc.

Puntos de Acceso WiFi

- Normalmente interconecta una LAN ethernet con clientes o redes inalámbricas.
- Diferentes alternativas:
  - APs comerciales.
  - APs comerciales con software libre.
  - APs “caseros”.
  - Gestores de APs múltiples.

Puntos de Acceso WiFi

- **Gestores de APs múltiples:**
  - **La complejidad de una red WiFi puede convertirse en inmanejable.**
  - **Redes amplias > WDS:**
    - **Wireless Distribution System.**
    - **Un única red WiFi compuesta de varios APs.**

Puntos de Acceso WiFi

- **Gestores de APs múltiples.**
  - **Características Principales:**
    - **Autentificación centralizada de usuarios.**
    - **Roaming transparente.**
    - **Cifrado de todas las comunicaciones**
    - **Listas de Control de Acceso.**
    - **Detección y anulación de otros APs.**
    - **Bastante caros:**
      - **300 € por AP gestionable + 12000 € por dispositivo de gestión.**

Puntos de Acceso WiFi

- **Gestores de APs múltiples.**

Antenas WiFi

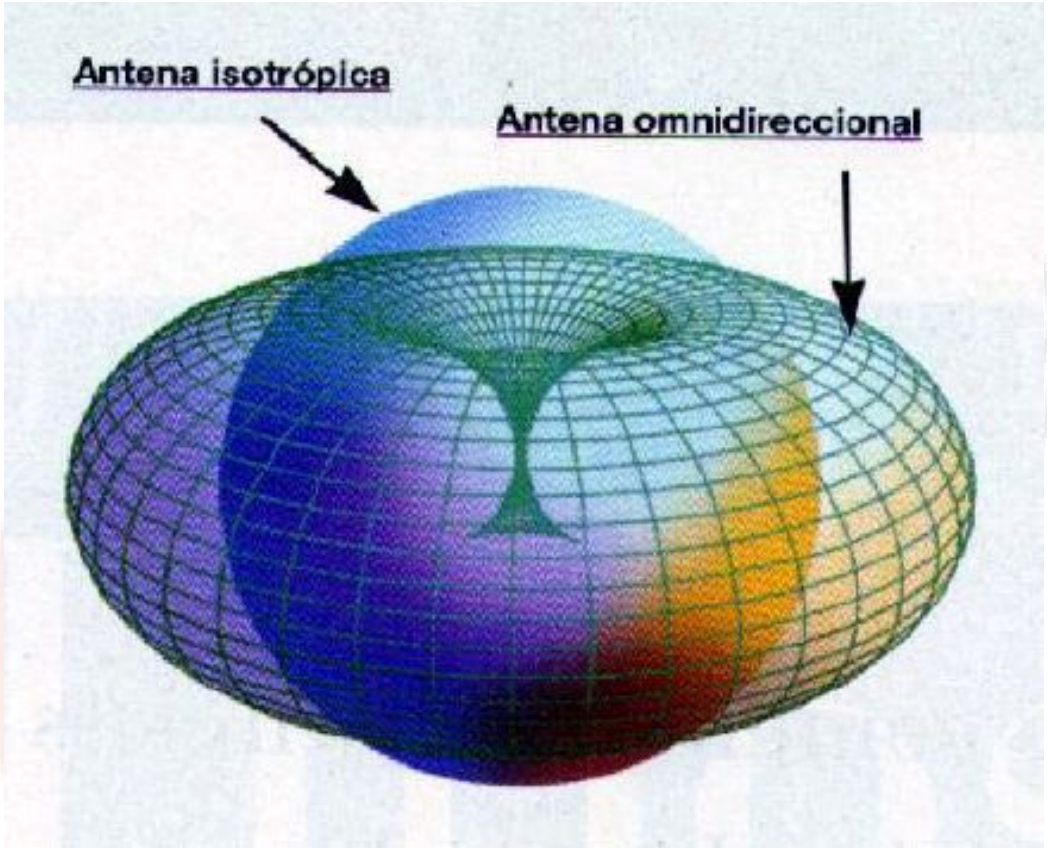
- **Consiguen aumentar la cobertura y el rendimiento de un enlace wireless.**
- **Diversos escenarios:**
  - **AP en el interior de un edificio.**
  - **AP en el exterior:**
    - **Conexión punto a punto.**
    - **Conexión punto a multipunto.**
    - **Hot-spot.**

Antenas WiFi

- Como podemos intuir, existen diferentes tipos de antenas:
  - Omnidireccionales
    - En todas las direcciones.
    - Ideales para APs o hot-spots.
  - Directivas
    - Hacia un sentido o un sector reducido.
    - Ideales para:
      - Clientes de un AP.
      - Interconexion LAN-to-LAN.

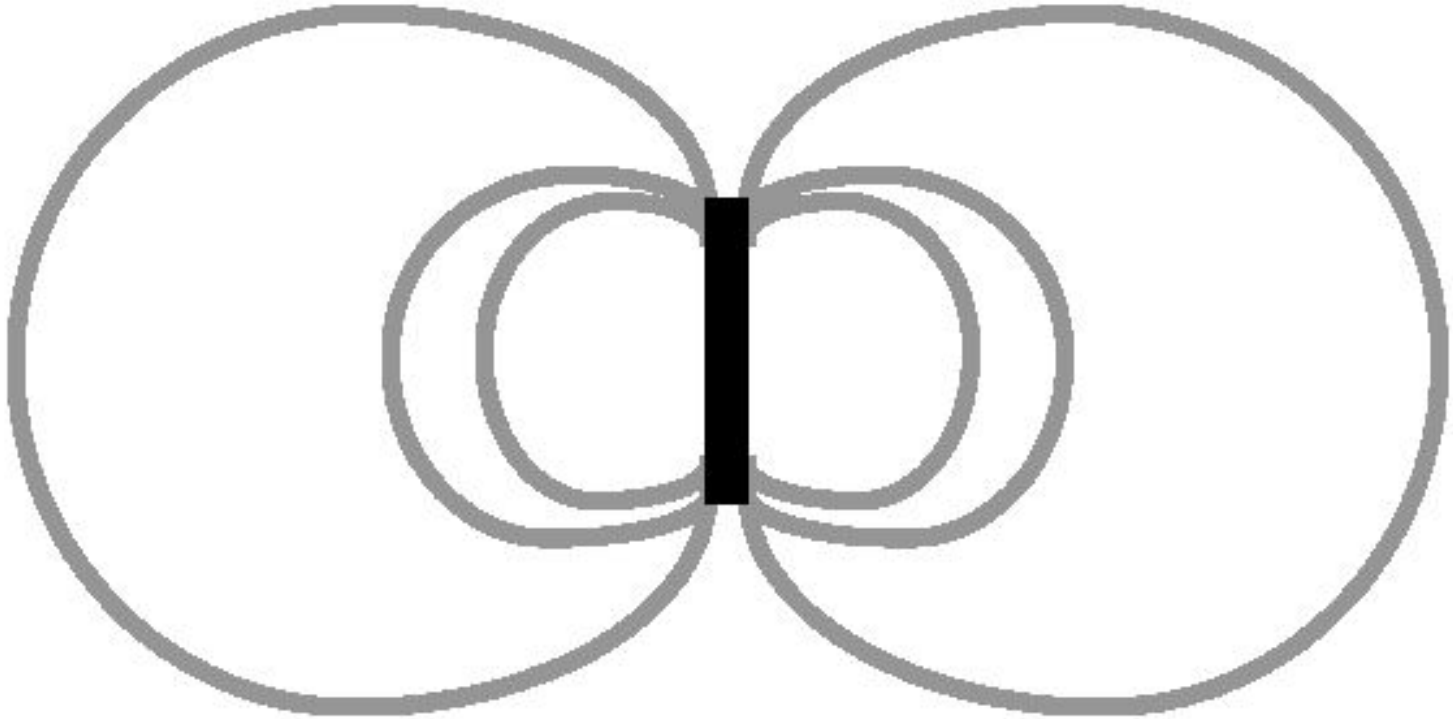
Antenas WiFi

– Omnidireccionales



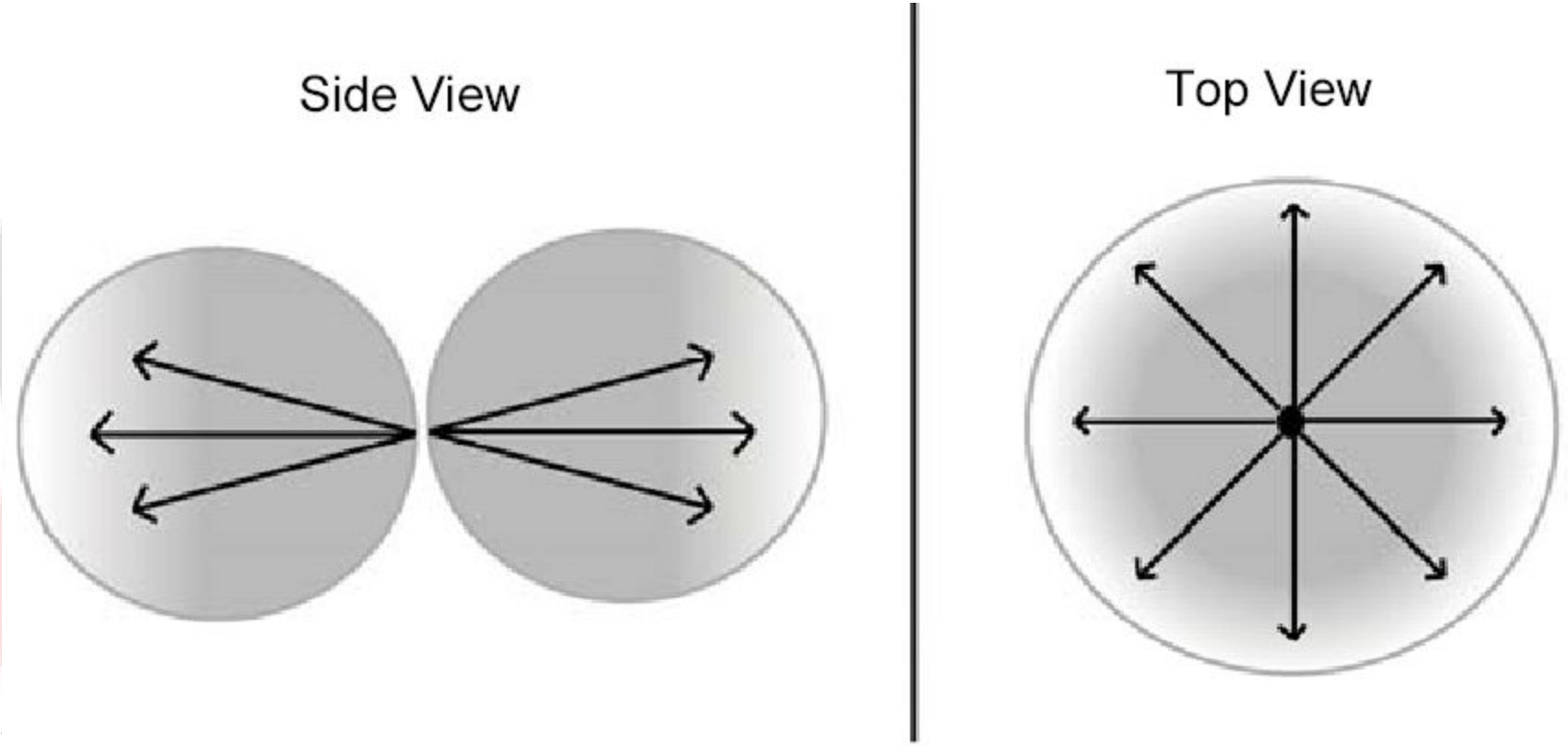
Antenas WiFi

– **Omnidireccionales. Dipolos:**



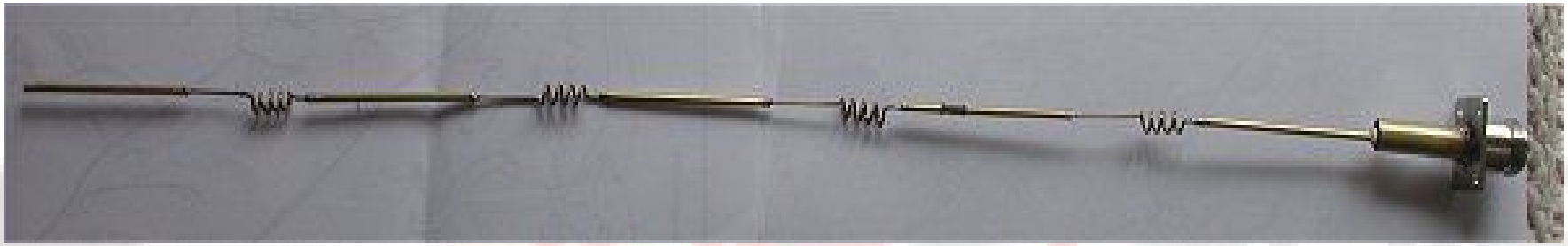
Antenas WiFi

– **Omnidireccionales. Dipolos:**



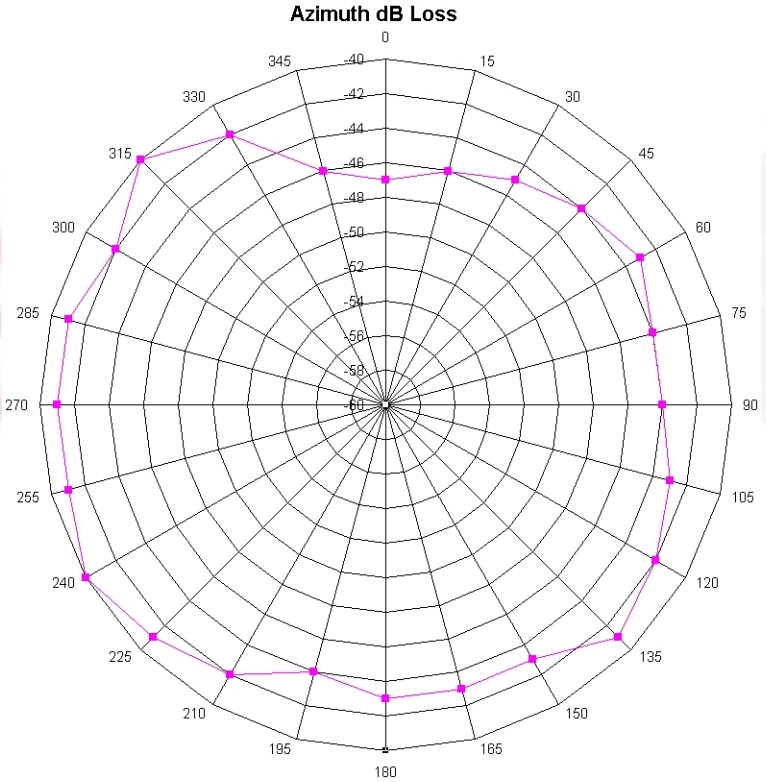
Antenas WiFi

– Omnidireccionales. Colineares:



Antenas WiFi

– Omnidireccionales. Diseños propios:



Antenas WiFi

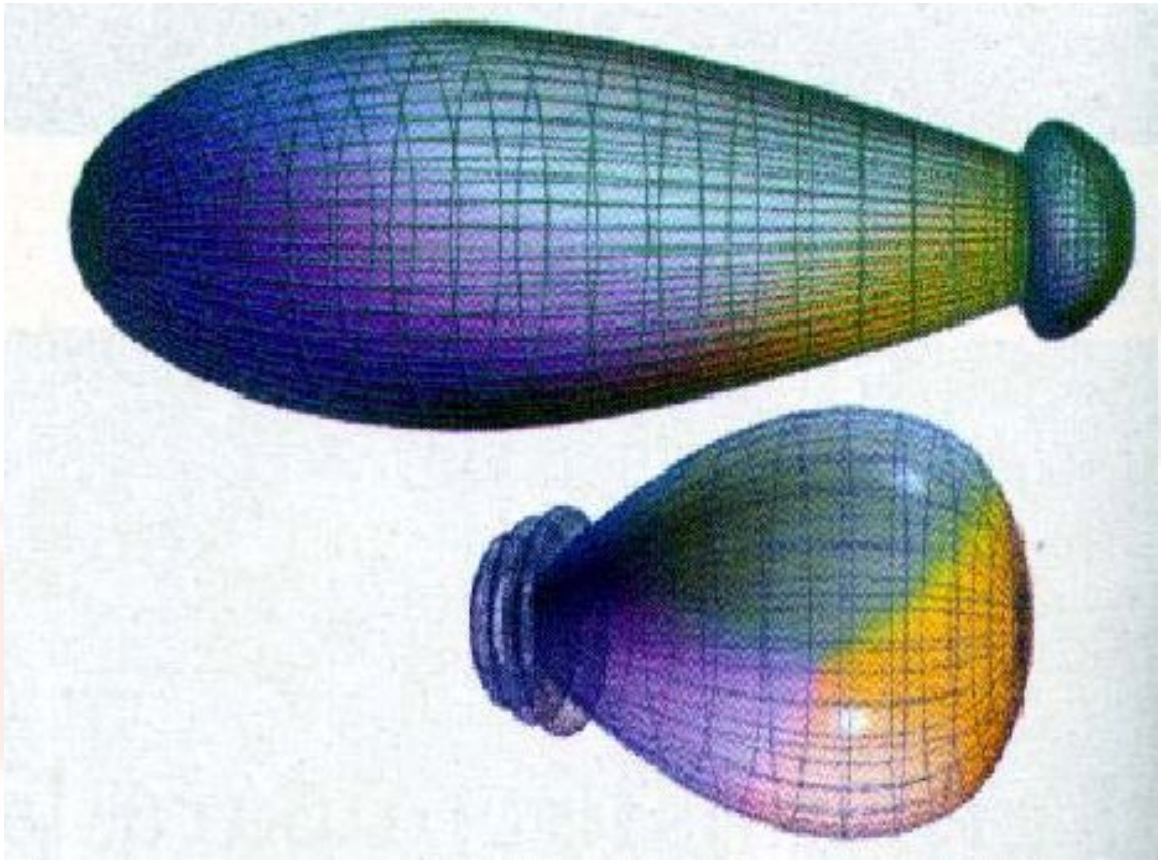
– **Omnidireccionales. Mini-omni, con cable coaxial:**

