CAPITULO 2

PROTOCOLO 802.11

Al trabajar en una laptop anteriormente se necesitaba estar conectado físicamente a la red para tener acceso a Internet u otros servicios, con el avance tecnológico logramos conectarnos a una red de manera inalámbrica, y esto lo podemos lograr gracias a los dispositivos que soportan el protocolo 802.11. En este capítulo se presenta de manera clara el protocolo 802.11, su operación, seguridad y topologías comúnmente usadas y la simbología usada para la ubicación de una red.

2.1 Introducción

El protocolo IEEE (*Institute of Electrical and Electronic Engineers*) 802.11 es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (*Open Systems Interconnection*) en las capas física y de enlace de datos, especificando sus normas de funcionamiento en una red inalámbrica. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps. y trabajaba en la banda de frecuencia de 2.4 Ghz. En la actualidad no se fabrican productos sobre este estándar. La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps también trabajaba en la frecuencia de 2.4 Ghz. También se realizo una especificación sobre

una frecuencia de 5 Ghz. que alcanzaba los 54 Mbps era la 802.11a y resultaba incompatible con los productos del 802.11b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g. (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps.). [IEEE]

Dado que la tecnología avanza a pasos agigantados, nombraremos las derivaciones del protocolo 802.11 para poder tener una idea de lo extenso que se ha vuelto.[IEEE] [SEGSECO] [GNIST]

802.11: Protocolo que proporciona de 1 a 2 Mbps. en el rango de frecuencia 2.4Ghz, usando: FHSS (*Frequency Hopping Spread Spectrum*) o DSSS (*Direct Sequence Spread Spectrum*).

802.11a: Revisión del protocolo 802.11 que proporciona 54 Mbps. estandarizado y hasta 72 y 108 Mbps. con tecnologías de desdoblamiento no estandarizado en el rango de frecuencia 5GHz, usando OFDM (*Orthogonal Frequency Division Multiplexing*) y DSSS.

802.11b: También llamado 802.11 *High Rate* o *Wi-Fi*, revisión del protocolo 802.11 que proporciona 11 Mbps. con reducciones a 5.5, 2 y 1 Mbps. en el rango de frecuencia 2.4 Ghz. usando DSSS.

802.11c: Define características de Punto de Acceso como puentes (*bridges*).

802.11d: Permite el uso de 802.11 en países restringidos por el uso de las frecuencias.

802.11e: Define el uso de QoS (*Quality of Service*).

802.11f: Define el enlace entre Estaciones y Puntos de Acceso en modo viajero (*Roaming).*

802.11g: Protocolo que proporciona 54 Mbps. en el rango de frecuencia 2.4 Ghz. manteniendo plena compatibilidad con el protocolo 802.11b. Puede trabajar con el protocolo 802.11a cambiando la configuración del dispositivo.

802.11h: Superior al 802.11a permite asignación dinámica de canales (coexistencia con el *HyperLAN*). Regula la potencia en función de la distancia.

802.11i: Estándar que define el cifrado y la autentificación para complementar, completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del WPA con su técnica llamada *Temporal Key Integrity Protocol* (TKIP), será aplicable a redes 802.11a (54Mbps.), 802.11b (11Mbps.) y 802.11g (22Mbps.). Lo desarrolla el comité formado por Cisco, VDG, Trapeze, Agere, IBM, Intersil y otros.

802.11j: Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB (*Association of Radio Industries and Businesses, Japan*) e HISWAN (*Hi Speed Wireless Access System*).

802.11k: Trabajo en proceso: proporciona información para hacer las redes inalámbricas más eficientes

- Decisiones viajero (*roaming).*
- Conocimiento del canal RF.
- Nodos Ocultos.
- Estadísticas de clientes.
- Transmisiones de control de energía (TPC).

802.11l: Saltado porque asimila al 802.11i

802.11m: Trabajo en proceso. Propuesto para mantenimiento de redes inalámbricas.

802.11n: Trabajo en proceso. Nuevo estándar de red inalámbrica.

- Construido desde cero. (No chips en modo turbo).
- Velocidad verdadera 100Mbps (250Mbps en el nivel Físico).
- Mejores distancias de operación.
- Posiblemente para finales del 2005.

802.11o: Trabajo en proceso: Exclusivo para voz en red inalámbrica (un cambio de código "*handoff*" más rápido, da la prioridad a tráfico de voz sobre datos).

802.11p: Trabajo en proceso: Usa la banda de 5.9 Ghz. para largo alcance.

802.11q: Trabajo en proceso: ayuda para la VLAN (*Virtual Lan*).

802.11r: Trabajo en proceso: r de *roaming*, manejando un cambio de código *"handoff")* rápido cuando hay un viajero "*roaming"* entre Puntos de Acceso.

802.11s: Trabajo en proceso. Redes de auto ayuda y de auto configuración.

802.11x: Se utiliza para resumir todos los estándares dentro del grupo de funcionamiento, pero no es un estándar.

2.2 Características del 802.11.

La especificación original de 802.11 preveía conexiones a velocidades de 1 ó 2 MB/s en la banda de los 2.4 GHz utilizando dos tipos de tecnología de espectro ensanchado (S*pread Spectrum*) por salto en frecuencia (FHSS) y secuencia directa (DSSS). El objetivo principal a la hora de utilizar el espectro ensanchado es transmitir ocupando una banda de frecuencias mayor de la requerida. Su creación se debe a investigaciones militares durante la Segunda Guerra Mundial, ya que de esta forma se evitaban ataques y escuchas. FHSS (salto en frecuencia) se basa en que transmite en diferentes frecuencias, produciéndose saltos de una a otra frecuencia de una forma aleatoria que es imposible predecir. Por lo contrario, con DSSS (secuencia directa) se envían varios bits por cada bit de información real.

Características del 802.11a

Mientras se desarrollaba la 802.11b, la IEEE crea una nueva extensión del estándar 802.11 denominada 802.11a. Debido a que la 802.11b ganó popularidad rápidamente, mucha gente cree que la 802.11a se creó después que ésta, aunque en realidad se desarrollaron a la vez. Debido a su alto costo, la 802.11a suele utilizarse en redes de empresas, mientras que la 802.11b se usa más en redes domésticas. La 802.11a soporta velocidades de hasta 54Mbit/s y trabaja a 5GHz. Comparada con la 802.11b, esta mayor frecuencia limita el rango de la 802.11a, además, el trabajar en una frecuencia mayor significa que tiene una mayor dificultad para atravesar muros y objetos. Por otro lado, como la 802.11a y la 802.11b utilizan frecuencias distintas, ambas tecnologías son incompatibles entre ellas. Algunos fabricantes ofrecen híbridos 802.11a/b, aunque estos productos lo que tienen realmente son las dos extensiones implementadas.

Ventajas: Velocidad máxima alta, soporte de muchos usuarios a la vez y no produce interferencias en otros aparatos.
Inconvenientes: Alto costo, bajo rango de señal que es fácilmente obstruible.

