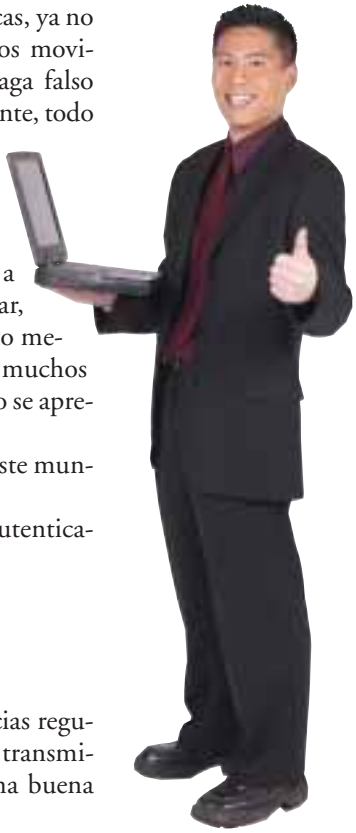
Wireless:

Todo lo que necesita saber

¡Ah, qué maravilla!, con las redes inalámbricas, ya no es necesario tener un cable que limite los movimientos, se desconecte o que a veces haga falso contacto. En una palabra "libertad". Desafortunadamente, todo tiene un precio, y las redes inalámbricas (*wireless*) tienen los defectos de sus cualidades. Esta misma libertad de movimiento, como se verá, puede tener un costo muy elevado.



Muchos vieron en este nuevo modo de conectarse a redes, como Internet, algo muy sencillo y fácil de usar, dejando de lado las consecuencias de usar el aire como medio de transporte. Muchas falsas ideas corren hoy, muchos creen estar cubiertos, invisibles, o protegidos... Como se apreciará, la seguridad nunca tiene una solución sencilla.

A lo largo de tres artículos viajaremos a través de este mundo en evolución,

%Todo lo que necesita saber: funcionamiento, autenticación, encripción

%Autopsia de un ataque

%Cómo asegurar su red inalámbrica

ASPETO FÍSICO

LAS FRECUENCIAS

Los equipos inalámbricos emiten señales en frecuencias reguladas y definidas. No entraremos en el detalle de las transmisiones de radiofrecuencia pero esta tabla les dará una buena idea de lo que soporta cada estándar:

	Velocidad (Mbps)	Banda de Frecuencia	Alcance	Popularidad
802.11a	6,9,12,18,24,26,48,54	5.180-5.800GHz	50 metros	No popular
802.11b	1 , 2 , 5.5 , 11	2.412-2.477GHz	150 metros	Muy popular
802.11g	1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 48, 54	2.412-2.477GHz	150 metros	popular

Los equipos que cumplen con 802.11g son compatibles con los equipos 802.11b (no al revés).

LOS CANALES

Para cada una de estas normas se definen canales (rangos de frecuencia) donde se puede emitir, dependiendo de los países.

En México se permiten los canales:

