Seguridad en WiFi (Técnico)

Por: Alejando Corletti Estrada.
Acorletti@hotmail.com

Madrid, mayo de 2005.

Este texo forma parte de una dupla que por razones de "Humanización", ha sido dividido en un Resumen Ejecutivo (más breve) y un informe técnico (casi inhumano). Basado en estas dos presentaciones se invita al lector a optar por el grado de detalle que desee. Los documentos son: Seguridad en WiFi (Resumen ejecutivo) - Seguridad en WiFi (Técnico).

Temario

DESARROLLO:

I. Presentación (Los estándares 802.11):

WiFi (Wireless Fidelity) es un nombre comercial desarrollado por un grupo de comercio industrial llamado WiFi Alliance (Inicalmente: 3Com – Aironet [hoy parte de CISCO] – Harris – Lucent – Nokia y Symbol technologies, hoy más de 150 miembros), el nombre "oficial" de esta alianza es **WECA** (Wireless Ethernet Compatibility Alliance) y son los primeros responsables de 802.11b.

WiFI describe los productos de WLAN basados en los estándares 802.11 y está pensado en forma más "Amigable" que la presentación eminentemente técnica que ofrece IEEE. Se podría llegar a discutir si

cubre o no todo lo que ofrece 802.11 o no, pues alguno de ellos podría ser puesto en duda, pero a los efectos de este texto, se hará más referencia a lo que establece 802.11, sin detenerse en estas diferencias.

La web de esta alianza es

www.wi-fi.org
www.wifi-alliance.net

En esas web se puede también consultar el estado "on Line" de los productos que se encuentran certificados, el path completo de esta consulta es:

http://www.wi-fi.org/OpenSection/Certified_Products.asp?TID=2

El estándar **802.11** de IEEE se publica en junio 1997, luego de seis años de proceso de creación. Propone velocidades de 1 y 2Mbps y un rudimentario sistema de cifrado (el **WEP**:Wired Equivalent Privacy), opera en 2,4 GHz con RF e IR. Aunque WEP aún se sigue empleando, ha sido totalmente desacreditado como protocolos seguro.

En septiembre de 1999 salen a la luz el estándar **802.11b** que ofrece 11Mbps y el **802.11a** que ofrece 54 Mbps, si bien los productos de la primera aparecieron en el mercado mucho antes.

Modo turbo: Algunos fabricantes ofrece velocidades de 72 e incluso 108 Mbps. Estos procesos, lo logran mediante la "Vinculación de canales", es decir, dos canales son multiplexados juntos empleando el total de velocidad de la suma de ambos. Esto si bien es favorable aparentemente, tiene las desventajas de no respetar el estándar y de sacrificar la mitad de los canales de 802.11a.

La familia 802.11, hoy se encuentra compuesta por los siguientes estándares:

- **802.11a:** (5,1-5,2 Ghz, 5,2-5,3 Ghz, 5,7-5,8 GHz), 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal
- **802.11b:** (2,4-2,485 GHz), 11 Mbps.
- 802.11c: Define características de AP como Bridges.
- 802.11d: Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).
- 802.11e: Calidad de servicio (QoS).
- 802.11f: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol.
- **802.11g**: (2,4-2,485 GHz), 36 o 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.
- 802.11h: DFS: Dynamic Frequency Selection, habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.
- **802.11i:** Seguridad (aprobada en Julio de 2004).
- 802.11j: Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).

- 802.11m: Mantenimiento redes wireless.

Quizás el tema más importante a destacar es la posibilidad de expansión de 802.11. El incremento constante de mayores velocidades, hace que los 11 Mbps de 802.11b, estén quedando pequeños. La migración natural es hacia 802.11g, pues sigue manteniendo la frecuencia de 2,4GHz, por lo tanto durante cualquier trancisión en la que deban convivir, ambos estándares lo permiten. En cambio si se comienzan a instalar dispositivos 802.11a, los mismos no permiten ningún tipo de compatibilidad con 802.11b, pues operan en la banda de 5 GHz.

Para acotar únicamente el tema de seguridad, se tratarán sólo 802.11a, b g y 802.11i.

Hoy en día se puede decir que existen tres estándares de WLAN:

- **HomeRF:** Es una inciativa lanzada por Promix, principalmente en EEUU y orientada exclusivamente al mercado residencial. Tiene sus bases en los estándares de teléfono digital inalámbrico mejorado (DECT)
- **BlueTooth:** Lo inició IBM, orientado al mercado comercial/ventas, y a la interconectividad de elementos de hardware. En realidad no compite con 802.11, pues tiene la intención de ser una estándar con alcance nominal de 1 a 3 metros y a su vez no supera los 1,5 Mbps
- **802.11:** Cubre todo el espectro empresarial.

Una iniciativa que se debe mencionar también es **HiperLAN** en sus versiones 1 y 2. Se trata de una verdadera analogía inalámbrica para ATM. Fue un competidor de 802.11 que opera en la frecuencia de 5 GHz y gozó del apoyo de compañías como Ericsson, Motorola, Nokia; Panasonic y Sony, se llegaron a crear regulaciones por parte de ETSI al respecto, pero no se logró imponer y hoy en día está prácticamente en desuso. En lo particular me hace acordar mucho a la batalle que hubo entre ATM y Ethernet (Fast ethernet, giga ethernet....).

Definiciones a tener en cuenta en este texto:

- **Access control:** Es la prevención del uso no autorizado de recursos.
- **Access Point** (**AP**): Cualquier entidad que tiene funcionalidad de estación y provee acceso a servicios de distribución vía **wireless medium** (**WM**) para estaciones asociadas.
- **Ad Hoc network**: red wireless compuesta únicamente por estaciones con iguales derechos.
- **Portal**: punto lógico desde el cual se conecta una red wireless con una no wireless.
- **Station** (**STA**):cualquier dispositivo que cumple con un nivel MAC conforme a 802.11 y un nivel físico que posee una interfaz wireless.
- **Portable station**: estación que puede ser movida de ubicación, pero que solo puede Tx o Rx en estado fijo.
- **Movile station**: Estación que permite Tx o Rx en movimiento.

El tema de seguridad, no puede ser tratado con seriedad, si previamente no se tienen en cuenta varios conceptos de BASE que hacen a la arquitectura WiFi. Una vez comprendido el funcionamiento básico de esta infraestructura, recién entonces se puede hablar de seguridad. En virtud de este concepto es que en este texto, se trata inicialmente una serie de conceptos básicos, para luego profundizar en los aspectos de seguridad WiFi.

II. Modelo de capas de 802.11.

1. La capa física de 802.11: (El detalle de la misma se puede ver en el **ANEXO 2**)

La capa física la componen dos subcapas:

- PLCP (Physical Layer Convergence Protocol): Se encarga de codificación y modulación.
  - Preámbulo (144 bits = 128 sincronismo + 16 inicio trama).
  - HEC (Header Error Control): CRC 32
  - Modulación (propagación) DSSS o FHSS o IR.
- PMD (Physical Medium Dependence): Es la que crea la interfaz y controla la comunicación hacia la capa MAC (a través del SAP: Service Access Point)

Este nivel lo conforman dos elementos principales:

- **Radio**: Recibe y genera la señal.

- **Antena:** Existe una gran variedad y no será tratado en este texto.

El estándar 802.11 define en el punto 12 del mismo todas las especificaciones de servicio para este nivel, las cuales no serán tratadas en este texto. Hay algunos aspectos físicos que vale la pena profundizar para la comprensión de WiFi, de los cuales se recomienda especialmente:

- FHSS (Frequency Hopping Spread Spectrum) para la banda de 2,4 GHz (ISM: Industrial, Scientific and Medical band) en el punto 14 de la recomendación.
- DSSS (Direct Sequence Spread Spectrum para 2,4 GHz, en el punto 15.
- IR (InfraRed), en el punto 16.

NOTA: Aunque esto no forma parte de los conceptos de WiFi, cuando se habla de transmisión, se deben diferenciar tres palabras:

- Modulación: Es el método de emplear una señal portadora y una moduladora (que da forma a la anterior). Cada una de ellas puede ser analógica o digital, con lo cual se obtienen cuatro posibles combinaciones de portadora y moduladora (AA – AD – DA y DD), con las cuales se conforman todas las técnicas de modulación. WiFi en la mayoría de los casos emplea la técnica QAM (Modulación en cuadratura de Fases con más de un nivel de amplitud).
- Propagación: Es la forma en la cual "van saliendo" las señales al aire. Aquí es donde verdaderamente se aplican las técnicas de DHSS y FHSS. SS (Spread Spectrum) es la técnica de emplear muchas subportadoras de muy baja potencia con lo cual se "expande" el espectro útil. En cuanto a DH y FH El ejemplo típico que se emplea para estas técnicas es la analogía con una terminal de trenes, en la cual existen varios andenes. Para DH, los trenes estarían saliendo, primero el andén 1, luego el 2, a continuación el 3, 4, 5... y así sucesivamente, respetando siempre este orden. Para FH, la salida de los trenes no respeta el orden y puede ser aleatoria o acorde a un patrón determinado (WiFi hace un muy buen uso de esto, pues en las subportadoras que recibe mucha interferencia no las usa o emplea menos cantidad de bits en las mismas).

- Codificación: Es la asociación de bit a cada "muestra" que se obtiene. WiFi en la mayoría de los casos emplea el código Barker.

2. La capa de enlace de 802.11:

Respetando el modelo OSI, en este texto se agrupará en el nivel de enlace, los dos subniveles que lo conforman (MAC: Medium Access Control y LLC: Logical Link Control). Desde el punto de vista de 802.11, solo interesa hacer referencia al subnivel MAC (En el **ANEXO 4: Capturas**, se pueden apreciar varios tipos de tramas).

- **Capa MAC**: Controla el flujo de paquetes entre 2 o más puntos de una red . Emplea CSMA/CA: Carrier Sense Multiple Access / Collision avoidance. Sus funciones principales son:
  - **Exploración:** Envío de Beacons que incluyen los SSID: Service Set identifiers O también llamados ESSID (Extended SSID), máximo 32 carateres.
  - **Autenticación:** Proceso previo a la asociación. Existen dos tipos:
    → Autenticación de sistema abierto: Obligatoria en 802.11, se realiza cuando el cliente envía una solicitud de autenticación con su SSID a un AP, el cual autorizará o no. Este método aunque es totalmente inseguro, no puede ser dejado de lado, pues uno de los puntos más fuertes de WiFi es la posibilidad de conectarse desde sitios públicos anónimamente (Terminales, hoteles, aeropuertos, etc.).
    → Autenticación de clave compartida: Es el fundamento del protocolo WEP (hoy totalmente desacreditado), se trata de un envío de interrogatorio (desafío) por parte del AP al cliente.
  - **Asociación:** Este proceso es el que le dará acceso a la red y solo puede ser llevado a cabo una vez autenticado
  - **Seguridad:** Mediante WEP, con este protocolo se cifran los datos pero no los encabezados.
  - **RTS/CTS:** Funciona igual que en el puerto serie (RS-232), el aspecto más importante es cuando existen "nodos ocultos", pues a diferencia de Ethernet, en esta topología SÍ pueden existir nodos que no se escuchen entre sí y que solo lleguen hasta el AP, (Ej: su potencia está limitada, posee un obstáculo entre ellos, etc), en estos casos se puede configurar el empleo de RTS/CTS. Otro empleo importante es para designar el tamaño máximo de trama (en 802.11 Es: mínimo=256 y máximo=2312 Bytes).
  - **Modo ahorro de energía:** Cuando esta activado este modo, el cliente envió previamente al AP una trama indicando "que se irá a dormir", El AP, coloca en su buffer estos datos. Se debe tener en cuenta que por defecto este modo suele estar inactivo (lo que se denomina Constant Awake Mode: CAM).
  - **Fragmentación:** Es la capacidad que tiene un AP de dividir la información en tramas más pequeñas.

3. Topología WiFi:

802.11 presenta dos topologías:

- **Ad Hoc (o peer to peer)**: Dos o más clientes que son iguales entre ellos.
- **Infraestructura**: Red centralizada a través de uno o más Access Point (AP).

Descripción general de componentes de las mismas:

- **BSS** (Basic Service Set): Es el bloque básico de construcción de una LAN 802.11. En el caso de tratarse de únicamente 2 estaciones ser denomina IBSS (Independent BSS), es lo que a menudo se denomina "Ad Hoc Netwok".
- **DS** (Distribution System): Es la arquitectura que se propone para interconectar distintos BSS. El **AP** es el encargado de proveer acceso al DS, todos los datos que se mueven entre BSS y DS se hacen a través de estos AP, como los mismos son también STA, son por lo tanto entidades direccionables.
- **ESS** (Extended Service Set): Tanto BSS como DS permiten crear wireless network de tamaño arbitrario, este tipo de redes se denominan redes ESS.
- La integración entre una red 802.11 y una No 802.11 se realiza mediante un **Portal**. Es posible que un mismo dispositivo cumpla las funciones de AP y Portal.