Características del 802.11b

La 802.11b utiliza la misma frecuencia de radio que el tradicional 802.11 (2.4GHz). El problema es que al ser ésta una frecuencia sin regulación, se podían causar interferencias con hornos microondas, teléfonos móviles y otros aparatos que funcionen en la misma frecuencia. Sin embargo, si las instalaciones 802.11b están a una distancia razonable de

otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el coste de sus productos, aunque esto suponga utilizar una frecuencia sin regulación.

Ventajas: Bajo costo, rango de señal muy bueno y difícil de obstruir.

Inconvenientes: Baja velocidad máxima, soporte de un número bajo de usuarios a la vez y produce interferencias en la banda de 2.4 GHz.

Características del 802.11g

Entre 2002 y 2003 ha aparecido un nuevo estándar denominado 802.11g. Este nuevo estándar intenta aprovechar lo bueno de cada uno de los anteriores 802.11a y 802.11b. La 802.11g permite velocidades de hasta 54 Mbs y utiliza la banda de frecuencia de 2.4 GHz. Además, al trabajar en la misma banda de frecuencia, la 802.11g es compatible con la 802.11b, por lo que puntos de acceso 802.11g pueden trabajar en redes 802.11b y viceversa.

Ventajas: Velocidad máxima alta, soporte de muchos usuarios a la vez, rango de señal muy bueno y difícil de obstruir.

Inconvenientes: Alto costo y produce interferencias en la banda de 2.4 GHz.

2.3 Operación del 802.11

La arquitectura 802.11 se compone de varios componentes y servicios que interactúan para proporcionar la movilidad de la estación a las capas más altas del nivel de la red. El estándar IEEE 802.11 está orientado al desarrollo de Redes de Área Local inalámbricas con aplicación dentro de espacios interiores.

Autentificación

Dado que las redes inalámbricas han limitado seguridad física para prevenir el acceso desautorizado, 802.11 define servicios de la autentificación para controlar el acceso a la red inalámbrica. La meta del servicio de la autentificación es proporcionar el control de acceso igual que en una red alámbrica (802.3). El servicio de la autentificación proporciona un mecanismo para una estación de identificar otra estación. Sin esta prueba de la identidad, la estación no permite utilizar la red inalámbrica para la entrega de los datos. Todas las estaciones 802.11, si son parte de un sistema de servicio básico BSS (*Basic Service Set*) independiente o de la red de un sistema de servicio extendido ESS (*Extended Service Set*), deben utilizar el servicio de la autentificación antes de comunicarse con otra estación. IEEE 802.11 define dos tipos de servicios de la autentificación. [ILUSPUB01]

Autentificación del sistema abierto

Este es el método de la autentificación por defecto, que es un proceso muy simple, de dos etapas. Primero la estación que desea autenticar con otra estación envía una trama que

contiene la identidad de la estación que envía. La estación de recepción entonces envía una trama que alerta si reconoce la identidad de la estación de autenticidad.

La autentificación dominante compartida

Este tipo de autentificación asume que cada estación ha recibido una llave compartida secreta con una independiente segura del canal de la red 802.11. Las estaciones autentican con el conocimiento compartido de la llave secreta. El uso de la autentificación dominante compartido requiere la puesta en práctica del cifrado vía WEP o el algoritmo de WEP.

De-autentificación

El servicio de la de-autentificación se utiliza para eliminar a un usuario previamente autorizado para tener acceso al uso de la red en un futuro. Una vez que se de-autentica una estación, esa estación no puede acceder a la red inalámbrica a menos que se ejecute nuevamente la autentificación. La de-autentificación es una notificación y no puede ser rechazada. Por ejemplo, cuando una estación desea ser quitada de un BSS, puede enviar una trama de de-autentificación al punto de acceso asociado para notificar el punto de acceso del retiro de la red. Un punto de acceso podía también de-autenticar una estación enviando una trama de la de-autentificación a la estación. [KERNE]

Privacidad.

El servicio de la privacidad del IEEE 802.11 es diseñado para proporcionar un nivel equivalente a la protección para los datos en la red inalámbrica como es proporcionado por una red alámbrica con restricción de acceso físico. Este servicio protege los datos solamente, dado que ellos atraviesan el medio inalámbrico. No está diseñado para proporcionar la protección completa de datos entre las aplicaciones que corren sobre una red mezclada. Con una red inalámbrica, todas las estaciones y otros dispositivos pueden "oír" los datos del tráfico tomando un lugar sin rango en la red, afectando seriamente el nivel de la seguridad de una conexión inalámbrica. IEEE 802.11 contraresta este problema ofreciendo una opción de servicio de privacidad que levante la seguridad de la red 802.11 a la de una red alámbrica. El servicio de privacidad, aplicándose a todas las tramas de los datos y a algunas tramas de la autentificación, es un algoritmo de cifrado basado en el algoritmo WEP del 802.11.

El servicio de entrega de los datos

El servicio de entrega de datos es similar al proporcionado por el resto del IEEE 802. El servicio de entrega de los datos proporciona la entrega confiable de las tramas de los datos de la MAC (*Medium Access Control*) de una estación al MAC en una u otras estaciones, con una mínima duplicación y reordenamiento de las tramas.

2.4 El formato de la trama MAC del 802.11

La trama del formato MAC se muestra en la figura 2 donde la dirección 2, 3 y 4, control de la secuencia, y campos del cuerpo de la trama no se encuentran en cada trama de transmisión. La trama de control es de 16 bits de longitud, y contiene la información de control básica de la trama, incluyendo el tipo del trama (datos, control del MAC o administración del MAC) y el subtipo, si la trama se origina o está limitado al DS (*Distribution System*) y si la trama está encriptada. El campo de duración/ID indica la duración del resto de una secuencia del intercambio de la trama y se utiliza normalmente para controlar el mecanismo virtual del sentido del portador.

Los campos de dirección, si están presentes, contienen uno de los siguientes 48-bits de las direcciones de la capa de enlace de la IEEE 802: Dirección de Destino, Dirección de la fuente, Dirección del Receptor, Dirección del Transmisor, Identificación del Sistema Básico de Servicio (BSSID). Para las redes de infraestructura, el BSSID es la dirección de la capa de enlace del Punto de Acceso. Para las redes ad hoc, el BSSID es un número aleatorio generado cuando se forma la red ad hoc. El receptor, el transmisor, y las direcciones de BSSID son las direcciones del MAC de las estaciones unidas a el BSS que son transmitidas o de recibidas de la trama sobre la red inalámbrica. El destino y las direcciones de la fuente son las direcciones MAC de las estaciones inalámbricas o de otra manera, las cuales son el último destino y fuente de la trama. En esos casos donde están dos direcciones iguales (por ejemplo, la estación del receptor y la estación del destino son una y son iguales), entonces un solo campo de dirección se utiliza. Cuatro campos de dirección están presentes solamente en el caso infrecuente donde está el DS implementado con red de

802.11, y solamente para las tramas que atraviesan el DS. Un caso más típico implica una trama que se origina en una estación inalámbrica en una infraestructura BSS que esté limitada para una estación en una red cableada como el 802.3. En este caso, el campo de la dirección 1 contiene el BSSID, el campo de la dirección 2 contiene la dirección de la estación de la fuente/transmisor, el campo de la dirección 3 contiene la dirección de la estación de destino, y el campo de la dirección 4 no esta presente. Incluyendo el BSSID y la dirección de destino (o la dirección de la fuente para las tramas que fluyen al BSS) en la trama evita requerir al Punto de Acceso mantener una lista de las direcciones MAC de las estaciones que no están en el BSS.

