



Universidad Nacional del Nordeste
Facultad de Ciencias Exactas y Naturales y Agrimensura
Licenciatura en Sistemas de Información

CÁTEDRA: Teleproceso y Sistemas Distribuidos



SEGURIDAD EN REDES WI-FI

Profesor: David L. La Red Martinez

Alumno: Domingo Alberto Rios

Año 2011

Indice

Introducción.....	Pag.4
Tecnologías WLAN.....	Pag.5
Topología WLAN.....	Pag.6
Redes Wireless-Bandas designadas por ITU.....	Pag.7
Redes Wireless - Protocolos 802x.....	Pag.7
Redes Wireless - Elementos activos.....	Pag.8
Redes Wireless-Servicio con AP.....	Pag.9
Redes Wireless-802.11 - Seguridad – SSID.....	Pag.9
Redes Wireless- Seguridad-Encriptación.....	Pag.9
Seguridad en WiFi con WEP.....	Pag.10
Vulnerabilidades en redes WiFi.....	Pag.10
Acceso a redes WiFi.....	Pag.10
Autenticación en WiFi.....	Pag.11
Conceptos básicos.....	Pag.11
Medidas de seguridad utilizadas hasta ahora.....	Pag.11
Cifrado WEP.....	Pag.11
Vulnerabilidades en WEP.....	Pag.11
Autenticación en redes WiFi.....	Pag.12
Autenticación y asociación.....	Pag.13
Métodos de autenticación típicos.....	Pag.13
Vulnerabilidades en APs.....	Pag.13
Ataques de Denegación de Servicio.....	Pag.14
Ataques Man-in-the-Middle.....	Pag.14
Vulnerabilidades: AP en modo bridge.....	Pag.15

Soluciones de seguridad WiFi.....	Pag.17
Portales Cautivos.....	Pag.17
802.1x.....	Pag.20
EAP.....	Pag.20
Protocolos de autenticación basados en EAP.....	Pag.21
LEAP (EAP-Cisco Wireless).....	Pag.21
EAP-MD5.....	Pag.22
EAP-TLS.....	Pag.22
EAP-TTLS.....	Pag.23
EAP-PEAP.....	Pag.23
Radius.....	Pag.24
WPA.....	Pag.24
802.11i.....	Pag.26
RSN.....	Pag.27
Conclusiones.....	Pag.28
Bibliografía.....	Pag.29

Introducción

Las tecnologías inalámbricas se presentan como las de mayor auge y proyección en la actualidad.

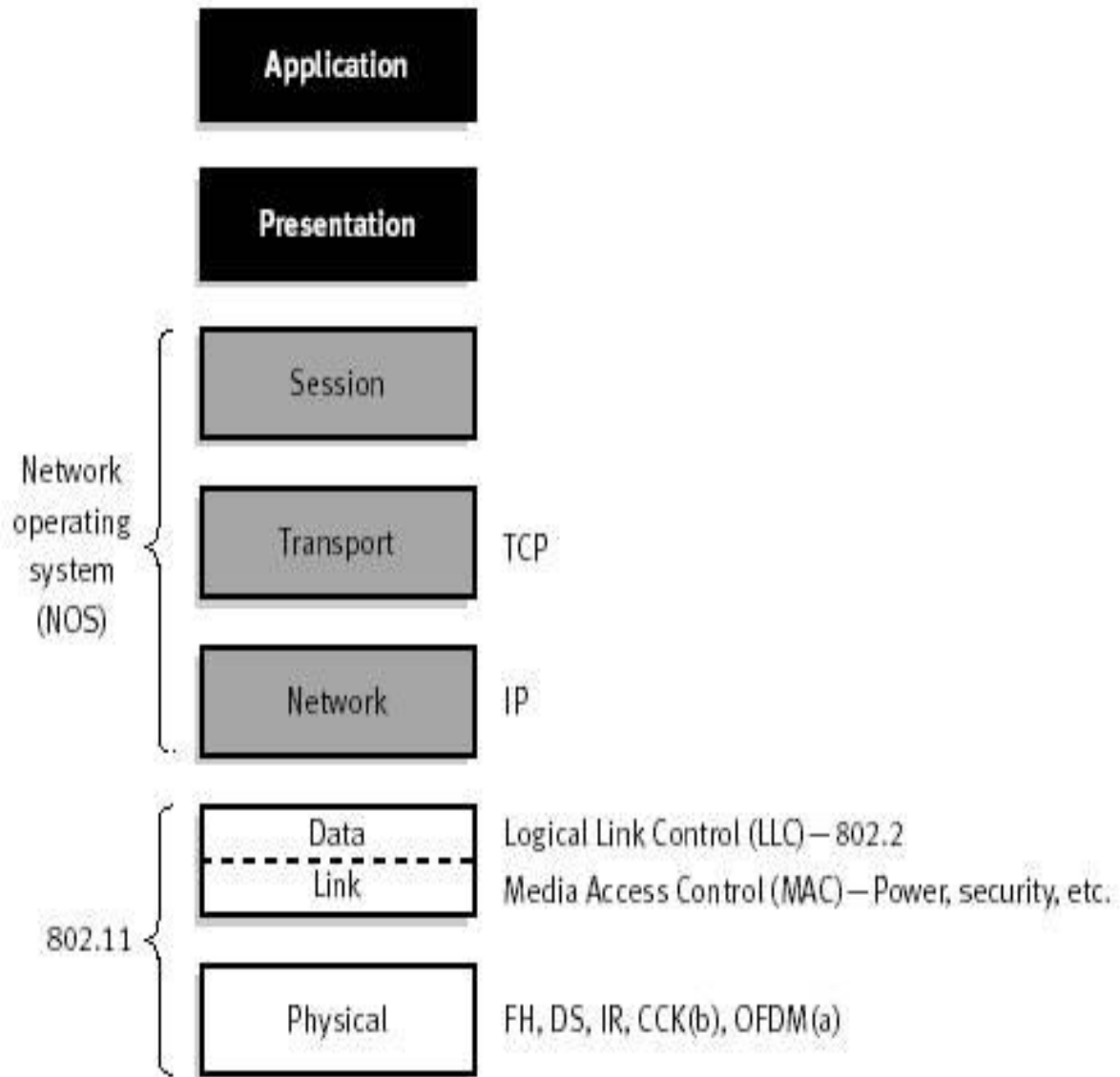
Permiten superar las limitantes de espacio físico y ofrecen una mayor movilidad de usuarios.