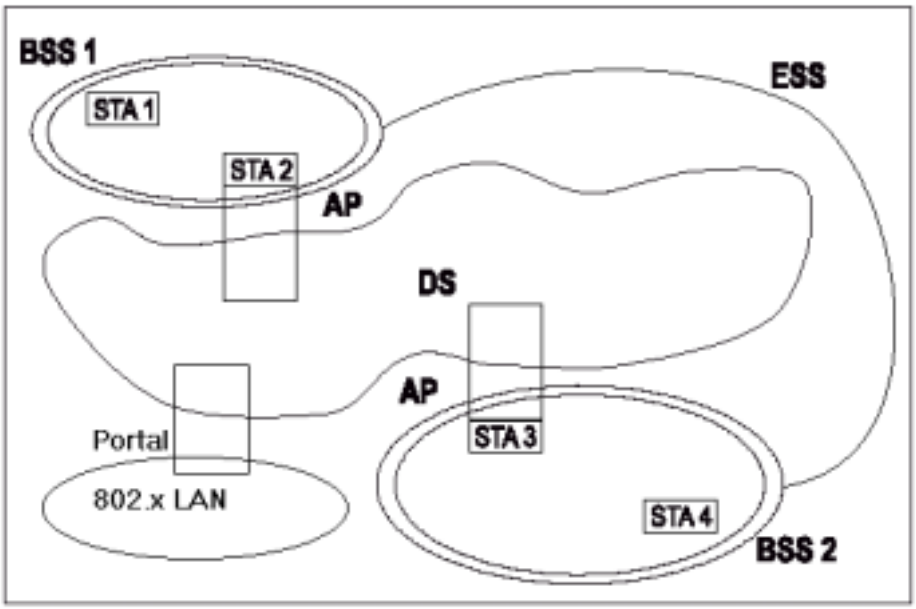


Figura 1 (Componentes de la arquitectura)

III. Seguridad en WiFi:

Los tres aspectos fundamentales que se deben tener en cuenta al diferenciar una red WiFi de una cableada, son:

- Autenticación
- Control de acceso
- Confidencialidad

1. Autenticación y control de acceso:

Los métodos que se emplean son los siguientes:

a. SSID (Service Set Identifier): Contraseña (**WEP**) El detalle de funcionamiento de WEP se presenta en el **ANEXO 2** de este texto.
   El estándar 802.1x (que se menciona a continuación), permite un empleo de WEP para autenticación que se denominó "Dynamic WEP", que permite emplear este algoritmo como parte de 802.1x, de forma un poco más segura que el "WEP estático", pero la alianza WiFI recomienda no emplear ninguno de ellos en entornos seguros.

b. Seguridad por restricción de direccionamiento MAC: Permite restringir a un lsitado de direcciones, las que se pueden conectar y las que no.
c. Contraseñas no estáticas:
   - Periódicas:
   - OTP (One Time Password): Contraseñas de un solo uso, también conocidas como token flexibles.

d. 802.1x: Este estándar no fue presentado para WiFi, sino para el acceso seguro PPP (en tecnologías de cable). Una de las grandes características de WiFi es la de "no reinventar la rueda" y emplear todas las herramientas que ya existen y pueden prestar utilidad al mismo. 802.1x es uno de los mejores ejemplos de esto.

   La arquitectura 802.1x está compuesta por tres partes:
   - **Solicitante:** Generalmente se trata del cliente WiFi
   - **Auenticador:** Suele ser el AP, que actúa como mero traspaso de datos y como bloqueo hasta que se autoriza su acceso (importante esto último).
   - **Servidor de autenticación:** Suele ser un Servidor RADIUS (Remote Authentication Dial In User Service) o Kerberos, que intercambiará el nombre y credencial de cada usuario. El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo.

   Otra de las grandes ventajas de emplear 802.1x es que el servidor de autenticación, permite también generar claves de cifrado OTP muy robustas, tema en particular que ya lo posiciona como imprescindible en una red WiFi que se precie de segura.

e. **802.11i:** El Task Group de IEEE 802.11i, se conformó en el año 2001, con la intención de analizar una arquitectura de seguridad más robusta y escalable, debido a la inminente demanda del mercado en este tema y en julio de 2004 aprobó este estándar. Por su parte la WiFi Alliance lo lanzó al mercado en septiembre de ese año.

   En forma resumida, este nuevo estándar, propone a 802.1x como protocolo de autenticación, pudiendo trabajar con su referencia **EAP** (Extensible Authentication Protocol: **RFC 2284**), este último proporciona una gran flexibilidad (sobre todo a los fabricantes) en la metodología de autenticación.

Previo al estándar, Cisco Systems ofreció el primer tipo de autenticación que se deniminó **LEAP** (Lightweight EAP), protocolo que inicialmente fue propietario de Cisco, pero en la actualidad lo emplean varios fabricantes. Cisco se está volcando hacia **PEAP** (se describe a continuación).

Por su parte Microsoft, inicialmente junto con Windows XP (hoy con todos sus SSOO), lanzó al mercado su protocolo denominado **EAP/TLS** (Extensible Authentication Protocol with Transport Layer Security - RFC: 2716), y fue aceptado por IEEE, se basa en certificados en lugar de contraseñas como credenciales de autenticación. Otros fabricantes han presentado **EAP/TTLS** (EAP with Tunneling Transport Layer Security), el cual realiza un túnel de nivel 2 entre el cliente y el AP, una vez establecido el túnel, EAP/TTLS opera sobre él, lo cual facilita el empleo de varios tipos de credenciales de autenticación que incluyen contraseñas y certificados, en realidad no deja de ser una variante de EAP/TLS.

La última variante es **PEAP** (Protected Extensible Authentication Protocol), inicialmente fue la versión "0" y ya está vigente la versión "1", el cual aplica una metodología muy similar a EAP/TTLS en cuanto al empleo de túnel y sobre el una amplia variedad de credenciales de autenticación, este último ya está soportado por los más importantes fabricantes. En general, se considera que PEAP es el método más seguro del momento. Este protocolo fue desarrollado por Microsoft, Cisco y RSA.

Todas estas variantes de autenticación están contempladas en 802.11i (Se detalla en el **ANEXO 3**)

2. Cifrado:

a. **WEP:** Emplea el algoritmo de cifrado de flujo **RC4** (Rivest Cipher 4), este algoritmo es una de las bases de RSA y cabe aclarar que es también empleado en el estándar SSL (Secure Socket Layer), se trata de un algoritmo robusto y veloz. Los problemas de WEP, no son por este algoritmo, sino por la debilidad de sus claves, tanto en 64, 128 (y hoy también 156) bits, de los cuales se deben excluir los 24 del VI (Vector de inicialización), hoy en día cualquier usuario con "Airsnort" lo descifra, sin tener ningún conocimiento especializado, incluso la metodología de "Airsnort" es pasiva, es decir, únicamente escucha tráfico, hoy existen herramientas mucho más potentes que operan de forma activa, que emplean varias técnicas para generar tráfico y basado en las respuestas de la red permiten acelerar exponencialmente el proceso. Estas últimas metodologías se denominan INDUCTIVAS y existen dos grandes familias: ataques de repetición y ataques de modificación de bits.

   Existen también ataques de fuerza bruta, basados principalmente en técnicas de diccionario, las cuales en el caso de WEP, son de especial interés, pues el nombre de usuario viaja en texto plano, lo cual ofrece una gran ventaja para generar posibles claves.

b. Las deficiencias presentadas por RC4 y WEP, se están tratando de solucionar en la actividad de cifrado, a través del protocolo **TKIP** (Temporal Key Integrity Protocol). Esta propuesta aparece a finales de 2002, también se basa en RC4, pero propone tres mejoras importantes:

- **Combinación de clave por paquete:** La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Pre-shared Key). Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.

- **VI** (Vector de inicialización) de **48 bits**: Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones. Si se realiza un gran simplificación (pues el caso es más complejo) y se divide 280 billones sobre 16 millones, el resultado es: 17.500.000, por lo tanto si un VI de 24 bits se repite en el orden de 5 horas en una red wireless de una mediana empresa, entonces un VI de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años, es decir se repetiría después de la Guerra de las Galaxias. Ya se pone complicada la cosa.....

- **MIC** (Message Integrity Check): Se plantea para evitar los ataques inductivos o de hombre del medio. Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y genera una alerta, que indica una posible falsificación del mismo.

Desafortunadamente TKIP, no está contemplado aún en la totalidad de los productos.

c. Microsoft ofrece otra alternativa que inicialmente denominó **SSN** (Simple Security Network), el cual es un subconjunto de 802.11i y al mismo tiempo una implementación de TKIP al estilo Microsoft. SSN lo adoptó 802.11i renombrándolo como **WPA** (WiFi Protected Access), en el año 2004 aparece **WPA2** que es la segunda generación del WPA . Este ya proporciona encriptación con AES (que se menciona a continuación), un alto nivel de seguridad en la autentificación de usuarios y está basado en la norma IEEE 802. 11i y forma parte de ella (Ver **ANEXO 3**).

Aunque la WPA impulsa la seguridad WLAN, muchos la consideran una solución temporal pues la solución de 802.11 se orienta más hacia el Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (Counter-Mode/CBC-Mac Protocol, que se abrevia: **CCMP**), que también forma parte de la norma 802.11i. Se trata de un nuevo modo de operación para cifrado de bloques, que habilita a una sola clave para ser empleada tanto en autenticación como para criptografía (confidencialidad). Se trata de un verdadero "Mix" de funciones, y su nombre completo proviene el "**Counter mode" (CTR**) que habilita la encriptación de datos y **el Cipher Block Chaining Message Authentication Code (CBC-MAC)** para proveer integridad, y de ahí su extraña sigla CCMP.

El protocolo **CCMP** usa la **Norma de Encriptación Avanzada** (**AES**) para proporcionar encriptación más fuerte. Sin embargo, AES no está diseñada para ser compatible con versiones anteriores de software.

A pesar de todos los esfuerzos realizados, muchas entidades siguen considerando a TKIP y WPA como métodos insuficientes de seguridad, el mayor exponente de esta posición es FIPS (Federal Information Process Standard), que excluye a RC4 en las comunicaciones confidenciales. Su publicación **FIPS-197** de finales del 2001, define al estándar **AES** (Advanced Encription Standard) que se mencionó en el punto anterior, con clave mínima de 128 bits, como el aplicable a niveles altos de seguridad. Este

estándar, propuesto por Rijndael, surgió como ganador de un concurso mundial que se celebró en el año 2000, para definir la ultima generación de estos algoritmos. La mayoría de los fabricantes están migrando hacia este algoritmo y se aprecia que será el estándar que se impondrá en el muy corto plazo.

El tema de AES tampoco es tan sencillo como parece, pues las implementaciones por software imponen una dura carga de trabajo al sistema, ocasionando demoras de rendimiento que pueden llegar al 50 % de la tasa efectiva de transmisión de información, por lo tanto, se debe optimizar este aspecto para que sea asumido por el mercado.

La WiFi Alliance propone dos tipos de certificación para lso productos, cuyas caracterísiticas se presentan a continuación:

- Modelo Empresas:
  - WPA:
    Autentication: IEEE 802.1x/EAP.
    Encryptation: TKIP/MIC.
  - WPA2:
    Autentication: IEEE 802.1x/EAP.
    Encryptation: AES-CCMP.

- Modelo personal (SOHO/personal):
  - WPA:
    Autentication: PSK.
    Encryptation: TKIP/MIC.
  - WPA2:
    Autentication: PSK.
    Encryptation: AES-CCMP.

3. VPNs: La última opción que se menciona aquí es la aplicación de VPNs directamente sobre la capa física de WiFi. Esta alternativa no responde a ningún estándar de WiFi, pero se trata de llevar al wireless toda la experiencia y solidez que tiene hoy esta tecnología. VPN nace (o mejor dicho crece) como respuesta a la inseguridad de Internet, red sobre la cual, muchas empresas se fueron volcando por el enorme abaratamiento que ofrece para interconectar puntos remotos de las mismas, dejando de lado carísimas líneas dedicadas. Existen muchos tipos de VPNs, que no se mencionarán aquí, por no ser parte de WiFi, pero sí se debe aclarar que es una opción muy válida y de hecho se está implementado cada vez con mayor frecuencia en las opciones de wireless.