Antenas WiFi

– **Omnidireccionales. Las propias de las tarjetas:**

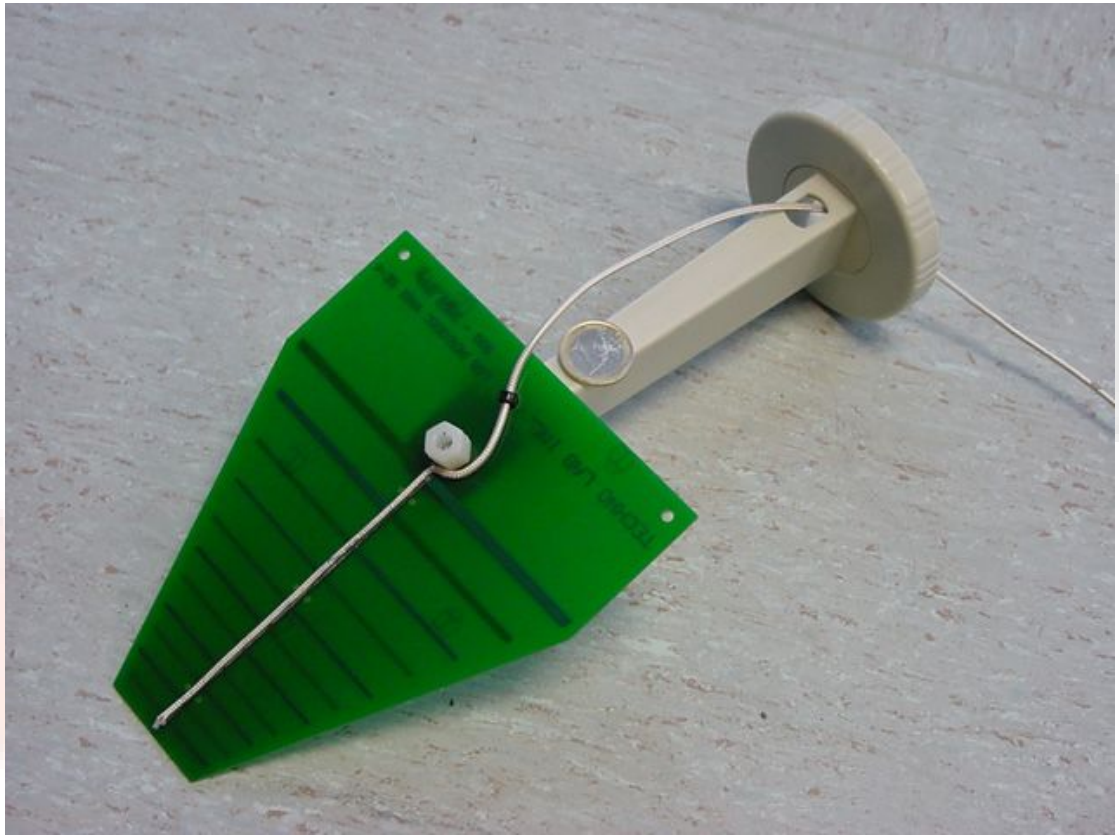
Antenas WiFi

– **Directivas:**



Antenas WiFi

– **Directivas. Circuito impreso:**



Antenas WiFi

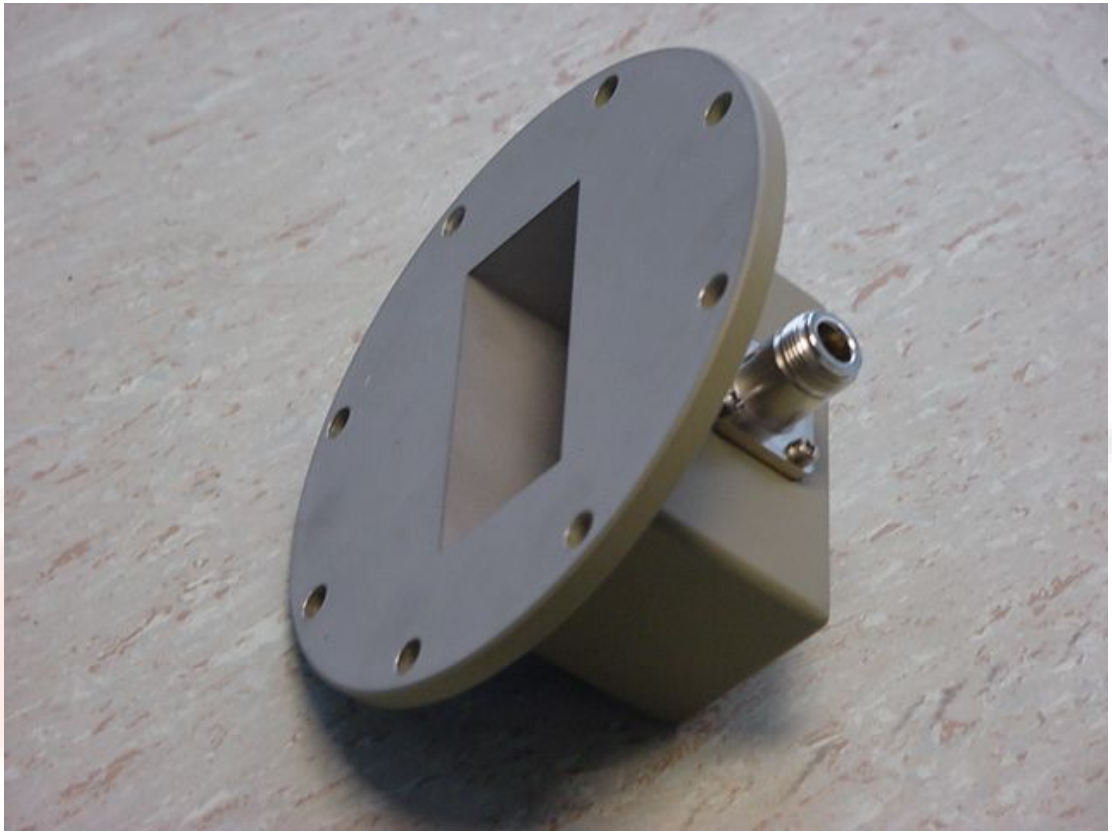
– **Directivas. Helicoidal:**

Antenas WiFi

– **Directivas. Helicoidal corta:**

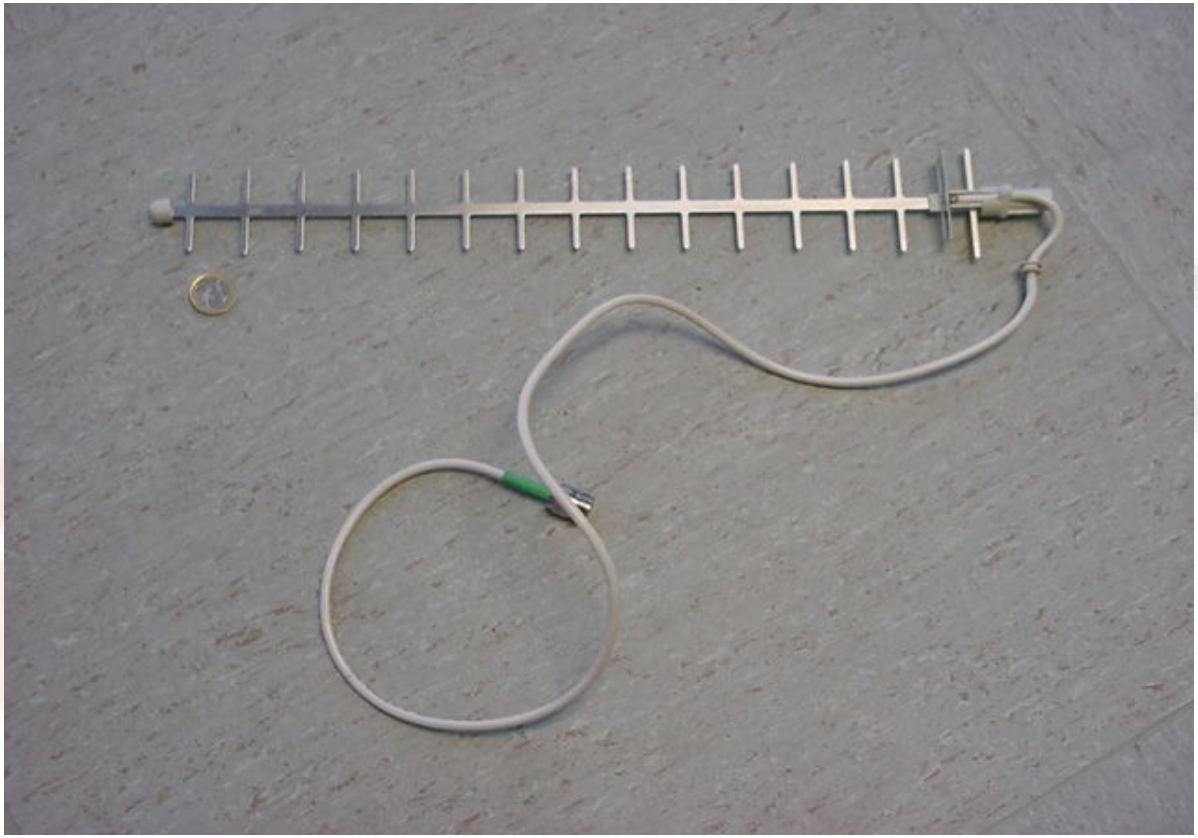
Antenas WiFi

– **Directivas. Panel:**



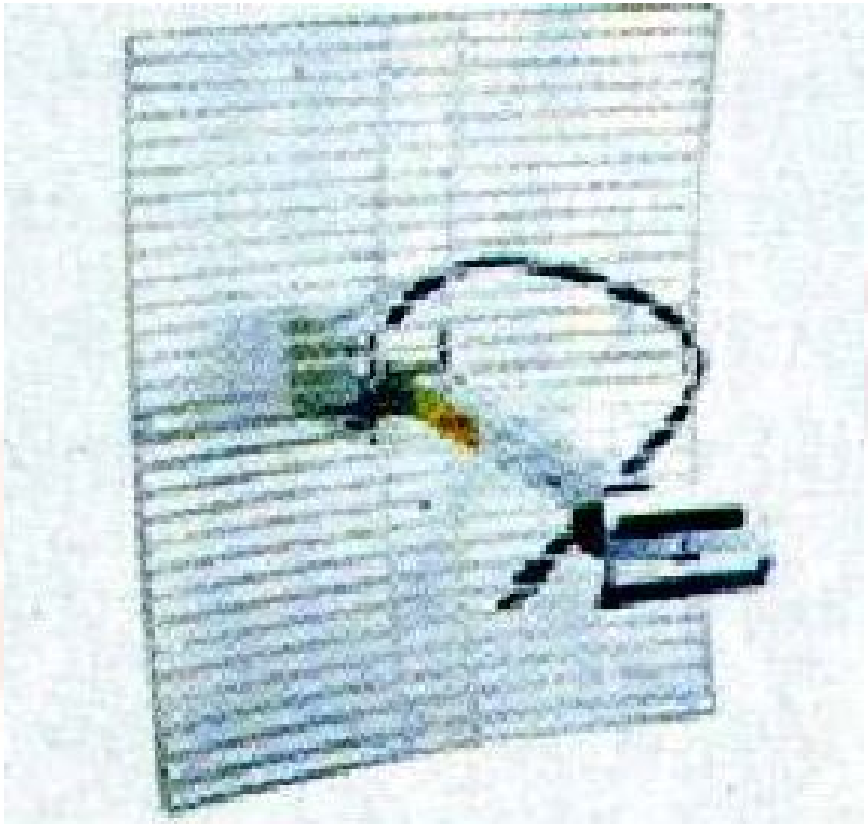
Antenas WiFi

– **Directivas. Yagi:**



Antenas WiFi

– **Directivas. Parabólica:**



Antenas WiFi

– **Directivas. Cantennas:**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido, Potencia:**
  - **Cantidad de energía irradiada**
  - **Se mide en:**
    - **Miliwatios**
    - **Decibelios**
      - **Principal unidad de medida en telecomunicación.**
      - **Se simboliza mediante: dB**
      - **Unidad logarítmica, medida relativa.**
    - **Ejemplo: Tarjetas PCMCIA:**
      - **30 mW ~ 15 dBm**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido, Sensibilidad:**
  - **Es la señal mínima que es capaz de recibir el receptor de forma intelegible.**
  - **Se mide en dBm con valor negativo.**
  - **Valores típicos: tarjeta Orinoco PCMCIA**
    - **11 Mbps: -82 dBm**
    - **5.5 Mbps: -87 dBm**
    - **2 Mbps: -91 dBm**
    - **1 Mbps: -94 dBm**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido, Pérdidas:**
  - **En cables coaxiales:**
    - **RG58: 1dB/m**
    - **RG: 213: 0.6dB/m**
    - **RG174: 2dB/m**
      - **Es el utilizado por los pigtail, debido a su estrechez.**
  - **Pérdidas en espacio libre:**
    - **Mayor distancia, mayores pérdidas.**
    - **Obstáculos**
    - **Lluvia: atenuación, inversión de la polarización, refracción, etc.**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido, Ganancia (antenas):**
  - **Es la capacidad de concentrar energía de una antena de forma eficiente.**
  - **Diferencia de energía en comparación con una antena isotrópica ideal.**
  - **Unidad utilizada: dBi**
  - **Cuanta mayor ganancia, más directiva es la antena.**
  - **La ganancia de la antena es la misma para recibir y retransmitir.**
  - **Ejemplo: Puntos de acceso:**
    - **Entre 2 y 5 dBi**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido, Energía irradiada:**
  - **Es la energía que es capaz de transmitir la tarjeta, menos las pérdidas en el cable más la ganancia de la antena.**
  - **Límite legal de energía irradiada para wireless son 100mW (20dBm) (PIRE).**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido:**

Ejemplo:

- **Tarjeta emisora, potencia: 32mW = 15 dBm**
- **Tarjeta receptora (sensibilidad: cuánta cantidad de señal es lo mínimo que puede recibir para distinguirla del ruido ambiente): -83 dBm**
- **Tenemos 98 dB's para "perder por el camino"**

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido:**

Lo = 32.5 + 20 log f (Mhz) + 20 log d (Km)

f = 2442 Mhz

d = 8 Km

Lo = 118 dB → Teníamos 98 dBs ;-(

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido:**

Pr = Pt – Lo + Gt + Gr

Añadimos dos antenas:

- **Antena emisora: 12 dBi (Gt)**
- **Antena receptora: 15 dBi (Gr)**

Pr = 15 dBm – 118 dB + 12 dBi + 15 dBi = -76 dBm

Sensibilidad = -83 dBm → La señal llega con un márgen de 7 dB

Antenas WiFi

- **Entendiendo los conceptos de Señal/Ruido:**
  - **SOM: Margen de Operación de Sistemas**
    - **> 15 dB: margen excelente**
    - **10-15 dB: margen recomendado**
    - **Cercano a 0: problemas de desconexiones, etc.**

En nuestro ejemplo: SOM = 7dB → un poco escaso

Vulnerabilidades en redes WiFi

- **Las redes WiFi tienen todos los problemas / fallos / vulnerabilidades de las redes cableadas.**
- **Además, tienen problemas adicionales relacionados con sus características inalámbricas:**
  - **Scanners de radio.**
  - **Radio jamming (DoS).**
  - **Flexibilidad vs Seguridad...**

Vulnerabilidades en redes WiFi

- **Vulnerabilidades.**
  - **Acceso: wardriving.**
  - **Cifrado WEP: Ataques FSM, KoreK, etc.**
  - **Ataques de Man-in-the-Middle: Rogue APs.**
  - **Vulnerabilidades en APs en modo "bridge": ARP Poisoning.**
  - **Ataques de Denegación de Servicio.**

Acceso a redes WiFi

- **Encontrar redes wireless:**
  - **Facilísimo.**
  - **Bastante divertido.**
  - **No es ilegal.**
  - **Hay muchas más de las que pensamos:**
    - **Hoteles.**
    - **Tiendas.**
    - **Despachos / Oficinas.**
    - **Aeropuertos.**

Acceso a redes WiFi

- **Encontrar redes wireless, material necesario:**
  - **Tarjeta wireless (modo Monitor).**
  - **PC / PDA ...**
  - **Sniffer.**
- **Material opcional:**
  - **GPS.**
  - **Antena direccional / omnidireccional.**
  - **Medio de transporte (coche, moto...).**
  - **Equipo electrógeno.**

Acceso a redes WiFi

- Encontrar redes wireless, pasos:
  1. Poner la tarjeta en modo monitor:
  2. Utilizar un sniffer que capture tramas 802.11b en modo monitor (http://www.personaltelco.net/index.cgi/WirelessSniffer)
  3. Salir a la calle

Acceso a redes WiFi

1. Poner la tarjeta en modo monitor:
   a. No todas las tarjetas son capaces de funcionar en modo monitor (más bien es problema del driver).
   b. La mayoría de sniffers configuran automáticamente la tarjeta en modo monitor.
   c. En Windows: utilizar software que sepa poner la tarjeta en modo monitor (netstumbler).
   d. En GNU/Linux:
      - Instalar wireless-tools / pcmcia-cs.
      - `iwpriv wlan0 monitor 1 1`.

