Editorial de la Universidad
Tecnológica Nacional

Estándar IEEE 802.11 X de las WLAN

Ing. Pablo Jara Werchau, Ing. Patricia Nazar

Departamento de Ingeniería en Sistemas de Información
Facultad Regional Tucumán
Universidad Tecnológica Nacional - U.T.N.

Editorial de la Universidad Tecnológica Nacional - edUTecNe

http://www.edutecne.utn.edu.ar

edutecne@rec.utn.edu.ar

Prólogo:

En el marco del Proyecto de investigación 25/P031 denominado "Efecto de la Foresta en las transmisiones electromagnéticas en una WLAN", durante el año 2009 el equipo de investigadores realizó búsquedas bibliográficas e investigaciones de campo respecto a los temas vinculados. Uno de los primeros objetivos fue desentrañar todo lo relativo a las WLAN, centrando la atención en el estándar 802.11 que es en el que nos basaremos.

De las investigaciones realizadas surge este artículo.

Introducción:

Una red inalámbrica es un sistema de comunicación de datos que proporciona conexión inalámbrica entre equipos situados dentro de la misma área (interior o exterior) de cobertura. En lugar de utilizar el par trenzado, el cable coaxial o la fibra óptica, utilizado en las redes LAN convencionales, las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas usando el aire como medio de transmisión.

Actualmente nos encontramos con los siguientes tipos de redes inalámbricas:

- WPAN (Wireless Personal Area Network - Red inalámbrica de ámbito personal). Estas redes están pensadas para cubrir un área del tamaño de una habitación. Tradicionalmente este tipo de redes fue basado en infrarrojos que permiten la comunicación entre dos elementos (ordenadores portátiles, PDAs, etc.) a baja velocidad y a una distancia cercana. Actualmente la tecnología de radio frecuencia denominada Bluetooth es el estándar en auge.
- WLAN (Wireless Local Area Network - Red inalámbrica de ámbito local). Son las redes que cubren el ámbito de una casa, una oficina o el edificio de una empresa.
- WWAN (Wireless Wide Area Network - Red inalámbrica de área extensa). Son las redes cuyo ámbito cubre áreas más amplias como por ejemplo: una ciudad. Por su gran tamaño, estas redes son explotadas por las empresas de telefonía móvil o ISPs (Internet Service Providers). Hasta la llegada de la telefonía móvil de tercera generación, el UMTS, la alternativa es el uso del GPRS, aunque su velocidad es bastante reducida.

Redes WLAN:

Una red de área local inalámbrica (WLAN) es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros. Permite que los nodos que se encuentran dentro del área de cobertura puedan conectarse entre sí. Existen varios tipos de tecnologías, entre ellas:

- IEEE 802.11 en sus variantes 802.11 a, b, g ofrecía hasta el año 2009 una velocidad máxima de 54 Mbps. A partir de octubre del 2009 con el advenimiento del estándar 802.11 n supera los 100 Mbps. El organismo internacional generador de estos estándares es el conocido como Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

- hiperLAN2 (High Performance Radio LAN 2.0), estándar europeo desarrollado por ETSI (European Telecommunications Standards Institute). HiperLAN 2 permite a los usuarios alcanzar una velocidad máxima de 54 Mbps en un área aproximada de cien metros, y transmite dentro del rango de frecuencias de 5150 y 5300 MHz.

ESTÁNDAR IEEE 802.11

Arquitectura del estándar 802.11

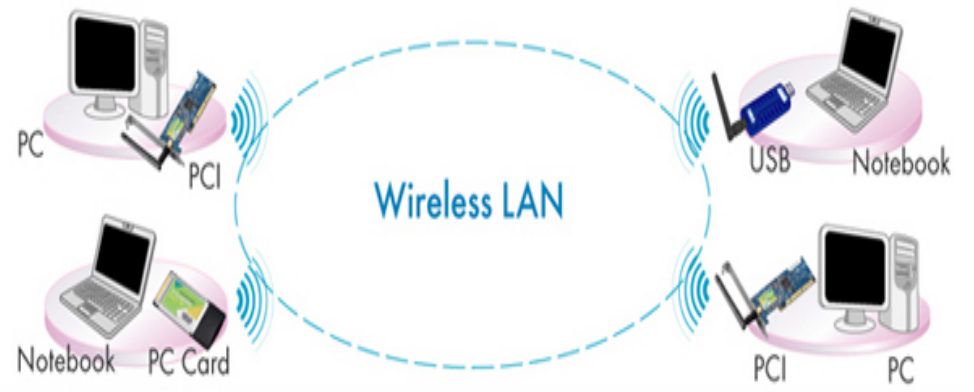
Las especificaciones del estándar definido por el IEEE denominado 802.11x (x comprende letras que definen las variantes de la norma 802.11 a, 802.11 b, 802.11 g, 802.11 n), abarcan las capas física (Capa 1) y la subcapa de acceso al medio (MAC) de la capa de enlace del modelo OSI.