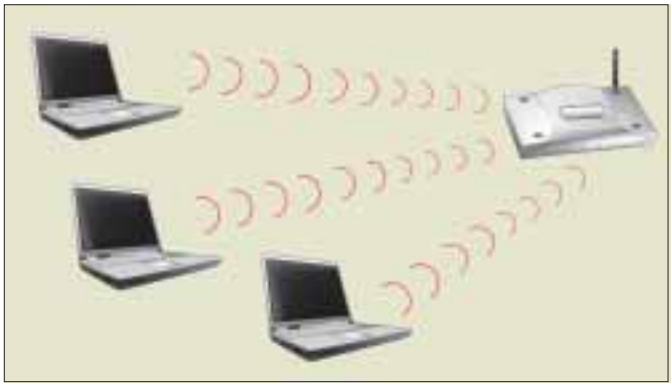
MODO DE COMUNICACIÓN

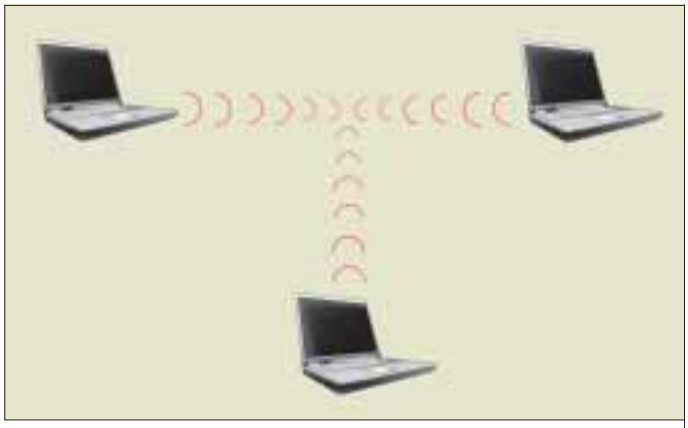
Existen dos modos de comunicación:

Modo Infraestructura.En éste, los clientes no pueden hablar directamente, deben pasar por un access point que identificaremos como AP. El AP es el punto de acceso a la red cableada.

VOCABULARIO

- Access Point (AP):equipo frontera entre una red inalámbrica y otra cableada. Controla los accesos a la red cableada, así como los modos de comunicaciones con los clientes inalámbricos (encripción, autenticación, filtros).
- Cliente Inalámbrico: cliente (laptop, computadora) que tiene la capacidad de comunicarse con un Access Point (modo infraestructura) u otro cliente (modo Ad-Hoc) para intercambiar datos. Este cliente se conecta con una tarjeta inalámbrica que puede ser PCI o PCMCIA. Debe soportar los mismos estándares físicos que el AP o los otros clientes (802.11a/b/g).
- Bridge (o Puente): equipo diseñado para conectar redes cableadas remotas (LAN) a través de una comunicacion inalámbrica. Los *bridges* usan antenas para amplificar las señales.
- Chipset: el chipset es el controlador de la tarjeta inalámbrica como tal. Varios fabricantes usan el mismo chipset. Es muy importante conocer el chipset de su tarjeta por lo mismo que, en Linux, ¡varios programas aplican al driver específico de un chipset! Escoger bien su tarjeta inalámbrica es parte muy importante para empezar a trabajar...
- Servidor de autenticación: su rol es permitir o no el acceso a la red mediante un protocolo de autenticación. Puede ser un servidor RADIUS o TACACS.





Modo Ad-Hoc: usado para levantar una red inalámbrica sin AP. Este modo no es muy usado porque la red está cerrada (se puede abrir si uno de los clientes implementa ruteo con acceso a otra red).

FORMATO DE LOS PAQUETES

FC	Duración	Dirección MAC 1	Dirección MAC 2
Dirección MAC 3	Sec. cont.	Contenido del paquete ...	
.....			
.....			CRC

paquete 802.11

Protocol Version (0)		Tipo		Subtipo			
To DS	From DS	More Frag	Retry	Pwr. Mgt	More Data	Crypt	Order

Detalle de los 2 octetos del campo FC (Frame Control)

- **Tipo 00** = paquete de administración. Usado para la asociación y la autenticación de un cliente con el AP. BEACON y PROBE son parte de éstos.
- **Tipo 01** = paquete de control. Asegura la calidad de servicio al nivel inalámbrico (transmission request, notificación de recibido)
- **Tipo 10** = paquete de datos.

En caso de una captura, el campo FC viene con los bits de peso bajo primero (al revés).

Los paquetes de control y administración siempre tienen "TO DS" y "From DS" a 0. En los paquetes de data, To DS = 1 si el paquete va del cliente al AP y From DS = 1 si el paquete viene del AP hacia un cliente.