El campo del control de la secuencia es 16 bits de longitud, y contiene el número de secuencia y los subcampos del número del fragmento. Las estaciones receptoras utilizan este campo para volver a reensamblar correctamente las tramas y para identificar y para desechar fragmentos duplicados de la trama.

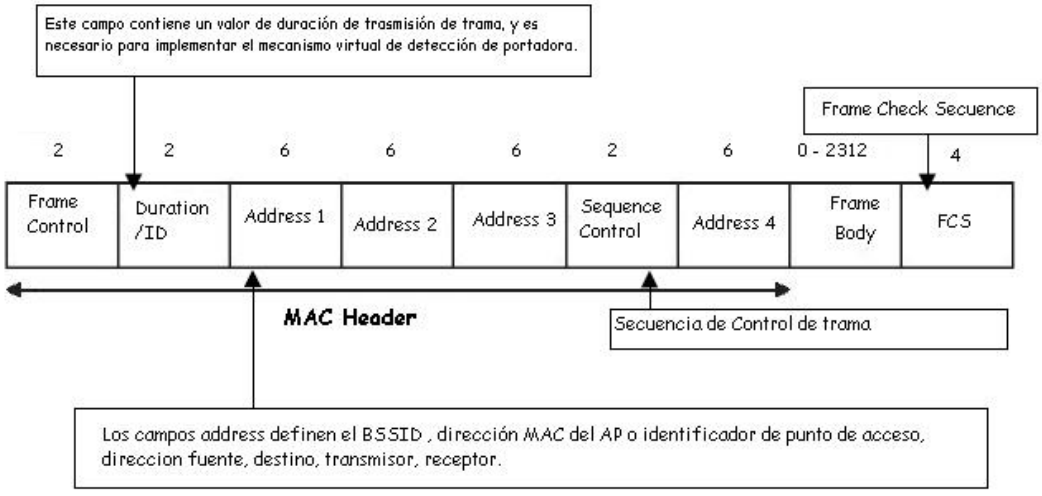

Figura 2. Trama de red inalámbrica

A continuación se muestra las tablas con los tipos de información que van contenidas en los paquetes de administración y control cuando se hace una conexión entre equipos o equipos y puntos de acceso.

- **Funciones de protocolo de autentificación/privacidad.**

El primer paso para un dispositivo en conexión a un BSS o un IBSS es autentificación. Esto puede ser un sistema de clave compartida o abierto. Si el cifrado WEP del paquete de datos está habilitado, la clave compartida deberá ser usada. La autentificación es manejada por un intercambio entre solicitar/responder de los paquetes de administración.	
Tipo de información	**Uso**
Autentificación ID.	Este es el nombre bajo el cual la estación actual se autentificó uniéndose a la red.
Habilitación WEP.	Si este campo es verdad, entonces la carga útil del paquete (pero no de los encabezados de la red inalámbrica) será cifrada usando WEP

- **Funciones del protocolo de red de membresía/topología.**

El segundo paso para un dispositivo en conexión con un BSS o un IBSS es asociarse al grupo o al punto de acceso. Al viajar, una unidad también necesita el desasociarse y el reasociarse. Estas funciones son manejadas por un intercambio de los paquetes de la administración, pero el estado actual se demuestra en los encabezados del paquete.	
Tipo de información	**Uso**
Asociación.	Los paquetes pueden mostrar la asociación actual del emisor.

	Asociación y reasociación son dirigidos por la petición/respuesta del administrador de paquetes. La desasociación es una simple declaración de un punto de acceso o algún dispositivo.
IBSSID o ESSID.	La identificación del grupo o de su punto de acceso. Un dispositivo se puede asociar solamente a un punto de acceso (mostrado por el ESSID) o al IBSS a la vez.
Prueba.	Estos son paquetes de la administración de petición/respuesta usados por los dispositivos viajeros en búsqueda de un punto de acceso o de un BSS. Ellos soportan las habilidades de unidades viajeras para moverse entre células mientras se mantengan conectados.

- **Funciones del protocolo de red condiciones/transmisión.**

El protocolo de red inalámbrica 802.11b soporta el ajuste rápido a las condiciones que cambian, siempre buscando el mejor rendimiento de procesamiento	
Tipo de información	**Uso**
Canal.	El canal usado para esta transmisión.
Velocidad de Datos.	La velocidad de datos usada para transmitir un paquete.
Fragmentación.	Las redes inalámbricas 802.11b imponen su propia fragmentación ante los paquetes, totalmente independientes de cualquier fragmentación impuesta por protocolos de la alto nivel tales como TCP/IP. Una serie de transmisiones cortas es

	menos vulnerable a interferencia en ambientes ruidosos. Esta fragmentación es dinámicamente fijado por el protocolo en un esfuerzo de reducir el número, o por lo menos el costo, de retransmisiones.
Sincronización.	Varias clases de sincronización son importantes en las redes inalámbricas. Los paquetes de administración de red llamados “beacon" mantienen los miembros de un BSS sincronizado. Además, los dispositivos divulgan el estado de su propia sincronización interna. Finalmente, todas las transmisiones contienen datos de tiempo.
Economía de Energía.	Las computadoras portátiles en la necesidad particular de conservar energía. Para facilitar esto, el protocolo utiliza un número de campos en los paquetes de los datos incluyendo el paquete de control del “save-poll” ahorrador de la energía para dejar a los dispositivos permanecer conectados a la red mientras están en el modo economizador.

- **Funciones del protocolo de control de transmisión.**

Aunque el protocolo en su totalidad controla realmente la transmisión de datos, los ciertos encabezados y paquetes del control tienen esto como trabajo particular.	
Tipo de información	**Uso**
RTS, CS, ACK.	Estos son paquetes del control usados al establecer la conexión ayudando a evitar las colisiones.

Versión.	La versión del protocolo 802.11 que se usado en la construcción del paquete.
Tipo y subtipo.	El tipo de paquete (datos, administrador o control), con un subtipo especificando su función exacta.
Duración.	En la ayuda de la sincronización y del acceso ordenado a las ondas de aire, los paquetes contienen un valor exacto por el tiempo que se debe asignar para el resto de la transacción de la cual este paquete forma parte.
Longitud.	Longitud del paquete.
Retransmisión.	La retransmisión es común. Es importante declarar cual de los paquetes son retransmitidos.
Secuencia	La Secuencia de información en paquetes ayuda a reducir las retransmisiones y otros errores potenciales.
Orden	Algunos datos, como las comunicaciones de voz, deben de ser dirigidos en estricto orden hasta el extremo de recepción.