IV. Problemas concretos de Seguridad en WiFi:

a. **Puntos ocultos:** Este es un problema específico de las redes inalámbricas, pues suele ser muy común que los propios empleados de la empresa por cuestiones de comodidad, instalen sus propios puntos de acceso. Este tipo de instalaciones, si no se controlan, dejan huecos de seguridad enormes en la red. El peor de estos casos es la situación en la cual un intruso lo deja oculto y luego ingresa a

la red desde cualquier ubicación cercana a la misma. La gran ventaja que queda de este problema es que es muy fácil su identificación siempre y cuando se propongan medidas de auditorías periódicas específicas para las infraestructuras WiFi de la empresa, dentro del plan o política de seguridad.

b. **Falsificación de AP:** Es muy simple colocar una AP que difunda sus SSID, para permitir a cualquiera que se conecte, si sobre el mismo se emplean técnicas de "Phishing", se puede inducir a creer que se está conectando a una red en concreto. Existen varios productos ya diseñados par falsificar AP, en la terminología WiFi se los suelen llamar "Rogue AP" o Fake AP", el más común es un concocido srcipt en Perl denominado justamente "FakeAP", que envía Beacons con diferentes ESSID y difernetes direcciones MAC con o sin empleo de WEP. Se puede descargar de :
Http://www.blackalchemy.to/project/fakeap/

c. **Deficiencias en WEP** (Características lineales de CRC32): Esta característica fue demostrada en teoría por Nikita Borisov, Ian Goldberg y David Wagner.
El ICV permite verificar la integridad de un mensaje, por lo tanto, el receptor aceptará el mensaje si su ICV es válido (Recuerdo que es un simple CRC32).
Esto presenta dos problemas:
   - El CRC es independiente de al clave empleada.
   - Los CRC son lineales CRC (m⊕k) = CRC (m) ⊕ CRC (k).

En virtud de esta linealidad, se puede generar un ICV válido. Un atacante debe interceptar un mensaje (conocido o no) y modificarlo en forma conocida para generar un mensaje m`, operando sobre el mismo obtendrá un paquete que será aceptado por el receptor.

d. **ICV independiente de la llave**: Esta característica fue demostrada en teoría por David Wagner.
Nuevamente se trata el ICV, el cual se calcula previamente a comenzar el proceso criptográfico, por lo tanto no depende de la clave ni del IV. Esta debilidad da lugar a que conocido el texto plano de un solo paquete encriptado con WEP, sea posible inyectar paquetes en la red.

e. **Tamaño de IV demasiado corto**:
El IV tiene 24 bits de longitud (2^{24} = 16.777.216) y viaja como texto plano. Un punto de acceso que opere con grandes volúmenes de tráfico comenzará a repetir este IV a partir de aproximadamente 5 horas. Esta repetición hace que matemáticamente se pueda operar para poder obtener el texto plano de mensajes con IV repetido (sin gran nivel de dificultad).
El estándar especifica que el cambio de IV es opcional, siendo un valor que empieza con cero y se va incrementando en uno.

f. Deficiencias en el método de autenticación:
Si un atacante captura el segundo y tercer mensaje de administración en una autenticación mutua. El segundo posee el desafío en texto plano y el tercero contiene el mensaje criptografiado con la clave compartida. Con estos datos, posee todos los elementos para autenticarse con éxito sin conocer el secreto compartido (Con esto sólo logra autenticarse, luego queda el acceso a la red).

g. **Debilidades en el algoritmo key Scheduling de RC4:** scott Fluhrer, Itsik Mantin y Adi Shamir publicaron en Agosto del 2001 la demostración teórica de la vulnerabilidad más devastadora de las

existentes hasta ahora en la encriptación WEP. Adam Stubblefield, un trabajador de AT&T Labs, fue la primera persona que implementó este ataque con éxito.
Demostraron que usando sólo la primera palabra de un keystream, podían obtener información de la clave secreta compartida. Se buscan IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición "*resolved condition*" o condición resuelta.
El número de paquetes que se necesitan recolectar antes de descubrir un byte de la llave varía en función de en que valor se encuentre el contador de IV's de las tarjetas que se estén monitorizando. Hay 9.000 IV's débiles en los 16 millones de IV's posibles.

¿Cuántos paquetes encriptados se necesitan recolectar para crackear la llave WEP?
- La mayoría de las llaves pueden ser adivinadas después de encontrar aproximadamente 2000 paquetes resueltos.
- Algunas llaves requieren que capturemos incluso más de 4000 paquetes resueltos

Se puede adivinar la llave después de recolectar de 5 a 10 millones de paquetes encriptados.
Poco después de que el trabajo realizado por estos tres autores y la vulnerabilidad práctica de Stubblefield fueran publicados, aparecieron dos herramientas en Internet que implementan totalmente el ataque:

- Wepcrack: http://wepcrack.sourceforge.net/
- Airsnort: http://airsnort.shmoo.com/

Esto fue la sentencia definitiva para WEP.

h. **Debilidad en WPA:** Un estudio realizado por Robert Moskowitz, director de ICSA Labs, indica que el sistema utilizado por WPA para el intercambio de la información utilizada para la generación de las claves de cifrado es muy débil.
Según este estudio, WPA en determinadas circunstancias es incluso más inseguro que WPE. Cuando las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque de diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red.
Es decir, a diferencia de WEP en que es necesario capturar un volumen significativo de tráfico para poder identificar las claves, en WPA únicamente capturando el tráfico de intercambio de claves para poder realizar este ataque de diccionario.
No es un problema nuevo, pues fue apuntado durante la verificación inicial del protocolo. Es solo una muestra que una implementación inadecuada puede afectar negativamente cualquier sistema de cifrado.
Como hemos indicado, el problema solo es explotable bajo una serie de circunstancias muy concretas. Este problema puntual no es, en absoluto, una indicación de la debilidad de WPA. Únicamente es un recordatorio de la necesidad de utilizar claves convenientemente largas y que incluyan caracteres especiales.

V. Medidas de Seguridad en WiFi:

a. Emplear las **mismas herramientas que los intrusos**: realizar la misma actividad, pero para el "lado bueno", es decir realizar controles periódicos con "Netstumbler", Escuchar tráfico e intentar obtener información trivial con "Kismet" o "AirSnort", medir potencias irradiadas con cualquier tarjeta desde los perímetros de la red.

b. **Mejorar la seguridad física**.

c. Cancelar puertos que no se emplean:

d. **Limitar el número de direcciones MAC** que pueden acceder. Esta actividad se realiza por medio de ACLs (Access List Control) en los AP, en las cuales se especifica (a mano) las direcciones MAC de las tarjetas a las que se les permitirá el acceso, negando el mismo a cualquiera que no figure en ellas. Cabe aclarar que es tremendamente fácil falsificar una dirección MAC (Ej: en los SSOO Linux es simplemente el comando *"ifconfig").*

e. Ya no se menciona el tema de cancelar la tramas Beacon en los AP, pues cualquier sistema de escucha, por más que no capture la trama Beacon, al capturar la trama PROVE REQUEST del cliente, o la trama PROVE RESPONSE del AP, en ellas también viaja el ESSID.

f. **Satisfacer la demanda:** Si se están empleando AP no autorizados por parte de los empleados, es porque les resulta útil, por lo tanto, se pueden adoptar las medidas para que se implanten, pero de forma segura y controlada, de otra forma, seguirán apareciendo, pero de forma clandestina.

g. **Controle el área de transmisión:** muchos puntos de acceso inalámbrico permiten ajustar el poder de la señal. Coloque sus puntos de acceso tan lejos como sea posible de las paredes y ventanas exteriores. Pruebe el poder de la señal para que usted únicamente pueda conectarse a estos sitios. Luego, asegúrese de cambiar la contraseña predeterminada en todos los puntos de acceso. Utilice una contraseña fuerte para proteger todos los puntos de acceso.

h. **Implemente la autenticación de usuario:** Mejore los puntos de acceso para usar las implementaciones de las normas WPA y 802.11i.

i. **Proteja la WLAN con la tecnología "VPN Ipsec" o tecnología "VPN clientless":** esta es la forma más segura de prestar servicios de autenticación de usuario e integridad y confidencialidad de la información en una WLAN. La tecnología adicional VPN no depende del punto de acceso o de la tarjeta LAN inalámbrica; por consiguiente, no se incurren en costos adicionales de hardware puesto que las normas de seguridad inalámbrica continúan evolucionando.

j. **Active el mayor nivel de seguridad que soporta su hardware:** incluso si tiene un equipo de un modelo anterior que soporta únicamente WEP, asegúrese de activarlo. En lo posible, utilice por lo menos una WEP con un mínimo de encriptación de 128 bits.

k. **Instale firewalls personales y protección antivirus en todos los dispositivos móviles:** la Alianza WiFi recomienda utilizar la política de seguridad de redes corporativas para imponer su uso continuo.

l. **Adquiera equipamiento que responda a los estándares** y certificado por "WiFi Alliance".

VI. Hardware y Software:

1. Tarjetas WiFi:

Las tarjetas Wi-Fi (802.11b) utilizan un chipset u otro según fabricante. Es posible que el mismo fabricante comercialice tarjetas con chipsets distintos, los chipsets más comunes son:

- Hermes (Lucent)
  - Lucent / Agere / Orinoco
    - → Orinoco, Avaya, Compaq, Lucent

- Prism 2 / 2.5 / 3 (Intersil)
  - D-Link, Linksys, Netgear, SMC, USR, Conceptronic

- Airo (Aironet)
  - Cisco

- TI ACX100 (Texas Instruments)
  - 3Com / USR, D-Link, Wisecom, Eusso, Linksys (WAP11 v2.2)

2. Herramientas:

Sistema Operativo Linux:
Kismet: http://www.kismetwireless.net/
Airsnort: http://airsnort.shmoo.com/
Ethereal: http://www.ethereal.com/

Sistema Operativo Windows:
Airopeek: http://www.wildpackets.com/products/airopeek
NetStumbler: http://www.netstumbler.com/

Instalar wireless-tools:
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Instalar pcmcia-cs: Pone a la tarjeta en modo MONITOR (Es como promiscuo de Ethernet, aunque no igual)
http://pcmcia-cs.sourceforge.net/

Si la tarjeta tiene el chipset Orinoco hay que parchear el pcmcia-cs para poder ponerla en modo monitor, el parche se puede encontrar en la siguiente página:

Orinoco Monitor Mode Patch Page
http://airsnort.shmoo.com/orinocoinfo.html

Medición de la capacidad de salida: Se refiere a la medición del desempeño de la red. Las herramientas más conocidas son:

- TCPSpeed de Maximed Software: www.maximed.com
- Chariot de MetIQ: www.netiq.com.

Aplicaciones que proporcionan autenticación, encriptación y/o privacidad con Software Libre sin emplear EAP:

- No Cat Auth: http://nocat.net
- LANRoamer: http://lanroamer.net
- Wireless Hearbeat: http://www.river.com/tools/authhb/
- FirstSpot: http://www.patronsoft.com/firstspot/
- WiCap: http://www.geekspeed.net/wicap/
- SLAN: http://slan.sourceforge.net/

BONUS:

QoS: Este aspecto es fundamental para audio y video (isócrono: igual en el tiempo) y sobre todo si se desea interactividad con ellos (Sincrónico), estos aspectos de Qos se pueden parametrizar con tres aspectos:

- Pérdida.
- Demora (o Latencia).
- Inestabilidad: Variación en la demora de paquetes.

Los estándares de IEEE que se refieren a estos temas son 802.1Q y 802.1D, que como se puede apreciar no son parte de 802.11, resumidamente, los mismos proponen el empleo de etiquetas (8 niveles) para calidad, las cuales permiten catalogar el tipo de paquete. Este tipo de etiquetas (con algunas variantes) se emplean en diferentes protocolos, de hecho hasta IP mismo las usa con la propuesta de DSCP (Differetiated Service Code Point, con 6 bits). WiFi ofrece la opción de tratar estas etiquetas de dos formas:

- Determinística: Un AP se hace cargo de la tarea de controlar y encolar los paquetes que le llegan.
- Estadística: Se basa en cálculos de estadística para la transferencia de paquetes, sin asegurar una regularidad de encolado.

A mediados de 2002 se crea el comité 802.11e por parte de IEEE, sobre los primeros esbozos del mismo salen al mercado las extensiones multimedia inalámbricas (WME: Wireless Multimedia Extensions) propuestas por grandes fabricantes (MS, Cisco, Atheos, Intel, etc). Estas dos propuestas están muy cercanas entre sí.

VII. Conclusiones

Como se trató de explicar en el texto, una red WiFi en si misma no es segura o insegura. **Este valor lo dará la implementación de la misma.**

Evidentemente se está haciendo un gran esfuerzo, tanto en los organismos de estandarización como en los fabricantes (que en definitiva son los mismos actores) para ofrecer productos que se puedan configurar tan seguros como una red cableada. Sobre esta tarea no puede haber dudas, pues el factor determinante es **LA CONFIANZA** que generen estas redes al público en general (como sucede con el comercio electrónico), si la gente no CONFÍA, entonces estos productos no se venden, como el interés de los fabricantes es la venta, su principal preocupación es generar esta CONFIANZA por medio del esfuerzo en **garantizar** la seguridad de las mismas.