Acceso a redes WiFi

1. Utilizar un sniffer que capture tramas 802.11b en modo monitor:
   a. Windows:
      - Netstumbler - Airopeek - AirLine
   b. GNU/Linux:
      - AirSnort - Kismet - Airtraf
   c. Mac OS X
      - iStumbler - KisMAC - MacStumbler
   d. Otros
      - MiniStumbler (PocketPC) - WiStumbler (BSD)

Acceso a redes WiFi

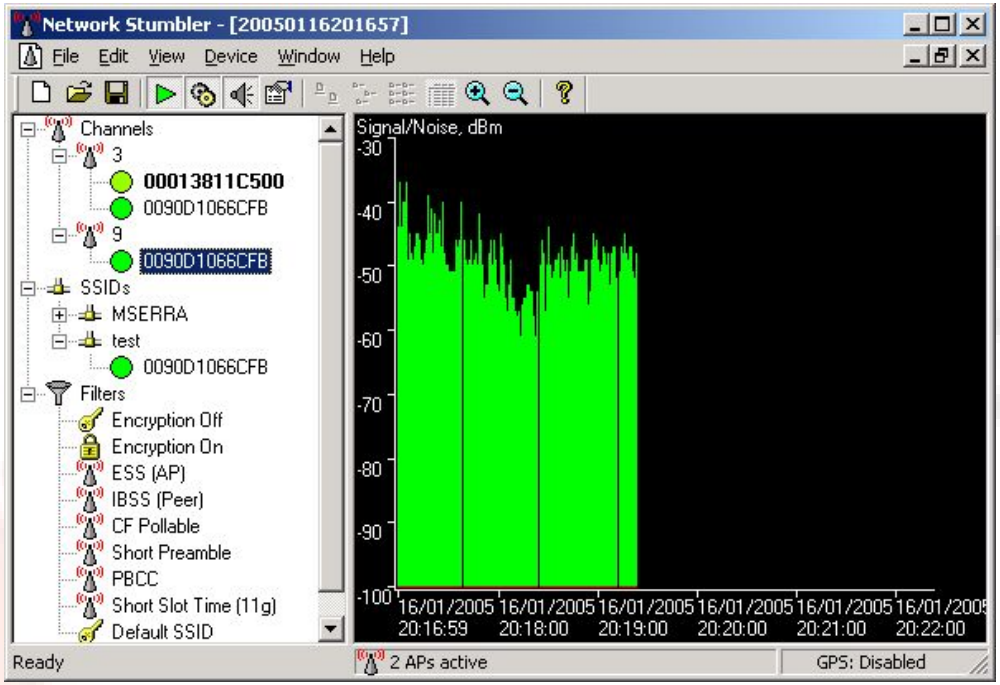
- **¿Es ilegal hacer WarDriving?**
  - **WiFi → ondas de radio en banda libre.**
  - **Espectro electromagnético troceado en regiones a nivel internacional (por la ITU, International Telecomunications Union).**
  - **Cada gobierno administra su región sin contravenir a la ITU → Cualquier transmisión radioeléctrica está regulada por la Dirección General de Telecomunicaciones.**
  - **La frecuencia WiFi (2.4 GHz) está reservada para uso público, cualquier dispositivo tiene que admitir interferencias inesperadas.**
  - **Es perfectamente legal transmitir "quiero ver http://www.nba.com" y esperar una respuesta.**

Acceso a redes WiFi

- **Herramientas para Microsoft Windows:**
  - **Netstumbler:**
    - **La más famosa.**
    - **Buen soporte de tarjetas.**
    - **http://www.netstumbler.com.**
  - **Airline:**
    - **En modo texto.**
    - **http://robota.net.**
  - **Aire.**
    - **En modo gráfico.**
    - **http://robota.net.**

Acceso a redes WiFi

- **Herramientas para Microsoft Windows:**
  - **Netstumbler:**



Acceso a redes WiFi

- **Herramientas para Microsoft Windows:**
  - **Airline:**

```
E:\WiFi>airline
AIRLINE - Wireless scanning application
(c) ROBOTA - http://www.robota.net
Usage: airline <device-index>
Available devices:
Index .... 1
Name ..... {5C5C1EB9-73BF-43F4-9E65-EF9EA2FD6A60}
Desc ..... Adaptador Ethernet PCI AMD PCNET Family
Key ...... SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\2

Index .... 2
Name ..... {F902BF24-4360-4B3B-AAA3-0520C5B81B80}
Desc ..... NETGEAR WG111 802.11g Wireless USB2.0 Adapter
Key ...... SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\9
```

Acceso a redes WiFi

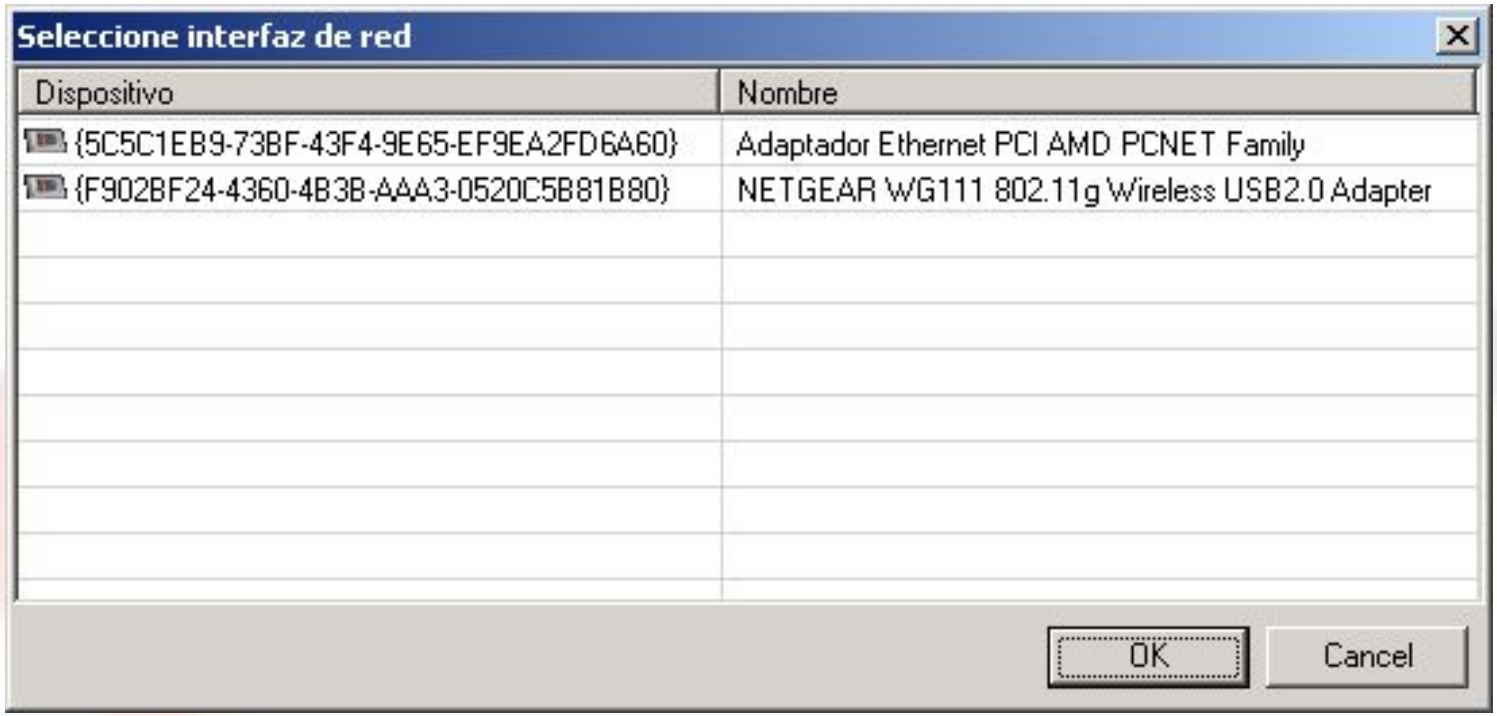
- **Herramientas para Microsoft Windows:**
  - **Airline:**

```
E:\WiFi>airline 2
AIRLINE - Wireless scanning application
(c) ROBOTA - http://www.robota.net
Selected device 2 (NETGEAR WG111 802.11g Wireless USB2.0
   Adapter)

Scanning... Press CTRL+C to terminate
[20:23][SSID:test][CH:2452000][WEP:NO][MODE:AP]
   [MAC:00:90:d1:06:6c:fb]
[20:23][SSID:][CH:16722][WEP:NO][MODE:PEER]
   [MAC:00:00:00:00:21:00]
```

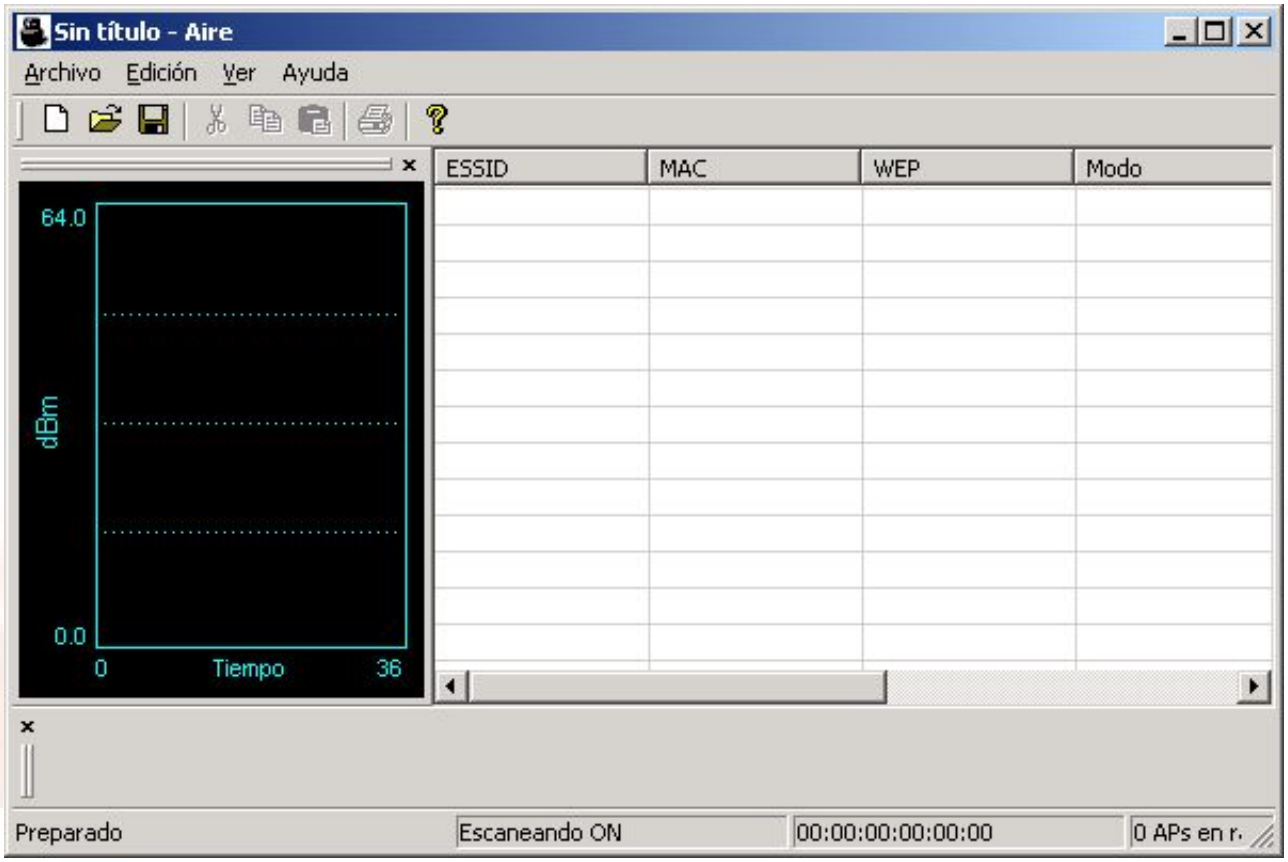
Acceso a redes WiFi

- **Herramientas para Microsoft Windows:**
  - **Aire:**



Acceso a redes WiFi

- **Herramientas para Microsoft Windows:**
  - **Aire:**



Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Kismet:**
    - **En modo texto.**
    - **Muy versátil y compatible con otros programas.**
  - **Airtraf:**
    - **En modo texto.**
    - **Muy sencillo de utilizar, similar al iptraf.**
  - **Airsnort:**
    - **En modo gráfico.**

Acceso a redes WiFi

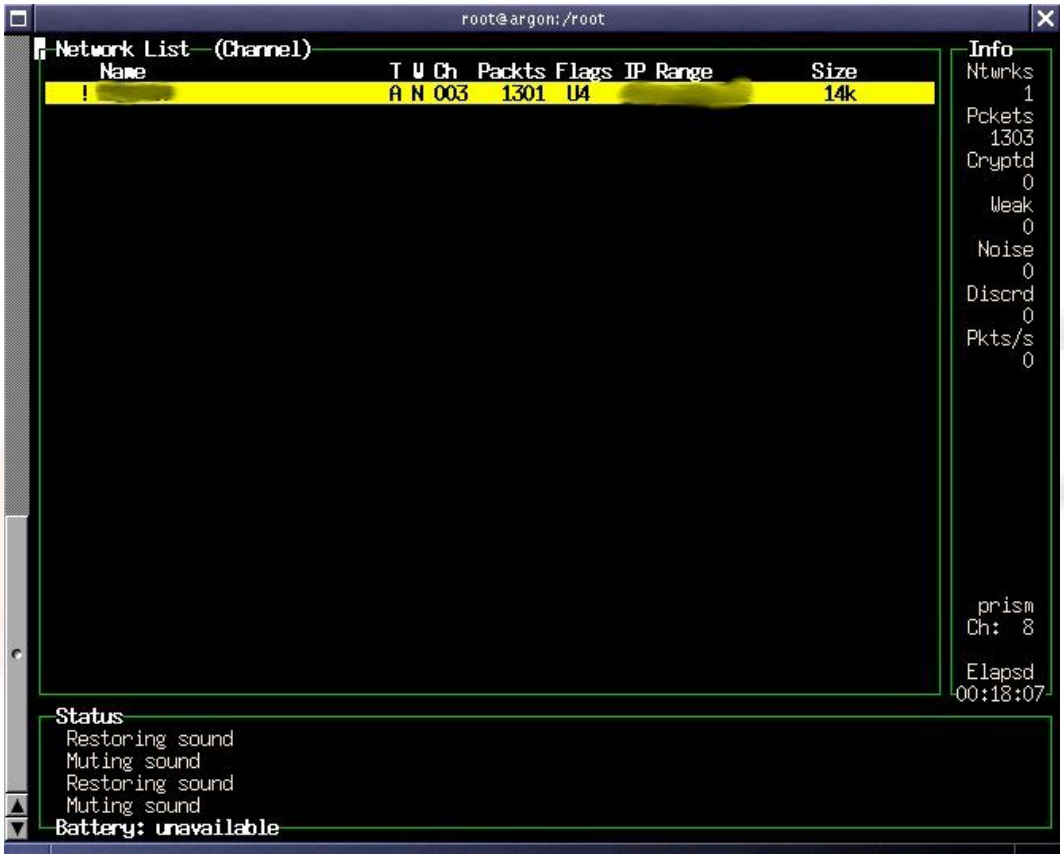
- **Herramientas para GNU/Linux:**
  - **Kismet:**
    - **Instalación:**
      - **apt-get install kismet**
      - **/etc/kismet/kismet.conf:**
        - » **suiduser=<cualquier cosa menos root>**
        - » **source=hostap,wlan0,prism**
        - » **logtemplate=/tmp/%n-%d-%i.%1**
    - **Ejecución:**
      - **# kismet**

Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Kismet:**
    - **Q: quit, salir de kismet.**
    - **q, volver al menú principal.**
    - **r, transfer rate, gráfica de la transmisión.**
    - **s, sort, ordenar por diferentes criterios.**
    - **i, network details, detalles de esa red.**
    - **p, packet types, paquetes que se capturan.**
    - **c, client list, lista de clientes.**
    - **d, dump, volcado de strings capturadas.**

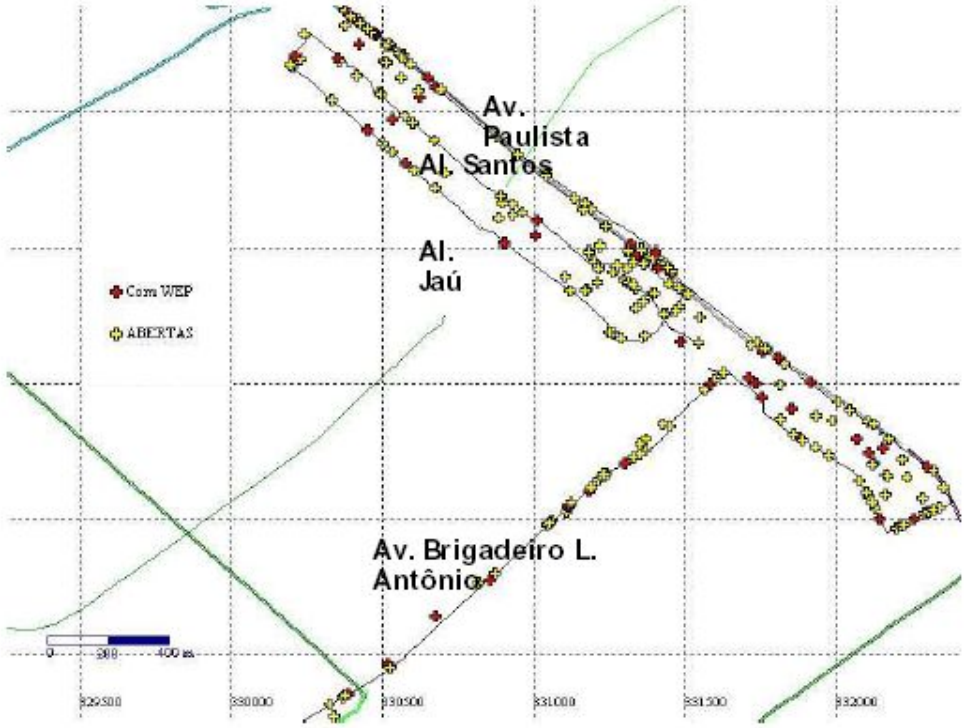
Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Kismet:**



Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Kismet + GPS: mapas de APs.**