- **Funciones del protocolo de enrutamiento.**

Otra vez, muchos campos se relacionan con el tráfico del enrutamiento, pero los siguientes se relacionan lo más directamente posible.	
Tipo de información	**Uso**
Dirección.	Hay cuatro campos de dirección en los paquetes de las redes inalámbricas 802.11b, en vez de los dos encontrados en

	Ethernet o los encabezados del IP. Estos deben acomodar la posibilidad de adelantar a, de, o a través DS. Además de las direcciones normales de destino y de la fuente, estos campos pueden mostrar el transmisor, el receptor, o la identificación de los BSS. Cuáles de los campos de dirección muestran que direcciones dependen o si (y cómo) el paquete está encaminado por el DS. Control y administración de los paquetes necesitan tres campos de dirección, porque nunca pueden ser encaminados a o desde (es decir, a través) el DS.
Hacia/de DS.	En un ESS, el tráfico se puede rutear desde un dispositivo usando un punto de acceso a un dispositivo usando un diverso punto de acceso en alguna parte a lo largo de la red. Estos campos describen el ruteo a través del DS y dicen al dispositivo de recepción cómo interpretar los campos de dirección.
Más datos.	Los puntos de acceso pueden recibir los datos de otros dispositivos. Este sirve para viajar a través de BSS o de células y de las características de la economía de energía. Cuando un dispositivo recibe un mensaje de un punto de acceso, puede ser que el punto de acceso tiene más datos en esperar.

2.5 CSMA/CA.

Una vez que una estación inalámbrica se asocie a un AP, puede comenzar a enviar y recibir las tramas de los datos hacia y desde el punto de acceso. Pero dado que múltiples estaciones pueden desear transmitir tramas de datos en el mismo tiempo y en el mismo canal, un protocolo múltiple del acceso es necesario para coordinar las transmisiones.

Este protocolo es obligatorio para estaciones y puntos de acceso. El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA (Carrier Sense Multiple Access / Collision Advoidance), que significa que cada estación monitorea el canal antes de transmitir, y se detiene cuando detecta el canal ocupado. Aunque las redes 802.3 y 802.11 utilizan detección de portador de acceso aleatorio, los dos protocolos del MAC tienen diferencias importantes. Primero, en vez de usar la detección de la colisión, 802.11 usa técnicas para evitar la colisión. En segundo lugar, debido a los índices relativamente altos del bit-error de los canales inalámbricos 802.11, utiliza un esquema de reconocimiento/retransmisión de la capa de enlace. Este protocolo funciona tal y como se describe a continuación:

1.- Si la estación detecta inicialmente que el canal está libre, transmite su trama después de un período del tiempo corto conocido como *Distributed Inter-frame Spacing (DIFS).*

2.- En caso contrario, la estación elige un valor al azar del *backoff* (tiempo de espera) y cuenta de regreso de este valor cuando el canal está libre. Cuando el canal es detectado como ocupado, el valor del contador continuará congelado.

3.- Cuando el contador alcanza cero (nota que esto puede ocurrir solamente cuando el canal es detectado como libre), las estaciones transmiten la trama entera y después esperan un reconocimiento de la misma.

4.- Si se recibe un reconocimiento, la estación que transmite sabe que su trama se ha recibido correctamente en la estación de destino. Si la estación tiene otra trama a enviar, comienza el protocolo de CSMA/CA en el paso 2. Si el reconocimiento no se recibe, la estación que transmite entra la fase del "*backoff*" de nuevo en el paso 2, con el valor al azar elegido de un intervalo más grande. (Los tiempos de espera son de 20µseg.)

El protocolo MAC del 802.11 también incluye un esquema efectivo de reserva (pero opcional) que las ayuda a evitar colisiones incluso en la presencia de terminales ocultas. Dicha solución permite que una estación utilice una corta trama de control llamada petición de envío (RTS) y una corta trama de control llamada limpio para enviar (CTS) para reservar el acceso al canal.

Cuando un dispositivo desea enviar una trama de datos, puede primero enviar una trama de RTS al AP, indicando el tiempo total requerido para transmitir la trama de los datos y la trama de reconocimiento (ACK). Cuando el AP recibe la trama del RTS, responde difundiendo la trama de CTS. Esta trama CTS tiene dos propósitos: Da al dispositivo que

envía permiso para enviar y también manda instrucciones a las otras estaciones para no enviar durante la duración reservada, esto se puede observar en la figura 3.

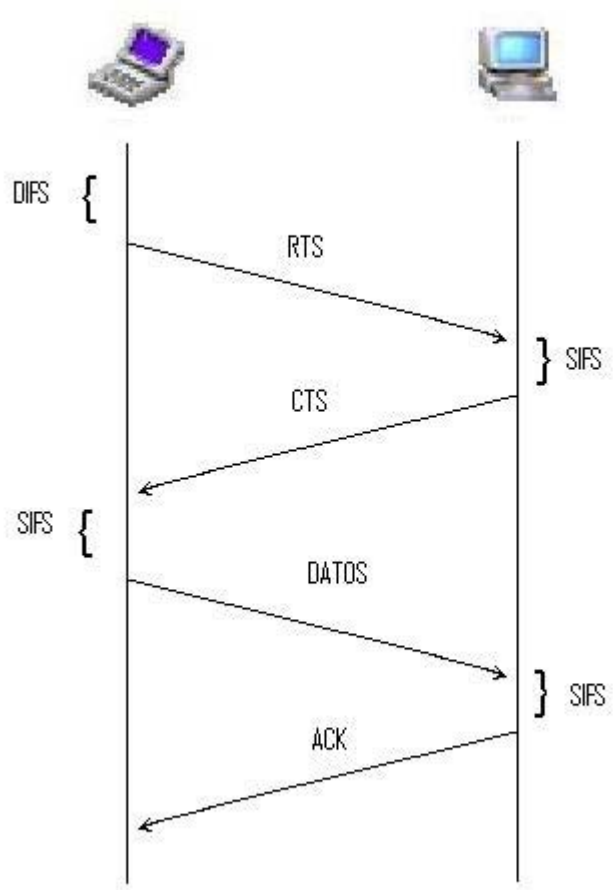

Figura 3. *Collision Avoidance* usando RTS y CTS.

2.6 Tipos de codificación del 802.11

Como nombramos en las características del 802.11, cada protocolo maneja diferente tipo de codificación, en el caso del 802.11a ocupa la codificación DSSS, en cambio el protocolo

802.11 b y el 802.11g ocupan FHSS con lo cual pueden trabajar o compartirse cualquiera de éstos.

Salto en Frecuencia (Frecuency Hopping Spread Spectrum Radio).