Algunos valores del primer octeto del campo FC (FC[0]) para paquetes de administración:

FC[0] 0x80

Descripción. BEACON: el AP lo envía 10 veces por segundo y contiene varios datos y características de la red inalámbrica, tales como: identificador (ESSID o SSID), canal de transmisión, velocidad soportada (1, 5.5, 11 Mbps) y modo de enciframiento (ninguno, WEP o WPA). Se puede quitar la información de SSID del BEACON activando "Disable SSID Broadcast" en el AP.

FC[0] 0x40

Descripción. Probe Request: los clientes mandan probe request al SSID de la red antes de asociarse. También sirve en los programas de descubrimiento activo como Netstumbler. Mandan Probe Request con SSID "any" esperando la respuesta con el buen SSID del AP.

FC[0] 0x50

Descripción. Probe Response: respuesta al paquete anterior. Algunos AP no contestan si el probe response no contiene el buen SSID.

FC[0] 0x10

Descripción. Authentication: cuando el cliente pide autenticarse. En el caso de WEP, el AP manda un challenge que el cliente regresa encifrado.

FC[0] 0x00

Descripción. Association Request: después de autenticarse, el cliente pide la asociación al AP.

FC[0] 0x10

Descripción. Association Response: el AP manda este mensaje al cliente para decirle si lo acepta. Algunos AP con filtro por dirección MAC no aceptan el cliente si su MAC no pertenece a la lista permitida.

FC[0] 0xA0

Descripción. Dissasociation: Se puede mandar del AP al cliente o al revés para informar de una desconexión. Puede sere muy poderoso para forzar a un cliente a empezar otra vez el proceso de autenticación en el caso de LEAP, WPA-PSK.

¿Cómo se manejan las MAC?

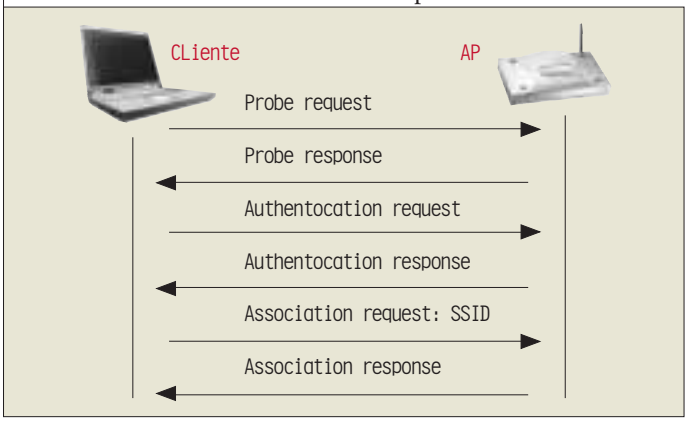
To DS	From DS	MAC 1	MAC 2	MAC 3
0	0	DA	SA	BSSID
1	0	BSSID	SA	DA
0	1	DA	BSSID	SA

SA = Source Address (Mac de la máquina fuente, que manda el paquete)

DA = Destination Address (Mac de la máquina destino, a quien se manda el paquete)

BSSID = Base Station Service Identifier (MAC del AP)

Inicio de comunicación sin encripción ni autenticación

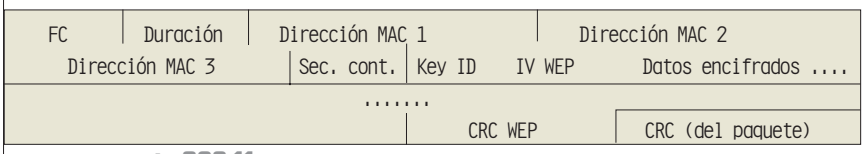


Una captura de OPEN authentication:

```
23. 534752 Proxim_51:5f:cd   BelkinCo_66:3f:4a  IEEE 8 Authentication
23. 534992                   Proxim_51:5f:cd (R IEEE 8 Acknowledgement
23. 535764 BelkinCo_66:3f:4a Proxim_51:5f:cd    IEEE 8 Authentication
23. 536025                   BelkinCo_66:3f:4a  IEEE 8 Acknowledgement
23. 536917 Proxim_51:5f:cd   BelkinCo_66:3f:4a  IEEE 8 Association Request, SSID: "WLAN"
23. 537185                   Proxim_51:5f:cd (R IEEE 8 Acknowledgement
23. 537763 BelkinCo_66:3f:4a Proxim_51:5f:cd    IEEE 8 Association Response
23. 538015                   BelkinCo_66:3f:4a  IEEE 8 Acknowledgement
```