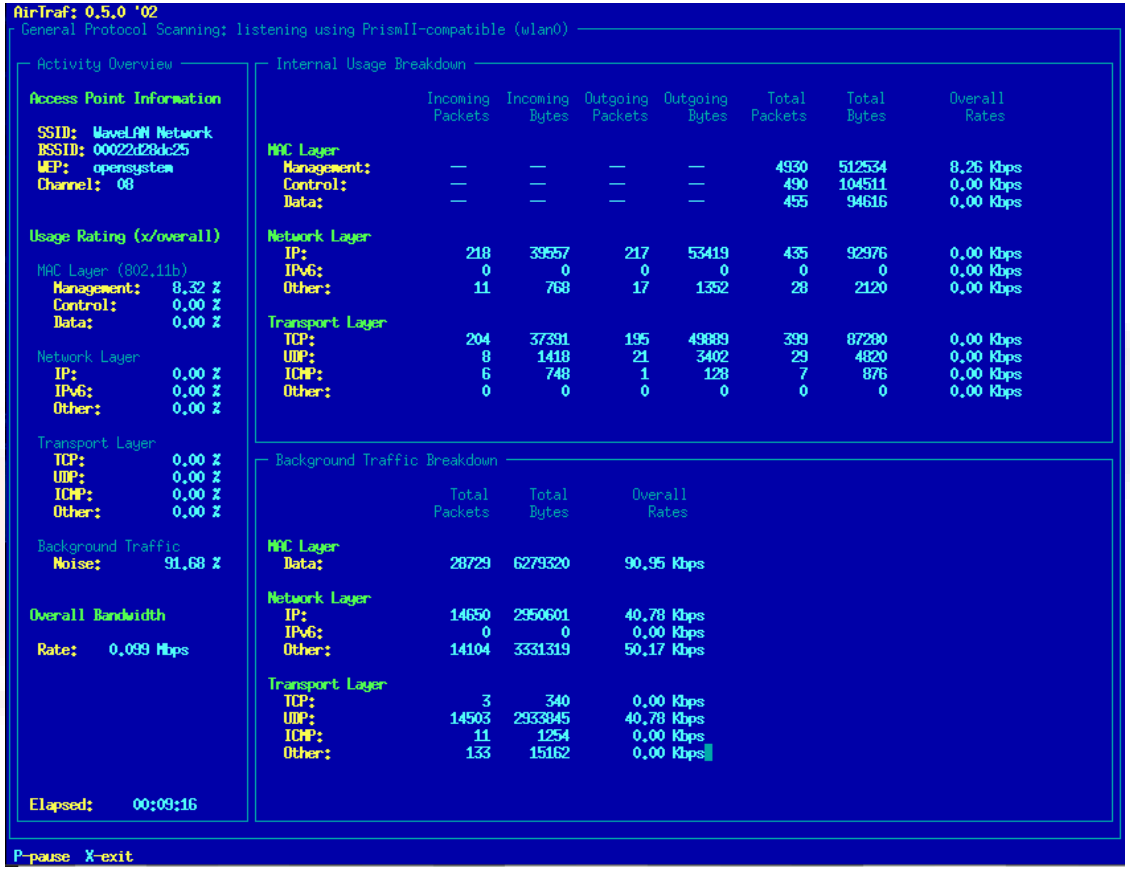


Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Airtraf:**
    - **Instalación:**
      - **Bajarlo de http://airtraf.sourceforge.net/download.php.**
      - **Compilar (make, make install).**
    - **Con versiones nuevas de HostAP da problemas:**
      - **HostAP crea wlan0 y wifi0 y no sabe cuál escoger.**
      - **El modo monitor de HostAP ha cambiado.**

Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Airtraf:**

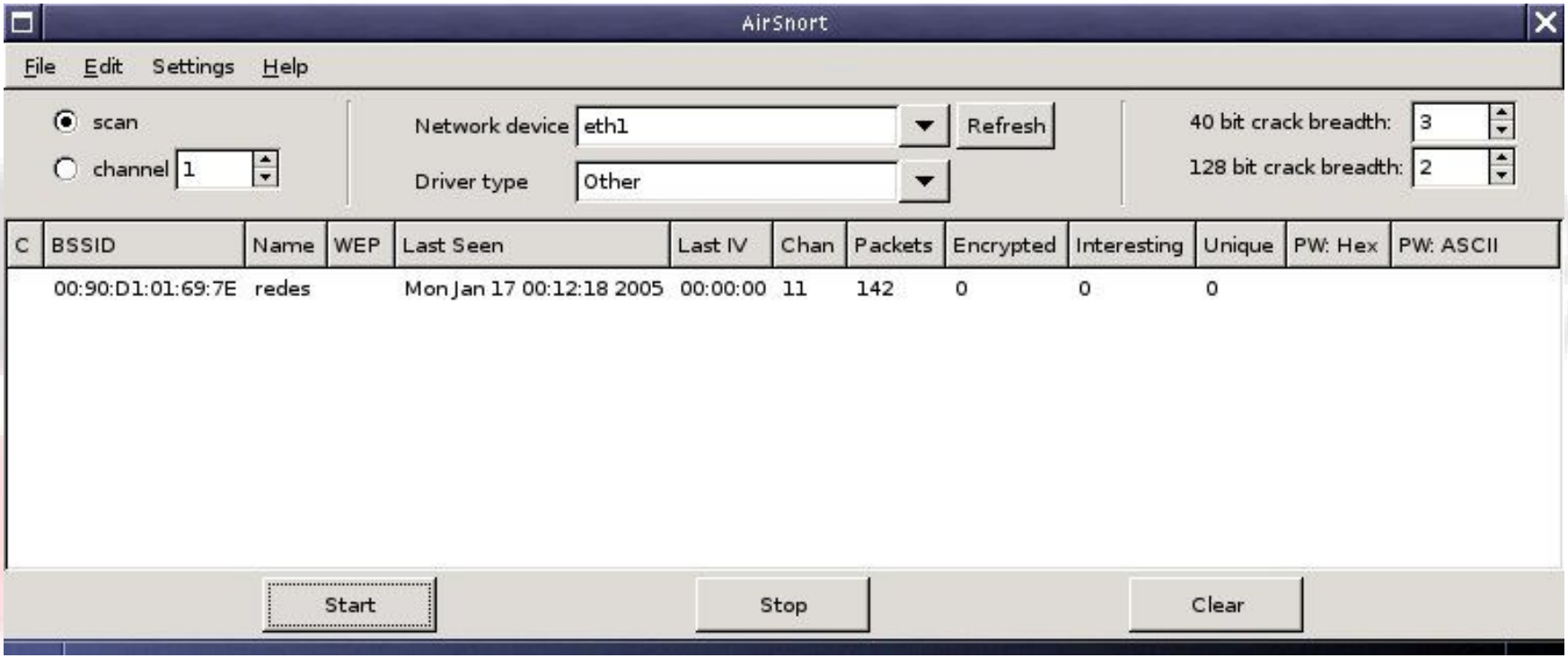


Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Airsnort:**
    - **Instalación: apt-get instalación airsnort.**
    - **En esta versión (0.2.7) no funciona con hostap (0.3.3).**
    - **Hay que bajarse los drivers nuevos de orinoco: http://www.ozlabs.org/people/dgibson/dldwd/orinoco-0.15rc1.tar.gz.**

Acceso a redes WiFi

- **Herramientas para GNU/Linux:**
  - **Airsnort:**



Autenticación en redes WiFi

- **Autenticación en WiFi, conceptos básicos:**
  - **WEP: Wired Equivalent Privacy:**
    Protocolo de encriptación basado en RC4.
  - **ESSID: Extended Service Set Identifier:**
    "Nombre" de la red. NO es un password.
  - **BEACON FRAMES:**
    Anuncios de la red emitidos por el AP.
    Normalmente contienen el ESSID.
  - **MANAGEMENT FRAMES:**
    Proceso de autenticación mutua y asociación.

Autenticación en redes WiFi

- **Medidas de seguridad utilizadas hasta ahora:**
  - **WEP:**
    - **Comunicación cifrada a nivel físico / enlace de datos.**
    - **Dificulta las cosas.**
  - **ACLs basados en IP y MAC:**
    - **El AP solo permite conectar a los clientes que “conoce”.**
  - **No emitir BEACON FRAMES e emitirlos sin el ESSID:**
    - **Si no sabemos el ESSID, no podremos conectarnos.**

Cifrado WEP

- **WEP.**
  - **Encriptación basada en RC4.**
  - **Utiliza llaves de 64, 128 y 256 bits.**

    (en realidad 40, 104 o 232 bits: IV = 24 bits).
  - **La llave se puede generar a partir de una passphrase o ser introducida directamente por el usuario.**
  - **La llave debe ser conocida por todos los clientes (secreto compartido).**

Vulnerabilidades en WEP

- **Algoritmo de integridad: características lineales CRC32**
  - **El ICV se calcula sólo haciendo un CRC32 del payload**
  - **Dos grandes problemas:**
    - **El ICV es independiente de la clave y del IV**
    - **Los CRC son lineales (CRC(m xor k) = CRC(m) xor CRC(k))**
    - **Mediante "bit-flipping" se podría regenerar un ICV válido para un mensaje modificado.**

Vulnerabilidades en WEP

- **Algoritmo de integridad: MIC independiente de la clave**
  - **No existe un Chequeo de Integridad del mensaje dependiente de la clave (el ICV es un CRC32 no dependiente de la clave).**
  - **Conocido el plaintext de un solo paquete sería posible inyectar a la red.**

Vulnerabilidades en WEP

- **Cifrado: Tamaño de IV demasiado corto**
  - **El IV mide 24 bits → 16.777.216 posibilidades**
  - **16 millones de tramas se generan en pocas horas en una red con tráfico intenso**
- **Cifrado: Reutilización de IV**
  - **Su corta longitud hace que se repita frecuentemente al generarse aleatoriamente.**
  - **Criptoanálisis estadístico.**
  - **El estándar dice que cambiar el IV en cada paquete es ¡opcional!.**

Vulnerabilidades en WEP

- **Cifrado: Vulnerabilidades de WEP posibilitan fuerza bruta**
  - **La passphrase suele ser un texto ASCII escribible → el bit de más peso es siempre 0 → reducimos el espacio de búsqueda de FF:FF:FF:FF a 7F:7F:7F:7F.**
  - **El generador pseudoaleatorio (PRNG) es un generador lineal congruente → los bits de menos peso son "menos aleatorios" → sólo las semillas de 00:00:00:00 a 00:FF:FF:FF producen llaves únicas.**
  - **¡¡Sólo necesitamos buscar hasta 00:7F:7F:7F!!**

Vulnerabilidades en WEP

- **Algoritmo de integridad: Ataque inductivo de Arbaugh**
  - **Se basa en:**
    - **Características lineales de CRC**
    - **MIC independiente de la clave**
  - **Necesitamos conocer una parte del texto cifrado → es fácil identificar un DHCP discover (origen 0.0.0.0, destino 255.255.255.255)**
  - **Creamos paquetes ICMP con la cantidad de texto capturada más un byte:**
    - **Si recibimos la respuesta, sabemos un byte más del keystream**
    - **Si no, probamos con otro (hay sólo 255 posibilidades)**

Vulnerabilidades en WEP

- **Cifrado: Debilidades en el algoritmo de Key Scheduling de RC4 (FMS)**
  - **Exiten IVs débiles (“resolved condition”):**
    - **Ausencia de información de un byte de la llave**
    - **Ese byte puede ser adivinado (probabilidad del 5%)**
  - **Cuando se han recolectado muchos IVs débiles, un análisis estadístico revela una tendencia hacia un valor concreto de cada byte de la llave**

Vulnerabilidades en WEP

- **Cifrado: Debilidades en el algoritmo de Key Scheduling de RC4 (FMS)**
  - **IV vulnerable:**
    - **El desarrollo de RC4 sólo afecta a bytes ya conocidos.**
    - **resolved condition: (A,B+3,X), no es necesario desarrollar RC4 (9000 de los 16.777.216 posibles).**
  - **Necesitamos capturar**
    - **de 1500 a 4000 IVs débiles.**
    - **de 5 a 10 millones de paquetes cifrados**
    - **de 5/6 horas a varios días**

Vulnerabilidades en WEP

- **Cifrado: Fluhrer-Mantin-Shamir (FMS):**
  - **Gran cantidad de paquetes “débiles” requerida.**
  - **Desde que en el verano de 2001 se publicara airsnort, los fabricantes fueron modificando el firmware de las tarjetas para hacerlas inmunes a este ataque.**
  - **Los nuevos firmwares parecen haberse olvidado de él y vuelven a ser vulnerables.**

Vulnerabilidades en WEP

- **Vulnerabilidades nuevas: KoreK's attacks**
  - **Estadísticos.**
  - **Requieren del orden de 500.000 paquetes (¡¡¡muchísimos menos que en el resto de ataques!!!), el resto del ataque se basa en análisis estadístico de los paquetes capturados.**
  - **Si se intenta con pocos IVs diferentes capturados, es prácticamente igual que fuerza bruta.**

Herramientas de cracking WEP

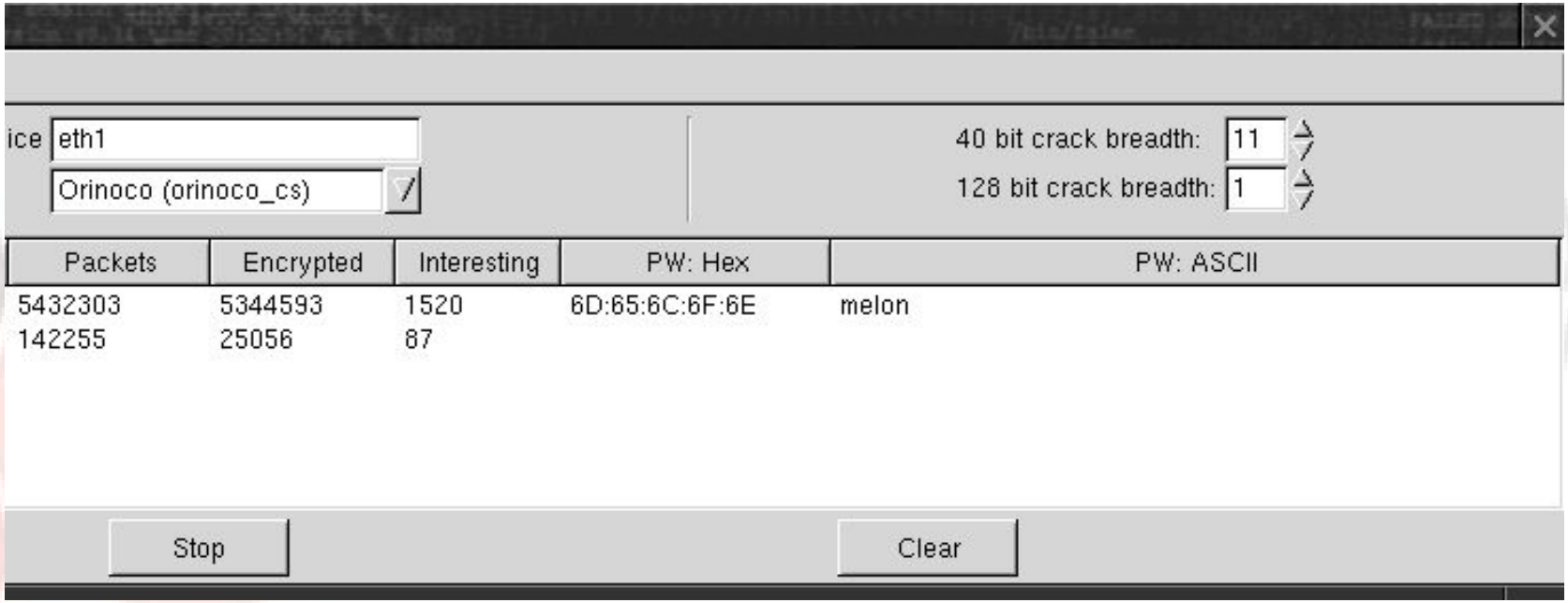
- **Herramientas para GNU/Linux:**
  - **Antiguas vulnerabilidades:**
    - **WepCrack.**
    - **Airsnort.**
  - **Nuevas vulnerabilidades (KoreK):**
    - **chopchop**
    - **Aircrack.**
    - **WepLab.**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **WepCrack:**
    - **Casi obsoleta, ataca solamente las vulnerabilidades más conocidas.**
    - **Scripts en Perl.**
    - **Ejecución:**
      - **pcap-getIV.pl –b 13 –f packets.pcap**
      - **WepCrack.pl**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Airsnort:**



Herramientas de cracking WEP

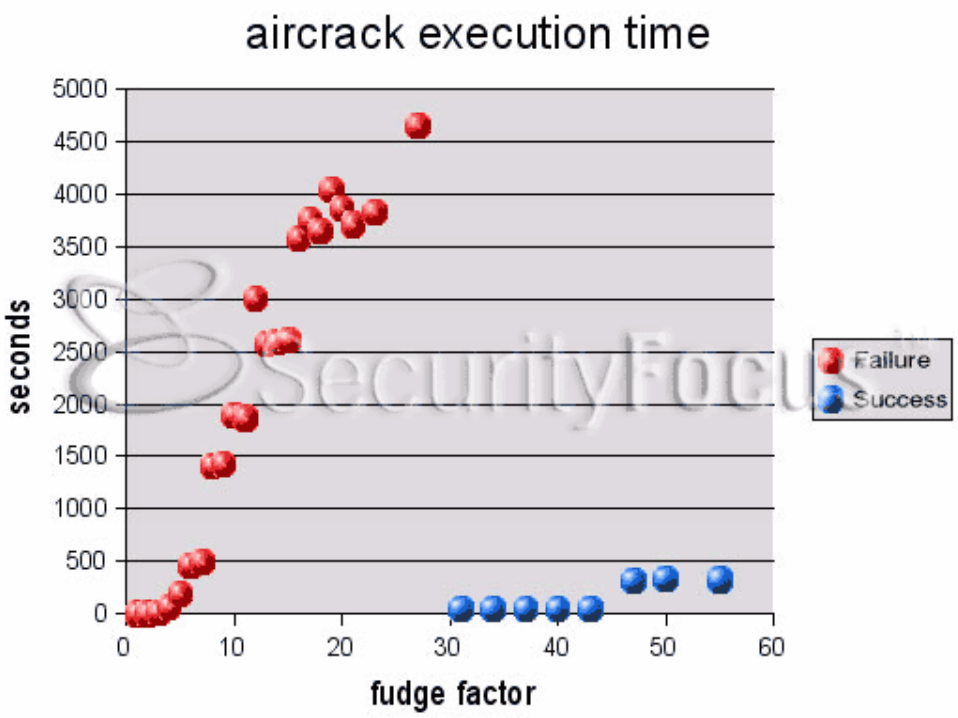
- **Herramientas para GNU/Linux:**
  - **Chopchop:**
    - **Se basa en utilizar el propio AP que se quiere atacar para ir generando paquetes cifrados correctamente, byte a byte.**
    - **Cuanto más complejo sea el paquete, más se tardará en adivinar que está formado correctamente.**
    - **Reinyecta paquetes a la red WiFi para que el AP genere nuevos IVs y sea más rápida la captura para su posterior crackeo (parchear host_ap o wlan-ng).**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Aircrack:**
    - **Ataques estadísticos: requiere capturar paquetes previamente para poder tener una muestra estadística válida:**
      - **WEP 64bits: 100.000 IVs.**
      - **WEP 128 bits: 500.000 IVs.**
    - **Uso:**
      - **airodump wlan0 wlan.pcap.**
      - **aircrack –f 4 –p 128 wlan.pcap.**

