UNIVERSIDAD NACIONAL AUTÓNOMA

DE MÉXICO

FACULTAD DE INGENIERÍA

ESTUDIO DEL COMPORTAMIENTO DEL ESTÁNDAR DE COMUNICACIONES IEEE 802.11 N

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN TELECOMUNICACIONES

PRESENTA:

JESÚS ALEJANDRO FLORES RAMIREZ

DIRECTOR DE TESIS:

DR. JAVIER GÓMEZ CASTELLANOS

CD. UNIVERSITARIA, MÉXICO, D.F. JUNIO 2009

DEDICATORIAS

A mis padres Salvador y Amelia,
por ser mis amigos, mis maestros, por apoyarme siempre
y por darme la vida.

A mis hermanos Salvador, Bibiana, Gabriela, Lorena y Mayra,
por sus consejos y por todo su cariño.

A Alejandra,
por impulsarme a alcanzar mis metas y por estar
a mi lado en todo momento.

A todos mis amigos,
por su paciencia y por brindarme su ayuda
incondicionalmente.

AGRADECIMIENTOS

Al Dr. Javier Gómez,
porque sin su ayuda esta tesis
no existiría.

Al Dr. Víctor García, Dr. Miguel Moctezuma,
M.I. Juventino Cuellar y M.I. Federico Vargas,
por brindarme sus conocimientos y su apoyo.

A la UNAM y a la Facultad de Ingeniería,
por la educación que recibí en sus aulas de clase.

Jesús Alejandro

Índice General

1. Introducción

Desde siempre ha existido la necesidad de comunicación entre las personas y esto se refleja en un aumento por transmitir información en el menor tiempo posible.

A través de los años se han inventado dispositivos para transmitir mayores cantidades de información en un menor tiempo; con el avance de la tecnología éstos han logrado disminuir su tamaño, peso y adecuar su forma, lo que les permite ser cómodos y transportarles con facilidad.

Las personas no siempre tienen acceso al lugar físico para poder conectarse a la red, ya sea porque las características del terreno no lo permiten o porque no cuentan con ese privilegio. Aún si tienen acceso al lugar, la libertad de movimiento del dispositivo para transmitir información es prácticamente nula por el cableado o muy dificultosa por comodidad, por lo que se ven obligadas a permanecer en un solo lugar.

Para contrarrestar lo anterior, el estándar de comunicaciones IEEE 802.11 define las características de una Red de Área Local Inalámbrica (WLAN), teniendo una cobertura desde unas decenas hasta cientos de metros, utilizando para ello las bandas de frecuencia de uso libre del espectro radioeléctrico (2.4 GHz y 5 GHz).

Muchos usuarios de redes inalámbricas trabajan perfectamente con el estándar de comunicaciones IEEE 802.11 G, que es la versión más popular del estándar y no utilizan la nueva versión IEEE 802.11 N, que aunque brinda una mayor tasa de transmisión y una mayor cobertura que la anterior, ellos prefieren esperarse a que se perfeccione su funcionamiento y disminuyan los costos de los dispositivos que la soportan. Sin embargo, para lograr esto es necesario que exista una mayor demanda de los dispositivos por parte los usuarios.

1.1. Objetivos y metas

Evaluar y analizar el comportamiento y las características del protocolo de comunicaciones inalámbricas IEEE 802.11 N, basándose en pruebas de comunicación entre dispositivos que lo soportan.

1.2. Redes Inalámbricas

1.2.1. Definición de una red inalámbrica

Una red inalámbrica es un conjunto de dispositivos que intercambian información utilizando ondas electromagnéticas y que usan como medio o canal de transmisión al aire. Las ondas electromagnéticas pueden ser ondas de radio (30Hz a 3GHz), las microondas (300MHz a 300GHz) y las infrarrojas (300 GHz a 384 THz) [6].

Las señales electromagnéticas utilizadas en las redes inalámbricas, al ser generadas por equipo electrónico se ven afectadas por el ruido térmico, el cual es generado por el paso de corriente a través de los elementos conductores de los circuitos provocando calor. Para estas mismas señales se emplean diferentes tipos de modulación dependiendo de la distancia que deban recorrer, de esta manera, se reduce la pérdida de información, es decir, existe un comportamiento inversamente proporcional entre la distancia y el número de bits por símbolo de cada modulación.

Las aplicaciones de las redes inalámbricas se encuentran en la navegación, la radiodifusión AM y FM, telefonía inalámbrica, telefonía celular, televisión satelital, Bluetooth y Zigbee.