En el FC vimos, en el segundo octeto, un bit Crypt; si su valor es 1, entonces el paquete viene encifrado.

Caso de un paquete con WEP:



paquete 802.11

El análisis de un paquete nos puede ayudar a entender un poco todo lo antes visto.

```
0x0000: 0842 0201 000C 5500      A5AF 0030 BD66 3F94
0x0010: 0007 50B7 4AD70075       DB12 FA00 FE48 91F2
0x0020: ..... 0106 1A2A
```

- FC[0] : 0x08 : 00001000 : paquete de datos (type = 10 y subtype = 0000)
- FC[1] : 00101010 Crypt = 1 , To DS=0 y From DS = 1, Paquet encifrado que viene del AP.
- MAC 1 : 00:0C:55:00:A5:AF : MAC destino – a quien se manda, esta dirección puede ser broadcast (ffffffffffff)
- MAC 2 : 00:30:BD:66:3F:94 . BBSID. MAC del AP
- MAC 3 : 00:07:50:B7:4A:D7 : MAC fuente. Dirección MAC de quien nos mandó el paquete. Puede ser una máquina ubicada en la LAN.
- IV : 0xDB12FA . Initialization Vector.
- KEYid : 0x00. Cuál llave usamos de 0, 1, 2, 3. Si el valor es 0x20, entonces estamos hablando de WPA.
- WEP ICV : 0x01061A2A . Checksum del WEP (cifrado).

WEP

WEP (Wired Equivalent Privacy) es un mecanismo que permite cifrar los paquetes emitidos usando el algoritmo RC4, desarrollado por Donald Rivest. Su uso es muy sencillo, se declara una llave privada compartida entre los clientes y el (o los) AP. Puede percatarse de que su administración es un poco pesada, porque para modificar la llave necesita cambiarla en todos los equipos, aun es mejor decir que regularmente nadie cambia la llave una vez escogida.

WEP está basado en RC4, un algoritmo que permite encifrar de forma rápida cadenas grandes. Su funcionamiento es el siguiente:

Los dos lados comparten una llave secreta de 40 o 104 bits.

Cada paquete que se manda por la red estará encifrado de la siguiente forma:

- Se crea un Initialization Vector (IV), con un valor sobre 24bits, que será diferente para cada paquete
- Se concatena el IV con la llave compartida que da un valor sobre 64bits o 128bits
- Este valor sirve para iniciar una secuencia pseudo-aleatoria para encifrar los paquetes
- Se calcula un CRC32 sobre el paquete a encifrar y se concatena al paquete no encifrado
- El algoritmo aplica una XOR entre el paquete a encifrar (con su CRC32, llamada Integrity Check Value, ICV) y la secuencia pseudo-aleatoria
- Finalmente se manda el paquete encifrado con el IV que sirvió (con la llave secreta) a iniciar la secuencia usada para encifrar.

La XOR es una operación bit a bit de suma en base 2. No se puede (en teoría) encontrar la secuencia inicial si no se sabe cuál fue la secuencia usada con la XOR.