Veamos algunos detalles que nos ayudarán a entender el funcionamiento y acotar los problemas con los que nos vamos a encontrar.

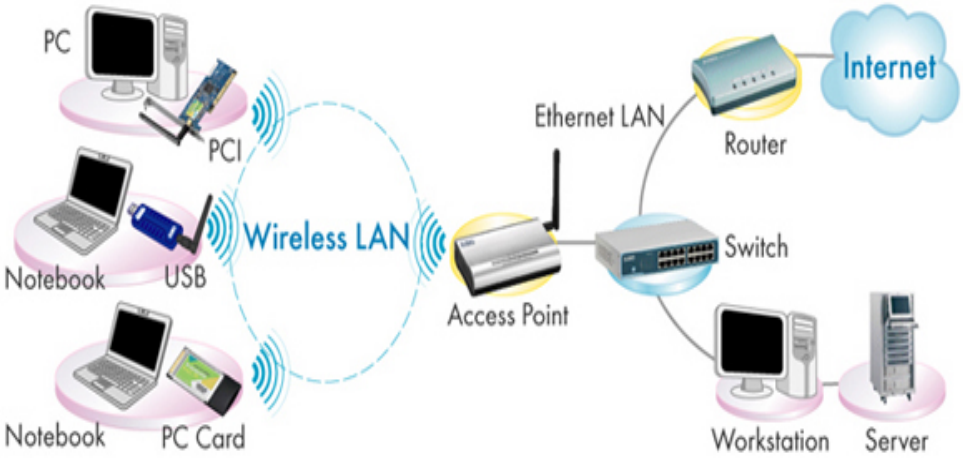
Topología de Red en 802.11

El estándar IEEE 802.11 define el concepto de Conjunto Básico de Servicio (BSS, Basic Service Set) que consiste en dos o más nodos inalámbricos o estaciones que se reconocen una a la otra y pueden transmitir información entre ellos.
Un BSS puede intercambiar información de dos modos diferentes:

1 – Cada nodo se comunica con el otro en forma directa y sin ninguna coordinación. Este modo es comúnmente llamado Ad-Hoc o IBSS (Independent Basic Service Set). Este modo solo permite la transmisión entre los nodos inalámbricos y no resuelve el problema de extender una LAN cableada.



2 – Existe un elemento llamado comúnmente AP (Access Point) que coordina la transmisión entre los nodos inalámbricos. Este modo es llamado modo Infraestructura y permite vincular la red inalámbrica con la red cableada ya que el AP actúa como bridge entre las dos redes. La existencia de varios AP conectados a un sistema de distribución (DS: Distribution System), que puede ser una LAN cableada es lo que denominamos EBSS (Extended Basic Service Set). La tecnología 802.11 permite el roaming entre los distintos AP.



Itinerancia (roaming)

La itinerancia es el proceso o capacidad de un cliente inalámbrico de moverse de una célula o BSS a otra sin perder la conectividad de la red. Los AP pasan el cliente de una a otro, siendo esto invisible para el usuario. El estándar no define como debe llevarse a cabo la itinerancia, pero si define los bloques constructivos básicos, que incluyen el escaneado activo y pasivo y el proceso de reasociación.

Servicios soportados por el sistema de distribución (DS)

Si bien el DS no es parte de la norma 802.11, la misma especifica los servicios que este sistema debe soportar, los cuales son:

1 – Servicios de Estación (SS: Station Services)

a) Autenticación: antes de que un nodo pueda unirse a la red, debe establecer su identidad, para ello debe superar una serie de tests que permitan saber que quien se quiere conectar es quien dice ser. 802.11 ofrece 2 tipos de servicios de autenticación:
    i. Autenticación Abierta (Open System Authentication), significa que cualquiera que solicite autenticarse será aceptado.
    ii. Autenticación de llave compartida (Shared Key Authentication), significa que para poder autenticarse en la red, el nodo debe conocer la frase de paso.
b) Deautenticación: ocurre cuando el AP o el nodo inalámbrico desea terminar la autenticación. Implica una desasociación.
c) Privacidad: está satisfecha en 802.11 con un sistema de encriptación llamado WEP (Wired Equivalent Privacy). Es opcional.
d) Transporte de unidad de Servicios de capa MAC (MSDU: MAC Service Data Unit Delivery): se ocupa de que la información necesaria para operación de la subcapa MAC sea transportada entre los distintos AP.