Con la técnica de salto en frecuencia se modula la señal de datos con una portadora que salta de frecuencia en frecuencia sobre una banda de frecuencias. En el estándar IEEE 802.11 la portadora saltará sobre la frecuencia de 2.4 Ghz entre los límites 2.4 Ghz y 2.483 Ghz. Esta técnica fue concebida a principios de la Segunda Guerra Mundial. Un patrón de salto determina las frecuencias en las que se transmitirá y en que orden. Para recibir la señal adecuadamente, el receptor debe conocer ese patrón y escuchar la señal en el momento justo y frecuencia correcta. La normativa de la FCC requiere que los fabricantes empleen 75 o más frecuencias por canal de transmisión con un intervalo de tiempo por frecuencia de 400ms. Esta técnica reduce la interferencia procedente de un sistema de banda estrecha, ya que afectará únicamente a la señal de espectro ensanchado si ambas se transmiten en la misma frecuencia y al mismo tiempo. Esto provocaría sólamente unos cuantos bits de error. Es posible operar varios equipos dentro de la misma banda de frecuencias empleando espectro ensanchado con patrones de salto diferentes. Mientras un equipo transmite en una cierta frecuencia otro lo hará en otra diferente sin interferirse en ese instante de tiempo.

Secuencia Directa (Direct Sequence Spread Spectrum Radio)

Espectro ensanchado por secuencia directa combina una señal de datos con otra secuencia detasa binaria elevada. A esta secuencia se le denomina código chip (ganancia de

procesado). Esta ganancia incrementa la resistencia de la señal frente a las interferencias. El estándar 802.11 exige un mínimo de 11 bits para formar la secuencia (11 chips). La siguiente figura muestra un ejemplo de funcionamiento de esta técnica de secuencia directa. Un código chip es asignado para representar un 1 y otro código para representar un 0. A esta secuencia de bits o chip se le denomina código Barker.

2.7 Topologías

Existen dos métodos de comunicación vía inalámbrica, los cuales son:

Modo Ad Hoc: Es el medio de comunicación por el cual uno se conecta a otro dispositivo suponiendo crear una red imaginaria entre dos equipos de computo, no existe un punto de acceso y la comunicación es uno a uno "*Peer to Peer"*.

Modo Infraestructura: Es el medio en el cual se requiere de almenos un Punto de Acceso, así todo el trafico pasa por el PA, siendo este el dispositivo que funciona como un HUB.

Modo Monitor: Permite monitorear paquetes sin asociarse al PA o a una red ad-hoc. [MAD04]

La estación *de red inalámbrica*

La estación (STA) es el componente más básico de la red inalámbrica. Una estación es cualquier dispositivo que contenga la funcionalidad del protocolo 802.11, la cual debe

manejar MAC (*Médium Access Control*), PHY (Capa Física) y una conexión al medio inalámbrica. Las funciones del 802.11 se ponen en ejecución típicamente en el hardware y en el software de una tarjeta de red (NIC, *Network Interface Card*). Una estación podía ser una PC o computadora portátil, un dispositivo PDA o un punto de acceso. Las estaciones pueden ser móviles, portátiles, o inmóvil y todas las estaciones deben soportar el 802.11, servicios de autentificación, de la de-autentificación, de privacidad, y de entrega de los datos.

2.7.1 Topologías existentes.

Las topologías se refieren a las maneras en que uno se conecta a la red inalámbrica o crea una propia red con su propio dispositivo. Estos dispositivos deben de soportar protocolo 802.11 para poder soportar el enlace, así como también tomar en cuenta que los dispositivos soporten el protocolo de la red que se está creando.

El servicio básico independiente fijó (IBSS)

La topología más básica de la red inalámbrica es un sistema de las estaciones, que se han reconocido una de otra y están conectadas vía inalámbrica de una manera de uno a uno (*peer-to-peer*). Esta forma de topología de red se refiere a un Servicio Básico Independiente fijó (IBSS) o una red ad hoc. En un IBSS, las estaciones móviles se comunican directamente entre ellas. Cada estación móvil puede no estar habilitada para comunicarse con otra estación debido a las limitaciones del rango ver Figura 4. [ITCUR]

IBSS

Figura 4. IBSS Sistema Independiente del Servicio Básico.

Sistema de Servicio Básico (BSS)

Una infraestructura de sistema de servicio básico BSS es un componente llamado punto de acceso (AP). El punto de acceso proporciona una función local de la comunicación para el BSS. Todas las estaciones en el BSS se comunican con el punto de acceso y ya no se comunican directamente entre ellas. Todas las tramas son retransmitidas entre las estaciones por el punto de acceso (AP). Esta función local de la comunicación dobla con eficacia el rango del IBSS. El punto de acceso puede también proporcionar la conexión a un sistema de distribución u otra red ver Figura 5. [ITCUR]

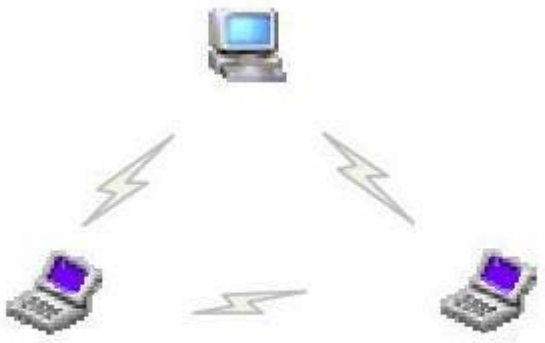

Figura 5. Infraestructura de Sistema de Servicio Básico (BSS).

El sistema de la distribución (DS)

El sistema de la distribución (DS) es el medio por el cual un punto de acceso se comunica con otro punto de acceso para intercambiar tramas para las estaciones en su respectiva BSS, las tramas se utilizan para seguir estaciones móviles conforme se vayan moviendo de un BSS a otro, e intercambia tramas por una red alámbrica. Como IEEE 802.11 lo describe, el sistema de distribución no es necesariamente una red, no es el lugar del estándar de alguna restricción en cómo es implementado el sistema de distribución, sólo en los servicios que debe proporcionar. Así el sistema de la distribución puede ser una red alámbrica como 802.3 o una red de propósito especial que interconecta los puntos de acceso y proporciona los servicios de distribución requeridos.

Sistema de Servicio Extendido (ESS)

La cobertura que extendía vía un Servicio Extendido Fijó (ESS) 802.11 prolonga el rango de la movilidad a un rango arbitrario a través del sistema extendido del servicio (ESS). Un sistema extendido del servicio es un sistema de la infraestructura BSS, donde los puntos de acceso se comunican entre sí mismos para remitir tráfico a partir de un BSS a otro para facilitar el movimiento de estaciones entre BSS. El punto de acceso realiza esta comunicación a través del sistema de la distribución. El sistema de la distribución es la espina dorsal de la red inalámbrica y se puede construir de una red alámbrica o de la red inalámbrica. El sistema de la distribución es típicamente una capa delgada en cada punto de acceso que determina el destino para el tráfico recibido de un BSS. El sistema de la distribución determina si el tráfico se retransmite de nuevo a un destino en el mismo BSS, se remite en el sistema de la distribución a otro punto de acceso, o se envía en la red alámbrica a un destino que no se encuentra en el sistema extendido del servicio. Las comunicaciones recibidas por un sistema de la distribución del punto de acceso se transmiten al BSS que serán recibidas por la estación móvil de destino ver Figura 6.