Ejemplo:

1 XOR 1 = 0
1 XOR 0 = 1
0 XOR 1 = 1
0 XOR 0 = 0

Si:

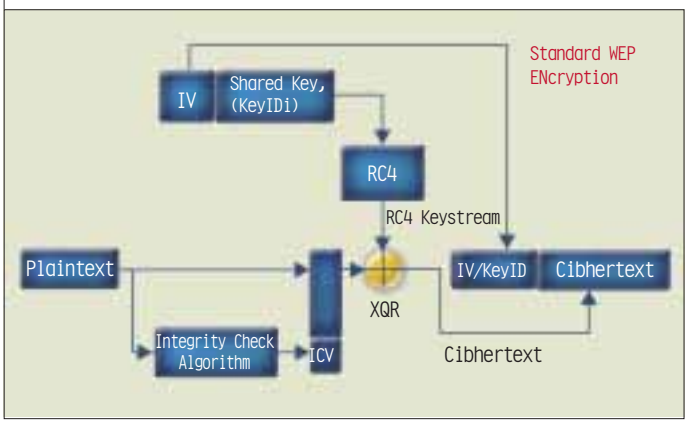
A=110110
B=011101

La operacion XOR tiene la siguiente característica:

A XOR B = 101011 = C
C XOR A = 011101 = B
C XOR B = 110110 = A

Para descifrar puede verse que si puede generarse la secuencia pseudo-aleatoria (lo que puede hacerse si se conoce IV + llave secreta) puede recuperarse el paquete descifrado a través de un XOR entre el paquete encifrado y la secuencia pseudo-aleatoria (por eso se manda el IV).

MECANISMO PARA CIFRAR:



En lugar de tener una sola llave, puden tenerse cuatro diferentes, así que se necesita decir cuál de las llaves se usa, lo que aparece en el KeyID (0-3).

La problemática de WEP hoy en día es que, teniendo una cierta cantidad de IV únicos, se puede encontrar la llave secreta de forma casi instantánea, como podrá verse en el siguiente artículo sobre ataques. La conclusión es muy sencilla: **no usar WEP solamente**.

En la práctica puede configurarse en los clientes la llave WEP de forma manual (introducir a mano los cinco o 13 octetos, 40bits o 104bits) o de forma "automática" usando una "passphrase" (palabra o sentencia) que generará la llaves automáticamente. El segundo permite implementar WEP de forma más sencilla dentro de los clientes, ¡pero tenga cuidado, sigue siendo WEP!

Existe una herramienta que permite hacerlo de forma manual, nwepgen (parte del paquete linux-wlan-ng).

¿QUÉ MÁS?

Debido a la debilidad de WEP, el IEEE trabajó sobre una extensión del estándar 802.11, llamado 802.11i (o WPA2). Mientras se desarrollaron sistemas muy cercanos a lo que iba a ser la norma, como Cisco LEAP o WPA. Para entender el funcionamiento de estos nuevos métodos de seguridad necesita conocer varios aspectos.

EL PROTOCOLO EAP

EAP (Extensible Authentication Protocol) fue desarrollado para convertirse en el modo de autenticación de PPP y poder usar nuevos modos de autenticación. De hecho, encontró su lugar con la llegada de las redes inalámbricas y la necesidad de autenticar los usuarios. EAP (RFC 2284) propone un sistema de autenticación modular que posee una base única. Así, cualquier sistema que use EAP podrá extenderse mediante módulos de autenticación.

EAP solamente tiene cuatro mensajes:

- EAP-Request
- EAP-Response
- EAP-Success
- EAP-Failure

Estos mensajes se intercambian entre el sistema que autentifica (el authenticator) y el sistema que pide la autenticación (supplicant). Al establecer la sesión, el authenticator manda varias "request" a las cuales el supplicant deberá responder. Cada request tiene un campo que permite definir el tipo de respuesta esperada por el authenticator:

- Identidad
- Challenge MD5
- One Time Password
- ...

Al finalizar el intercambio de autenticación el authenticator dará el resultado de la autenticación a través de los mensajes (EAP-Success o EAP-Failure).