Se desarrollan a diario mejores estándares en la búsqueda de mayores tasas de transmisión y niveles de seguridad más altos.

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red cableada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos; tal es el caso de Intel que fabrica el chipset Centrino para computadores portátiles.

Tecnologías WLAN

802.11 & Modelo OSI:

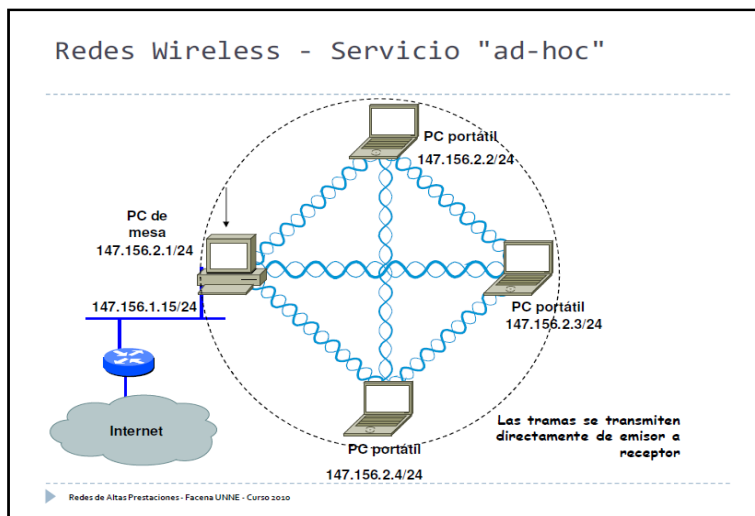


Topología WLAN

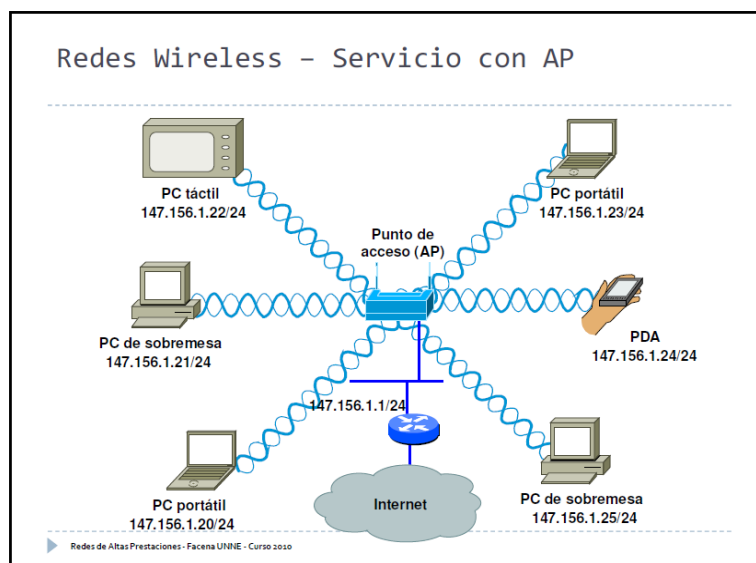
Una WLAN se puede conformar de dos maneras:

- En estrella. Esta configuración se logra instalando una estación central denominada punto de acceso (Access Point), a la cual acceden los equipos móviles. El punto de acceso actúa como regulador de tráfico entre los diferentes equipos móviles. Un punto de acceso tiene, por lo regular, un cubrimiento de 100 metros a la redonda, dependiendo del tipo de antena que se emplee, y del número y tipo de obstáculos que haya en la zona.
- Red ad hoc. En esta configuración, los equipos móviles se conectan unos con otros, sin necesidad de que exista un punto de acceso.

Redes en modo ad-hoc



Redes en modo infraestructura AP



Redes Wireless-Bandas designadas por ITU

Banda	Ancho	Uso en WLAN
13 553 – 13 567 kHz	14 kHz	No
26 957 – 27 283 kHz	326 kHz	No
40.66 – 40.7 MHz	40 kHz	No
902 – 928 MHz	26 MHz	Sistemas propietarios antiguos (en EEUU y Canadá)
2 400 – 2 500 MHz	100 MHz	802.11, 802.11b, 802.11 g
5 725 – 5 875 MHz	150 MHz	802.11 a
24 – 24.25 GHz	250 MHz	No

Redes Wireless - Protocolos 802.x

802.11

La versión original del estándar IEEE 802.11. Especifica dos velocidades de transmisión teóricas de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2,4 GHz.

Define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso.

802.11b

La revisión 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el método de acceso CSMA/CA. Funciona en la banda de 2.4 GHz. En la práctica, la velocidad máxima de transmisión es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

La extensión 802.11b introduce CCK (Complementary Code Keying) para llegar a velocidades de 5,5 y 11 Mbps (tasa física de bit).

802.11a

Opera en la banda de 5 GHz y utiliza soportadoras (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. Utilizar la banda de 5 GHz representa una ventaja dado que se presentan menos interferencias.

802.11 g

Es la evolución del estándar 802.11b. Utiliza la banda de 2.4 GHz, pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22.0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a.

Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares.

Para construir equipos bajo este nuevo estándar se pueden adaptar los ya diseñados para el estándar b.

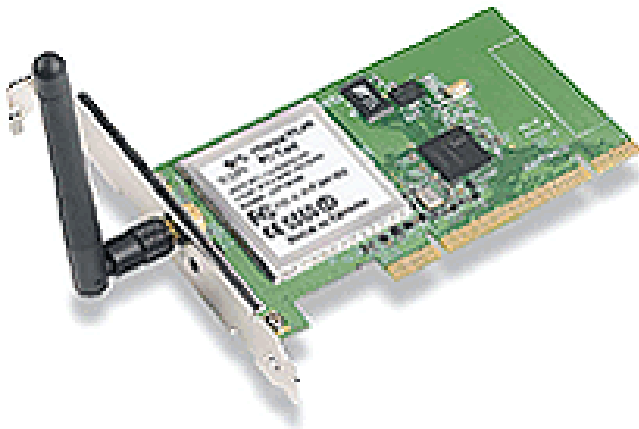
Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

802.11 Súper G

Hoy en día el estándar 802.11 Súper G, con una banda de 2.4 GHz, alcanza una velocidad de transferencia de 108 Mbps. Esto es proporcionado por el chipset Atheros.