2 – Servicios provistos por el Sistema de Distribución DS

a) Asociación: un nodo inalámbrico debe estar asociado a un AP para poder hacer uso de la red. Solo puede estar asociado a un AP por vez, así el DS sabe perfectamente en que AP se encuentra el nodo. Es iniciado por el nodo.
b) Reasociación: este servicio permite que un nodo deje la asociación de un AP para pasar a asociarse a otro AP. Es también iniciado por el nodo.
c) Desasociación: el servicio que permite a cualquiera de las partes (AP o nodo) terminar la asociación.

d) Distribución: es el servicio por el cual se llevan los datos desde el origen al destino. Los datos son enviados al AP local, de ahí a través del DS al AP remoto (donde está asociado el nodo destino) y este lo pasa al nodo destino directamente. El servicio de distribución se invoca inclusive si ambos nodos están asociados al mismo AP.
e) Integración: es el servicio que permite integrar el sistema inalámbrico a otra red, por ejemplo una LAN cableada, realizando las conversiones de protocolo necesarias.

La capa Física en 802.11

La capa física de la especificación IEEE 802.11 ofrece dos tipos de técnicas para las transmisiones en frecuencias de radio y una especificación para transmisiones infrarrojas.
Las técnicas de radio frecuencia trabajan basadas en el concepto de "Espectro Ensanchado" o Spread Spectrum (SS). Este concepto se basa en un ensanchamiento forzado del espectro de ancho de banda usando una función XOR con una secuencia Numérica Pseudorandómica larga, esto disminuye la densidad de potencia espectral y reduce la potencia de pico. La potencia total transmitida no varía pero la señal se hace mucho mas inmune a las interferencias y al ruido ambiente.

Las dos técnicas previstas en la norma 802.11 son:

i. Salto de Frecuencia (Frecuency Hoping Spread Spectrum, FHSS)
Es la forma más simple de modulación de espectro ensanchado, normalmente la mayoría de los sistemas de salto de frecuencia definen un conjunto de saltos uniformes dentro de una banda de frecuencia aunque esto no es absolutamente necesario ya que ambos extremos de la transmisión conocen de antemano el patrón de salto de frecuencias utilizado. Esta técnica consigue una alta inmunidad a las interferencias y al ruido ambiente, sobre todo cuando usa patrones aleatorios de salto de frecuencia. La desventaja de esta técnica es que solo se ha desarrollado en el mercado para velocidades que no superan los 2 Mbps. Existen 75 subcanales de 1 MHz que permiten definir secuencias de saltos que no se solapan entre si.

ii. Secuencia Directa (Direct Secuence Spread Spectrum, DSSS)
En la técnica de secuencia directa se usa un código de pseudo-ruido generado localmente para codificar la señal digital a transmitir. Este código

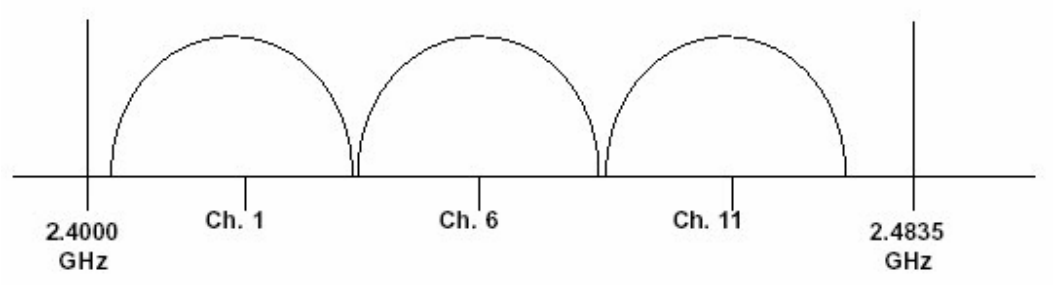
se ejecuta a frecuencias varias veces más altas que la frecuencia de la señal. Si ejecutamos una función EXOR con la señal, obtenemos una señal codificada que luego será modulada usando BPSK (Binary Phase Shift Key) antes de ser transmitida.
Esta señal, al ser recibida en el otro extremo, es decodificada usando una réplica local del código de pseudo-ruido usado en el emisor. De este modo, el receptor solo decodificará la señal que esté codificada con un código determinado, resultando en un filtro natural para las interferencias y señales espurias.