El encabezado EAP contiene los campos:

- Code : describe el tipo de paquete
- 1 : EAP-Request
- 2 : EAP-Response
- 3 : EAP-Success
- 4 : EAP-Failure
- Identifier : provee un número de identificación que permite asociar una respuesta a una petición
- Length : longitud del paquete
- Data : los datos necesarios a EAP. En el casos de EAP-Request y Response, el campo Data contiene 2 subcampos Type y Type-Data.
- Type : indica el tipo de request / response
- Type-Data : provee los datos asociados como challenge, respuesta al challenge.

Ejemplos de Type:

- 1 : Identity
- 2 : Notification
- 3 : Nak
- 4 : EAP-MD5
- 5 : EAP-OTP
- 6 : EAP-GTC
- 7 : EAP-PAP
- 13 : EAP-TLS
- 17 : LEAP (cisco)
- 21 : EAP-TTLS
- 25 : PEAP

El mensaje Identity sirve para pedir el login del supplicant (cliente) en caso de una autenticación que usa usuario/contraseña. El mensaje Notification permite intercambiar informaciones no relacionadas con el proceso y Nak sirve para notificar a la otra parte que no soporta el método proporcionado. Los otros Type definen los métodos EAP.

En la vida real, EAP se usa en conjunto con 802.1x, éste se basa en EAP porque es una buena respuesta a las necesidades de 802.1x.

802.1x permite controlar el acceso a una red, al imponer una autenticación a los elementos conectados, puede aplicarse tanto a redes cableadas como inalámbricas. Y si antes no fue muy popular en las redes de cable, encuentra su lugar en las redes inalámbricas que necesitan un método para autenticar a los usuarios.

La arquitectura 802.1x tiene tres componentes:

- El supplicant, que pide la autenticación (el cliente)
- El authenticator, que autoriza o no el acceso (el Access Point)
- El servidor de autenticación que valida o no la autenticacion (servidor RADIUS con bases de datos de usuarios/contraseñas como Active Directory, por ejemplo)

La autenticación 802.1x empieza por un paquete EAPoL-Start o EAP-W-Start (caso inalámbrico) y la sesión se acaba con EapoL-Logoff o EapoW-Logoff.

802.1x es un estándar muy genérico como tal. Lo que debe recordarse son los roles que definen al supplicant, al authenticator y al servidor de autenticación.

MÉTODOS DE AUTENTICACIÓN SOPORTADOS POR EAP

Como se ha visto, EAP es un protocolo que permite realizar varios métodos de autenticación. Ahora se verá un poco acerca de ellos.

EAP-MD5

Permite autenticar un usuario a través de un clásico challenge/response. El problema aquí es que un pirata que capture el challenge y la respuesta podrá empezar un ataque al estilo *brute-force*.

EAP-PAP

Usa el mismo que PAP y manda la contraseña en texto claro. ¡No muy buena idea! Como se verá, se puede usar pero en combinación con un método *tunelisado*.

EAP-SIM

Permite autenticación a través de tarjetas con chip.

LEAP (LIGHTWEIGHT EAP)

Fue desarrollado por CISCO y usa una doble autenticación MSCHAPv2, así que permite a ambos lados autenticarse uno al otro. El problema de LEAP es su vulnerabilidad a ataques con diccionarios (vea el siguiente artículo).

MÉTODOS *TUNELISADOS*

Con estos métodos, primero se levanta un túnel seguro y después se autentica el usuario. Los tres métodos son EAP-TLS, EAP-TTLS y PEAP.

EAP-TLS

Es un sistema de doble autenticación que usa certificados. Es un método seguro y fuerte, pero su problema es que tanto el cliente como el servidor deben tener su propio certificado lo que impone instalar una arquitectura PKI interna, lo que no siempre es posible.

EAP-TTLS

Primero, el cliente se conecta al servidor, recibe su certificado y levanta un túnel cifrado. Sigue autenticar con otro método al cliente a través del túnel.