Redes Wireless - Elementos activos

Tarjeta de red 802.11b



Acces Point



Wireless con adaptador USB



Redes Wireless-Servicio con AP

Cuando una estación se enciende busca un AP en su celda. Si recibe respuesta de varios atiende al que le envía una señal más potente.

La estación se registra con el AP elegido. Como consecuencia de esto el AP le incluye en su tabla MAC.

El AP se comporta para las estaciones de su celda como un hub inalámbrico. En la conexión entre su celda y el sistema de distribución el AP actúa como un puente.

El rendimiento real suele ser el 50-60% de la velocidad nominal.

El overhead se debe a:

- Mensajes de ACK (uno por trama).
- Mensajes RTS/CTS (si se usan).
- Fragmentación (si se produce).
- Protocolo MAC (colisiones, esperas aleatorias, intervalos entre tramas).
- Transmisión del Preámbulo (sincronización, selección de antena, etc.) e información de control, que indica entre otras cosas la velocidad que se va a utilizar en el envío, por lo que se transmite a la velocidad mínima (1 Mb/s en FHSS y DSSS, 6 Mb/s en OFDM). Solo por esto el rendimiento de DSSS a 11 Mb/s nunca puede ser mayor del 85% (9,35 Mb/s).

Redes Wireless-802.11 - Seguridad – SSID

Se dispone de mecanismos de autenticación y de encriptación.

La encriptación permite mantener la confidencialidad aun en caso de que la emisión sea capturada por un extraño. El mecanismo es opcional y se denomina WEP (Wireless Equivalent Privacy). Se basa en encriptación de 40 o de 128 bits. También se usa en Bluetooth.

Los clientes y el punto de acceso se asocian mediante un SSID (System Set Identifier) común. El SSID sirve para la identificación de los clientes ante el punto de acceso, y permite crear grupos 'lógicos' independientes en la misma zona (parecido a las VLANs).

Esto no es en sí mismo una medida de seguridad, sino un mecanismo para organizar y gestionar una WLAN en zonas donde tengan que coexistir varias en el mismo canal

Redes Wireless- Seguridad-Encriptación

WPA (Wireless Protected Access)

Ofrece dos tipos de seguridad, con servidor de seguridad y sin servidor.

Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor).

No todos los dispositivos wireless lo soportan.

WEP (Wired Equivalent Privacy).

Ofrece dos niveles de seguridad, encriptación a 64 o 128 bit. La encriptación usa un sistema de claves. La clave de la tarjeta de red del ordenador debe coincidir con la clave del router.

64-bits (10 hex digits): Se pueden introducir 5 caracteres ASCII o 10 dígitos hexadecimales (0 a 9 y a a F).

128-bit WEP: usa una clave más larga y, por tanto, más complicada de acertar. Es prácticamente la misma, sólo que ahora hay que introducir 13 caracteres ASCII ó 26 dígitos hexadecimales.

Seguridad en WiFi con WEP

Todo el tráfico es accesible a un atacante.

- Servicios de seguridad necesarios.
- Autenticación: Identificación con un grado aceptable de confianza de los usuarios autorizados.
- Confidencialidad: La información debe ser accesible únicamente a las personas autorizadas.
- Integridad: La información debe mantenerse completa y libre de manipulaciones fortuitas o deliberadas, de manera que siempre se pueda confiar en ella.
- ¡WEP no consigue ofrecer ninguno!.

Vulnerabilidades en redes WiFi

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

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)

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.

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

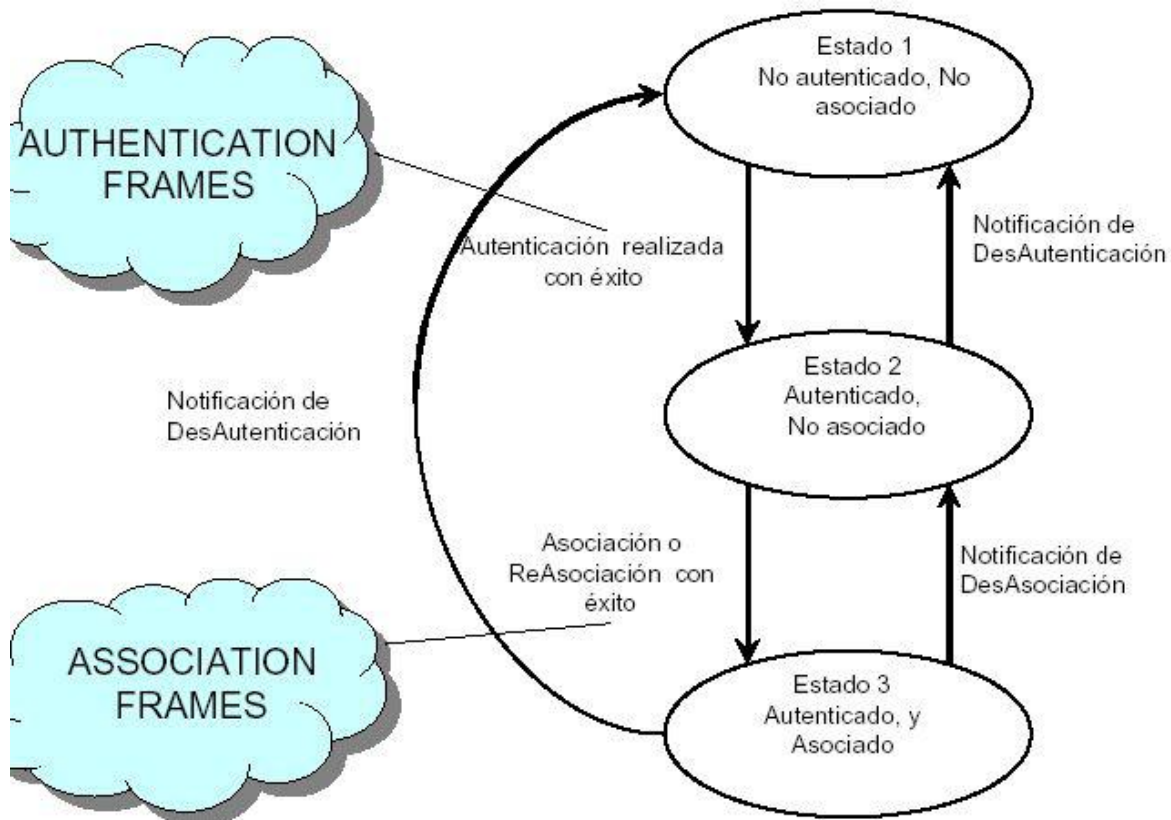
- Algoritmo de integridad: características lineales CRC32
 - El ICV se calcula sólo haciendo un CRC32 del payload
 - Dos grandes problemas:
 - El ICV es independiente de la clave y del IV