El equipo de la red fuera del sistema extendido de servicio ve el ESS y todas sus estaciones móviles como una sola red de la capa MAC donde todas las estaciones están físicamente inmóviles. Así, el ESS oculta la movilidad de las estaciones móviles de todo el exterior del ESS. Este nivel de dirección proporcionado por la arquitectura del 802.11 permite a los protocolos de red existentes que no tienen ningún concepto de la movilidad operen correctamente con una red inalámbrica donde hay movilidad. [IITCUR] [INSEG]

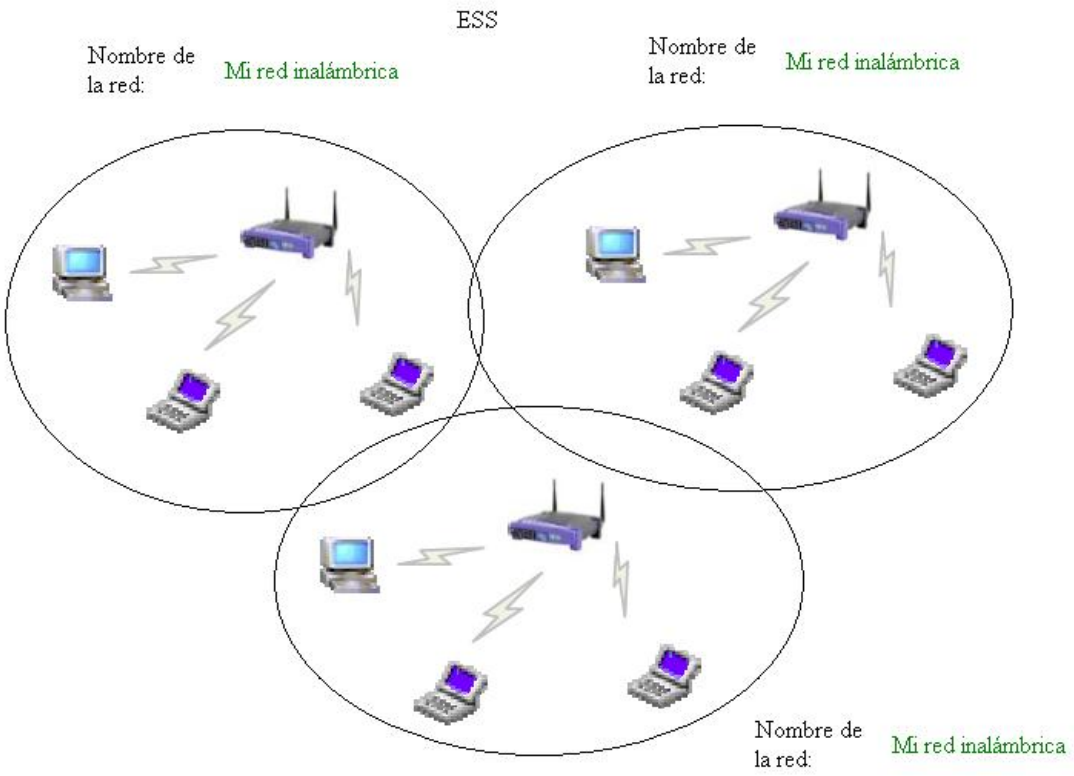

Figura 6. Sistema de Servicio Extendido (ESS).

2.8 Tramas de programas Ethereal, Omni Peek y Netstumbler.

En éste parte del capítulo daremos una breve explicación de los programas Ethereal [EHTE], Omni Peek [OPEEK], Network Stumbler [NETSTB] para poder conocer de una manera práctica lo que nos tratan de dar a entender, para así comprender el funcionamiento de la red, tanto inalámbrica como alámbrica. En el apéndice A se hablara del programa Ethereal y de su funcionamiento básico, tanto captura como archivos capturados.

En la Figura 7 podemos observar que en el programa Ethereal las tramas están numeradas, en este caso está remarcada la trama 14 la cual se grabo en el segundo 1.7921, dándonos a

conocer la fuente del acceso que se hizo en ese momento y el destino al cual iba dirigido el mismo, de ésta manera nos da a conocer el tipo de protocolo que se está usando en el momento de la captura, y una pequeña parte la cual nos dice de una manera sencilla la información que transmite al medio, esto de una manera codificada, en esta información se transmiten datos como por ejemplo al momento de hacer una conexión se hace un llamado al broadcast puesto que se hace un ingreso, y se hace un llamado a una dirección IP, para saber si es ocupada por algún usuario, o si puede ser reasignada.

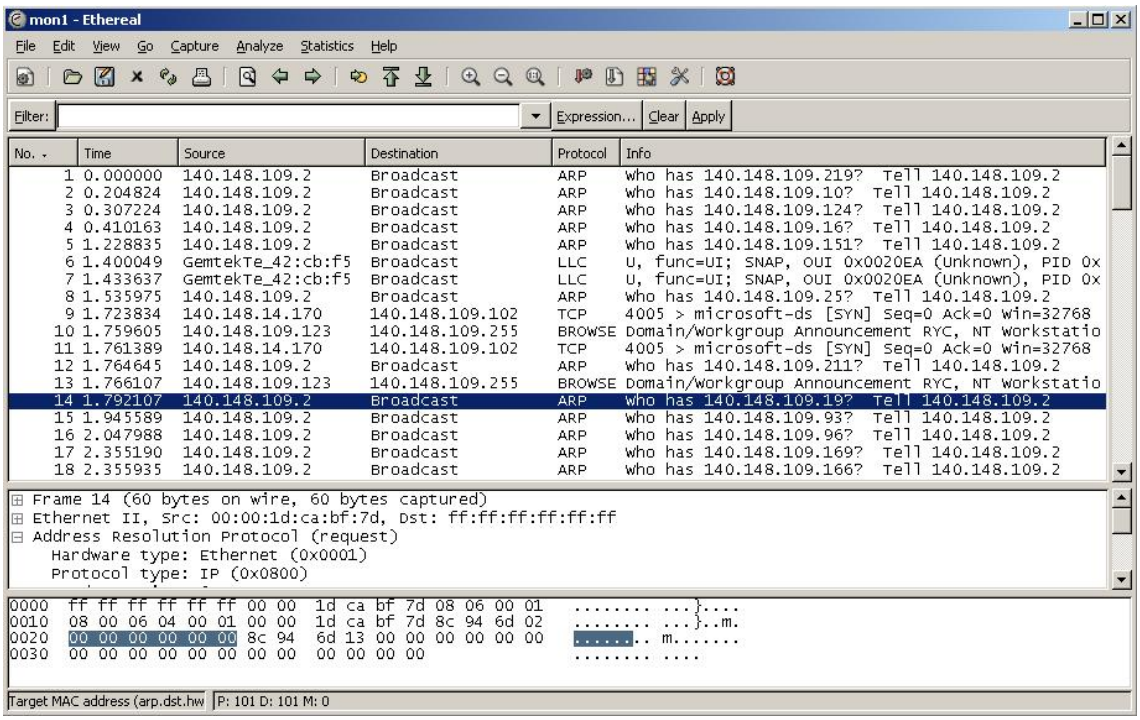

Figura 7. Trama de Ethereal. [ETHE]