Lo que se puede afirmar al analizar el estándar **802.11i**, es que se están haciendo las cosas bien, pues tanto **802.1x**, como **AES (o CCMP)**, son dos mecanismos extremadamente sólidos y que actualmente se los puede catalogar como seguros en los tres aspectos fundamentales que hoy se ponen en dudas respecto a WiFi, es decir en autenticación, control de accesos y confidencialidad.

A lo largo de este texto se trató de describir brevemente la infraestructura WiFi, para avanzar luego en los tres aspectos más importantes (Autenticación, control de accesos y confidencialidad). Lo que se debe destacar es el **estándar 802.11i como algo importante en la seguridad WiFi** y que en definitiva **presenta una oferta SEGURA,** tanto (o más) que una red cableada, si se lo configura adecuadamente.

Las reflexiones finales son:

- Los **datos y la voz viajarán juntos** (ojo con esto que rompe muchas estructuras actuales), lo cual hará imprescindible metodologías inalámbricas por el concepto de movilidad.
- El **futuro se viene desde el aire** (WiFi y UMTS {que se trata en otro texto}).
- El factor **seguridad** debe ser una **preocupación de cada enlace**, y bien hecho (**802.11i**) puede ser tan seguro como antes. Por eso es importante **respetar** productos que apliquen **este estándar** (y no propietarios), y configurar sus parámetros correctamente.
- Si se implementas las medidas adecuadas en WiFi, es más simple ingresar a una empresa y conectar una portátil a la primera boca de red libre, que tomarse el trabajo de “escuchar”, decodificar e intentar ingresar por aire.

Bibliografía:

Estándares IEEE: 802.11, 802.11, 802.11b, 802.11.d, 802.11i

802.11 (Wi-Fi) Manual de redes Inalámbricas, N.Reid – R.Seide, McGrawHill, 2003.

Thomas Schmidt. Cómo reforzar la seguridad inalámbrica**.**
http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_3245.html

http://www.wi-fi.org

Intercepting Mobile Communications: The Insecurity of 802.11:
www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Weaknesses in the Key Scheduling Algorithm of RC4, Scott Fluhrer, Itsik Mantin, and Adi Shamir:
www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

The protocol analyzers from Network Associates (www.nai.com), WildPackets:
www.wildpackets.com

Network Instruments:
www.networkinstruments.com

Ataque a RC4: (cierta complejidad matemática):
http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf

Autenticación e Integridad en Wireless, Toni Diaz (toni@madridwireless.net), Campus-Party 2003 Valencia: http://madridwireless.net.

Wireless LANs – The 802.1x Revolution, Bernard Aboba (bernarda@microsift.com):
http://www.drizzle.com/~aboba/IEEE/

ANEXO 1: Descripción más detallada del nivel Físico y Subnivel MAC de 802.11.

Se presenta a continuación un breve resumen de los aspectos más importantes del nivel físico del estándar. Se ha respetado la puntuación del mismo para quien desee profundizar en esos puntos.

5.3. Servicios Lógicos: 802.11 propone dos categorías de servicios empleados en el subnivel MAC:

- Station Service (SS): Son los servicios específicos de las STAs.
- Distribution System Service: Estos servicios se emplean para pasar en cualquier sentido entre DS y BSS.

Los servicios, determinarán distintos tipos de mensajes que fluirán por la red, independientemente de su categoría, la totalidad de los servicios (y/o mensajes) son:

a. Authentication: A diferencia de una red cableada, en 802.11 no existe una seguridad a nivel físico para prevenir el acceso no autorizado, por lo tanto este estándar ofrece la capacidad de autenticación por medio de este servicio. Si entre dos estaciones no se establece un adecuado nivel de autenticación, la asociación no podrá ser establecida. 802.11 soporta dos metodologías de autenticación:
   - Open System Authentication (OSA): Cualquier STA puede ser autenticada. Null Authentication).
   - Shared Key Authentication: Este mecanismo requiere la implementación de Wireless Equivalent Privacy (WEP) y será tratado más adelante.

b. Deauthentication: Este servicio es invocado si una autenticación debe ser finalizada. Se trata de una notificación, no una solicitud, por lo tanto no puede ser rechazada, y puede ser invocado tanto por una STA (No AP), como por un AP.

c. Association: Antes que una STA pueda enviar mensajes vía un AP, la misma deberá encontrarse Asociada a este último. Este servicio permite al DS conectar distintas STA dentro de una LAN Wireless, ubicando a cada una de ellas. En cualquier instante de tiempo, una STA solo podrá estar asociada a un único AP. Este servicio es siempre iniciado por una STA no AP, (nunca por un AP).

d. Deassociation: Este servicio es invocado si una asociación debe ser finalizada. Se trata de una notificación, no una solicitud, por lo tanto no puede ser rechazada, y puede ser invocado tanto por una STA (No AP), como por un AP.

e. Reassociation: Permite cambiar una asociación de un AP a otro, o también cambiar los parámetros de asociación de una STA con el mismo AP.

f. Distribution: Este tipo de mensajes se producen al ingresar información a un DS proveniente de un BSS. El encargado de generar estos mensajes será un AP y su objetivo es alcanzar el destino buscado.

g. Integration: Los mensajes que van o vienen dirigidos hacia/desde un portal, harán uso de este servicio.

h. Privacy: 802.11 al igual que sucede con autenticación (y por las mismas causas) provee la posibilidad de criptografiar el contenido de los mensajes a través de este servicio. Este servicio que es opcional, también se lleva a cabo por WEP. Es muy discutible la solidez del

mismo, pero la decisión fue tomada como una medida que permite tener un nivel de seguridad “al menos tan seguro como un cable”.

i. MSDU delivery: Responsable de entregar la información al nivel físico

Existe una relación entre asociación y autenticación que provoca los tres “Estados” en los que se puede encontrar una STA en cualquier intervalo de tiempo:

- Estado 1: No autenticado – No asociado.
- Estado 2: Autenticado – No asociado.
- Estado 3: Autenticado – Asociado.

Estos servicios generan distintos tipos de mensajes, los cuales están clasificados en:

a. Data:
b. Control:
c. Management:

7. Formatos de trama :

7.1. tramas MAC:

Estas tramas poseen tres componentes:

- MAC Header.
- Body.
- Frame Check Sequence (FCS).

Octetos:

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Body	FCS
MAC Header							***Body***	***FCS***

A continuación se desarrollan en detalle cada uno de los campos:

Si se analiza en detalle los dos octetos del **campo control**, los mismos están compuestos por los siguientes subcampos (Que se corresponden a los 2 octetos [16 bits] del campo “Frame Control”):

Bits:

2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More data	WEP	Order

a. Protocol Version (2 bit): El estándar actual es Versión 0.
b. Type (2 bit): 00= Management, 01=Control, 10=Data, 11=Reserved.
c. Subtype (4 bit): Definen el detalle del servicio y/o Primitiva (Ej: Association request y response, reassociation request y response, Beacon, Power Save, RTS, CTS, ACK, CF, etc...).
d. To DS (1 bit): En tramas de datos dirigidas hacia un DS=1, cualquier otro caso=0.
e. From DS (1 bit): En tramas que salen de un DS=1, cualquier otro caso=0.

f. More Frag (1 bit): En tramas de data o Management que poseen más fragmentos de MSDU=1, cualquier otro caso=0.
g. Retry (1 bit): Si es retransmisión de una trama anterior=1, cualquier otro caso=0.
h. Pwr Mgt (1 bit): Modo Power-Save=1, Modo Active=0
i. More Data (1 bit): Si una STA se encuentra en modo Power-Save y el AP posee más MSDU para ella=1, cualquier otro caso=0.
j. WEP (1 bit): Si el Body posee información que ha sido procesada con WEP=1, cualquier otro caso=0.
k. Order (1 bit): Si se emplea el servicio de Strictly Ordered=1, cualquier otro caso=0. (Este servicio permite reordenar la emisión de Broadcast y Multicast).

El segundo campo de la trama MAC es Duration ID, el cual consta también de 2 octetos. En la mayoría de los casos indica la duración de la trama, cuyo valor oscila entre 0 y 32767. La única excepción es cuando se trata de una trama de type=control con subtype= Power-Save, en cuyo caso los bit 14 y 15 son=1 y los restantes 14 bit indican la Association Identity (AID) de la estación que generó la trama, su valor oscila entre 1 y 2007.

Los otros campos que incluye la trama son los de direcciones, los cuales son empleados para indicar el BSSID. El formato de los mismos es el estándar de 48 bits (definido en IEEE 802-1990), respetando las mismas estructuras de Unicast, Multicast y Broadcast. Si bien en algunas tramas pueden no aparecer los cuatro, lo más normal es que sean los siguientes:

- Destination Address (DA): Identifica el recipiente final de la MSDU.
- Source Address (SA): Identifica el host que inició la transferencia de la MSDU.
- Receiver Address (RA): Identifica el recipiente inmediato al que será entregada la trama sobre el WM.
- Transmitter Address (TA): Identifica la STA que ha transmitido sobre el WM la MPDU

El campo que queda es el de Sequence Control Field que tiene 16 bits y consiste en 2 subcampos:

Bits:	4	12
	Fragment Number	Sequence Number

- Sequence Number: (12 bits) es un valor que se asigna a cada MSDU generada y oscila entre 0 y 4096, incrementándose en 1 por cada trama.
- Fragment Number: (4 bits) Si se emplea fragmentación (operación admitida por 802.11), este campo indica cada uno de los fragmentos, caso contrario es cero.

La cola de una trama 802.11 es el FCS (Frame Control Sequence) que es el CRC de grado 32, que corresponde al estándar IEEE CRC-32.

$$G_{(x)} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

7.2. Formato de tipos de trama:

Volviendo al campo de control de la trama, como se detalló en el punto 7.1. El subcampo Type, identifica 3 tipos de trama: 00= Management, 01=Control, 10=Data. Por lo tanto, acorde a estos

valores, se definen cada una de estas tramas, y su formato en cada caso difiere del formato genérico de la trama (definido en el punto 7.1.). A continuación se detallan cada uno de estos tipos.

7.2.1. Tramas de control:

Son las que en el subcampo Type tienen valor=01, y se emplean para control de red. Los distintos subtipos de tramas de control se detallan a continuación:

7.2.1.1. Formato de trama RTS (Request to send):

Octetos:	2	2	6	6	4
	Frame Control	Duration	RA	TA	FCS

- Frame Control, RA, TA y FCS, son los mismos anteriormente descriptos.
- Duration: Este valor es el tiempo en microsegundos requeridos para transmitir los datos pendientes (o también una trama de administración) + una trama CTS + una trama ACK + 3 intervalos SIFS.

7.2.1.2. Formato de la trama Clear to Send (CTS):

Octetos:	2	2	6	4
	Frame Control	Duration	RA	FCS

- RA es copiado del valor e TA de la trama RTS inmediatamente previa.
- Duration: es el mismo que el de la trama RTS inmediatamente previa – el tiempo requerido para transmitir esta trama (CTS) y el SIFS que espera la misma.

7.2.1.3. Formato de la trama Acknowledgment (ACK):

Este formato es exactamente igual al de CTS.

7.2.1.4. Formato de la trama Power-Save (PS-Poll)

Octetos:	2	2	6	6	4
	Frame Control	AID	BSSID	TA	FCS

- BSSID: Es la dirección de la STA contenida en el AP.
- AID: Es el valor asignado a la STA transmitiendo la trama, en respuesta (o durante) una asociación.

7.2.1.5. Formato de la trama CF-End (Contention Free-End):

Octetos:	2	2	6	6	4
	Frame Control	Duration	RA	BSSID	FCS

- BSSID: es la dirección del AP.

- RA: es la dirección Broadcast de grupo.
- Duración: Debe ser siempre=0.

7.2.1.6. Formato de la trama CF-End + CF-ACK:

Es exactamente igual a la anterior.

7.2.2. Tramas de datos:

Estas tramas son independientes del subtipo, y los únicos detalles significativos son los campos Address que dependerán del valor de los bits To DS y From DS, presentando diferentes contenidos (o significados) en base a las cuatro combinaciones de estos dos bits. Las mismas no serán tratadas en este texto.

7.2.3. Tramas de administración:

El formato genérico de estas tramas es el que se detalla a continuación

Octetos:	2	2	6	6	6	2	0-2312	4
	Frame Control	Duration	DA	SA	BSSID	Sequence control	Body	FCS

Sobre este formato, basado en diferentes valores del Frame Control, se distinguen los subtipos de trama que presentan, las cuales pueden ser las siguientes:

7.2.3.1. Beacon frames:

El cuerpo (body) de una trama de administración “Subtipo” Beacon contiene la siguiente información:

- Timestamp:
- Beacon Interval:
- Capability Information:
- SSID:
- Supported rates
- FH Parameter Set:
- DS Parameter Set:
- IBSS Parameters Set:
- TIM: (Sólo presente en tramas generadas por AP).