Herramientas de cracking WEP

- **Fudge factor: factor de desviación en el análisis estadístico (cuanto mayor es, más tiempo de ejecución, pero más posibilidades de acertar).**



Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Weplab:**
    - **No solamente ataca WEP con ataques estadísticos, también:**
      - **brute-force y brute-force restringido.**
      - **ataque mediante diccionario.**
    - **Programado por José Ignacio Sánchez, TopoLB, de Barakaldo, antiguo alumno de la Universidad de Deusto.**
    - **Con un GUI en wxpython en desarrollo.**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Weplab:**
    - **Instalación:**
      - **Compilar: ./configure && make && make install (requiere el paquete libpcap-dev).**
    - **Uso:**
      - **Captura**
      - **Análisis de la captura**
      - **Fuerza bruta**
      - **Diccionario**
      - **Estadísticos**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Weplab:**
    - **Uso, captura:**
      - **weplab –c –i wlan0 captura.pcap**
      - **weplab –c –i wlan0 --caplen 150 captura.pcap**
    - **Uso, análisis de la captura:**
      - **weplab –a captura.pcap**
      - **weplab –a --fcs captura.pcap**
      - **weplab –a --prismheader captura.pcap**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Weplab:**
    - **Uso, fuerza bruta:**
      - **weplab –b --key 64 captura.pcap**
      - **weplab –b --ascii --key 64 captura.pcap**
      - **Se necesitan por lo menos 10 paquetes capturados para hacer un ataque bruteforce sin falsos positivos.**
      - **El total de combinaciones para 128 bits son 2^14, así que a 100.000 c/s se tardaría más de 6 trillones de años.**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Weplab:**
    - **Uso, diccionario:**
      - **john -w:words.txt -rules -stdout | weplab -y --key 64 captura.pcap**
      - **john -w:words.txt -rules -stdout | weplab -y --key 64 --attacks 1 captura.pcap**
      - **john -w:words.txt -rules -stdout | weplab -y --key 64 --attacks 2 captura.pcap**

Herramientas de cracking WEP

- **Herramientas para GNU/Linux:**
  - **Weplab:**
    - **Uso, estadísticos:**
      - **weplab --key 128 –r ./captura.pcap**
      - **weplab --debugkey 01:02:03:04:05:06:07:08:09:10:11:12:13--key 128 –r ./ captura.pcap**
      - **weplab --key 128 --fcs –r ./captura.pcap**
      - **-perc: % success ~= fudge factor de aircrack**

Herramientas de cracking WEP

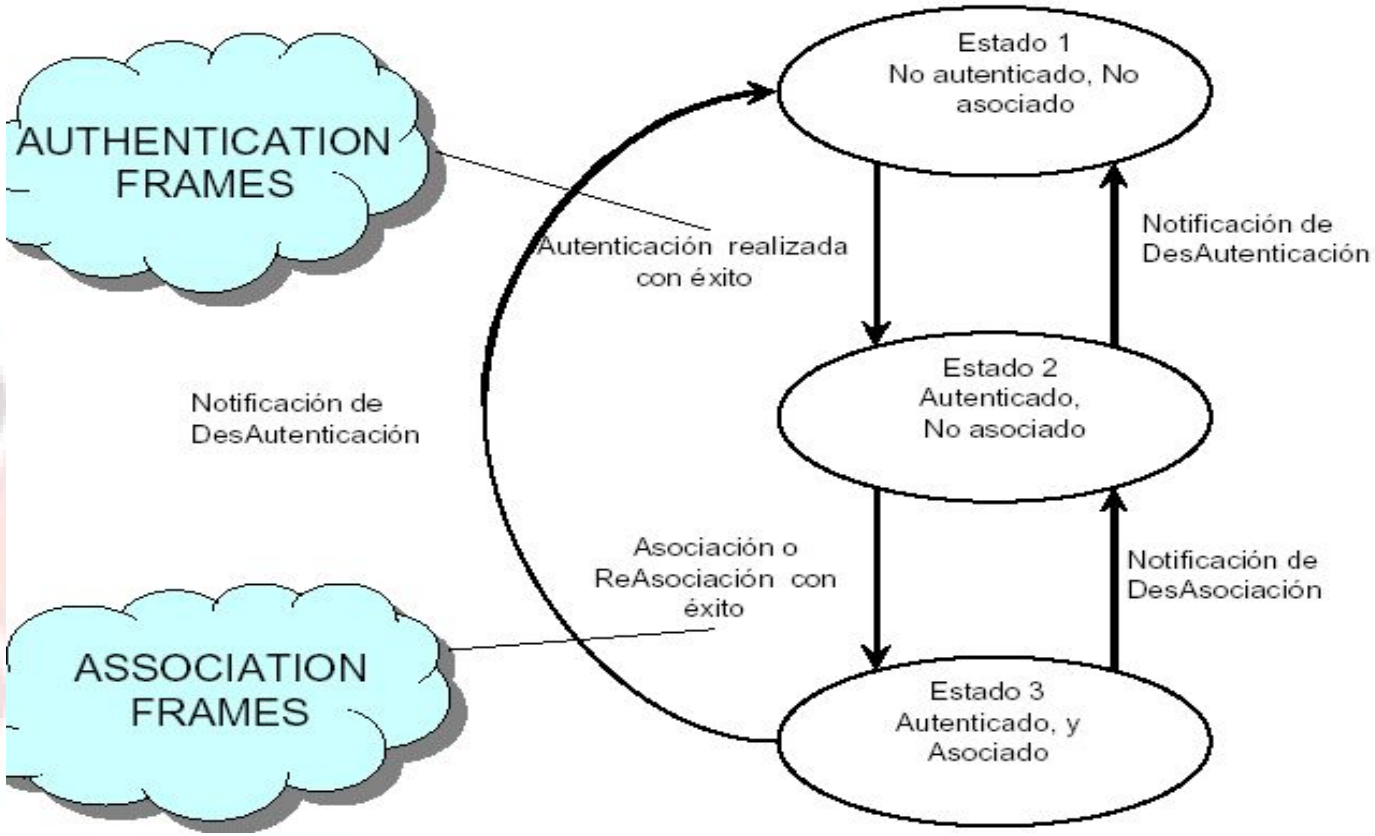
- **Mejora MUY sustancial en tiempo y MB capturados utilizando inyectores de paquetes:**
  - **Parcheo de host_ap y / o wlan-ng.**
  - **Aircrack: aireplay.**
  - **Airpwn.**
  - **Airjack.**

Autenticación en redes WiFi

- **Proceso de conexión de un cliente a una red wireless:**
  - **Los APs emiten BEACON FRAMES cada cierto intervalo fijo de tiempo.**
  - **Los clientes escuchan estos BEACON FRAMES e identifican al AP**
    - **El cliente también puede enviar una trama "PROVE REQUEST" con un determinado ESSID para ver si algún AP responde.**

Autenticación en redes WiFi

- **Autenticación y asociación :**



Autenticación en redes WiFi

- **Métodos de autenticación típicos:**
  - **Open System Authetication**
    - **Protocolo de autenticación por defecto**
    - **Es un proceso de autenticación NULO:**
      - **Autentica a todo el que pide ser autenticado**
      - **Las tramas se mandan en texto plano aunque esté activado WEP**
  - **Shared Key Authentication**
    - **Protocolo cifrado de autenticación con WEP**
    - **Vulnerabilidades propias de WEP**
  - **802.1x**

Vulnerabilidades en filtrado

- **Romper filtros basados en IPs o MACs**
  - **Sniffer para conseguir una lista de MAC válidas (White List)**
  - **Dos opciones:**
    - **Esperar a que una de ellas deje de transmitir**
    - **Tirar a una de ellas con un DoS y utilizar esa MAC**
  - **Modificar la MAC**
    - **Windows: Propiedades de la tarjeta**
    - **GNU/Linux: `ifconfig eth1 hw ether MAC`**

Vulnerabilidades en filtrado

- **Establecer filtros basados en MACs**
  - **`iwpriv wlan0 maccmd <0,1,2,3,4>`**
    - **`0: open policy`**
    - **`1: allow`**
    - **`2: deny`**
    - **`3: flush ACL`**
    - **`4: kick all`**
  - **`iwpriv wlan0 addmac MAC`**
  - **`iwpriv wlan0 delmac MAC`**
  - **`iwpriv wlan0 kickmac MAC`**

Vulnerabilidades en APs

- **Descubrir ESSID ocultados**
  - **Algunos administradores entienden el ESSID como una contraseña (erroneo)**
  - **No emiten BEACON FRAMES o los emiten sin el ESSID**
  - **Cuando un cliente se conecta, vemos el ESSID en la trama PROVE REQUEST**
    - **Podemos esperar**
    - **Podemos desconectar a un cliente (DoS)**

Vulnerabilidades en APs

- **Ocultar ESSID**
  - **Es necesario tener una versión del firmware 1.6.3 o superior en la tarjeta (mirar dmesg).**
  - **Ocultar:**
    - **iwpriv wlan0 enh_sec 1**
  - **Para actualizar el firmware de la tarjeta:**
    - **http://linux.junsun.net/intersil-prism/**

Vulnerabilidades en APs

- **Ocultar ESSID: FakeAP**
  - **Script en perl que envía beacons con diferentes ESSID y diferentes direcciones MAC a la red con o sin wep utilizando el driver hostap.**
  - **No es un AP válido sino uno falso que no sirve para dar servicio.**
  - **Requisitos: Tener una máquina con hostap al menos del 31/7/2002 instalado y funcionando.**

Vulnerabilidades en APs

- **Ocultar ESSID: FakeAP**
  - **Instalación:**
    - **Descargar, descomprimir y desempaquetar: http://www.blackalchemy.to/project/fakeap/**
    - **Instalar los módulos de Perl requeridos (Getopt::Long, Time::HiRes):**

      # perl -MCPAN -e shell

      cpan> install nombre::modulo

Vulnerabilidades en APs

- **Ocultar ESSID: FakeAP**
  - **Uso:**

```
# ./fakeap.pl --interface wlan0 --channel 10 -words lists/stefan-wordlist.txt --sleep 2
   -vendors lists/stefan-maclist.txt -power 15
fakeap 0.3.1 - Wardrivring countermeasures
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved
Using interface wlan0:
Sleeping 2 sec
Static channel 10
Generating ESSIDs from lists/stefan-wordlist.txt
Vary Tx power up to 15
Using 53068 words for ESSID generation
Using 20 vendors for MAC generation
------------------------------------------------------------------------
3: ESSID=pompey chan=10 Pwr=12 WEP=N MAC=00:04:E2:39:31:F3
4: ESSID=straub chan=10 Pwr=1 WEP=N MAC=00:02:2D:C0:B2:35
7: ESSID=galois chan=10 Pwr=14 WEP=N MAC=00:80:0F:5F:B7:1E
------------------------------------------------------------------------
Run complete
```

Ataques de Denegación de Servicio

- Configurar nuestra tarjeta en modo Master y con la MAC del AP (con un sniffer)
- Enviar tramas de desasociación:

```
while true; do iwpriv wlan0 kickmac MAC; done
```

- Ataque DoS masivo:

```
while true; do iwpriv wlan0 maccmd 4; done
```

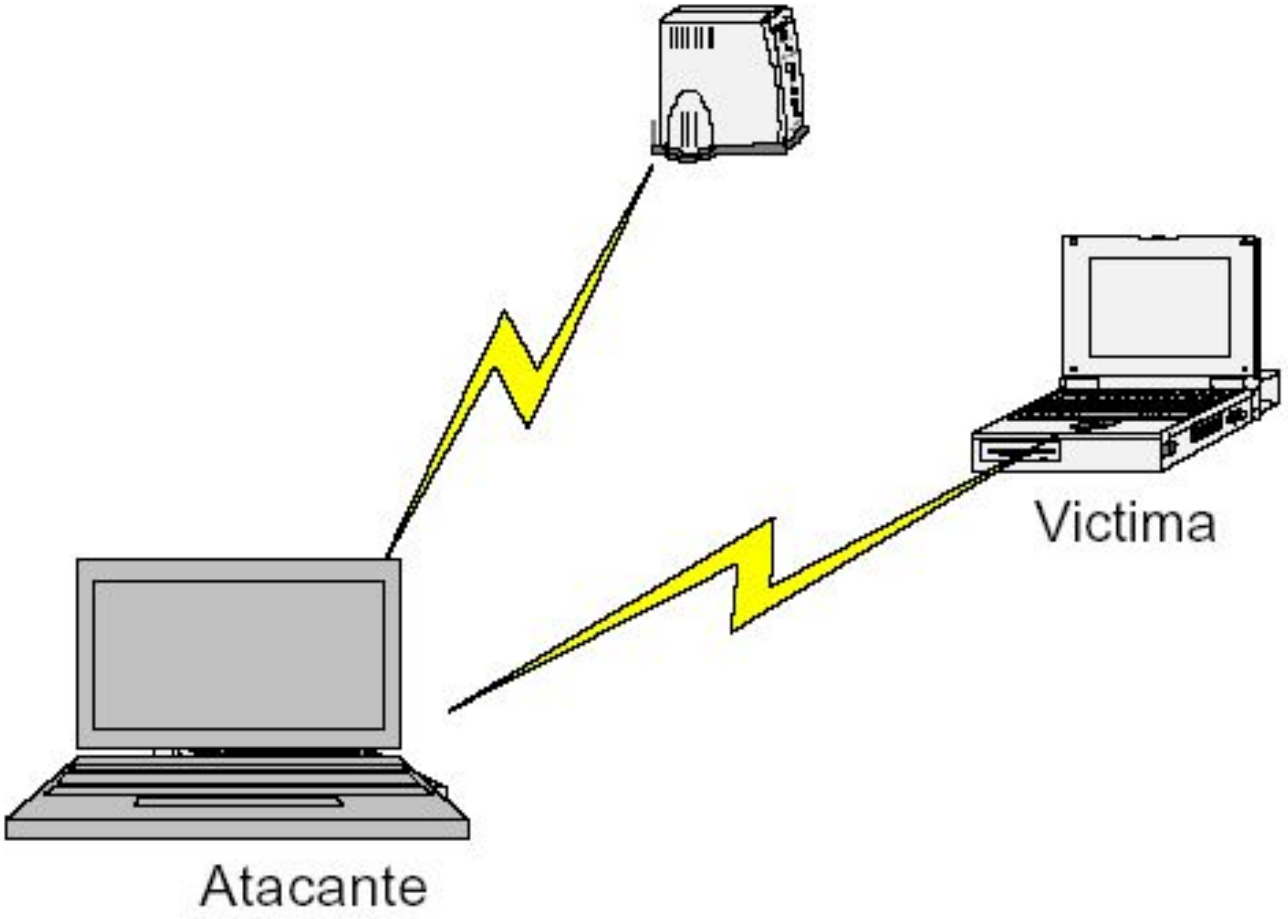
Ataques de Denegación de Servicio

- Ataques contra la capa física/enlace de datos de 802.11:
  - CSMA/CA: Colission Avoidance.
  - CCA: Clear Channel Assessment.
  - Emitiendo CCAs nulos negamos que ningún canal esté libre tanto para APs como para clientes.

Ataques Man-in-the-Middle

- Dos tarjetas WiFi
  - Con una nos hacemos pasar por el AP
  - Con la otra nos hacemos pasar por la victima
- Enviamos una trama DEAUTH a la víctima para que busque un AP al que conectarse
- Hacemos creer a la víctima que somos el AP original, pero operando en otro canal
- Nos conectamos al AP original con la otra tarjeta, haciéndonos pasar por la víctima

Ataques Man-in-the-Middle



Ataques Man-in-the-Middle

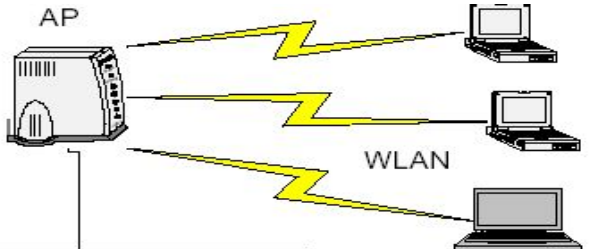
- El ataque ha sido realizado a nivel de enlace: se tiene control sobre todas las capas superiores.
- Muchas soluciones de seguridad presuponen que la capa física y de enlace son seguras.
- Cuidado con implementaciones de VPNs que presuponen esto.