Las técnicas no son interoperables entre si.

En cualquiera de los dos casos, las señales de Espectro Ensanchado (SS) se convierten en señales que tienen una baja probabilidad de interferencia con señales de espectro estrecho debido a que la energía es desparramada en un ancho de banda que puede ser 100 veces el ancho de banda de la señal a transmitir.

Este tipo de modulación es exigida por la FCC de los EEUU y por la mayoría de los entes regulatorios de los países para utilizar las bandas de frecuencias libres llamadas ISM (Industrial, Scientific and Medical) que operan entre los 2.400 GHz y los 2.483 GHz y también entre los 5.725 y los 5.875 GHz.

Para lograr velocidades de 1, 2, 5.5 y 11 Mbps, es necesario un AB de alrededor de 20 MHz por canal por lo que se debe entender que la norma 802.11 tiene solamente 3 canales no solapados en la banda ISM de 2.4 GHz



En los sistemas de secuencia directa (DS), es necesario compensar el ruido que se introduce en cada canal debido a su ancho de banda, para ello cada bit de datos se convierte en una serie de patrones de bits redundantes llamados “chips”. La redundancia que presenta cada chip combinada con el ensanchamiento de la señal a través de los 20 MHz provee un mecanismo solido de detección y corrección de errores, minimizando las retransmisiones.

La capa de Enlace en 802.11

La capa de enlace de datos en 802.11 consiste en dos subcapas:

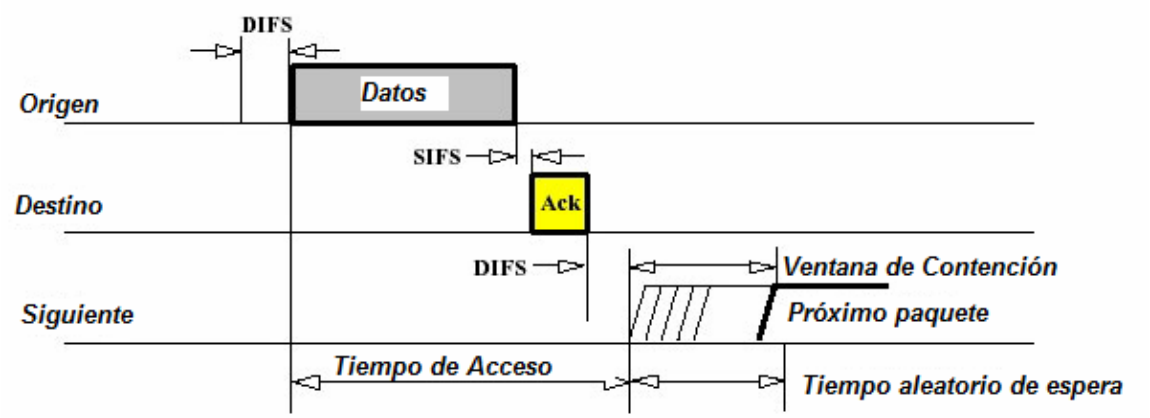
1. Capa de Control lógico de Enlace, o Logical Link Control (LLC)
2. Capa de Control de Acceso al Medio o Media Access Control (MAC) o capa de Acceso Múltiple.