7.2.3.2. IBSS Announcement Traffic Indication Mesage (ATIM):
7.2.3.3. Disassociation:
7.2.3.4. Association Request:
7.2.3.5. Association Response:
7.2.3.6. Reassociation Request:
7.2.3.7. Reassociation Response:
7.2.3.8. Probe Request:
7.2.3.9. Probe Response:

7.2.3.10. Authentication:
Posee un campo de 2 octetos llamado Authentication Algoithm Number que tiene definido dos valores:
0= Open System y 1=Shared Key, Todo otro valor está reservado.
7.2.3.11. Deauthentication:

9. Descripción funcional de subnivel MAC:

La arquitectura de este subnivel incluye dos funciones principales: Función de coordinación distribuida (DCF) y Función de coordinación puntual (PCF), que se desarrollan a continuación:

9.1.1. DCF:
El método de acceso fundamental de 802.11 es conocido como CSMA/CA (Carrier Sense Multiple Access / Colision Avoidance) y opera de la siguiente forma: Una STA para transmitir, primero debe escuchar el canal para determinar si otra está transmitiendo. Si el medio está libre, entonces podrá transmitir acorde a los tiempos de espera correspondientes (que se detallarán más adelante), pues siempre debe dejar "ciertos intervalos de tiempo". Si el medio está ocupado, entonces la STA deberá esperar a que finalice la presente transmisión. En este último caso, como así también cuando acaba de transmitir la propia STA y desea enviar otra trama, la STA generará un valor random (y teniendo en cuenta también los tiempos que impone el estándar) y lo irá decrementando, hasta hacerse cero. Llegado este valor, podrá transmitir. Un aspecto que puede ser empleado también para acceso al medio, son las tramas RTS y CTS, que del mismo modo que la interfaz RS-232, solicita autorización y se habilita la Tx, por medio de estos cortos mensajes.

9.1.2. PCF:
Este método sólo puede ser empleado en modo infraestructura. Emplea un Poin Coordinator (PC), quien coordinará dentro del BSS qué STA tiene permiso para transmitir. La operatoria es el conocido sondeo (Poll), realizado desde el PC. Esta PC posee un mecanismo prioritario de acceso al canal a través de las tramas de Management "Beacon", configurando lo que se denominará NAV (Network Allocation Vector). Este acceso prioritario, provisto por el PC puede ser utilizado para crear lo que se denomina Contention-Free (CF) Access Method (Método de acceso libre de colisiones).

9.1.3. Coexistencia de DCF y PCF:
Cuando un PC esté operando en un BSS, ambos métodos se irán alternando y pueden convivir.

9.2.3. Espacio entre tramas (IFS: Interframe Space):
Los intervalos de tiempo entre tramas son los IFS. Se definen cuatro tipos de IFS, para establecer prioridades de acceso al medio:

a. SIFS (Short IFS): Este intervalo se emplea en tramas ACK, CTS o en las sucesivas tramas de una operación de fragmentación. También en cualquier respuesta a un sondeo realizado por un PC. Es el intervalo más corto.
b. PIFS (PCF IFS): Se emplea en modo PCF (Excepto en las respuestas a sondeos)

c. DIFS (DCF PFS): Se emplean en modo DCF par envío de tramas de administración y de datos.
d. EIFS (Extended IFS): Este intervalo se emplea cuando el nivel físico le informa al subnivel MAC que una trama que se ha transmitido, no tuvo una correcta recepción con incorrecto FCS. Se emplea este valor máximo de intervalo, para dar tiempo suficiente a la STA receptora, de informar este error de recepción.

9.2.4. Random Backoff time:

Cuando una STA desea transmitir, y la función "Carrier Sense" detecta ocupado el canal, deberá desistir de la Tx hasta que se desocupe el medio y durante un intervalo DIFS finalizada la Tx anterior si esta llega con éxito, si es motivo de errores, el intervalo de espera deberá ser EIFS. Una vez finalizado cualquiera de estos dos intervalos, generará un valor aleatorio denominado "Random Backoff Time", que deberá esperar antes de transmitir. El objetivo del mismo es minimizar colisiones. Este valor se compone de:

Backoff Time = Random () * Slot Time.

El valor Random está relacionado a un parámetro denominado "Contention Window" (Mínima y máxima) y sus límites oscilarán entre 0 y $\mathbf{2^n-1}$ Siendo "n" la cantidad de intentos de acceso (Muy similar a la técnica de tratamiento de colisiones de 802.3). Y el Slot time es un valor que depende de las características físicas del canal.

11. Entidad de administración de subnivel MAC :

Todas las STA que estén dentro de un BSS, estarán sincronizadas por un reloj común. La responsable de esta actividad es la función sincronización de tiempo (TSF).
En un Red tipo Infaestructura el AP será el "Timing Master" y llevará a cabo la TSF. Transmitirá periódicamente tramas "Beacon" que contienen copias del "TSF timer". Cualquier STA siempre aceptará estas tramas provenientes del que sirve su BSS.

11.2. Power Mode:

Una STA puede permanecer en dos estados:

- Despierta (Awake): Está en condicioones normales de operación.
- Dormida (Doze): No está en capacidad de Tx o Rx, y consume mucha menos potencia. Escucha periódicamente las tramas "Beacon", para ver si su AP necesita cambiarla de estado, para enviarle información.

La transición entre estos dos estados es controlada por cada STA (configurada). Lo importante a tener en cuenta aquí es que cuando una STA modifica su Power Mode, inmediatamente debe indicarlo a su AP a través de una trama de administración con los bit de PS configurados acorde al estado. El AP lleva una tabla de control de todas las STA, llamada "Traffic Indication Map" (TIM)

12. Especificaciones de servicio de nivel físico (PHY).

El estándar 802.11 posee diferentes especificaciones físicas, pero cada una de ellas siempre posee dos funciones:

- Función de convergencia: Adapta la trama MAC con el PMD.

- Sistema PMD (Physical Medium Depend): Define las características y métodos de Tx y Rx de datos a través de WM.

14. Especificaciones de FHSS (Frecuency Hopping Spread Spectrum), para la banda 2,4 Ghz ISM (Industrial, Scientific and Medical Band).

14.3.2. Formato de la trama a nivel físico:

Hasta ahora se ha tratado el formato de la trama MAC. A partir de ahora se analiza el formato de la trama en el nivel inferior del modelo, es decir, este nivel físico recibe la PDU de nivel 2 (es decir la trama MAC completa) a través del SAP correspondiente, arma su Header, lo suma a la PDU recibida y este conjunto es lo que va a Tx por el WM.
El conjunto total de bits que se inyectarán en el canal de comunicaciones, a través de este nivel se puede clasificar en tres grandes partes:

- Preámbulo: Se emplea para sincronizar la transmisión con todos los nodos que vayan a escucharla. Contiene dos campos:
  - Sincronización (SYNC) de 80 bits alternando ceros y unos.
  - Delimitador de inicio de trama (SFD) de 16 bits (0000 1100 1011 1101).
- Header: Contiene tres campos:
  - PLW (Physical Length Word): 12 bits que indican la longitud d el campo de datos.
  - PSF (Physical Signaling Rate): 4 bits, de los cuales, el primero debe ser cero (Reservado), y las 9 combinaciones de los 3 bits siguientes indican a qué velocidad de transferencia de datos operará esta trama, desde 1 Mbps (000) hasta 4,5 Mbps (111), incrementándose de 0,5 Mbps.
  - HEC (Header Error Check): 16 bits que emplean la técnica de CRC con el polinomio Generador $G_{(x)} = X^{16} + X^{12} + X^5 + 1$
- Datos: PDU de nivel 2. Cabe destacar aquí que en este nivel, los datos emplean la técnica de “Scrambler frame Synchronous”, organizando bloques de 127 bits, que se irán mezclando en filas y columnas para minimizar los efectos de ráfagas de errores que puedan sufrir en el WM.

ANEXO 2: Teoría y funcionamiento de WEP.

Conceptos:

Se debe distinguir entre: texto plano (P) y texto cifrado (C).

El proceso de reconvertir un texto cifrado en texto plano se denomina descifrado (D).
Un algoritmo criptográfico es un función matemática empleada para cifrar y descifrar.

Los algoritmos actuales suelen emplear secuencias de clave (k), para modificar la salida de la función matemática.

En el caso de Criptografiar un texto (o Encriptar {aunque este término no esté aún reconocido por la RAE}), se dice que la función E opera sobre P par a producir C y se representa:

$$E_k(P) = C$$

El proceso inverso sería: $D_k(C) = P$

La clave se forma a partir de la parafrase, la cual se ordena en palabras de a 4 Byte y se realiza una operación XOR palabra a palabra, dando como resultado una "Semilla" de 32 bit.

Esta Semilla es el punto de partida con el cual, la función PRNG a través de 40 iteraciones, creará cuatro claves de 40 bit. De estas claves se seleccionará solo una (que estará indicada dentro de la trama).

La STA que inicia esta operación, calcula el CRC de todo el Payload y lo agrega al final del mismo, este valor se denomina Integrity Check Value (ICV). Otro valor que entra en juego es el IV, que no es más que un contador que oscila entre 0 y 4096 (dentro del mismo se incluirán dos bits que identificarán a la clave elegida de las 4 generadas).
Por lo tanto quedan dos bloques:

IV	Clave

Payload (Texto plano)	ICV (CRC)

El IV de 24 bit, incluye entonces 2 bit que identifican la clave elegida (entre las 4 generadas) y la clave por defecto es de 40 bit, formando un bloque de 64 bits. Existe también la posibilidad de trabajar con claves de 128 bits, en cuyo caso se mantienen los 24 bits de IV y se genera una clave de longitud 104 bits, dando el total de 128.

Este bloque es el que conforma la "Semilla" de WEP (PNRG), con la cual se genera el flujo de cifrado de bloque realizando nuevamente un XOR con el bloque: Texto plano + ICV.

El algoritmo WEP, perteneciente a RSA, no se detalla en este texto.

Con esta última operación quedan conformados todos los bloques con los que se armará finalmente la trama que quedará constituida por los siguientes campos:

	24	n >= 1	4
Header	IV (+Nº clave)	Payload (Datos >=1)	ICV
← TEXTO PLANO →		← CIFRADO →	

Se debe tener muy en cuenta aquí que el IV viaja como texto plano, y con cada IV generado (secuencialmente), se crea una nueva semilla y por lo tanto se ingresa a WEP con distintos valores clave.

El algoritmo WEP, presenta varios puntos vulnerables, en particular si se opera con clave de 64 bits (de los cuáles sólo 40 son desconocidos, pues los 24 del IV van en texto plano), pero en este punto cabe mencionar uno de los principales. Si se tiene en cuenta que el IV es secuencial y su valor máximo es 2^{24} (16 millones), el mismo en una red con mediana tasa de tráfico, comenzaría a repetirse en el orden de 5 horas, si se logra obtener valores repetidos del mismo, el espacio de claves se reduce a algoritmos triviales de descifrar.

ANEXO 3: 802.11i

Este estándar se desarrolla en este apartado pues es el punto clave en temas de seguridad y por ser el referente más actual en seguridad WiFi. El mismo fue aprobado a mediados de 2004 y presenta las siguientes novedades:

- Privacidad: AES.
- Autenticación: 802.1x.

Antes de entrar de lleno en el estándar, es conveniente aclarar un poco el tema de 802.1x. Para poder empezar a hablar del mismo, hay que tener en cuenta su historia, la cual comienza con el protocolo PPP (Point to Point Protocol), el que se impone como estándar de acceso a Internet por marcación telefónica (si bien existía mucho antes), luego también por cable modem y ADSL. PPP forma parte del protocolo L2TP (Link 2 Tunneling Protocol). El enorme empleo que se ha dado a PPP hizo que vaya mucho más allá del acceso a Internet, llegando a estar en casi todos los segmentos de la red. Una parte de PPP se encarga de autenticación, inicialmente se empleó a través de usuario y contraseña, tema que hoy se conoce perfectamente en todas sus debilidades. Para solucionar esta debilidad, nació EAP (Extensible Authentication Protocol), el cual se encuentra dentro del protocolo de autenticación de PPP (es decir que es parte de este), el gran aporte de este es su flexibilidad y compatibilidad con diversos métodos de autenticación, los cuales van desde el empleo de contraseñas hasta el uso de certificados.

Resumen de estándar IEEE 802.11i (23 de julio de 2004).

Resumen:

Este estándar es una enmienda a los mecanismos de seguridad que ofrece 802.11 (IEEE 802.11, 1999). Las mejoras que propone están referidas al empleo de **TKIP** y **CCMP,** los cuales porporcionan mecanismos más robustos de protección. Se introducen también conceptos de asociación segura a través de mecanismos de "**4-Way Handshake**", y por último especifica también el empleo de **802.1x** para autenticación.