Vulnerabilidades: AP en modo bridge

- **Ataques de ARP Poisoning**
  - **Objetivo: envenenar la caché ARP para redirigir el tráfico de una LAN hacia nuestra situación**
  - **Sólo se puede hacer cuando el atacante está en la misma "LAN lógica":**
    - **Hubs, bridges y switches (pero no routers).**
    - **¡La mayoría de APs funcionan como bridges!**

Vulnerabilidades: AP en modo bridge

- **Ataques de ARP Poisoning**



PC 1
192.168.1.1

PC 2
192.168.1.2

PC 3
192.168.1.3

Tabla ARP – PC 1

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.3	3C:2A:4A:59:1A:7A

Tabla ARP – PC 3

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.1	6A:8F:5E:99:2B:78

Tabla ARP – PC 2

Dirección IP	Dirección MAC
192.168.1.1	6A:8F:5E:99:2B:78
192.168.1.3	3C:2A:4A:59:1A:7A

Vulnerabilidades: AP en modo bridge

- **Ataques de ARP Poisoning**

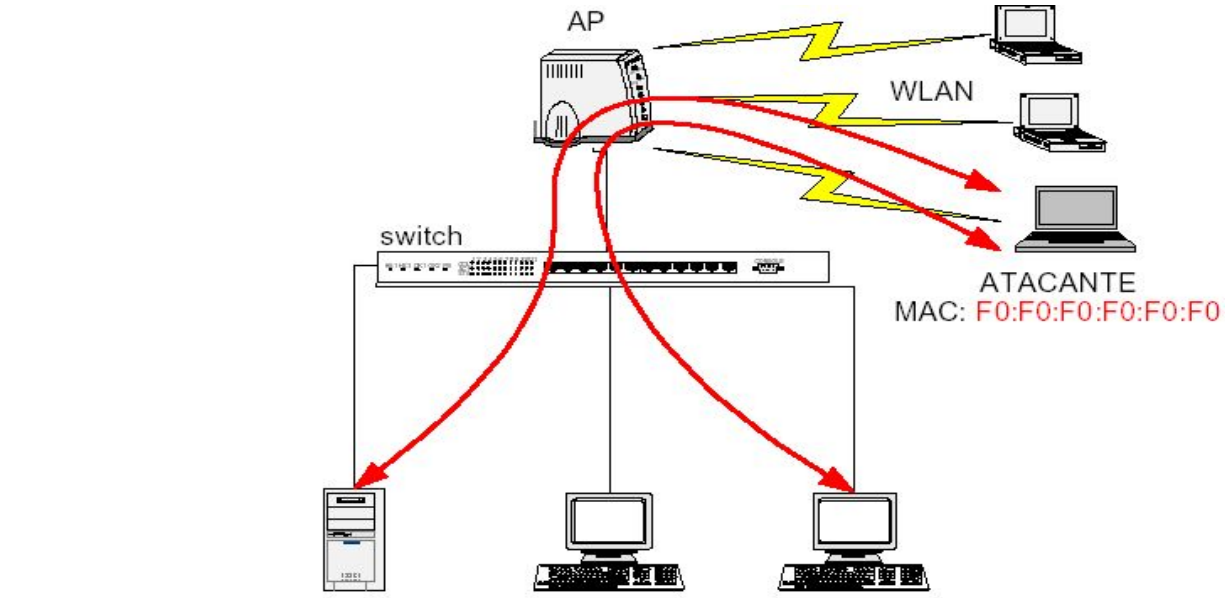


Tabla ARP – PC 1

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.3	F0:F0:F0:F0:F0:F0

Tabla ARP – PC 3

Dirección IP	Dirección MAC
192.168.1.2	3B:AF:44:F8:2C:B3
192.168.1.1	F0:F0:F0:F0:F0:F0

Tabla ARP – PC 2

Dirección IP	Dirección MAC
192.168.1.1	6A:8F:5E:99:2B:78
192.168.1.3	3C:2A:4A:59:1A:7A

Soluciones de seguridad WiFi

- Soluciones “antiguas”:
  - WEP:
    - 64 bit
    - 128 bit
    - 256 bit
  - Shared Key Authentication
  - Filtros por IP o por MAC
  - Ocultar ESSID

¡TODAS VULNERABLES!

Soluciones de seguridad WiFi

- **Soluciones actuales:**
  - **Portales cautivos**
  - **802.1x**
  - **WPA (WEP2)**
  - **802.11i (WPA 2)**

Portales Cautivos

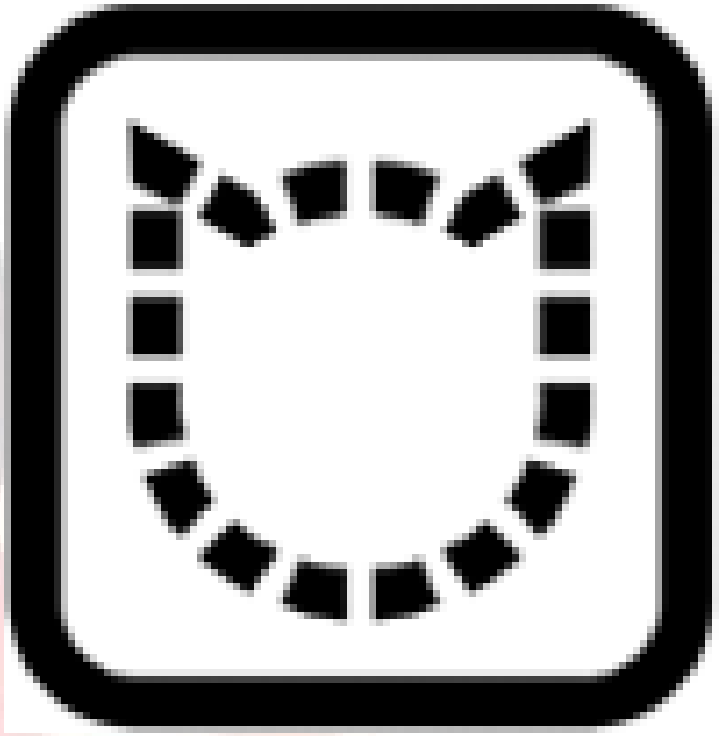
- Sistema de validación de clientes para nodos wireless.
- Según el tipo de usuario asigna ancho de banda y da acceso a servicios diferentes.
- Basado normalmente en “tokens” temporales gestionados por HTTP-SSL (443/TCP).

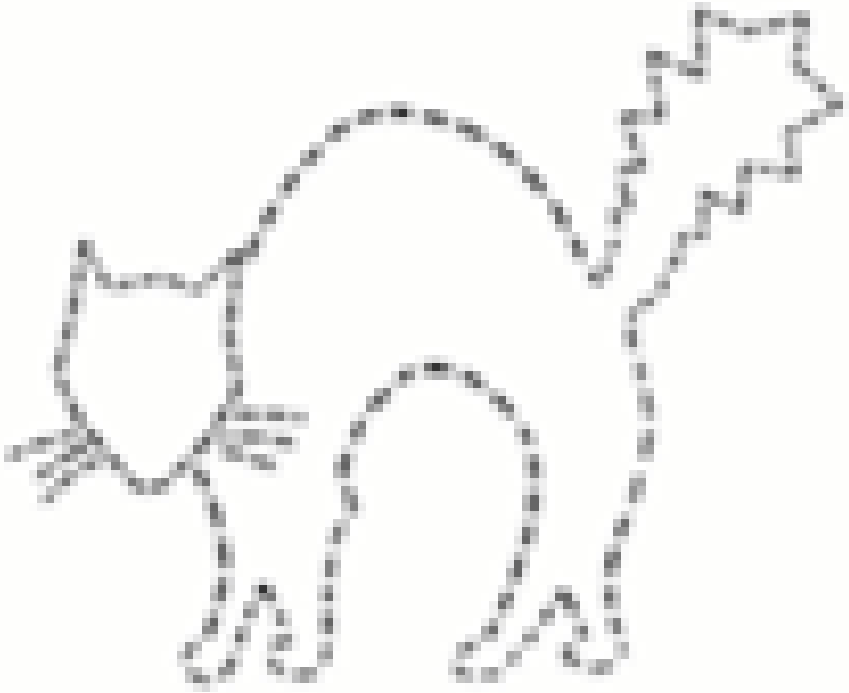
Portales Cautivos

- Diferentes implementaciones:
  - NoCat Auth: http://nocat.net
  - LANRoamer: http://www.lanroamer.net
  - Wireless Heartbeat: http://www.river.com/tools/authhb/
  - NetLogon - Linköping University
  - FisrtSpot (PatronSoft): http://www.patronsoft.com/firstspot/
  - WiCap (OpenBSD): http://www.geekspeed.net/wicap/

Portales Cautivos

- **NoCat:**





Portales Cautivos

- **NoCat:**
  - **Lo desarrolla la comunidad wireless de Sonoma County -Schuyler Erle-, California (E.E.U.U.).**
  - **Colaboran SeattleWireless, PersonalTelco, BAWUG, Houston WUG además de personas y grupos de todo el mundo.**

Portales Cautivos

- **NoCat, Características:**
  - **Autenticación segura basada en SSL (navegador).**
  - **Autoriza mediante usuario contraseña.**
  - **Informa de la entrada y salida del usuario en la red.**
  - **Añade la implementación de QoS por usuarios y grupos.**

Portales Cautivos

- **NoCat, Modos de funcionamiento:**
  - **Captive Portal (Portal Cautivo):**
    - **Captura las peticiones de usuarios a una web.**
    - **Comprueba las credenciales del usuario y máquina contra una base de datos.**
    - **Login obligatorio para el usuario.**
    - **Mantiene la sesión mientras está autenticado.**

Portales Cautivos

- NoCat, Modos de funcionamiento:
  - Passive Portal:
    - Como Captive pero se usa cuando hay un Firewall entre el AP y el gateway NoCat.
  - Open Portal:
    - Simplemente muestra una web con las condiciones de uso, no requiere credenciales.

Portales Cautivos

- **NoCat, Componentes:**
  - **NoCat Auth: Servicio de autenticación.**
  - **NoCat Gateway: Servicio de redirección y firewall.**
  - **Auth Database: Fichero propio (MD5), Base de Datos, Ldap, Radius, PAM, Samba, IMAP.**
  - **Access Point.**

Portales Cautivos

- **NoCat, Proceso de autenticación:**
  1. **El cliente se asocia con un AP y le asigna una IP.**
  2. **El AP reenvía las peticiones al gateway.**
  3. **El gateway redirige a la página de login del Auth Server:**

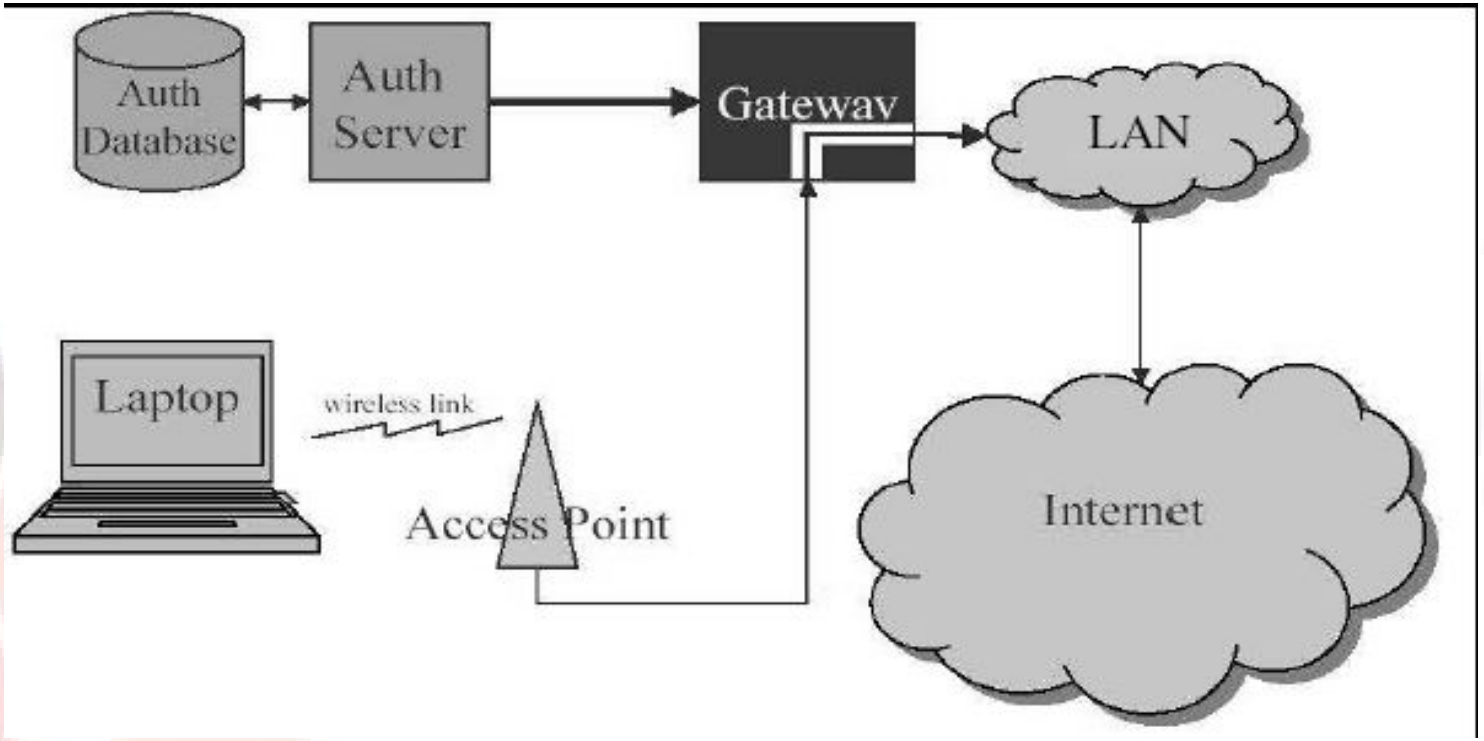
     iptables -t nat -A PREROUTING -s 10.10.21.0/24 -p tcp --dport 80 –j REDIRECT -d 10.10.21.2 --to-port 443
  4. **La conexión es autenticada vìa SSL.**

Portales Cautivos

- **NoCat, Proceso de autenticación:**
  1. **El Auth Server pide usuario y contraseña al cliente (via SSL) y la comprueba con la Auth Database.**
  2. **Los mensajes de autorización van firmados con PGP/GnuPG, el gateway utiliza la clave pública del Auth Server.**
  3. **Si la autenticación ha sido satisfactoria, el gateway redirige el tráfico a la LAN y/o Internet.**

Portales Cautivos

- **NoCat, Proceso de autenticación:**



Portales Cautivos

- NoCat, Necesidades del cliente:
  - Navegador (Mozilla, Netscape, Opera, Galeon, Konqueror o MSIE) con soporte SSL.
    - Independiente del SO.
    - No necesita plugins.
- Tarjeta wireless.
- Cuenta de acceso (para Captive Mode).

Portales Cautivos

- NoCat, Necesidades en el servidor:
  - Servidor web (Apache)
  - OpenSSL.
  - GnuPG.
  - Perl y modulos de perl correspondientes.
  - Servidor DNS.
  - Servidor DHCP (en el AP o en el gateway).
  - Servidor para centralizar cuentas de usuarios.

Portales Cautivos

- **NoCat, Ventajas:**
  - **Autenticación (en modo Captive).**
  - **Administración sencilla.**
  - **Traffic Shaping (QoS con CBQ).**
  - **User Friendly: aprendizaje rápido y fácil para los usuarios.**
  - **Bajo coste.**
  - **Software Libre: modificar según necesidades.**

Portales Cautivos

- NoCat, Inconvenientes:
  - Comunicación no cifrada (por defecto).
  - Implementar VPN: el cliente necesita software específico.
  - Spoofing y hi-jacking mientras dura el token temporal.

Portales Cautivos

- **NoCat, Requisitos:**
  - **Linux 2.4 ó 2.6 con soporte para iptables.**
  - **gpgv, verificador PGP incluido en la suite GnuPG.**
  - **Servidor DNS local.**
  - **Servidor DHCP opcional.**
  - **QoS: tc de iproute2.**
  - **Requisitos del AuthService.**

Portales Cautivos

- NoCat, Requisitos del AuthService:
  - Un servidor web con soporte SSL (apache + mod_ssl) con un certificado SSL.
  - Perl 5 (5.6 o superior recomendado).
    - Módulos Perl:
      - Digest::MD5
      - DBD::MySQL
  - GnuPG.
  - Servidor MySQL recomendado.

Portales Cautivos

- **NoCat, Instalación:**
  - **Descargarlo de http://nocat.net.**
  - **Descomprimir.**
  - **Compilar e instalar:**
    - **Gateway.**
    - **AuthService.**

Portales Cautivos

- NoCat, Instalación:
  - Gateway:
    - Compilar: make gateway.
    - Editar /usr/local/nocat/nocat.conf.
    - Arrancar gateway: /usr/local/nocat/bin/gateway.
  - AuthService:
    - Compilar: make authserv && make pgpkey.
    - Editar /usr/local/nocat/nocat.conf (datasource).
    - Crear back-end de usuarios (fichero, MySQL, etc.).
    - Comprobar permisos.
    - Recargar servidor web con SSL.

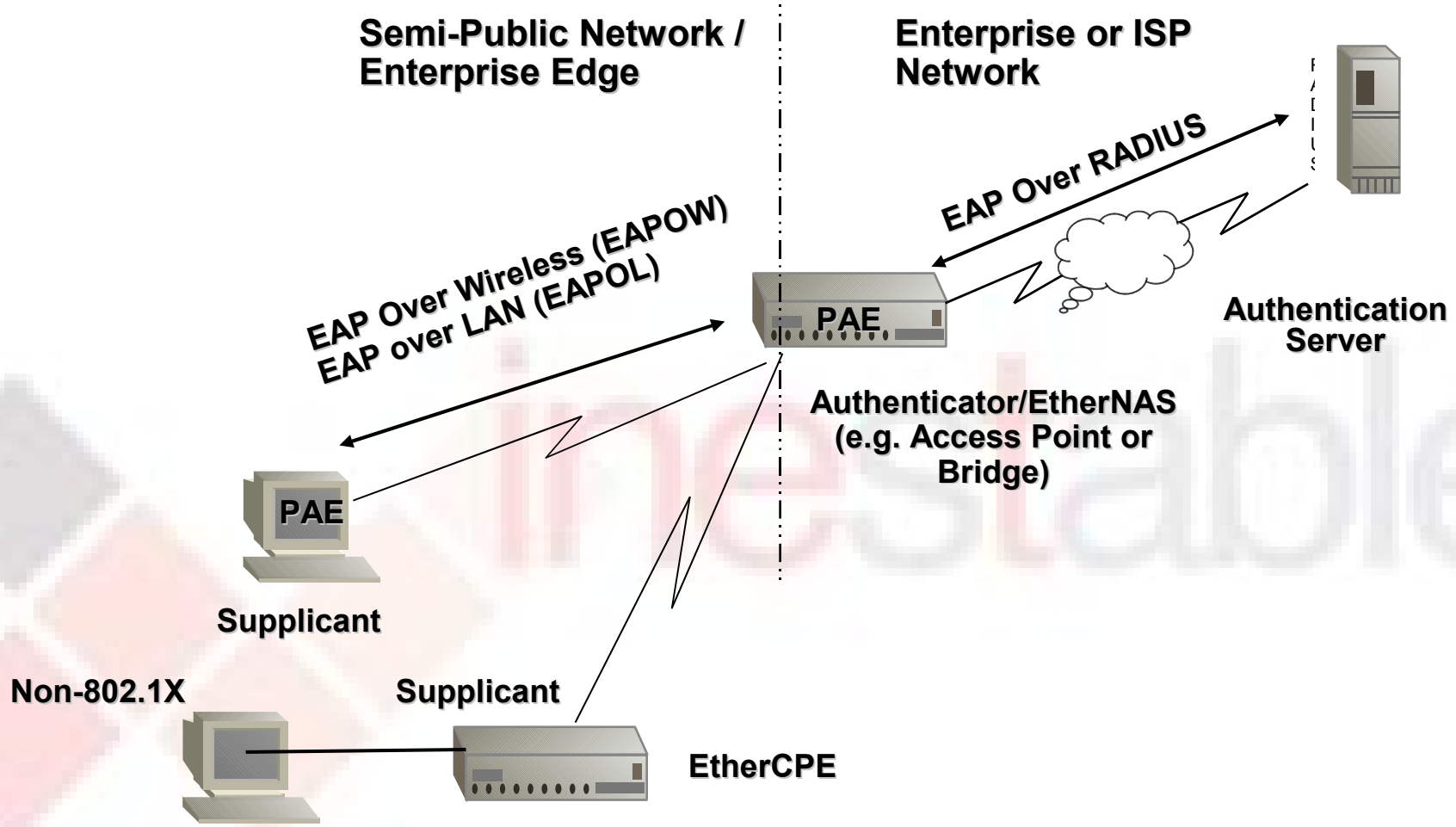
Soluciones de seguridad WiFi

- **Mejoras con nuevos protocolos:**
  - **Control de acceso al medio: autenticación.**
    - **Tecnologías y estándares:**
      - **802.1x.**
      - **EAP y derivados.**
      - **RADIUS.**
  - **Seguridad de los datos: cifrado.**
    - **Tecnologías y estándares:**
      - **AES.**
      - **CCMP.**
      - **Michael.**

802.1x

- Mecanismo estándar para autenticar centralmente estaciones y usuarios.
- No es específico de redes inalámbricas, originariamente se pensó para cableadas.
- Estándar abierto, soporta diferentes algoritmos de encriptación.
- Proporciona la base para un control de acceso a nivel superior (EAP).