En la Figura 8 podemos observar otro de nuestros programas a ocupar, en el cual la primera trama se auto ajusta a manera de que siempre se mostrará la primera MAC que halla sido captada, sin importar si pierde su señal, también de una manera clara observamos que tiene

colores, los cuales nos hacen notar el nivel de intensidad de la señal, esto quiere decir que entre mas cerca se encuentre uno del AP estará de color verde y viceversa si uno se aleja va decolorando a amarillo y después rojo, hasta llegar a un punto oscuro el cual significa falta de señal, algo que es de notar es que el programa nos da la MAC *address* del Punto de Acceso, desde aquí podemos observar que nos deja ver de una manera en como el dispositivo se conecta al Punto de Acceso, también nos da el nombre del SSID (*Service Set Identifier*) el cual es el nombre que se le asigna al Punto de Acceso, también nos da a conocer el canal que esta usando, la marca del dispositivo que hace la función del Punto de Acceso, los decibeles que captó en su ultimo muestreo, y en algunos casos su subred, así como también la velocidad.

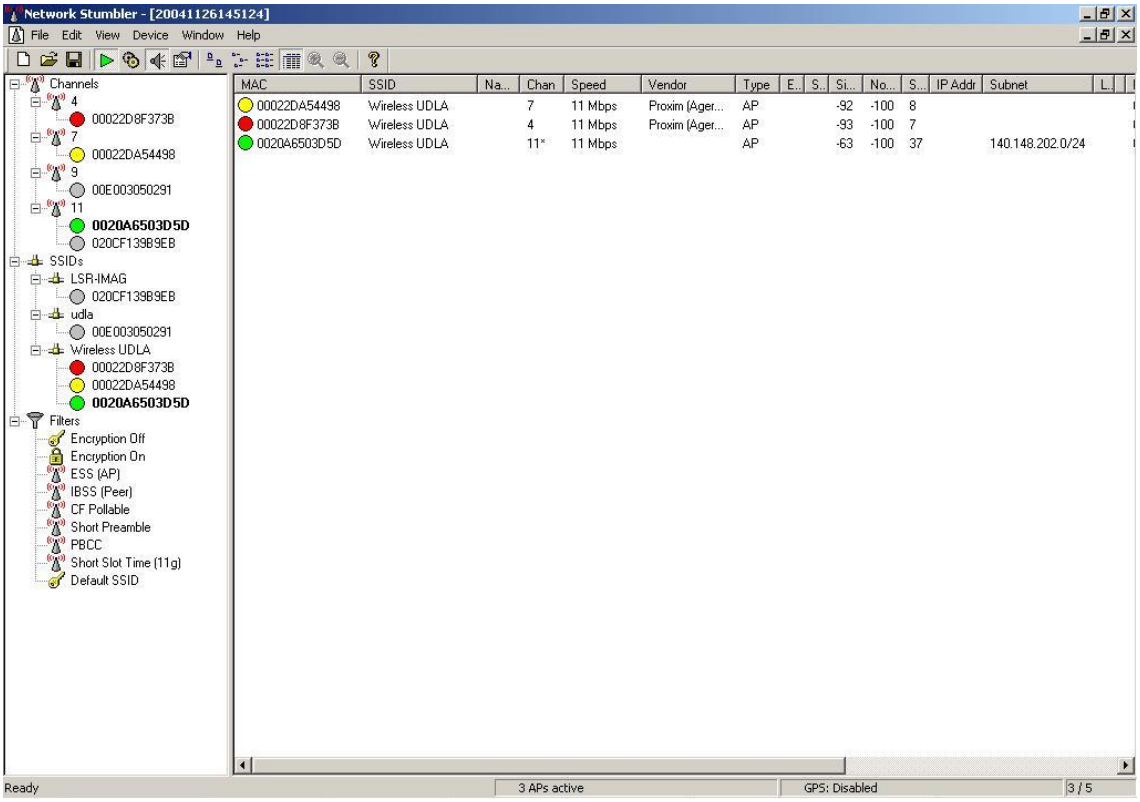

Figura 8. Tramas del Network Stumbler. [NETSTB]

En la Figura 9 podemos observar el programa Omni Peek el cual tiene las mismas funciones que el programa Ethereal, aunque este nos lo muestra de manera mas fácil y clara todos los datos que el programa Ethereal nos proporciona, pero teniendo un orden, y delimitando con colores las especificaciones para poder tener un entendimiento mas claro de lo que se analiza, así como el Ethereal nos deja ver el código en bits, que se observa en la parte baja del programa, es decir, descifra el código de transmisión, nos simplifica y nos expresa de una manera más clara el funcionamiento de la red, el único inconveniente es que no es *freeware* (Software libre).