Definiciones clave:

- AES (Advanced Encryptation Standard – FIPS PUB 197-2001):
- AKM (Authentication and Key Management):
- CCM (Counter with CBC-MAC [Cipher-Block Chaining with Message Authentication Code] – RFC: 3610, 2003):
- CCMP (Counter Mode [CTR] with CBC-MAC Protocol):
- EAP (Extensible Authentication Protocol – RFC: 3748, 2004):
- MIC: Message Integrity Code): Valor generado por una función criptográfica de clave simétrica que se emplea para verificación de integridad de los mensajes y evitar la aceptación de mensajes falsos.
- Michael: Denominación que se ha dado al empleo de MIC en TKIP.

- 4-Way Handshake: Mecanismo de autenticación mutua, que permite validar la identidad del cliente y del servidor.
- Group Key Handshake:
- IEEE 802.1x: Estándar de IEEE que facilita y securiza los mecanismos de autenticación
- RC4:
- RSN (Robust Security Network):
- TKIP (Temporal Key Integrity Protocol):
- PSK (Pre Shared Key): Clave compartida previamente por algún mecanismo fuera de banda.
- WEP (Wired Equivalent Privacity): Mecanismo de confidencialidad especificado en 802.11, hoy no recomendado.
- Pairwise: Dos entidades que se encuentran asociadas una con la otra. Este término suele emplearse para describir la jerarquía de claves que se encuentran compartiendo únicamente entre ellas dos.
- PMK (Pairwise Master Key): El más alto orden de clave empleado en este estándar. Puede derivarse de EAP o PSK.

A continuación se presentan los puntos que trata el estándar, incorporando los comentarios que se aprecian necesarios para aclarar todos los conceptos, se respetará la puntuación que emplea el estándar, para facilitar cualquier búsqueda que desee realizar el lector.

5. Descripción General:

En este apartado hace de forma genérica, varias referencias, modificaciones y comparativas, respecto a lo que planteaba 802.11 y lo que hace 802.11i, los puntos más importantes son:

Componentes (y mejoras) de la arquitectura 802.11:

Conceptos de DS (Distribution System):

- RSNA (RSN Association): Se trata de una serie de caracterísitcas nuevas que se suman a WEP y a la autenticación propuesta por 802.11, las mismas incluyen:
    - Mejora de los mecanismos de autenticación de los clientes.
    - Algoritmos de administración de claves.
    - Establecimiento de claves criptográficas.
    - Ampliación de los mecanismos de encapsulamiento. Aquí es donde aparece CCMP y permite el uso opcional de TKIP.

Presentación de los servicios:

Asociación:

Incluye nuevos párrafos para mejorar esta actividad.

Describe claramente los conceptos de asociación y autenticación y cómo 802.1x diferencia el estado de las combinaciones de ambos para restringir o autorizar el pasaje de datos a nivel puerto (controlado y no controlado).

Autenticación:

Introduce como nuevos conceptos de autenticación PSK, EAP, sin especificar ningún método de EAP en particular. Hace referencia en los distintos mecanismos que permiten autenticación entre DS, IBSS y ESS.

Confidencialidad:

Propone tres algoritmos criptográficos para la protección de datos: **WEP**, **TKIP** y **CCMP**. Aclara que por defecto todas las estaciones 802.11 trasmiten en texto plano (decir verdad no queda claro si se modificó o no el párrafo que dice “esta política es inaceptable”.....). Lo que si aclara perfectamente es que si una estación está configurada con políticas de confidencialidad, directamente descartará toda trama que llegue en texto plano, sin siquiera entregarla al Logical Link Control LLC.

Administración de claves:

Introduce el concepto de 4-Way Handshake.

Autenticación de origen de datos:

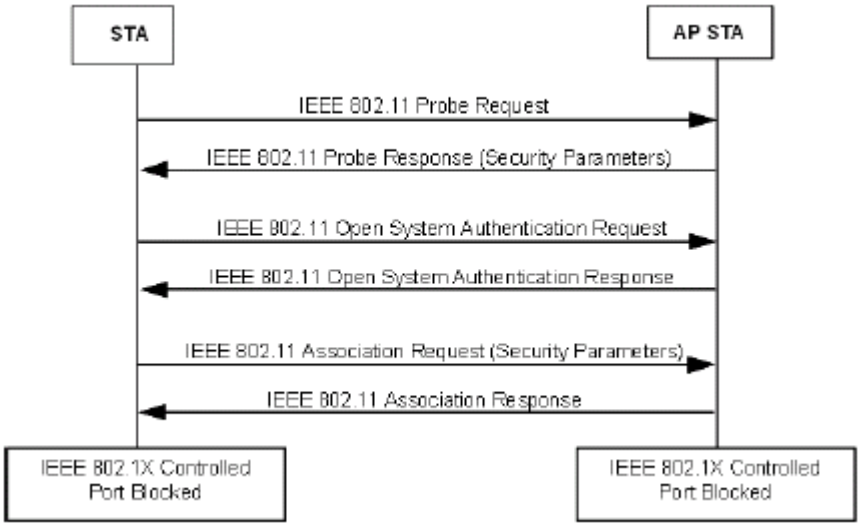
Define un mecanismo a través de CCMP o TKIP, para que cualquier estación que reciba datos de otra, pueda determinar fehacientemente su origen, para evitar falsificación de estaciones. Este mecanismo solo aplica a tramas unicast

Detección de retransmisión:

Se define un mecanismo por medio del cual una estación que recibe una trama de otra estación, puede determinar si se trata de una retransmisión no autorizada, este mecanismo está proporcionado por medio de CCMP o TKIP.

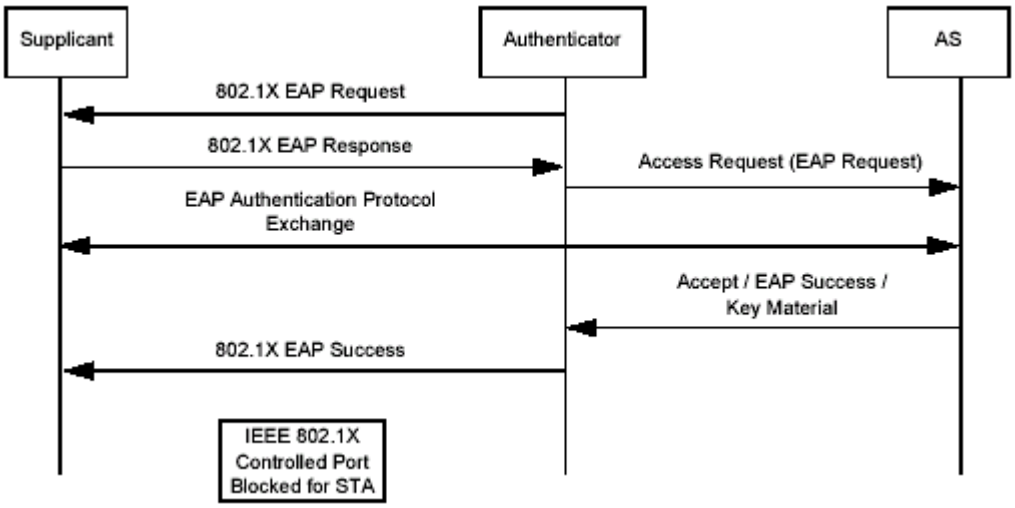
Autenticación y administración de claves (AKM):

Realiza una comparativa en cuanto al mecanismo empleado por 802.11 y el que propone 802.1x. Esta comparativa queda reflejada en las siguientes figuras:



Establecimiento de una asociación con 802.11

Para que quede establecido el 4-Way Handshake, el autenticador y el solicitante deben autenticarse mutuamente. (802.1x controla los puertos Bloqueados y no bloqueados para permitir (o no) el tráfico de datos, esta actividad se aprecia en la siguiente sigura.



Establecimiento de una asociación con 802.1x empleando EAP.

Establecimiento de “Pairwise” y clave de grupo

6. Definición del servicio MAC.

La seguridad está provista por el servicio de autenticación y los mecanismos WEP, TKIP y CCMP, a los propósitos de este estándar, WEP, TKIP y CCMP, son servicios lógicos ubicados en el Subnivel MAC del modelo de referencias.
Los servicios de seguridad que proveen estos mecanismos son:

- Confidencialidad.

- Autenticación.
- Control de accesos.

7. Formatos de trama:

Especifica el formato de las tramas y las modificaciones respecto a 802.11.
7.1.3. Tramas de control:

Los campos a destacar son:
- Campo de control (2 octetos).
- Campo de trama protegida (1 bit) En realidad este bit pertenece al campo de control (es el bit 14) y se ha cambiado en cuanto a su denominación, pues antes indicaba si era WEP o no y ahora anuncia si está protegida la trama.

7.2.3. Tramas de Administración:

7.2.3.1. tramas “Beacon”: Se introduce el campo 21 que identifica RSN.
7.2.3.4. tramas de solicitud de asociación: Se introduce el campo 8 que identifica RSN.

7.2.3.6. tramas de solicitud de Reasociación: Se introduce el campo 9 que identifica RSN.

7.2.3.9. tramas de “Probe response”: Se introducen los campos 21 y 22-n que identifican RSN y los elementos solicitados por la trama de solicitud.

7.3. Componentes del cuerpo(body) de las tramas de administración:

7.3.1.7. Campo “Reason Code”: incluye en los códigos 12 al 24 parámetros para: MIC, 4-Way Hamdshake , Chipher pairwise, RSN, 802.1x y suites de cifrado.

7.3.1.9. Campo “Status Code”: incluyen opciones similares al anterior en los códigos 27 al 46.

7.3.2. Información de elementos: Reemplaza los Ids 43 al 49, para reconocer RSN.

7.3.2.25. Información de elemento RSN: Este campo contiene información de suites de cifrado y autenticación, capacidades de RSN, identificadores PMK y está limitado a 255 octetos. Tiene todo el detalle necesario para informar y coordinar los protocolos y tamaños de claves que se podrán establecer entre pares.

8. Seguridad:

Este estándar define dos clases de algoritmos de seguridad para redes 802.11:

- Algoritmos RSNA (Robust Secure Network Association):
  - TKIP.

- CCMP
- Procedimientos de establecimiento y terminación RSNA que incluyen el empleo de autenticación por 802.1x.
- Procedimientos de administración de claves.

- Algoritmos pre-RSNA: WEP y autenticación de entidad IEEE802.11.

8.1.3. Establecimiento RSNA:

Define los modos de establecer una RSNA:
- Con 802.1x.
- Con PSK para ESS.
- Con PSK para IBSS.

8.2. Métodos de seguridad Pre-RSNA.

Excepto para autenticación de sistemas abiertos (OSA), este estándar **desaprueba** todos los mecanismos Pre-RSNA de autenticación, por las deficiencias que presentan. Las nuevas implementaciónes, deberían soportarlos, únicamente para facilitar la migración.

8.2.1.2. Formato de WEP MPDU.

Este tema es importante pues extiende el formato del campo MSDU de WEP a 8 octetos, cuatro para el ICV (Integrity Check Value) y 4 para el IV (Vector de inciación). Este último fue una de las mayores debilidades de WEP.

8.2.1.3. WEP State:

Hace referencia a que WEP no se puede emplear como método de autenticación, únicamente para criptografía y hace hincapié en el empleo de clave de 104 bit (más los 24 de IV). Continúa luego con todos los pasos para encriptar con WEP, generación de semilla, encapsulado, desencapsulado y bucles de cifrado.

8.2.2 Autenticación Pre-RSNA:

En un ESS tanto el AP como los clientes deben haber completado todo el proceso de autenticación para poder asociarse. Todas las tramas de autenticación deberán ser unicast y la misma es ejecutada entre pares de elementos. Multicast y Broadcast no está permitido. Si pueden ser multicast las tramas de de-autenticación.

La autenticación por clave compartida no se aconseja y no debería implementarse excepto por razones de migración con pre-RSNA.

8.2.2.2. Open System Authentication:

Se trata del algoritmo de autenticación nulo, es el algoritmo por defecto de pre-RSNA. Emplea una secuencia de transacción de dos mensajes (Request Authentication y Result Authentication), si el "Result" es Successful", entonces las estaciones se declaran mutuamente autenticadas.

8.2.2.3 Autenticación por clave compartida:

La autenticación por clave compartida, solo puede emplearse si a sido seleccionado el algoritmo WEP.

Este mecanismo implica una distribución de claves por canal seguro, independiente de 802.11. Este secreto es almacenado en una MIB dentro de cada STA. Para la autenticación emplea cuatro tramas que intercambian un desafío entre pares para verificar, por medio de su descifrado, el conocimiento o no del secreto comartido. Se recuerda que esta autenticación no es aconsejada por este estándar.

8.3. Protocolos de confidencialidad de datos de RSNA.

Este estándar define como protocolos de confidencialidad e integridad de datos a TKIP y CCMP, siendo mandatorio este último en dispositivos que soliciten certificaciones RSNA. La implementación de TKIP es opcional para RSNA.