1.2.2. Tipos de redes inalámbricas

Red de Área Personal Inalámbrica (WPAN)

Esta es una red inalámbrica de corto alcance, su radio de cobertura es hasta 10 metros. Consiste de una serie de dispositivos conectados a la red que se encuentran dentro del espacio personal de un individuo como laptops,

auriculares para teléfonos celulares, periféricos inalámbricos, teléfonos inalámbricos o un Asistente Digital Personal (PDA). Las tecnologías en WPAN son el Bluetooth y Home RF [1].

Red de Área Local Inalámbrica (WLAN)

Es una red inalámbrica de área local cuya cobertura es de unos cientos de metros sobre un edificio, oficina o campus. Las tecnologías en WLAN son HiperLAN e IEEE 802.11 Wi-Fi.

Las terminales pertenecientes a una WLAN pueden comunicarse en modo ad hoc o mediante un Punto de Acceso (AP). Mediante el primer modo pueden presentarse colisiones de datos debido a los problemas de terminales ocultas y expuestas, lo que se puede resolver sensando y reservando el canal para la transmisión de la información (RTS/CTS). Mediante el segundo modo se evitan las colisiones, ya que se asignan los turnos de transmisión a las terminales y puede incrementarse la distancia de comunicación entre ellas, debido a que los AP retransmiten la información dentro de la red.

Red de Área Metropolitana Inalámbrica (WMAN)

Es una red inalámbrica que cubre una ciudad, es decir, ofrece cobertura en un radio de varios kilómetros. Una gran ventaja de este tipo de redes es que se puede comunicar a múltiples puntos que se encuentran distantes sin la necesidad de tener una línea de transmisión como un hilo de cobre o fibra óptica. Las tecnologías en WMAN son HiperMAN e IEEE 802.16 WiMAX.

Red de Sensores Inalámbrica (WSN)

Esta es una red de sensores (dispositivos ligeros con memoria, pila y sistema operativo) los cuales son desplegados en una región específica y con un propósito particular, por ejemplo: monitorear la humedad, temperatura, velocidad de un objeto, rastrear equipo médico en un hospital o detectar la intrusión de un individuo en un determinado lugar.

Los sensores operan en modo ad hoc y el senso se realiza de manera esporádica o periódica. Las tecnologías en WSN son Zigbee y la Identificación por Radio Frecuencia (RFID) [1].

Red de Área Extensa Inalámbrica (WWAN)

Estas redes ofrecen la mayor cobertura, su alcance es de algunas decenas de kilómetros. Este tipo de redes se diferencian de las WLAN porque usan tecnologías de redes celulares y se comunican mediante antenas o sistemas satelitales [11].

Las tecnologías en WWAN son el Sistema Global para las Comunicaciones Móviles (GSM), el Servicio General de Paquetes vía Radio (GPRS), el Sistema Universal de Telecomunicaciones Móviles (UMTS) y las tasas de Datos Mejoradas para la Evolución de GSM (EDGE).

Resumen del capítulo.

En la actualidad las redes inalámbricas son de gran utilidad porque brindan movilidad a las terminales. Su implementación es más rápida y de menor costo que una red cableada.

Existen diferentes tecnologías que han sido ampliamente aceptadas por los usuarios en cada tipo de red inalámbrica, son de uso común y permiten que las personas tengan comunicación en múltiples lugares.

El objeto de estudio de esta tesis es mostrar el comportamiento, ventajas y desventajas que tiene el protocolo de comunicaciones IEEE 802.11 N frente al estándar IEEE 802.11 G.

En los siguientes capítulos se muestran las características principales de la tecnología IEEE 802.11, las técnicas de seguridad en redes inalámbricas, la descripción del protocolo de comunicaciones IEEE 802.11 N y una serie de pruebas que permiten comparar a este protocolo con el estándar IEEE 802.11 G.

2. Protocolo de comunicaciones IEEE 802.11

2.1. Descripción

Es un estándar propuesto por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para las WLAN, el cual se enfoca en proporcionar movilidad y altas tasas de transmisión a los usuarios.

Para poder comunicarse las redes WLAN utilizan las bandas de frecuencia de 2.4 y 5 GHz de las bandas denominadas ISM. Este nombre proviene de las bandas de frecuencia utilizadas por dispositivos industriales, científicos y médicos.

Son tres las bandas ISM: 902 a 928 MHz, 2.4 a 2.4835 GHz y 5.725 a 5.850 GHz. No se requiere de una licencia para su uso [6].

Los dispositivos que usan estas bandas de frecuencia utilizan como máximo 1 watt de potencia con la finalidad de evitar interferencias entre ellos.