- Los CRC son lineales ($CRC(m \text{ xor } k) = CRC(m) \text{ xor } CRC(k)$)
- Mediante “bit-flipping” se podría regenerar un ICV válido para un mensaje modificado.
- 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.
- 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!
- Cifrado: Vulnerabilidades de WEP posibilitan fuerza bruta.
- Cifrado: Debilidades en el algoritmo de Key Scheduling de RC4 (FMS)

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 “PROBE REQUEST” con un determinado ESSID para ver si algún AP responde.

Autenticación y asociación:



Métodos de autenticación típicos

- Open System Authentication
- 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 APs

- Descubrir ESSID ocultos
- 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 PROBE REQUEST
- Podemos esperar
- Podemos desconectar a un cliente (DoS)

- 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

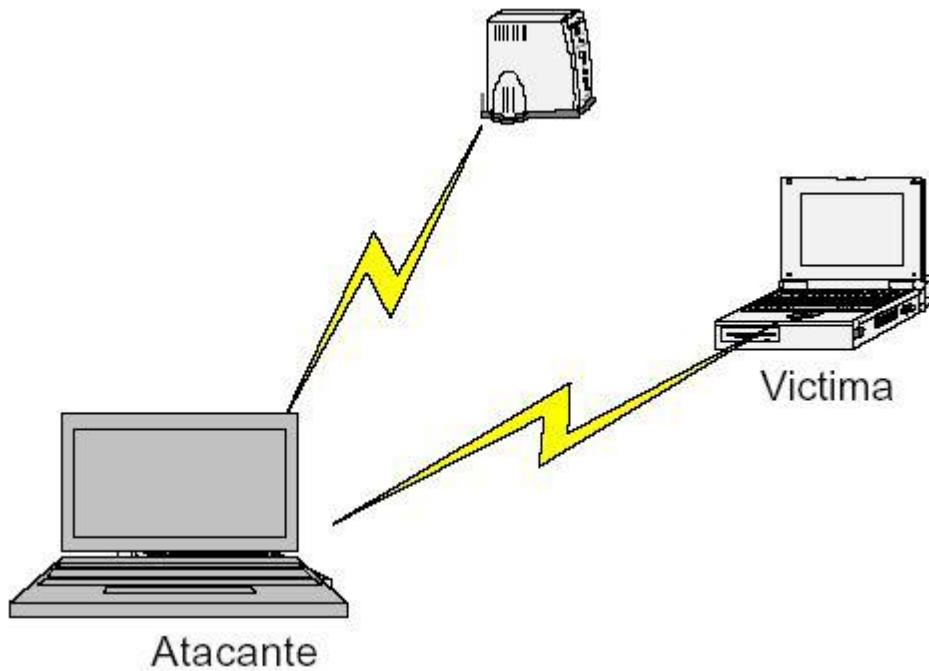
Ataques de Denegación de Servicio

- 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 contra la capa física/enlace de datos de 802.11:
 - CSMA/CA: Collision 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 víctima
- 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

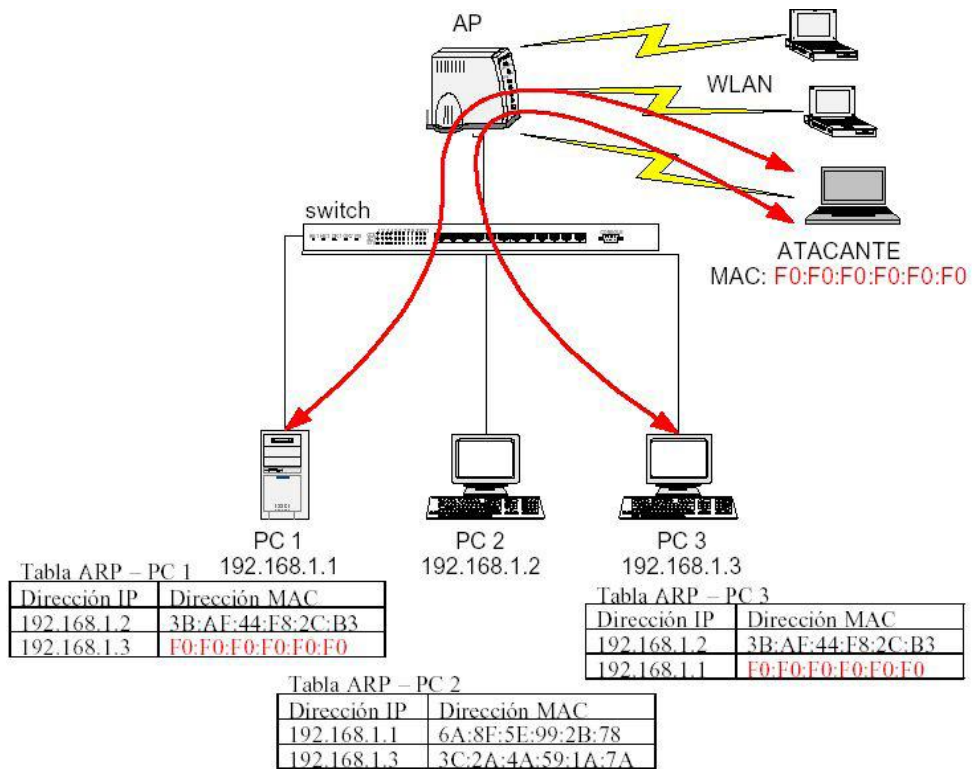
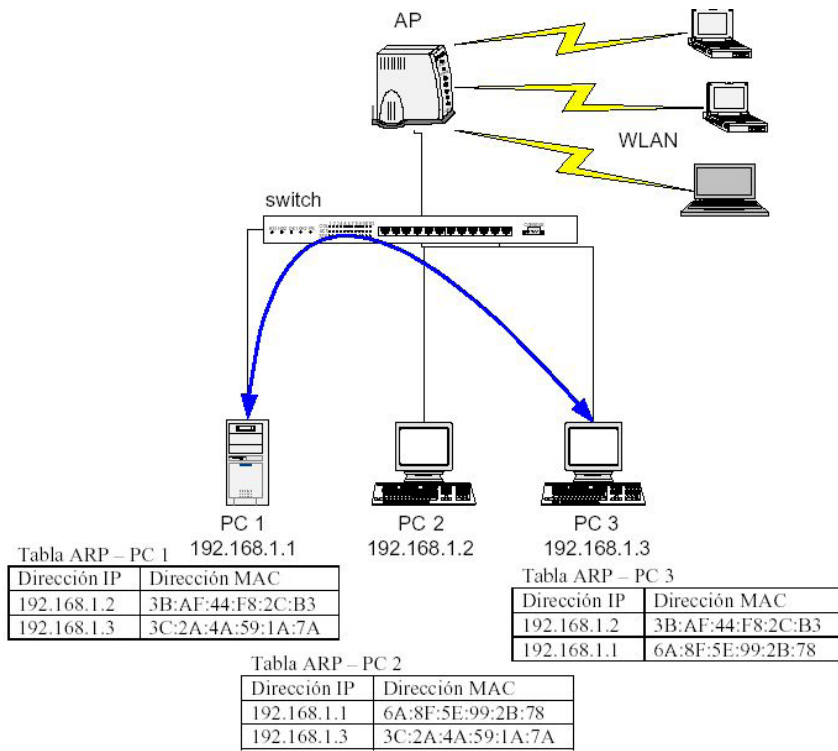
Ataques Man-in-the-Middle