802.1x

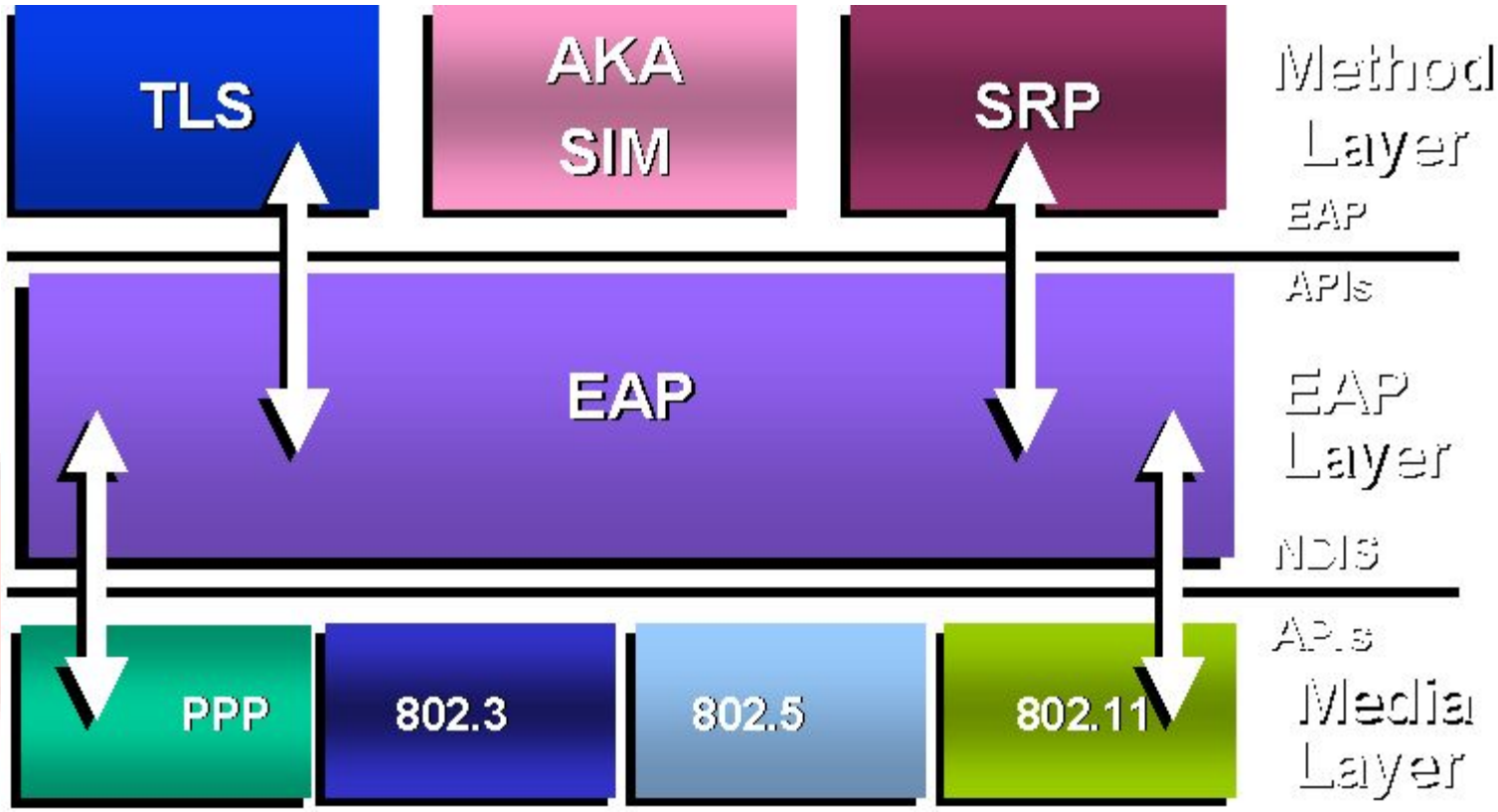

Semi-Public Network /
Enterprise Edge
Enterprise or ISP
Network
EAP Over RADIUS
EAP Over Wireless (EAPOW)
EAP over LAN (EAPOL)
PAE
Authentication
Server
Authenticator/EtherNAS
(e.g. Access Point or
Bridge)
PAE
Supplicant
Non-802.1X
Supplicant
EtherCPE

802.1x

- **EAP:**
  - **Extensible Authentication Protocol.**
  - **Proporciona un método flexible y ligero de control de acceso a nivel de enlace.**
    - **No depende de IP.**
    - **ACK/NAK.**
    - **Puede trabajar sobre cualquier capa de enlace.**
    - **No asume una capa física segura.**

802.1x

- **EAP:**


TLS
AKA
SIM
SRP
Method
Layer
EAP
APIs
EAP
EAP
Layer
NDIS
APIs
PPP
802.3
802.5
802.11
Media
Layer

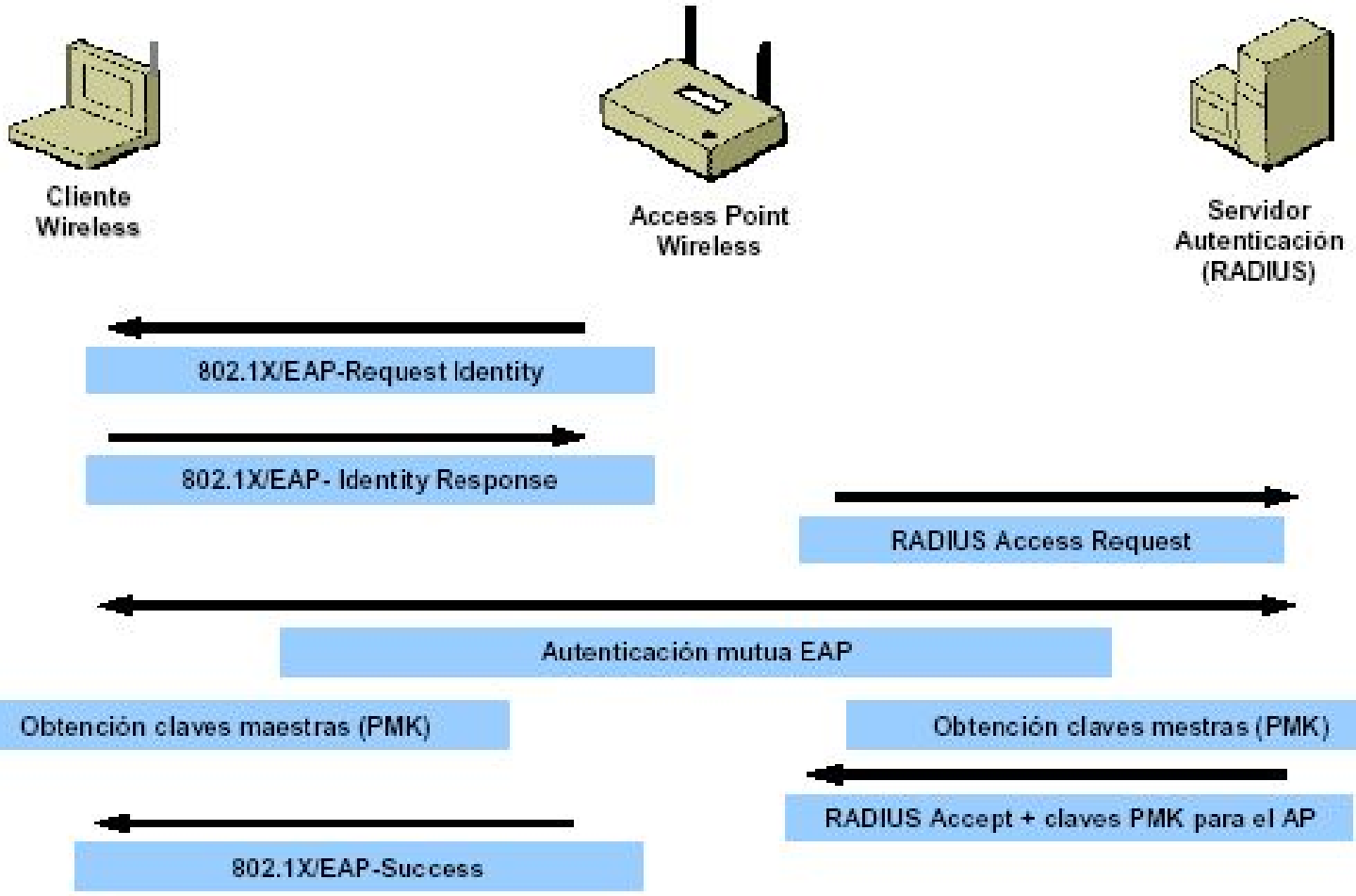
802.1x

- **EAP:**
  - **Descrito en el RFC2284.**
  - **4 tipos de mensajes:**
    - **Petición (Request Identity): usado para el envío de mensajes del punto de acceso al cliente.**
    - **Respuesta (Identity Response): usado para el envío de mensajes del cliente al punto de acceso.**
    - **Éxito (Success): enviado por el punto de acceso para indicar que el acceso está permitido.**
    - **Fallo (Failure): enviado por el punto de acceso para el rechazo del acceso.**

802.1x

- **EAP:**
  - **Requiere cliente (Xsuplicant), Punto de Acceso y servidor de autenticación.**
  - **EAP es soportado por muchos Puntos de Acceso y por HostAP**
  - **Antes de la autenticación sólo se permite tráfico 802.1X (petición de autenticación).**

802.1x


Cliente Wireless
Access Point Wireless
Servidor Autenticación (RADIUS)
802.1X/EAP-Request Identity
802.1X/EAP- Identity Response
RADIUS Access Request
Autenticación mutua EAP
Obtención claves maestras (PMK)
Obtención claves mestras (PMK)
RADIUS Accept + claves PMK para el AP
802.1X/EAP-Success

802.1x

- **Protocolos de autenticación basados en EAP:**
  - **LEAP.**
  - **EAP-MD5.**
  - **EAP-TLS.**
  - **EAP-TTLS.**
  - **EAP-PEAP**

802.1x

- LEAP (EAP-Cisco Wireless)
  - Basado en Nombre de Usuario y Contraseña
  - Soporta plataformas Windows, MacOSX y GNU/Linux.
  - Patentado por Cisco (basado en 802.1x).
  - El Nombre de Usuario se envía sin protección.
  - La Contraseña se envía sin protección.
    - Sujeto a ataques de diccionario.
    - MSCHAP v1 & v2.
- No soporta One Time Password.
- Requiere Infraestructura Cisco Wireles.

802.1x

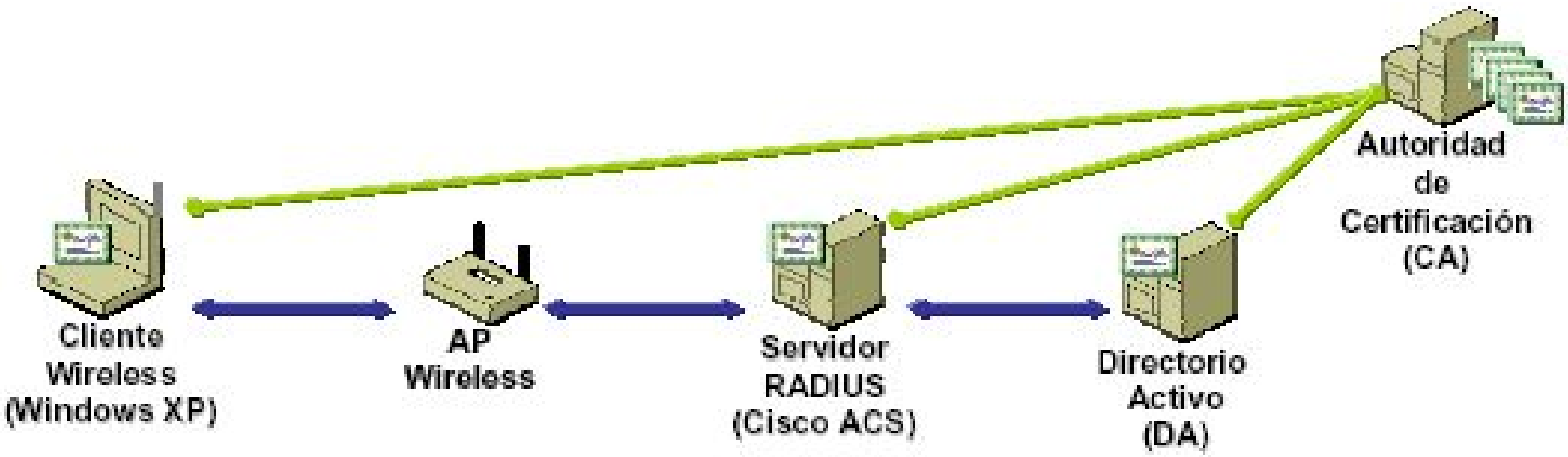
- EAP-MD5
  - Basado en Nombre de Usuario y Contraseña.
  - El Nombre de Usuario se envía sin protección:
    - Sujeto a ataques de diccionario.
  - Requiere una clave fija manual WEP.
  - No ofrece distribución automática de llaves.
  - Solo autentica el cliente frente al servidor (no el servidor frente al cliente):
    - Sujeto a ataques man-in-the-middle

802.1x

- **EAP-TLS**
  - **Desarrollado por Microsoft.**
  - **Ofrece fuerte autenticación mutua, credenciales de seguridad y llaves dinámicas.**
  - **Requiere la distribución de certificados digitales a todos los usuarios así como a los servidores RADIUS.**
  - **Requiere infraestructura de gestión de certificados (PKI).**
  - **Windows XP contiene un cliente EAP-TLS, pero obliga a emplear solo certificados Microsoft.**
  - **Intercambio de identidades desprotegido.**

802.1x

- **EAP-TLS**



802.1x

- **EAP-TLS**

802.1x

- EAP-TLS ¿Certificados Cliente?
  - Difíciles de gestionar.
  - Debe asignarlos una Autoridad Certificadora.
  - Requiere conocimiento del cliente:
    - Requiere que el cliente establezca el certificado.
  - Incómodo para establecer múltiples dispositivos, transferir certificados.
  - Los administradores son reacios a su uso.

802.1x

- **EAP-TLS, vulnerabilidades:**
  - **Fase de identificación: el cliente manda el mensaje EAP-Identity sin cifrar:**
    - **Un atacante podría ver la identidad del cliente que está tratando de conectarse.**
  - **Envío de la aceptación/denegación de la conexión (EAP-Success/EAP-Failure hacia el autenticador) sin cifrar:**
    - **Puede ser enviado por un atacante que se haga pasar por el servidor de autenticación.**

802.1x

- **EAP-TTLS**
  - **Permite a los usuarios autenticarse mediante Nombre de Usuario y Contraseña, sin pérdida de seguridad.**
  - **Ofrece fuerte autenticación mutua, credenciales de seguridad y llaves dinámicas.**
  - **Requiere que los certificados sean distribuidos solo a los servidores RADIUS, no a los usuarios.**

802.1x

- **EAP-TTLS**
  - **Compatible con las actuales bases de datos de seguridad de usuarios (Windows Active Directory, SQL, LDAP...)**
  - **Soporta CHAP, PAP, MSCHAP y MSCHAPv2.**

802.1x

- **EAP-TTLS, Ventajas:**
  - **El más sencillo de instalar y gestionar.**
  - **Seguridad difícil de traspasar: corrige EAP-TLS.**
  - **No requiere Certificados Cliente.**
  - **Autentica de manera segura los usuarios.**
  - **Facilidad:**
    - **Despliegue contra infraestructuras existentes.**
    - **Los usuarios se conectan con sus Nombres de Usuario y Contraseñas habituales.**
    - **Parámetros pre-configurados para el cliente.**

802.1x

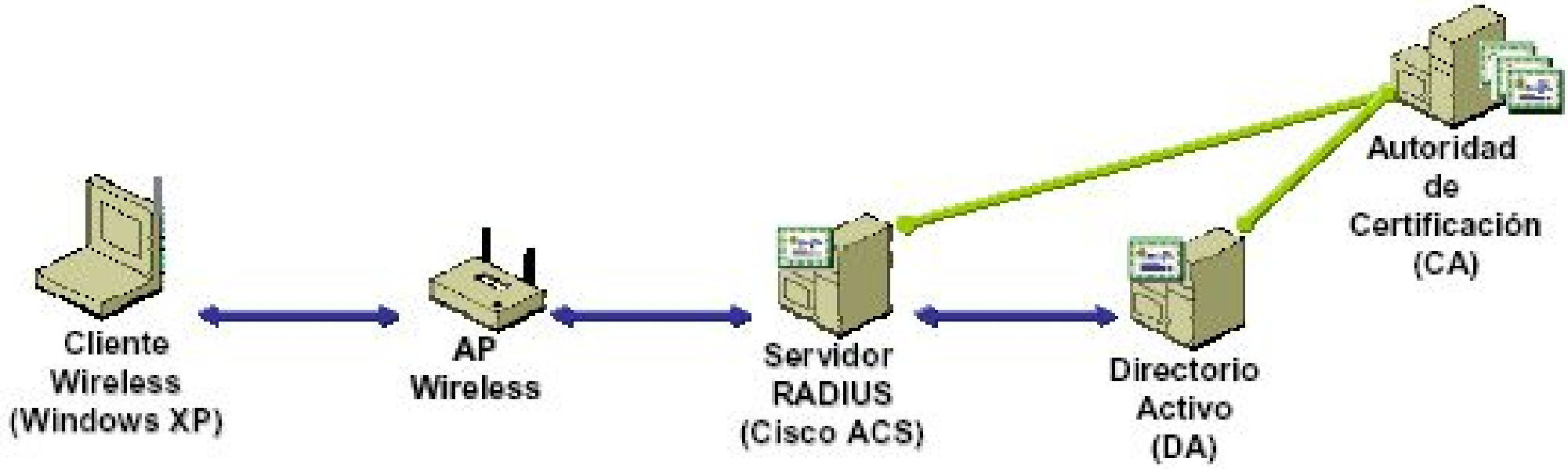
- **EAP-PEAP**
  - **Propuesto por Microsoft/Cisco/RSA Security.**
  - **No requiere Certificados Cliente.**
  - **Utiliza TLS para establecer el túnel.**
  - **Se incluye en el SP1 de WinXP y en Win2003.**

802.1x

- EAP-PEAP, corrige vulnerabilidades en EAP-TLS: proceso en dos fases:
  - Fase 1: obtención de un canal seguro “genérico”.
    - Esta fase puede realizarla cualquier atacante.
  - Fase 2: autenticación a través de ese canal seguro.
    - El atacante no tiene autenticación válida, por lo que no le sirve el canal seguro creado anteriormente.