Hace hincapié en que los mecanismos de confidencialidad e integridad de TKIP no son tan robustos como CCMP. TKIP está más orientado a operar con dispositivos que tengan limitaciones de hardware o con pre-RSNA. Los dispositivos RSNA solo emplean TKIP cuando se comunican con otros que no soorten CCMP.

8.3.2. TKIP (Temporal Key Integrity Protocol):
TKIP es una suite de cifrado que amplía al protocolo WEP sobre hardware pre-RSNA. Las modificaciones que incluye en WEP son:

- **Combinación de clave por paquete:** La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Pre-shared Key).

- **VI** (Vector de inicialización) de **48 bits**: Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones.

- **MIC** (Message Integrity Check): Se plantea para evitar los ataques inductivos o de hombre del medio. Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y genera una alerta, que indica una posible falsificación del mismo.

Se describe aquí también todo lo referido a encapsulado, desencapsulado y el formato de las tramas Aquí es donde se describe la modificación sobre los 8 octetos para acomodar los nuevos campos respecto a WEP y el MIC [Michael]).

Michael genera un MIC de 64 bit, que se divide en dos palabras de 32 bits, este opera sobre cada MSDU. Este MIC es procesado iterativamente con cada valor de clave y aplicada a una función de

bloque por cada mensaje, este algoritmo forma un bucle de N tiempos y da como resultado dos nuevas palabras que será anexado al MSDU. Nótese aquí el error que justamente se le critica a este MIC, y es el de no operar sobre la totalidad de la trama es decir sobre la MPDU.

Hay buen comentario acerca de los ataques que no soportaba WEP y cómo se solucionan con MIC. Describe también con todo lujo de detalles el funcionamiento y los fallos de TKIP.

En el anexo D y H de este estándar se definen todas las variables para TKIP y para su MIC.

8.3.2.5. TKIP mixing function:

Este punto describe algo importante de TKIP y consta de las dos fases que emplea para la generación de claves. La fase 1 es referida a la clave temporal (TK) y la fase dos mezcla la salida de la fase 1 con la TSC (Temporal Sequence number) y la TK para producir la "semilla" (Seed), también llamada per-frame key, es decir la que se empleará en cada trama. Tanto la fase 1 como la 2 se llevan a cabo en lo que se denomina S-Box y se trata de una substitución no lineal.

8.3.3. CTR with CBC-MAC Protocol (CCMP)
Recordatorio:

- CTR: Counter Mode → *Confidencialidad*.
- CBC-MAC: Cipher-Block Chaining with Message Authentication Code → *Autenticación de origen.*

Este apartado define el funcionamiento de este protocolo el cual provee confidencialidad, autenticación, integridad y protección anti réplica. CCMP es mandatorio para el cumplimiento de RSN.

CCMP está basado en CCM de AES. CCM combina la confidencialidad de CTR y CBC-MAC para autenticación e integridad. Con esto queda protegido todo el MPDU (tanto encabezado como datos).

El algoritmo AES está definido en FIPS PUB 197. CCM está definido por la RFC 3610.

CCM es un modo genérico que puede ser empleado con cualquier algoritmo de cifrado de bloques y tiene dos parámetros M=8 que indica que el MIC es de 8 octetos y L=2 que indica que la longitud de l campo es de 2 octetos (lo cual alcanza para identificar la longitud máxima de cualquier MPDU de 802.11 expresada en octetos). CCM requiere una actualización de clave temporal para cada sesión y emplea un número de paquete (PN) de 48 bits para este propósito. Se debe rechazar el empleo de PN con el mismo número de clave temporal, para no debilitar al protocolo.

En el anexo H del estándar se especifican todos los parámetros de CCM.

El procesado de CCMP expande el tamaño original de la MPDU con 16 octetos. 8 para el encabezado de CCMP y 8 para el MIC. El encabezado de CCMP está construido sobre la base del PN, Ext IV y los subcampos de clave. Se debe notar aquí que CCMP no emplea el ICV de WEP.
Se describen aquí todos los campos de la MPDU, su encapsulado y desencapsulado y los pasos para el enctriptado de la totalidad de la MPDU

8.4. RSNA Security association management:

Una Asociación de Seguridad (SA) es un conjunto de políticas y claves empleadas para proteger información, la información en esta SA es almacenada en cada parte de la misma.
Existen cuatro tipos de SA soportadas por una RSN STA:

- PMKSA: Es el resultado de un intercambio con éxito de802.1x con información PMK pre compartida.
- PTSKA: Es el resultado de un 4-Way HandShake.
- GTKSA: Es el resultado de Group Key Handshake o un 4-Way Handshake
- STAKeySA: Es el resultado de un STAKey Handshake.

Se describe en detalle cada uno de ellos.

8.4.2. Selección de RSNA:

Una STA que esté preparada para establecer una RSNA advertirá sus capacidades incluyendo la información de RSN en las tramas Beacon y Probe Response. En ellas especificará todas las suite de cifrado y autenticación que tiene habilitadas.

8.5. Claves y distribución de claves.

Se describen aquí todos los formatos de claves de autenticación y cifrado, las tramas que emplea y los mecanismos de distribución e intercambio de las mismas.

8.6. Mapeo de claves EAPOL a IEEE 802.11

Describe la metodología para el empleo de las claves EAP en 802.11

ANEXO 4: Capturas de tráfico

1. Captura ARP:

No. Time Source Destination Protocol Info
1307 277.735814 10.64.135.73 Broadcast ARP Who has 10.64.135.73? Gratuitous ARP

Frame 1307 (60 bytes on wire, 60 bytes captured)
Arrival Time: Mar 30, 2005 03:20:00.869297000
Time delta from previous packet: 1.001503000 seconds
Time since reference or first frame: 277.735814000 seconds
Frame Number: 1307
Packet Length: 60 bytes
Capture Length: 60 bytes
Protocols in frame: wlan:llc:arp
IEEE 802.11
Type/Subtype: Data (32)
Frame Control: 0x0008 (Normal)
Version: 0
Type: Data frame (2)
Subtype: 0
Flags: 0x0
DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = WEP flag: WEP is disabled
0... .... = Order flag: Not strictly ordered
Duration: 0
Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
Source address: 00:02:2d:22:43:c9 (10.64.135.73)
BSS Id: 02:02:2d:22:43:c9 (02:02:2d:22:43:c9)
Fragment number: 0
Sequence number: 64
Logical-Link Control
DSAP: SNAP (0xaa)
IG Bit: Individual
SSAP: SNAP (0xaa)
CR Bit: Command
Control field: U, func=UI (0x03)
000. 00.. = Command: Unnumbered Information (0x00)

```
      .... ..11 = Frame type: Unnumbered frame (0x03)
   Organization Code: Encapsulated Ethernet (0x000000)
   Type: ARP (0x0806)
Address Resolution Protocol (request/gratuitous ARP)
   Hardware type: Ethernet (0x0001)
   Protocol type: IP (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (0x0001)
   Sender MAC address: 00:02:2d:22:43:c9 (10.64.135.73)
   Sender IP address: 10.64.135.73 (10.64.135.73)
   Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
   Target IP address: 10.64.135.73 (10.64.135.73)

0000  08 00 00 00 ff ff ff ff ff ff 00 02 2d 22 43 c9   ............-"C.
0010  02 02 2d 22 43 c9 00 04 aa aa 03 00 00 00 08 06   ..-"C...........
0020  00 01 08 00 06 04 00 01 00 02 2d 22 43 c9 0a 40   ..........-"C..@
0030  87 49 00 00 00 00 00 00 0a 40 87 49               .I.......@.I
```

2. Captura trama BEACON :

```
No.     Time        Source              Destination         Protocol Info
    81 17.550689   D-Link_ac:83:92      Broadcast           IEEE 802.11 Beacon frame, SSID: "WLAN"

Frame 81 (78 bytes on wire, 78 bytes captured)
   Arrival Time: Mar 20, 2005 13:16:29.143037000
   Time delta from previous packet: 0.551679000 seconds
   Time since reference or first frame: 17.550689000 seconds
   Frame Number: 81
   Packet Length: 78 bytes
   Capture Length: 78 bytes
   Protocols in frame: wlan
IEEE 802.11
   Type/Subtype: Beacon frame (8)
   Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
      Flags: 0x0
         DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From DS: 0)
(0x00)
         .... .0.. = More Fragments: This is the last fragment
         .... 0... = Retry: Frame is not being retransmitted
         ...0 .... = PWR MGT: STA will stay up
         ..0. .... = More Data: No data buffered
```

```
        .0.. .... = WEP flag: WEP is disabled
        0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:0f:3d:ac:83:92 (D-Link_ac:83:92)
    BSS Id: 00:0f:3d:ac:83:92 (D-Link_ac:83:92)
    Fragment number: 0
    Sequence number: 2648
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x00000072DE7CF037
        Beacon Interval: 0,102400 [Seconds]
        Capability Information: 0x0411
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... .... .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
            .... .... ...1 .... = Privacy: AP/STA can support WEP
            .... .... ..0. .... = Short Preamble: Short preamble not allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... .1.. .... .... = Short Slot Time: Short slot time in use
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
    Tagged parameters (42 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag length: 4
        Tag interpretation: WLAN
        Tag Number: 1 (Supported Rates)
        Tag length: 8
        Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 6,0 12,0 24,0 36,0 [Mbit/sec]
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 6
        Tag Number: 5 ((TIM) Traffic Indication Map)
        TIM length: 4
        DTIM count: 0
        DTIM period: 1
        Bitmap Control: 0x00 (mcast:0, bitmap offset 0)
        Tag Number: 7 (Country Information)
        Tag length: 6
        Tag interpretation: Country Code: GB, Any Environment, Start Channel: 1, Channels: 13, Max
TX Power: 20 dBm
        Tag Number: 42 (ERP Information)
        Tag length: 1
        Tag interpretation: ERP info: 0x4 (no Non-ERP STAs, do not use protection, short or long
preambles)
        Tag Number: 50 (Extended Supported Rates)
```

```
    Tag length: 4
    Tag interpretation: Supported rates: 9,0 18,0 48,0 54,0 [Mbit/sec]

0000  80 00 00 00 ff ff ff ff ff ff 00 0f 3d ac 83 92   ............=...
0010  00 0f 3d ac 83 92 80 a5 37 f0 7c de 72 00 00 00   ..=.....7.|.r...
0020  64 00 11 04 00 04 57 4c 41 4e 01 08 82 84 8b 96   d.....WLAN......
0030  0c 18 30 48 03 01 06 05 04 00 01 00 00 07 06 47   ..0H...........G
0040  42 20 01 0d 14 2a 01 04 32 04 12 24 60 6c         B ...*..2..$`l
```

3. Captura trama DATA que emplea protocolo WEP :

```
No.     Time        Source              Destination         Protocol Info
    43 6.046709    Airespac_15:5b:00    AppleCom_04:c6:a9    IEEE 802.11 Data

Frame 43 (134 bytes on wire, 134 bytes captured)
   Arrival Time: Mar 30, 2005 03:15:29.180192000
   Time delta from previous packet: 0.003586000 seconds
   Time since reference or first frame: 6.046709000 seconds
   Frame Number: 43
   Packet Length: 134 bytes
   Capture Length: 134 bytes
   Protocols in frame: wlan:data
IEEE 802.11
   Type/Subtype: Data (32)
   Frame Control: 0x4208 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 0
      Flags: 0x42
         DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
         .... .0.. = More Fragments: This is the last fragment
         .... 0... = Retry: Frame is not being retransmitted
         ...0 .... = PWR MGT: STA will stay up
         ..0. .... = More Data: No data buffered
         .1.. .... = WEP flag: WEP is enabled
         0... .... = Order flag: Not strictly ordered
   Duration: 258
   Destination address: 00:30:65:04:c6:a9 (AppleCom_04:c6:a9)
   BSS Id: 00:0b:85:1f:63:40 (Airespac_1f:63:40)
   Source address: 00:0b:85:15:5b:00 (Airespac_15:5b:00)
   Fragment number: 0
   Sequence number: 2831
   WEP parameters
      Initialization Vector: 0x000000
```

```
    Key: 0
    WEP ICV: 0xe62136e2 (not verified)
Data (102 bytes)

0000  08 42 02 01 00 30 65 04 c6 a9 00 0b 85 1f 63 40   .B...0e.......c@
0010  00 0b 85 15 5b 00 f0 b0 00 00 00 00 72 30 53 f9   ....[.......r0S.
0020  3e 09 71 bc dc be e9 0e 6b e5 9f cd 71 59 05 9c   >.q.....k...qY..
0030  0c fc 28 50 2a 01 09 01 f7 11 4b ba e8 8d db fb   ..(P*.....K.....
0040  5e 91 3e 80 fe 96 88 8d 6d 7c ab 82 03 04 52 93   ^.>.....m|....R.
0050  2e 0b 6b 0a 60 47 05 81 9c 85 20 51 b9 30 e3 ad   ..k.`G.... Q.0..
0060  fc 87 b4 c1 dc 66 4e a1 69 e1 c7 2e b0 9c a3 bc   .....fN.i.......
0070  09 d7 cd 94 31 84 28 33 83 89 2c 24 26 d0 39 63   ....1.(3..,$&.9c
0080  05 17 e6 21 36 e2                                 ...!6.
```