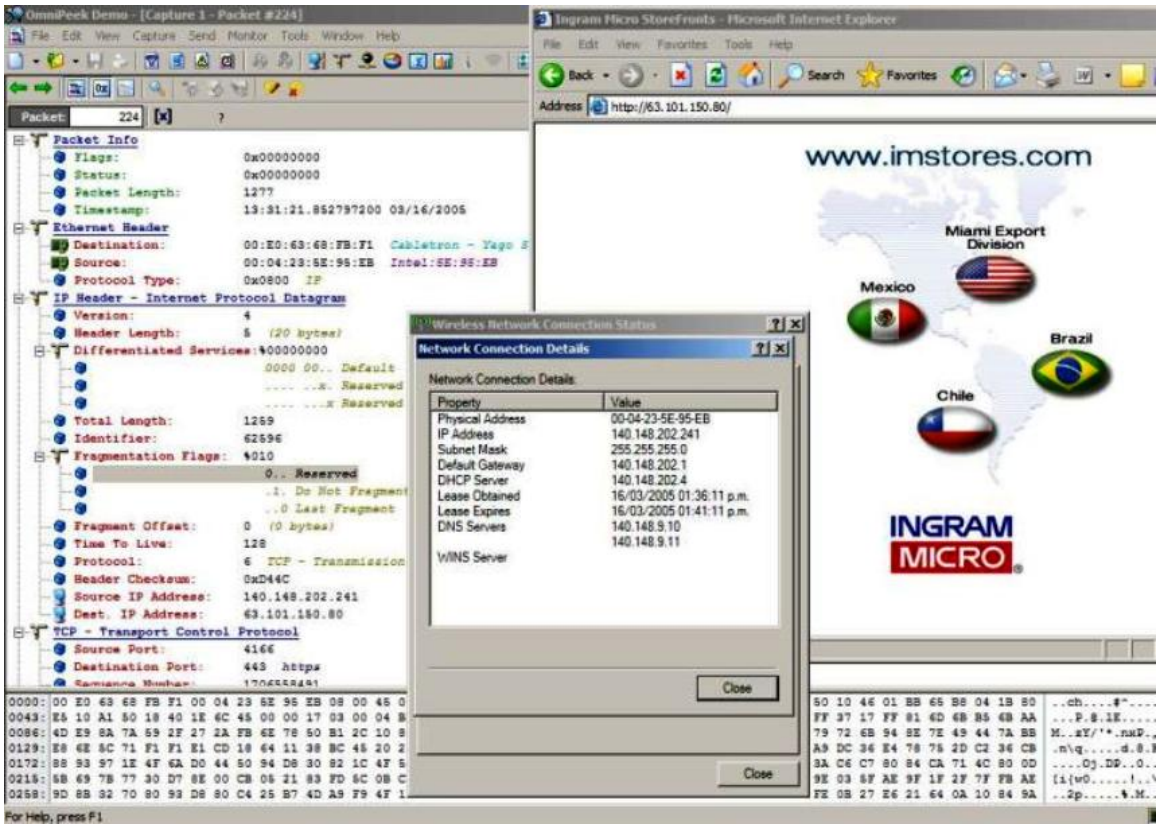

Figura 9. Tramas del programa Omni peek. [OPEEK]

2.9 Técnicas de Acceso.

¿Cómo detecta un cliente que hay un Punto de Acceso disponible? Los Puntos de Acceso transmiten tramas de guía cada cierto intervalo de tiempo fijo. Para asociarse con un Punto de Acceso y unirse a una red, un cliente escucha en busca de tramas de seguimiento para identificar el Punto de Acceso.

El cliente también puede enviar una trama de petición de prueba (*prove request*) que contenga un ESSID determinado para ver si le responde un Punto de Acceso que tenga el mismo ESSID. [SEGSECO]

2.9.1 Métodos de autenticación:

Open System Authentication

Es un protocolo de autenticación por defecto para 802.11b. Es un proceso de autenticación nulo, es decir, que autentica a cualquier cliente que pide ser autenticado. Las tramas se mandan en texto plano aunque esté activado el cifrado WEP. La estación que quiere autenticarse (cliente), envía una trama de petición de autentificación indicando que quiere utilizar una “clave compartida”. [INSEG]

Shared Key Authentication

El destinatario (Punto de Acceso) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente. El desafío se genera con la clave compartida y un vector de inicialización (IV) aleatorio utilizando el PRNG (Generador lineal). Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el *payload* (carga útil) de una nueva trama que encripta con WEP utilizando la *passphrase* y añade un nuevo IV (Vector de Inicio) elegido por el cliente. Una vez construida esta nueva trama encriptada, el cliente la envía al Punto de Acceso. El Punto de Acceso desencripta la trama recibida y comprueba que el ICV (*Integrity Check Value*) sea válido. El texto de desafío concuerde con el enviado en el primer mensaje. Si la comprobación es correcta se produce la autenticación del cliente con el Punto de Acceso. Se vuelve a repetir el proceso pero esta vez el primero que manda la trama con la petición de autentificación es el Punto de Acceso, de esta manera se asegura una autentificación mutua. [KERNE]

2.10 Simbología

Para podernos dar una idea de cómo es la simbología de redes inalámbricas tendremos que remontarnos un poco en la historia donde hace 70 años, durante la gran depresión que tuvo lugar en EEUU, se crearon una serie de símbolos que escritos cerca de determinados lugares, daban información de la proximidad de sitios donde se podía conseguir algo de comida. Los tiempos han cambiado, y ahora en Londres han retomado el escribir esos símbolos por la calle para avisar de la existencia de una conexión inalámbrica a Internet que sea decente. De esta manera se presenta el *Weblog warchalking* donde en la Figura 10

se muestra la manera simplificada de encontrar una red y en la Figura 11 observamos la manera mas compleja donde podemos obtener datos como las velocidades de conexión y el tipo de protocolo que se ocupa en esa red, sin olvidar si es libre o es cerrada. La cuestión es ir marcando con símbolos descriptivos la existencia de redes inalámbricas. [MAD04]

Figura 10. Diagramas de Acceso a redes inalámbricas simples. [MAD04]

Figura 11. Diagramas de Acceso WLAN complejos [MAD04]

En la Figura 12 podemos observar como funciona el *warchalking* (monitoreo caminando) y la manera en que se debería de mostrar al publico transeúnte, para poder conocer la red que se encuentra en ese lugar preciso.

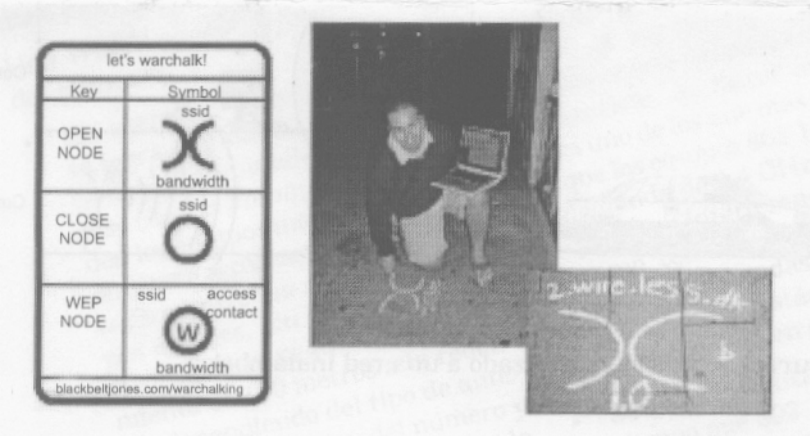

Figura 12. *Warchalking* en lugares públicos.[MAD04]

2.11 Consideraciones de diseño

Como paso previo a la aplicación de medidas de protección de una red inalámbrica, es importante diseñar la red de forma correcta. Algunas medidas básicas a implementar son:

- Establecer redes privadas virtuales (VPN), a nivel de *firewall,* para el cifrado del tráfico de la red inalámbrica.

- No deben conectarse directamente los Puntos de Acceso a la red interna alámbrica de la empresa. Las redes inalámbricas deben recibir el mismo trato que cualquier

otra red insegura, como puede ser la conexión a Internet. Por tanto, entre la red inalámbrica y la red alámbrica deberá existir un *firewall* y mecanismos de autentificación. [SEC02]

- Como ampliación del punto anterior, no deben colocarse los Puntos de Acceso detrás del *firewall*.

- Los clientes de las redes inalámbricas deben acceder a la red utilizando mecanismos tales como *Secure Shell* (SSH), redes privadas virtuales (VPN) o IPSec (*IP Security*). Estos mecanismos son los mínimos necesarios en lo referente a la a autorización, autenticación y cifrado del tráfico.