- 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!



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

Portales Cautivos

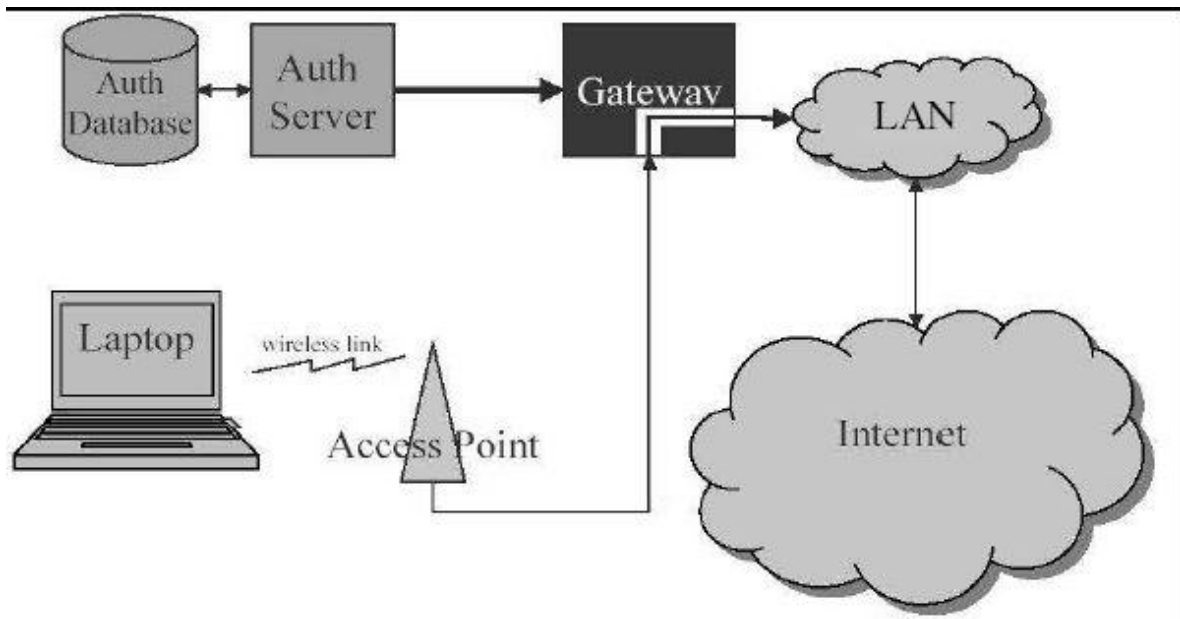
- Sistema de validación de clientes para nodos wireless.
 - Según el tipo de usuario asigna ancho de banda y da acceso a servicios diferentes.
 - Basado normalmente en “tokens” temporales gestionados por HTTP-SSL (443/TCP).
-
- Diferentes implementaciones:
 - NoCat Auth: <http://nocat.net>
 - LANRoamer: <http://www.lanroamer.net>
 - Wireless Heartbeat:
<http://www.river.com/tools/authhb/>
 - NetLogon - Linköping University
 - FisrtSpot (PatronSoft):
<http://www.patronsoft.com/firstspot/>
 - WiCap (OpenBSD)
-
- 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.
 - 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.

- 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.
 - 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.

- 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.

- 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 --toport-443`
 4. La conexión es autenticada vía SSL.

- NoCat, Proceso de autenticación:
 1. El Auth Server pide usuario y contraseña al cliente (via SSL) y la comprueba con la Auth Data base.
 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.



- 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).