1. La subcapa de Control Lógico de Enlace (capa LLC)

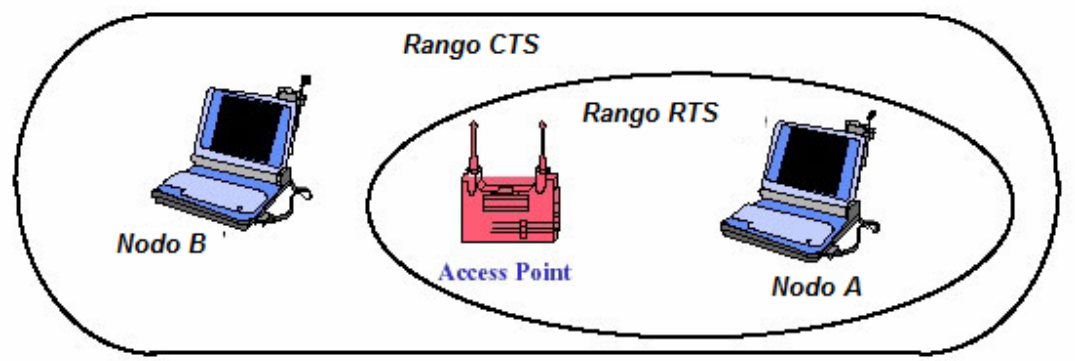
Esta capa es exactamente igual a la capa LLC utilizada por las redes cableadas del tipo 802.3 con un sistema de direccionamiento de 48 bits idéntico (MAC Address). Esto permite simplificar al extremo los puentes (bridges) entre los dos tipos de red.

2.- La subcapa de Acceso Múltiple en 802.11 (capa MAC)

El método de acceso múltiple en IEEE 802.11 es la llamada Función de Distribución Coordinada (Distributed Cordination Function, DCF) que utiliza el conocido método de Acceso Múltiple por Censado de Portadora con Prevención de Colisiones, (Carrier Sense Multiple Access / Collision Avoidance, CSMA/CA). Este método requiere que cada nodo inalámbrico escuche el medio compartido para saber si otros nodos se encuentran transmitiendo. Si el canal está desocupado, el nodo puede transmitir, caso contrario, el nodo escucha hasta que la transmisión finalice, y entra en un período de espera aleatorio para luego volver a ejecutar el procedimiento. Esto previene que algunas estaciones monopolicen el canal al comenzar a transmitir inmediatamente después que termine la otra.
La recepción de los paquetes en el DCF requiere de confirmaciones por parte del destino. Hay un corto período de tiempo entre el envío del ACK por parte del destinatario llamado Short Inter Frame Space, SIFS. En 802.11, los paquetes de confirmación ACK tiene prioridad frente a cualquier otro tráfico, logrando una de las características sobresalientes que es la gran velocidad de las confirmaciones.
Cualquier transmisión distinta a un ACK deberá esperar por lo menos un DIFS (DCF Inter Frame Space) antes de transmitir algún dato. Si el transmisor detecta un medio ocupado nuevamente, vuelve al tiempo de BackOff pero reduciendo el tiempo de espera. Asi se repetirá hasta que el tiempo de espera llegue a CERO donde se habilita al nodo a transmitir, luego de que termine la próxima transmisión.



Este método es similar al utilizado en el protocolo Ethernet 802.3 y supone que todos los nodos escuchan simultáneamente el canal.
Esto no es siempre cierto en un canal inalámbrico, donde se puede dar el caso del Nodo oculto. Veamos el siguiente caso, los nodos A y B están dentro del rango del Access Point pero el Nodo B no sabe que existe el Nodo A porque está fuera de su rango y por lo tanto no puede saber si está transmitiendo o no.



Esto se resuelve usando un segundo método de sensado de portadora llamado Sensado Virtual de Portadora (Virtual Carrier Sense) que habilita a un nodo a reservar el canal por un determinado período de tiempo usando tramas RTS/CTS. En el ejemplo de arriba, El Nodo A envía un RTS (Request To Send) al Access Point. Este RTS, tiene un campo que especifica el tiempo que solicita la reserva y no es escuchado por el Nodo B porque esta fuera del alcance. La información de la reserva es almacenada por los restantes nodos dentro del alcance de A en una base llamada Network Allocation Vector (NAV). El AP responde con un CTS que contiene el tiempo asignado para la reserva. El nodo B que recibe el CTS del AP actualiza su tabla NAV de acuerdo a la info suministrada, resolviendo así el problema del nodo oculto.

Las tramas (frames) del estándar IEEE 802.11

Para analizar el funcionamiento de una WLAN basada en 802.11 usando un analizador de paquetes, debemos comprender los distintos tipos de paquetes que circulan y cual es su función específica.

En forma general, podemos decir que el estándar 802.11 define una serie paquetes que son usados por los nodos y los AP para establecer la comunicación entre ellos y mantener el link entre ellos.

Cada trama tiene un campo de control que define la versión del protocolo 802.11, *el tipo de trama* y algunos indicadores más. Cada trama tiene también la dirección MAC del origen y del destino, el número de secuencia de la trama y una secuencia de redundancia para detección de errores.