802.1x

- **EAP-PEAP, proceso en dos fases:**

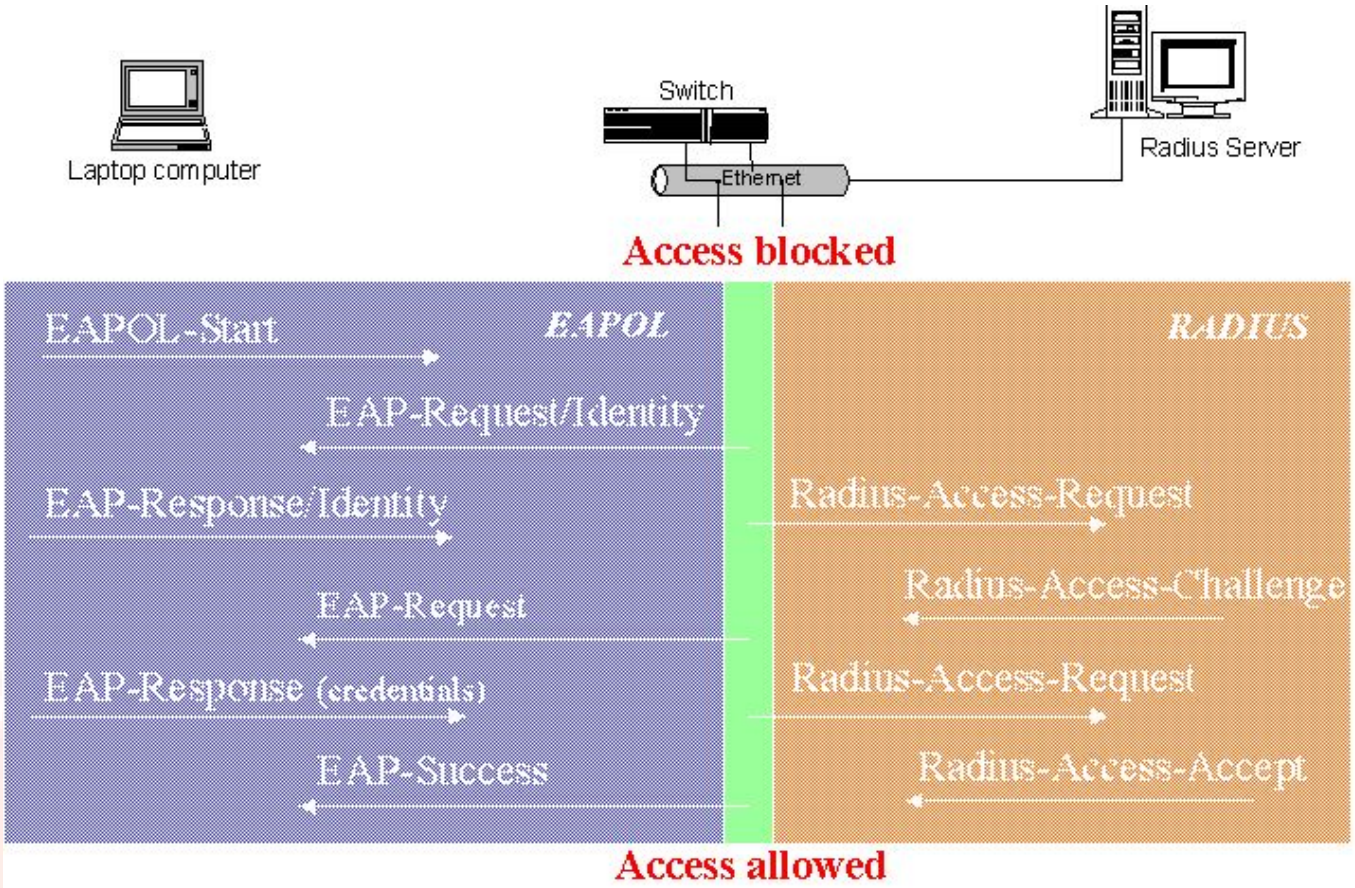


802.1x

- **Radius:**
  - **Remote Access Dial In User Access.**
  - **Soporta autenticación, autorización y contabilidad de los accesos a red.**
  - **Estándar muy utilizado en ISPs.**
  - **Microsoft apuesta por RADIUS para la autenticación de usuarios remotos.**

802.1x

Radius:



WPA

- Apareció como solución provisional a la aprobación final de 802.11i (WPA2).
- También conocido como WEP2.
- Distribución dinámica de claves:
  - duración limitada (TKIP).
- IV más robusto:
  - 48 bits, minimizando la reutilización de claves.
- Técnicas de integridad y autenticación:
  - MIC o Michael

WPA

- Incluye, parcialmente:
  - 802.1X:
    - Control de Acceso por puerto.
    - Solo permite tráfico EAP hasta autenticación.
  - EAP
    - Autenticación:
      - Estación.
      - Servidor de autenticación (RADIUS).
  - TKIP
  - MIC
    - Integridad de los datos.

WPA

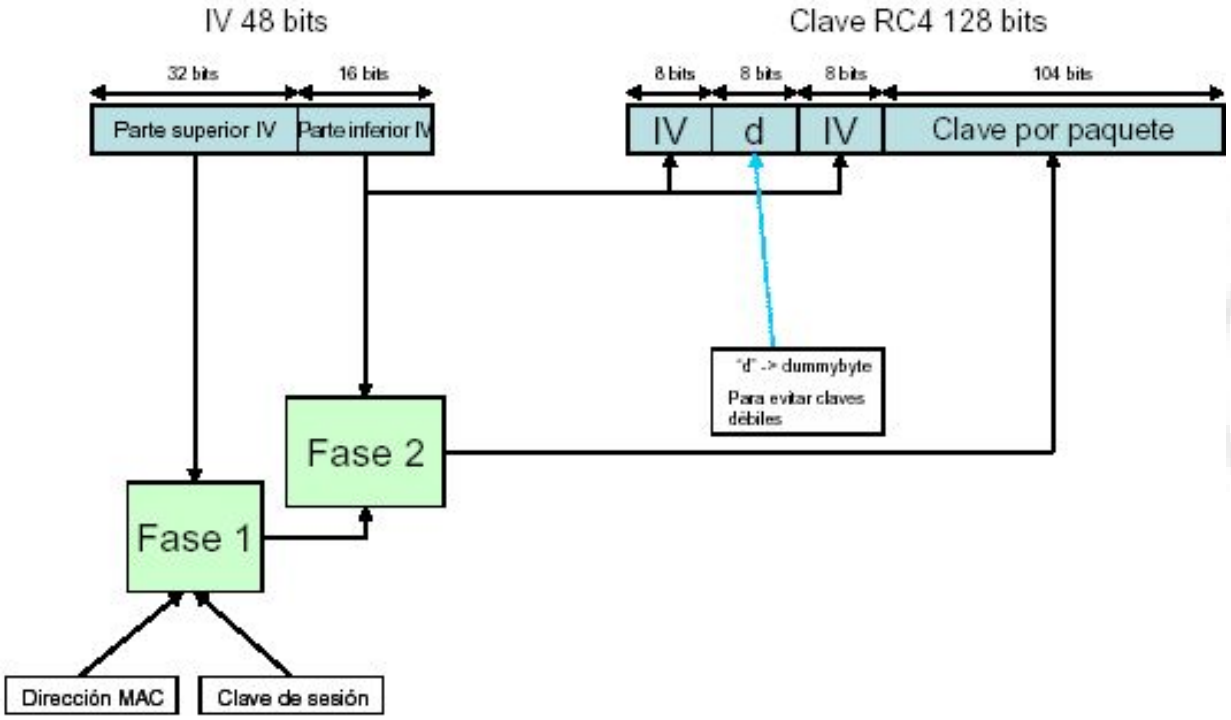
- TKIP (Temporal Key Integrity Protocol)
  - Sigue empleando RC4, pero sin compartir la clave entre todos los clientes.
  - Cambio de clave cada 10.000 paquetes aproximadamente.
  - Solamente requiere una actualización de firmware.
  - ¡Solución temporal! Hasta la llegada de 802.11i.
  - Información sobre el estado del proyecto:
    - http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

WPA

- **TKIP, Mejoras:**
  - **Enhanced IV (EIV):**
    - **Incremento de 32 bits en el IV, dejando un byte (dummybyte) para evitar IVs débiles (48 bits de IV).**
  - **TKIP Secuence Counter (TSC):**
    - **El IV como número de secuencia.**
    - **Si un IV ha sido recibido previamente, se descarta.**
    - **Evita reply-attacks.**

WPA

- **TKIP, Enhanced IV (EIV):**



WPA

- **Ventajas:**
  - **Vectores de Inicialización (EIV):**
    - **48 bits de longitud.**
    - **Reglas de Secuencia especificadas.**
  - **ICV (Integrity Check Value):**
    - **Se elimina la comprobación por CRC32.**
    - **Se utiliza algoritmo MIC.**
  - **Sustitución de mecanismo autenticación:**
    - **Antes: WEP, MAC...**
    - **Ahora: 802.1X, EAP, RADIUS.**

WPA

- Implementación:
  - Empresas: WPA-Enterprise.
    - Servidor RADIUS.
  - Usuarios Domésticos: WPA-Personal.
    - También conocido como WPA-PSK (Pre-Shared Key): Clave inicial compartida para autenticación (PSK).

WPA

- **Debilidades:**
  - **El sistema utilizado por WPA para el intercambio de información utilizada para la generación de claves es débil.**
  - **Claves preestablecidas “inseguras” (WPA-PSK):**
    - **Sujetas a ataques de diccionario.**
    - **No es necesario captura de gran cantidad de tráfico: solo capturamos el intercambio de claves.**

802.11i

- Aprobado por el IEEE y aceptado por Wi-Fi Alliance en Sept 2004.
- También conocido como WPA2.
- Utiliza algoritmo AES con claves de 128 bits:
  - ¡Requiere nuevo hardware!
- Nuevo sistema de Integridad.
  - CCMP.
- Soporte para redes ad-hoc.
- Compatible con WPA.

802.11i

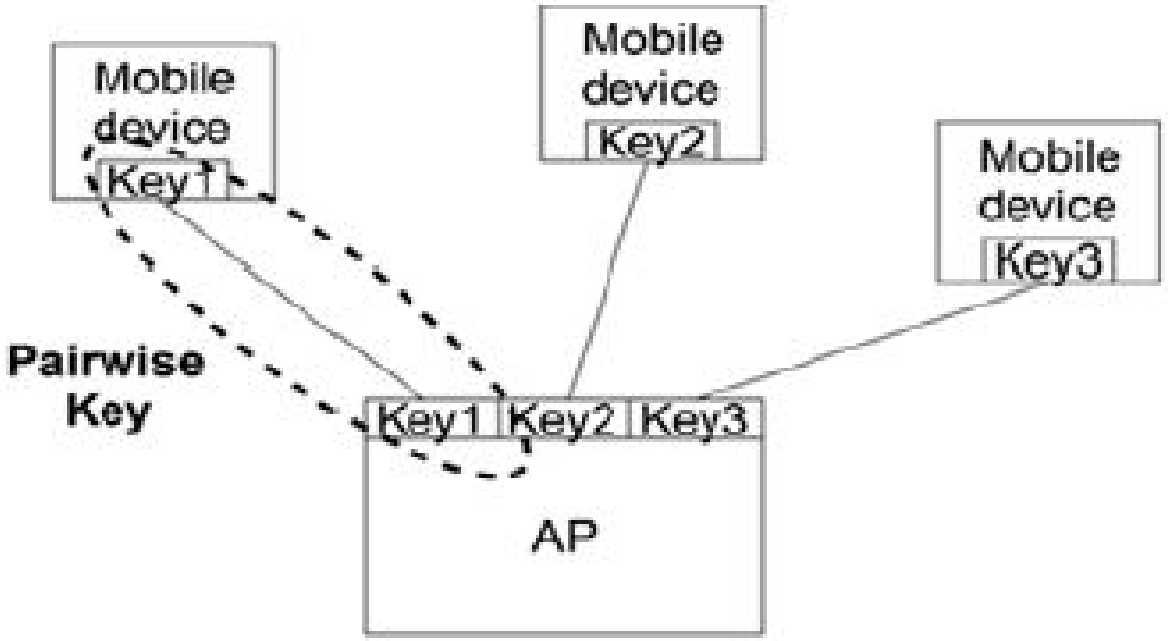
- **Requerimiento de nuevo hardware:**
  - **Se precisa un nuevo chip en las tarjetas para la criptografía necesaria de este protocolo (AES).**
  - **Atheros ya lo incluye en sus tarjetas**

802.11i

- **Gestión de claves:**
  - **Dos tipos de claves:**
    - **PKH:**
      - **Pairwise Key Hierarchy.**
      - **Del AP al cliente, punto a punto.**
    - **GKH:**
      - **Group Key Hierarchy.**
      - **Del AP a todos los clientes: broadcasting.**

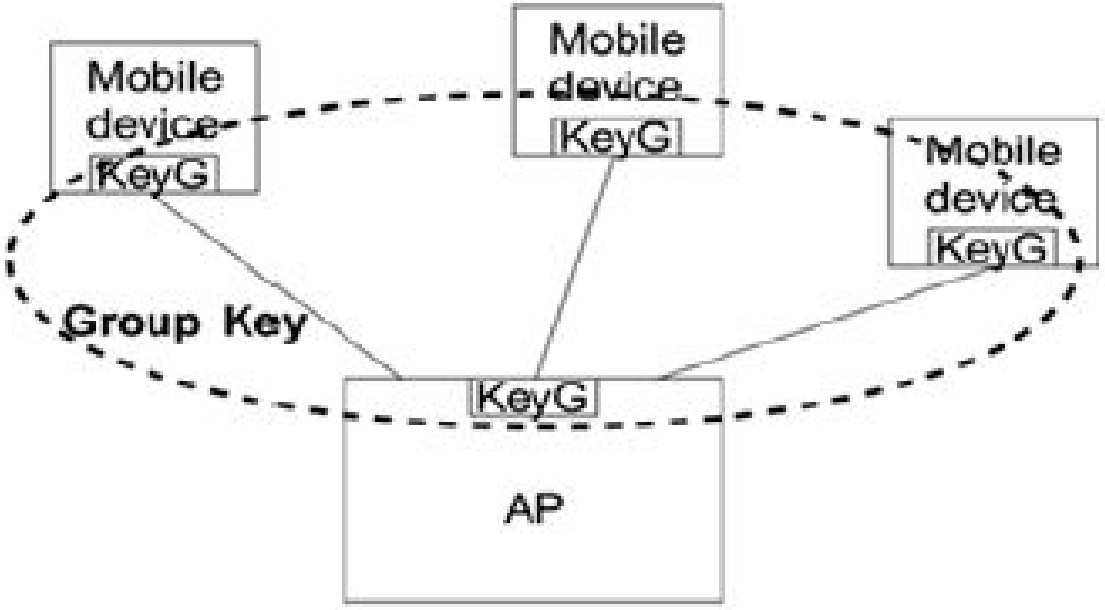
802.11i

- **PKH:**


Mobile device
Key1
Mobile device
Key2
Mobile device
Key3
Pairwise Key
Key1
Key2
Key3
AP

802.11i

- **GKH:**


Mobile device
KeyG
Mobile device
KeyG
Mobile device
KeyG
Group Key
KeyG
AP

802.11i

- **RSN**
  - **Red cuyo acceso y gestión de claves se apoya en el estándar IEEE 802.1X.**
  - **Tanto el cliente como el punto de acceso contienen una entidad IEEE 802.1X que facilita estos servicios de autenticación y de manejo de claves.**
  - **Se utiliza esta nomenclatura porque WPA y WPA2 son marcas registradas de la Wi-Fi Alliance.**

802.11i

- **RSN, Características técnicas:**
  - **Mecanismos de autenticación mejorados para el punto de acceso y para el**
  - **cliente.**
  - **Algoritmos de manejo de claves.**
  - **Claves dinámicas.**
  - **Métodos de encriptación de datos mejorados llamados CCMP y TKIP.**

Comparativa

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

802.1x, 802.11i, WPA

- **Implementación en GNU/Linux:**
  - **hostapd, demonio de HostAP.**
  - **Cliente:**
    - **WPA_supplicant.**
    - **Xsupplicant (http://www.open1x.org).**
  - **RADIUS: FreeRADIUS.**

Referencias

- Presentaciones y trabajos de Irontec, PoF, Dmescal, Tony F. Díaz, Santiago Estepa y Arturo Martínez, Ricardo Galli, Cisco Networks, Lucent, Avaya, Intel.
- Todas las imágenes son propiedad de sus respectivos dueños.