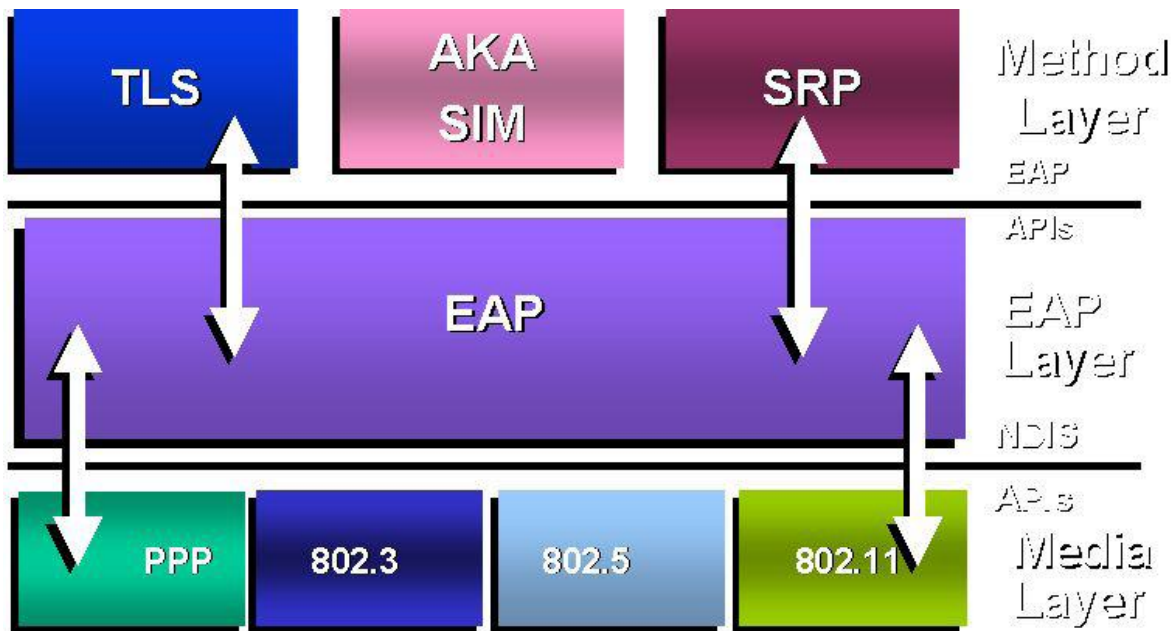
- NoCat, Necesidades en el servidor:
 - Servidor web (Apache)
 - OpenSSL.
 - GnuPG.
 - Perl y módulos de perl correspondientes.
 - Servidor DNS.
 - Servidor DHCP (en el AP o en el gateway).
 - Servidor para centralizar cuentas de usuarios.

- 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.

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

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).
- 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.

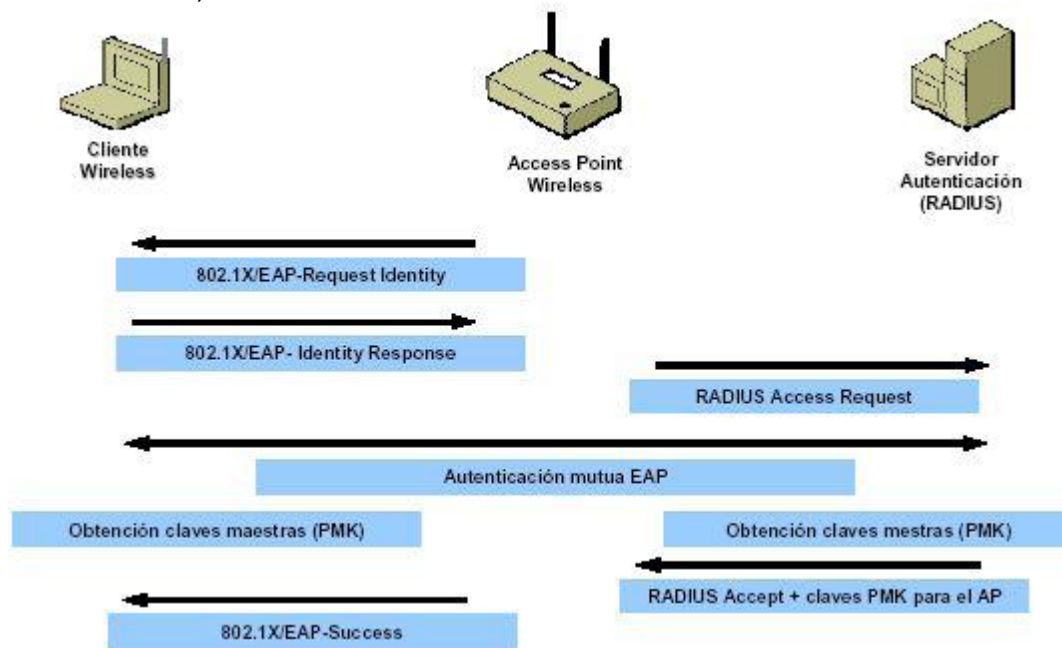


- EAP:
 - Descrito en el RFC2284.
 - 4 tipos de mensajes:
 - Petición (Request Identity): usado para el envío de mensajes del punto de acceso al cliente.
 - Respuesta (Identity Response): usado para el envío de mensajes del cliente al punto de acceso.

- 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.

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).



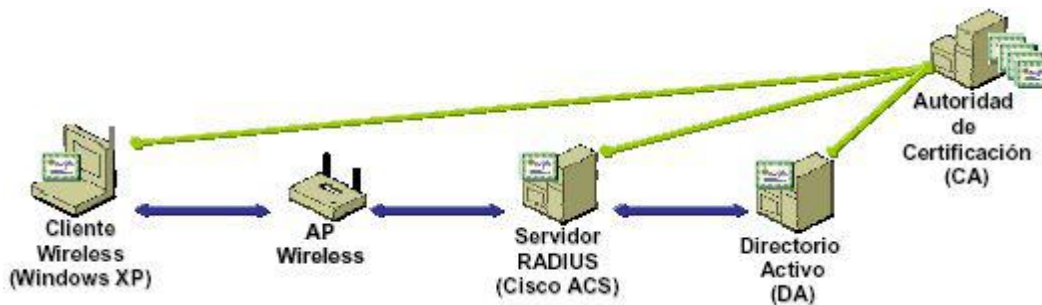
• Protocolos de autenticación basados en EAP:

- LEAP.
- EAP-MD5.
- EAP-TLS.
- EAP-TTLS.
- EAP-PEAP

• 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.

- 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
- 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.