4. Captura Solicitud DNS sin criptografiar :

```
No.     Time        Source                Destination           Protocol Info
  26288 1110.471290 10.9.247.246          10.9.1.1              DNS      Standard query A ns-de1.
pepemann.es

Frame 26288 (98 bytes on wire, 98 bytes captured)
    Arrival Time: Feb 28, 2005 18:45:45.002766000
    Time delta from previous packet: 0.027011000 seconds
    Time since reference or first frame: 1110.471290000 seconds
    Frame Number: 26288
    Packet Length: 98 bytes
    Capture Length: 98 bytes
    Protocols in frame: wlan:llc:ip:udp:dns
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0108 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x1
            DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 258
    BSS Id: 00:40:96:a0:6e:1a (AironetW_a0:6e:1a)
    Source address: 00:02:2d:81:7d:9d (10.9.247.246)
    Destination address: 00:02:a5:4b:2d:a5 (10.9.1.1)
```

```
    Fragment number: 0
    Sequence number: 764
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func=UI (0x03)
        000. 00.. = Command: Unnumbered Information (0x00)
        .... ..11 = Frame type: Unnumbered frame (0x03)
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 10.119.24.26 (10.119.24.26), Dst Addr: 10.119.24.1 (10.119.24.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 66
    Identification: 0x6955 (26965)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0xc44c (correct)
    Source: 10.119.24.26 (10.119.24.26)
    Destination: 10.119.24.1 (10.119.24.1)
User Datagram Protocol, Src Port: 4390 (4390), Dst Port: domain (53)
    Source port: 4390 (4390)
    Destination port: domain (53)
    Length: 46
    Checksum: 0xc334 (correct)
Domain Name System (query)
    Transaction ID: 0x8973
    Flags: 0x0100 (Standard query)
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Questions: 1
```

```
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
   Queries
      ns-de1.mannesmann.de: type A, class IN
         Name: ns-de1. pepemann.es.
         Type: A (Host address)
         Class: IN (0x0001)

0000  08 01 02 01 00 40 96 a0 6e 1a 00 02 2d 81 7d 9d   .....@..n...-.}.
0010  00 02 a5 4b 2d a5 c0 2f aa aa 03 00 00 00 08 00   ...K-../........
0020  45 00 00 42 69 55 00 00 80 11 c4 4c 0a 09 f7 f6   E..BiU.....L....
0030  0a 09 01 01 11 26 00 35 00 2e c3 34 89 73 01 00   .....&.5...4.s..
0040  00 01 00 00 00 00 00 00 06 6e 73 2d 64 65 31 0a   .........ns-de1.
0050  6d 61 6e 6e 65 73 6d 61 6e 6e 02 64 65 00 00 01   pepemann.es...
0060  00 01                                             ..
```

5. Captura EAP Request :

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Airespac_1f:63:40	10.64.135.73	EAP	Request, Identity [RFC3748]

```
Frame 1 (65 bytes on wire, 65 bytes captured)
   Arrival Time: Mar 29, 2005 17:46:03.553229000
   Time delta from previous packet: 0.000000000 seconds
   Time since reference or first frame: 0.000000000 seconds
   Frame Number: 1
   Packet Length: 65 bytes
   Capture Length: 65 bytes
   Protocols in frame: eth:eapol:eap
Ethernet II, Src: 00:0b:85:1f:63:40, Dst: 00:02:2d:22:43:c9
   Destination: 00:02:2d:22:43:c9 (10.64.135.73)
   Source: 00:0b:85:1f:63:40 (Airespac_1f:63:40)
   Type: 802.1X Authentication (0x888e)
802.1x Authentication
   Version: 1
   Type: EAP Packet (0)
   Length: 47
   Extensible Authentication Protocol
      Code: Request (1)
      Id: 0
      Length: 47
      Type: Identity [RFC3748] (1)
      Identity (42 bytes): \000networkid=GSS,nasid=AlcatelGSS,portid=2
```

```
0000  00 02 2d 22 43 c9 00 0b 85 1f 63 40 88 8e 01 00   ..-"C.....c@....
0010  00 2f 01 00 00 2f 01 00 6e 65 74 77 6f 72 6b 69   ./.../..networki
0020  64 3d 47 53 52 53 2c 6e 61 73 69 64 3d 41 6c 63   d=GSS,nasid=Alc
0030  61 74 65 6c 47 53 52 53 2c 70 6f 72 74 69 64 3d   atelGSS,portid=
0040  32
```

6. Captura NetBIOS sin criptografiar:

```
No.     Time       Source                Destination           Protocol Info
163 37.430877   192.168.10.22         192.168.10.255        NBNS     Name query NB SERVIDOR<20>

Frame 163 (110 bytes on wire, 110 bytes captured)
    Arrival Time: Mar 20, 2005 13:16:49.023225000
    Time delta from previous packet: 37.430877000 seconds
    Time since reference or first frame: 37.430877000 seconds
    Frame Number: 163
    Packet Length: 110 bytes
    Capture Length: 110 bytes
    Protocols in frame: wlan:llc:ip:udp:nbns
IEEE 802.11
    Type/Subtype: Data (32)
    Frame Control: 0x0208 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x2
            DS status: Frame is exiting DS (To DS: 0  From DS: 1) (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    BSS Id: 00:80:c8:ad:30:82 (D-Link_ad:30:82)
    Source address: 00:e0:7d:84:10:8f (Netronix_84:10:8f)
    Fragment number: 0
    Sequence number: 182
Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
    Control field: U, func=UI (0x03)
```

```
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
   Organization Code: Encapsulated Ethernet (0x000000)
   Type: IP (0x0800)
Inet Protocol, Src Addr: 192.168.10.22 (192.168.10.22), Dst Addr: 192.168.10.255 (192.168.10.255)
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..0. = ECN-Capable Transport (ECT): 0
      .... ...0 = ECN-CE: 0
   Total Length: 78
   Identification: 0x1b7b (7035)
   Flags: 0x00
      0... = Reserved bit: Not set
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
   Fragment offset: 0
   Time to live: 128
   Protocol: UDP (0x11)
   Header checksum: 0x9cbe (correct)
   Source: 192.168.10.22 (192.168.10.22)
   Destination: 192.168.10.255 (192.168.10.255)
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
   Source port: netbios-ns (137)
   Destination port: netbios-ns (137)
   Length: 58
   Checksum: 0x94ea (correct)
NetBIOS Name Service
   Transaction ID: 0x839d
   Flags: 0x0110 (Name query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Name query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... ...1 .... = Broadcast: Broadcast packet
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
   Queries
      SERVIDOR<20>: type NB, class IN
         Name: SERVIDOR<20> (Server service)
         Type: NB
         Class: IN
```

```
0000  08 02 00 00 ff ff ff ff ff ff 00 80 c8 ad 30 82   ..............0.
0010  00 e0 7d 84 10 8f 60 0b aa aa 03 00 00 00 08 00   ..}...`.........
0020  45 00 00 4e 1b 7b 00 00 80 11 9c be c0 a8 00 16   E..N.{..........
0030  c0 a8 00 ff 00 89 00 89 00 3a 94 ea 83 9d 01 10   .........:......
0040  00 01 00 00 00 00 00 00 20 46 44 45 46 46 43 46   ........ FDEFFCF
0050  47 45 4a 45 45 45 50 46 43 43 41 43 41 43 41 43   GEJEEEPFCCACACAC
0060  41 43 41 43 41 43 41 43 41 00 00 20 00 01         ACACACACA.. ..
```

7. Captura PROBE REQUEST :

No. Time Source Destination Protocol Info
292 50.496332 NokiaDan_c0:31:4e Broadcast IEEE 802.11 Probe Request, SSID: Broadcast

```
Frame 292 (35 bytes on wire, 35 bytes captured)
    Arrival Time: Mar 30, 2005 04:56:13.385882000
    Time delta from previous packet: 0.000653000 seconds
    Time since reference or first frame: 50.496332000 seconds
    Frame Number: 292
    Packet Length: 35 bytes
    Capture Length: 35 bytes
    Protocols in frame: wlan
IEEE 802.11
    Type/Subtype: Probe Request (4)
    Frame Control: 0x0040 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 4
        Flags: 0x0
            DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From DS: 0) (0x00)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = WEP flag: WEP is disabled
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
    Source address: 00:0e:ed:c0:31:4e (NokiaDan_c0:31:4e)
    BSS Id: ff:ff:ff:ff:ff:ff (Broadcast)
    Fragment number: 0
    Sequence number: 19
IEEE 802.11 wireless LAN management frame
    Tagged parameters (11 bytes)
```

Tag Number: 0 (SSID parameter set)
Tag length: 0
Tag interpretation:
Tag Number: 1 (Supported Rates)
Tag length: 4
Tag interpretation: Supported rates: 1,0 2,0 5,5 11,0 [Mbit/sec]
Tag Number: 10 (Reserved tag number)
Tag length: 1
Tag interpretation: Not interpreted

```
0000  40 00 00 00 ff ff ff ff ff ff 00 0e ed c0 31 4e   @.............1N
0010  ff ff ff ff ff ff 30 01 00 00 01 04 02 04 0b 16   ......0.........
0020  0a 01 07                                         ...
```

8. Captura PROBE RESPONSE :

No. Time Source Destination Protocol Info
293 50.497300 Airespac_1f:63:41 NokiaDan_c0:31:4e IEEE 802.11 Probe Response, SSID: “RSE"

Frame 293 (65 bytes on wire, 65 bytes captured)
Arrival Time: Mar 30, 2005 04:56:13.386850000
Time delta from previous packet: 0.000968000 seconds
Time since reference or first frame: 50.497300000 seconds
Frame Number: 293
Packet Length: 65 bytes
Capture Length: 65 bytes
Protocols in frame: wlan
IEEE 802.11
Type/Subtype: Probe Response (5)
Frame Control: 0x0850 (Normal)
Version: 0
Type: Management frame (0)
Subtype: 5
Flags: 0x8
DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
.... .0.. = More Fragments: This is the last fragment
.... 1... = Retry: Frame is being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = WEP flag: WEP is disabled
0... .... = Order flag: Not strictly ordered
Duration: 314
Destination address: 00:0e:ed:c0:31:4e (NokiaDan_c0:31:4e)

```
   Source address: 00:0b:85:1f:63:41 (Airespac_1f:63:41)
   BSS Id: 00:0b:85:1f:63:41 (Airespac_1f:63:41)
   Fragment number: 0
   Sequence number: 1924
IEEE 802.11 wireless LAN management frame
   Fixed parameters (12 bytes)
      Timestamp: 0x00000000772A4393
      Beacon Interval: 0,102400 [Seconds]
      Capability Information: 0x0431
         .... .... .... ...1 = ESS capabilities: Transmitter is an AP
         .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
         .... .... .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
         .... .... ...1 .... = Privacy: AP/STA can support WEP
         .... .... ..1. .... = Short Preamble: Short preamble allowed
         .... .... .0.. .... = PBCC: PBCC modulation not allowed
         .... .... 0... .... = Channel Agility: Channel agility not in use
         .... .1.. .... .... = Short Slot Time: Short slot time in use
         ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
   Tagged parameters (29 bytes)
      Tag Number: 0 (SSID parameter set)
      Tag length: 3
      Tag interpretation: RSE
      Tag Number: 1 (Supported Rates)
      Tag length: 8
      Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 6,0 9,0 12,0 18,0 [Mbit/sec]
      Tag Number: 3 (DS Parameter set)
      Tag length: 1
      Tag interpretation: Current Channel: 6
      Tag Number: 7 (Country Information)
      Tag length: 6
      Tag interpretation: Country Code: ES, Any Environment, Start Channel: 1, Channels: 13, Max TX
Power: 20 dBm
      Tag Number: 42 (ERP Information)
      Tag length: 1
      Tag interpretation: ERP info: 0x7 (Non-ERP STAs, use protection, short or long preambles)

0000  50 08 3a 01 00 0e ed c0 31 4e 00 0b 85 1f 63 41   P.:.....1N....cA
0010  00 0b 85 1f 63 41 40 78 93 43 2a 77 00 00 00 00   ....cA@x.C*w....
0020  64 00 31 04 00 03 54 4d 45 01 08 82 84 8b 96 0c   d.1...RSE.......
0030  12 18 24 03 01 06 07 06 45 53 20 01 0d 14 2a 01   ..$.....ES ...*.
0040  07
```