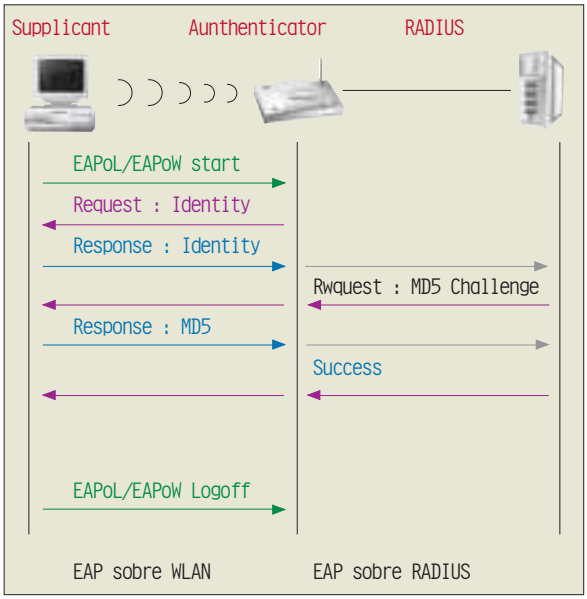
PEAP

Producto de Microsoft y Cisco, funciona igual que EAP-TTLS pero no permite modo de autenticación UAP (User Authentication Protocols).

La ventaja de los modos tunelisados es que una vez levantado el túnel entre el supplicant (cliente) y el servidor, cualquier método EAP se puede usar sin riesgo de intercepción y crackeo por *brute-forcing* o diccionario. Hoy en día un sistema seguro debería implementar EAP-TTLS/PEAP y otro modo de autenticación dentro del túnel.

Nota: el servidor de autenticación debe soportar los métodos EAP usados (no siempre es el caso).

Ejemplo con EAP-MD5 y 802.1x:



WPA

WPA (Wi-fi Protected Access) fue un predesarrollo de la norma 802.11i cuando todavía no estaba finalizada. WPA incluye todos los mecanismos necesarios para cumplir con la 802.11i (WPA2).

- TKIP (Temporal Key Integrity Protocol): cada paquete esta encifrado por una llave única y basado en sesión (significa llaves diferentes por todos los usuarios y por paquete). A diferencia de WEP, que usa siempre la misma llave secreta para la generación de la secuencia pseudo-aleatoria (MIC es una subparte de TKIP).
- MIC (Message Integrity Checksum): mecanismo más fuerte de control de erores o modificación
- Initialization Vector (IV) sobre 32bits (en lugar de 24bits) que reduce los riesgos de colisión y ofrece un mayor rango disponible
- EAP y 802.1x : permite autenticación del usuario, lo que no se podía con WEP solamente.

WPA PERMITE DOS MODOS DE AUTENTICACIÓN:

- Modo Pre-Shared Key (WPA-PSK): cada lado tiene una llave secreta preconfigurada, vulnerable a ataques con diccionarios.
- Modo autenticación 802.1x/EAP: más seguro si está bien implementado (use modo *tunelisado*).

LINK

Para más sobre WPA:
http://www.wi-fi.org/OpenSection/pdf/WPA_for_Public_Access_Final.pdf

WPA2 O 802.11I

WPA2 es igual a WPA, solamente que provee encripción con AES (un gran paso a comparación de WEP) y tiene un modo de pre-autenticación para el roaming.

CONCLUSIÓN

Como se apreció, al inicio 802.11 era muy pobre en métodos muy seguros. La llegada de 802.11i promete un uso más seguro y confidencial de las redes inalámbricas mediante un servidor de autenticación externo y protocolos para cifrar más robustos (AES). Ahora el asunto es la migración, no siempre sencilla, pero necesaria hacia por lo menos WPA o WPA2 **en conjunto con un método de autenticación *tunelisado* (PEAP, EAP-TTLS).**

LINKS

[1] Ethereal - snifer : www.ethereal.com
[2] Network Sorcery : http://www.networksorcery.com/enp/protocol/eap.htm