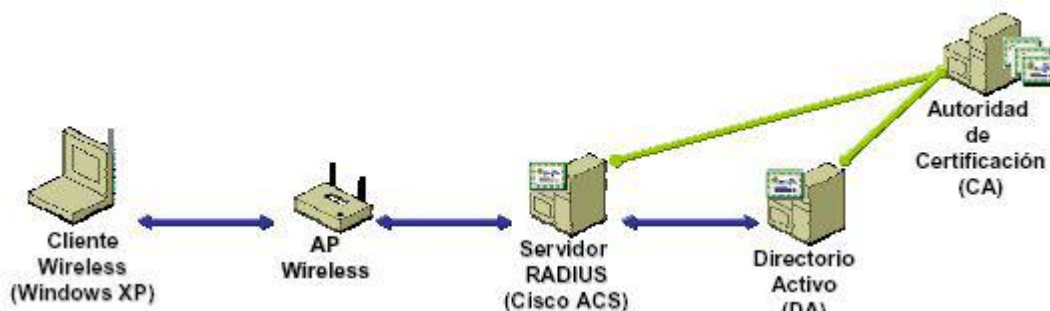


- EAP-TLS ¿Certificados Cliente?
 - Difíciles de gestionar.
 - Debe asignarlos una Autoridad Certificadora.
 - Requiere conocimiento del cliente:
 - Requiere que el cliente establezca el certificado.
 - Incómodo para establecer múltiples dispositivos, transferir certificados.
 - Los administradores son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

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

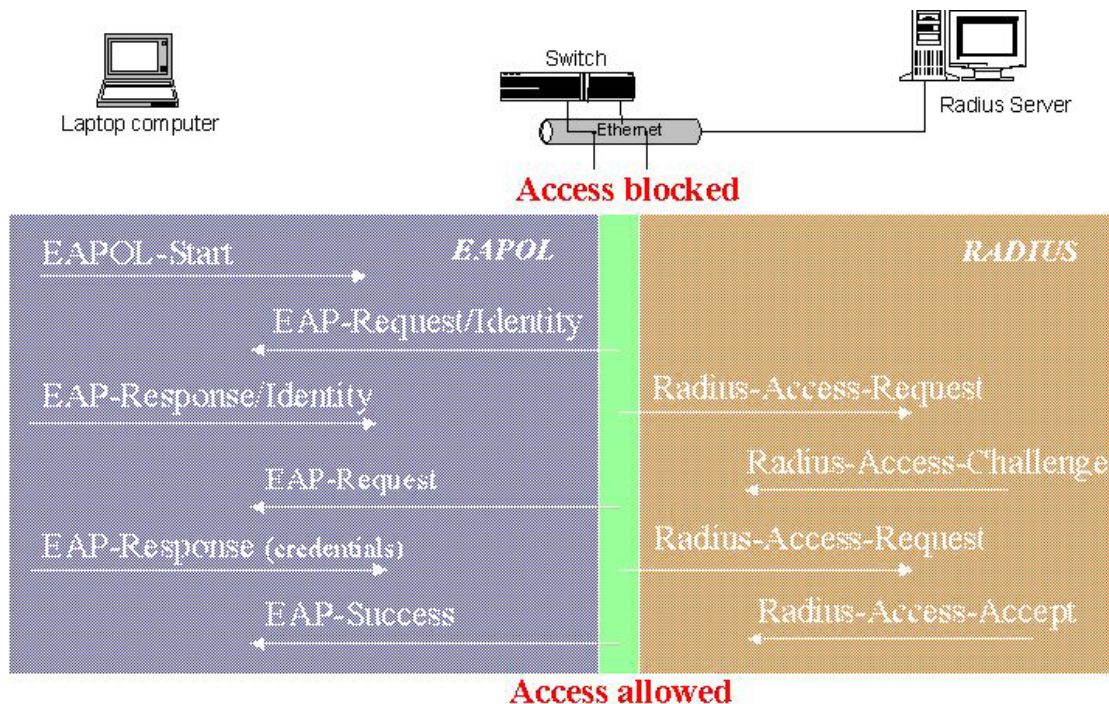
- EAP-TTLS, Ventajas:
 - El más sencillo de instalar y gestionar.
 - Seguridad difícil de traspasar: corrige EAP-TLS.
 - No requiere Certificados Cliente.
 - Autentica de manera segura los usuarios.
 - Facilidad:
 - Despliegue contra infraestructuras existentes.
 - Los usuarios se conectan con sus Nombres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

- 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.
 - 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.



- 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.



WPA

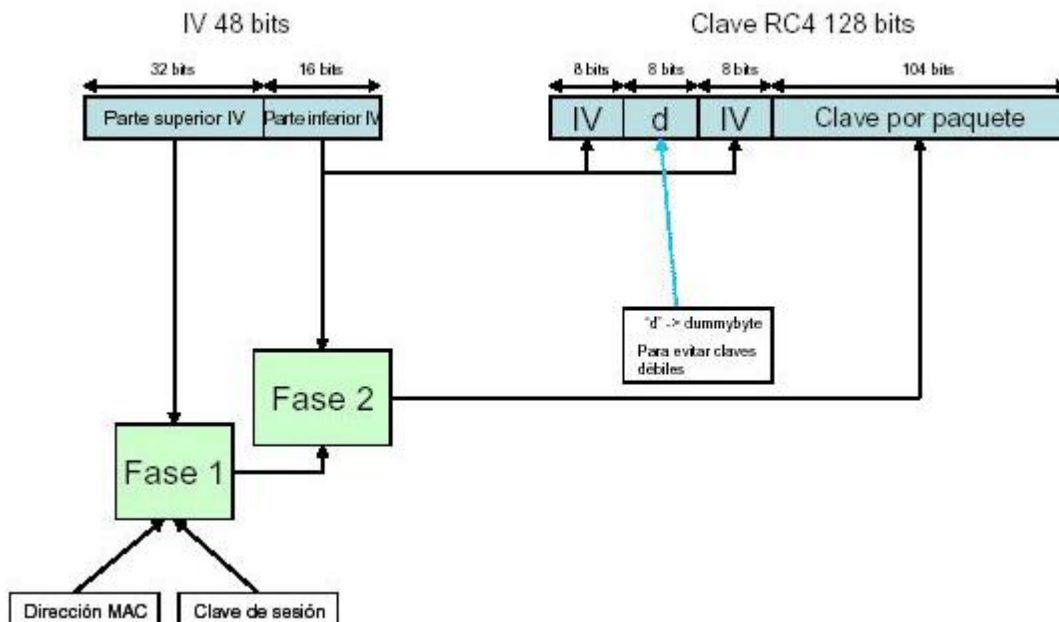
- Apareció como solución provisional a la aprobación final de 802.11i (WPA2).
- También conocido como WEP2.
- Distribución dinámica de claves:
 - duración limitada (TKIP).
- IV más robusto:
 - 48 bits, minimizando la reutilización de claves.
- Técnicas de integridad y autenticación:
 - MIC o Michael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

- 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

- 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 Sequence Counter (TSC):
 - El IV como número de secuencia.
 - Si un IV ha sido recibido previamente, se descarta.
 - Evita reply-attacks.