La primer parte del estándar IEEE 802.11 se dio a conocer en junio de 1997 y contiene las características a nivel capa Física y MAC. Dos partes adicionales se publicaron en 1999, posteriormente una en el 2002 y la última es del año 2007.

En la capa Física se maneja la luz infrarroja y el Espectro Disperso (SS), esto es, el esparcimiento de la potencia de la señal sobre una banda de frecuencias. Las técnicas de Espectro Disperso son por Secuencia Directa (DS) y por Salto de Frecuencias (FH), ambas técnicas operan en 2.4 GHz.

En el Espectro Disperso por Secuencia Directa (DSSS) el transmisor emplea la función XOR para multiplicar cada bit de información por una cadena o código de 11 chips, este código es enviado previamente al receptor para que pueda decodificar correctamente. Al llegar la secuencia al receptor mediante la función XOR la multiplica por el código de 11 chips y logra descifrar la información.

El estándar 802.11 maneja el siguiente código para los bits 1 y 0 respectivamente:

-1,+1,-1,-1,+1,-1,-1,-1,+1,+1,+1 y +1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1

A continuación se muestra un ejemplo al transmitir y recibir los bits de información 101 utilizando DSSS:

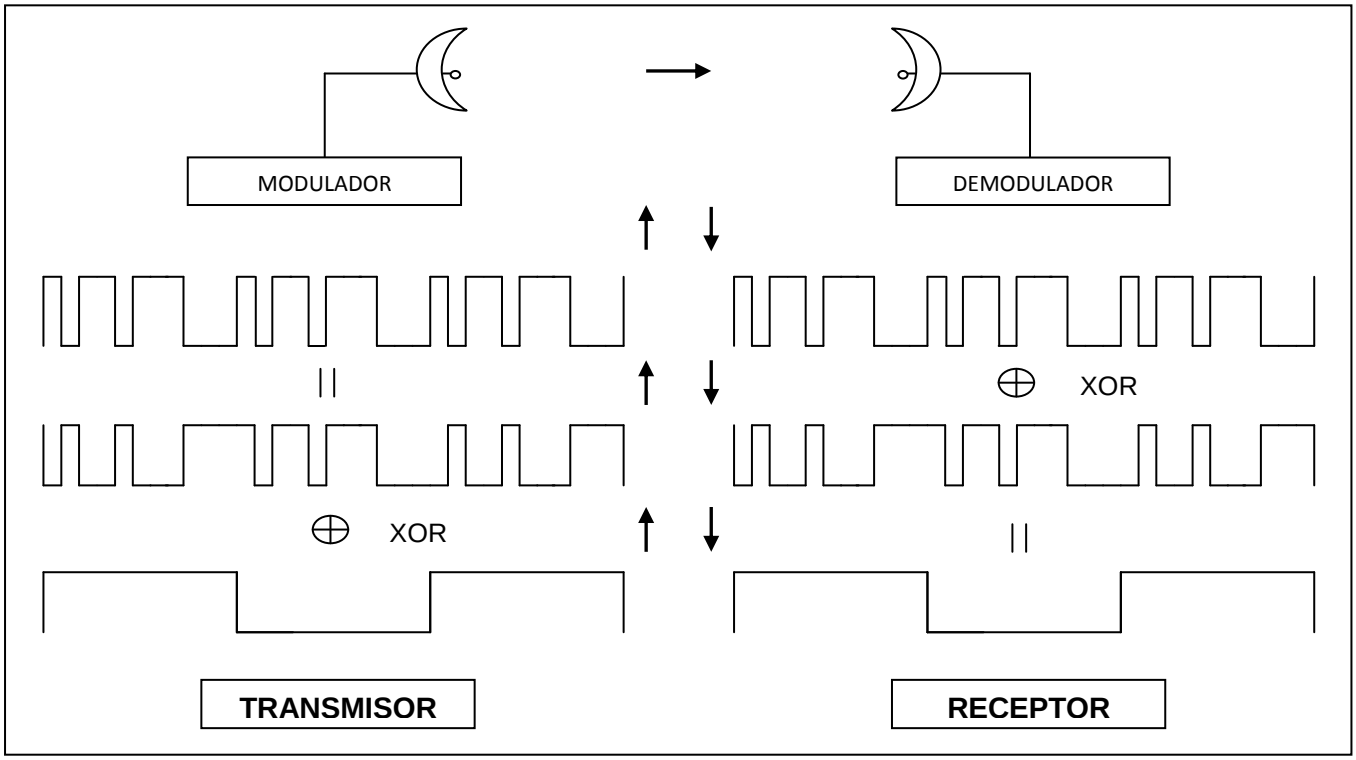


Figura 1.- Representación de la transmisión y recepción de los bits 101 utilizando DSSS.