Tramas de Manejo de Conexión

Permiten a los nodos establecer y mantener la comunicación entre ellos. Podemos encontrar los siguientes subtipos:

1. Tramas de Autenticación: como ya dijimos, la autenticación es el proceso por el cual un Access Point acepta o rechaza la identidad de un nodo que pretende conectarse con el. El nodo inicia el procedimiento enviando una trama de autenticación, si la autenticación es Abierta, el AP simplemente contesta con una trama de respuesta afirmativa o negativa. Si el AP tiene definido el tipo opcional de Autenticación por frase de paso compartida (Shared Key Authtentication), el AP responde con una trama de respuesta conteniendo una frase de texto. El nodo deberá ahora enviar una versión encriptada de la palabra de paso usando su clave WEP para encriptar. El AP se asegura que el nodo tiene la clave WEP correcta desencriptando y comparando la frase de texto con la que envió previamente. Una vez validada la identidad del nodo, el AP envía una trama de respuesta afirmativa al nodo.
2. Tramas de Desautenticación: es una trama enviada por un nodo a otro nodo para terminar la conexión segura entre ellos.
3. Tramas de solicitud de asociación: la asociación en 802.11 habilita a un AP a disponer de recursos para establecer una conexión con un nodo estación. El nodo estación comienza la solicitud de asociación enviando una trama de este tipo. Esta trama contiene información sobre el nodo estación como las velocidades soportadas y el SSID al cual desea asociarse. El AP evalúa el requerimiento del nodo y si decide aceptar reserva un espacio de memoria para permitir el intercambio de datos y establece un número de asociación (Association ID) para el nodo.
4. Trama de respuesta de Asociación: es la trama con el que el AP responde a una solicitud de asociación del tipo 3. La trama contiene información

relativa a la asociación en cuestión como el Association ID, las velocidades aceptadas, etc.

5. Tramas de Reasociación: las tramas de solicitud de reasociación se envían cuando un nodo se mueve y encuentra otro AP con mayor señal (Beacon Signal) que el actual al que está asociado. El nuevo AP al recibir esta señal coordina a través del DS (Red cableada probablemente) el envío de los paquetes que pudieran estar pendientes en el viejo AP para transmitirlos al nodo y luego envía una trama de respuesta de reasociación con los nuevos datos de Association ID y las velocidades aceptadas.
6. Trama de desasociación: es una trama que suele enviar un nodo estación cuando desea cancelar la asociación en forma ordenada. Esta trama instruye al AP para que libere la memoria y el Association ID relacionado a este nodo.
7. Trama de balizamiento (beacon): es una trama que el AP envía periódicamente para anunciar su presencia y recabar información tales como el SSID y otros parámetros que le indican al AP si los nodos siguen a su alcance. Los nodos estación permanentemente escanean los canales de radio escuchando los beacons para establecer a cual AP conviene asociarse.
8. Tramas de prueba: las tramas de requerimiento de prueba son los que envían los nodos estación para saber que otras radios están al alcance. Al recibirlos, el otro extremo responde con una trama de respuesta a la prueba conteniendo capacidades, velocidades soportadas, etc.

Tramas de Control

Son tramas que dan asistencia a la transferencia entre estaciones inalámbricas

1. Tramas RTS: implementan la función RTS para salvaguardar la presencia de nodos ocultos.
2. Tramas CTS: implementan la función CTS para salvaguardar la presencia de nodos ocultos
3. Trama ACK: implementan la función de confirmación de recepción de tramas de datos sin error.

Tramas de Datos

Son las tramas que transportan la información entre los nodos y los AP.

Bibliografía:

Fundamentos de Redes Inalámbricas, Cisco Networking Academy Program, Cisco Systems, Cisco Press, 2006

Recursos WEB:

Tutorial 802.11 MAC Layer Defined
By Jim Geier
http://www.wi-fiplanet.com/tutorials/article.php/1216351

Tutorial Understanding 802.11 Frame Types
By Jim Geier
http://www.wi-fiplanet.com/tutorials/article.php/1447501

Wikipedia: IEEE 802.11
http://es.wikipedia.org/wiki/IEEE_802.11

A Technical Tutorial on IEEE 802.11 Standard
BreezeCom Wireless Comunications
http://sss-mag.com/pdf/802_11tut.pdf

Wireless LAN (Wifi) Tutorial
Tutorial-Reports.com
http://www.tutorial-reports.com/wireless/wlanwifi/index.php?PHPSESSID=f363004d5d4ea4638c805f7f71e3bd6f