TKIP Enhanced IV (EIV):



- Ventajas:
 - Vectores de Inicialización (EIV):
 - 48 bits de longitud.

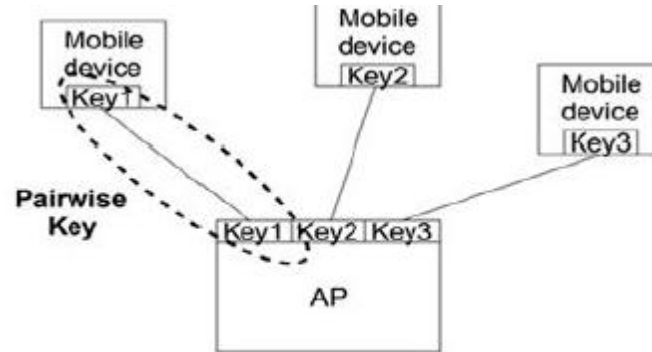
- Reglas de Secuencia especificadas.
 - ICV (Integrity Check Value):
 - Se elimina la comprobación por CRC32.
 - Se utiliza algoritmo MIC.
 - Sustitución de mecanismo autenticación:
 - Antes: WEP, MAC...
 - Ahora: 802.1X, EAP, RADIUS.
 - Implementación:
 - Empresas: WPA-Enterprise.
 - Servidor RADIUS.
 - Usuarios Domésticos: WPA-Personal.
 - También conocido como WPA-PSK (Pre-Shared Key): Clave inicial compartida para autenticación (PSK).
- Debilidades:
 - El sistema utilizado por WPA para el intercambio de información utilizada para la generación de claves es débil.
 - Claves preestablecidas “inseguras” (WPAPSK):
 - Sujetas a ataques de diccionario.
 - No es necesario captura de gran cantidad de tráfico: solo capturamos el intercambio de claves.

802.11i

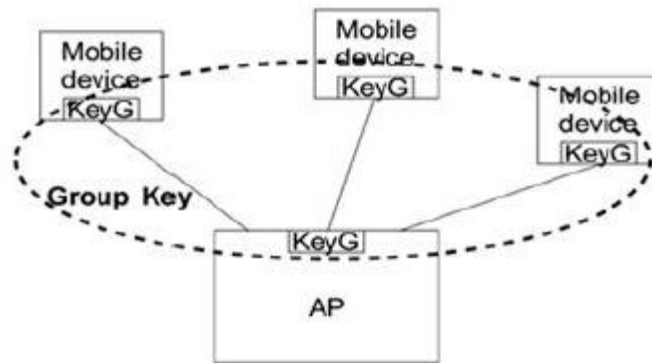
- Aprobado por el IEEE y aceptado por Wi-Fi Alliance en Sept 2004.
- También conocido como WPA2.
- Utiliza algoritmo AES con claves de 128 bits:
 - ¡Requiere nuevo hardware!
- Nuevo sistema de Integridad.
 - CCMP.
- Soporte para redes ad-hoc.
- Compatible con WPA.
- Requerimiento de nuevo hardware:
 - Se precisa un nuevo chip en las tarjetas para la criptografía necesaria de este protocolo (AES).
 - Atheros ya lo incluye en sus tarjetas
- 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.

• PKH:



• GKH:



• 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.

• 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.

CONCLUSIONES

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, la gran cantidad de las redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Existen diversas soluciones para mejorar la seguridad en las redes inalámbricas.

Su implementación depende del uso que se vaya a dar a la red (casera o empresarial), de si es una red ya existente o una nueva, y del presupuesto del que se disponga para implantarla, entre otros factores.

La restricción de acceso mediante direcciones MAC es insuficiente para cualquier red, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta cualquiera.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, el uso de WEP está formalmente desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico. El uso de las VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de un servidor o una serie de servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

La alternativa de 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva. Puede usarse la solución de WEP con clave dinámica, o la de WPA; ambas ofrecen un excelente grado de protección.

Bibliografía

- Seguridad En Redes Inalámbricas 802.11 a/b/g .Protección y vulnerabilidades. Pablo Garaizar Sagarminaga.-
<http://www.e-ghost.deusto.es/docs/SeguridadWiFilnstable2005.pdf>. Fecha de visita 10/ 01/2011
- Seguridad En Redes Inalámbricas. Trabajo ampliación en redes 5 año Ingeniería en Informática Universidad de Valencia.-
<http://documentos.shellsec.net/otros/SeguridadWireless.pdf>. Fecha de visita 11/ 02/2011.
- Seguridad en Redes Inalámbricas. II Jornadas de Telemática. Ing. Fabian Alejandro Molina.-
http://www.acis.org.co/memorias/JornadasTelematica/IIJNT/Seguridad_en_Redess_Inalámbricas.ppt. Fecha de visita 28/03/2011.
- Seguridad en redes inalámbricas 802.11. Juan Manuel Madrid Molina. Universidad Icesi .
<http://www.abcdatos.com/tutoriales/tutorial/z333.html>. Fecha de visita 05/04/2011.
- Apuntes de redes de altas prestaciones 2010. Lic. José Ríos. Facultad de Ciencias Exactas y Naturales y de Agrimensura UNNE.
- Seguridad en redes inalámbricas WiFi. Gonzalo Álvarez Marañón Pedro Pablo Pérez García
<http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf>. Fecha de visita 05/04/2011.
- Protocolos de seguridad en redes inalámbricas. Saulo Barajas Doctorado en Tecnologías de las Comunicaciones Universidad Carlos III de Madrid
<http://www.saulo.net/pub/inv/SegWiFi-art.htm>. Fecha de visita 05/04/2011.