En el Espectro Disperso por Salto de Frecuencias (FHSS) se hace que la portadora salte de frecuencia de acuerdo a una secuencia pseudoaleatoria, es decir, se transmite en una frecuencia durante un intervalo de tiempo (menor a 400 ms) y posteriormente se cambia de frecuencia.

La siguiente figura muestra el modo de operación del Espectro Disperso por Salto de Frecuencia:

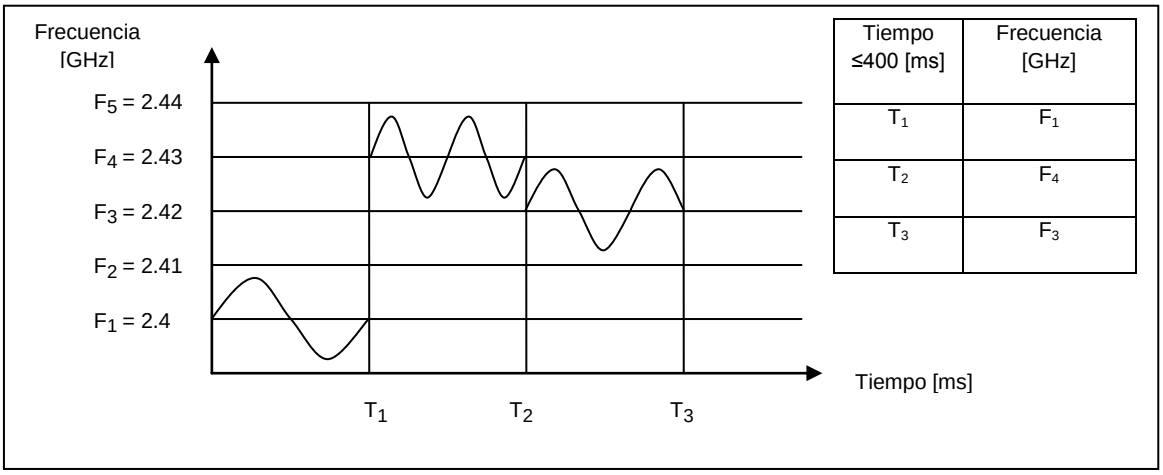


Figura 2.- Representación del Espectro Disperso por Salto de Frecuencia.

Las ventajas del Espectro Disperso son:

a) Resistencia a la intercepción, ya que alguna persona puede recibir fácilmente la señal pero al no poseer el código no puede decodificar el mensaje.

b) Resistencia a la interferencia. Cuando las señales llegan al receptor sin haber sido multiplicadas por el código de 11 chips son desechadas.

En la luz infrarroja (850 nm a 950 nm) no es necesaria la Línea de Vista (LOS) entre el transmisor y el receptor, ya que se utilizan las superficies del ambiente para reflejar la señal, lo que permite un radio de cobertura de hasta 20 metros. Sin embargo, para aumentar el rango de cobertura se recomienda tener una buena línea de vista, es por eso que las WLAN que usan luz infrarroja se suelen utilizar en recintos cerrados donde no haya muchos objetos que obstruyan el paso de la señal y sí muchas superficies reflectoras.

A fin de que el canal de comunicación sea utilizado por muchos usuarios de manera simultánea en una WLAN se usan el Acceso Múltiple por División de Código (CDMA) y el Multiplexaje por División de Frecuencias Ortogonales (OFDM), los cuales se explican a continuación.

- Acceso Múltiple por División de Código (CDMA)

Esta técnica ocupa el Espectro Disperso y es común que utilice el de Secuencia Directa. Cada terminal usa una secuencia diferente llamada código, la cual mediante la función XOR multiplica al mensaje original y hace que se expanda en frecuencia. Para que el receptor pueda decodificar correctamente la señal, es necesario que conozca el código que utilizó el transmisor [4].

Para evitar interferencias y una correcta decodificación se necesita que cada terminal transmita con un buen código, este debe seguir las siguientes dos reglas:

1. Debe ser ortogonal a los otros códigos, es decir, el producto punto entre códigos debe ser cero.

$$C_m \cdot C_n = 0$$

2. Debe parecer aleatorio, es decir, debe evitar repeticiones adyacentes de un mismo digito dentro del código.

En esta técnica de acceso múltiple las terminales usan la totalidad del espectro disponible durante todo el tiempo gracias a la ortogonalidad de los códigos [7].

Abajo se muestra la representación de esta técnica.

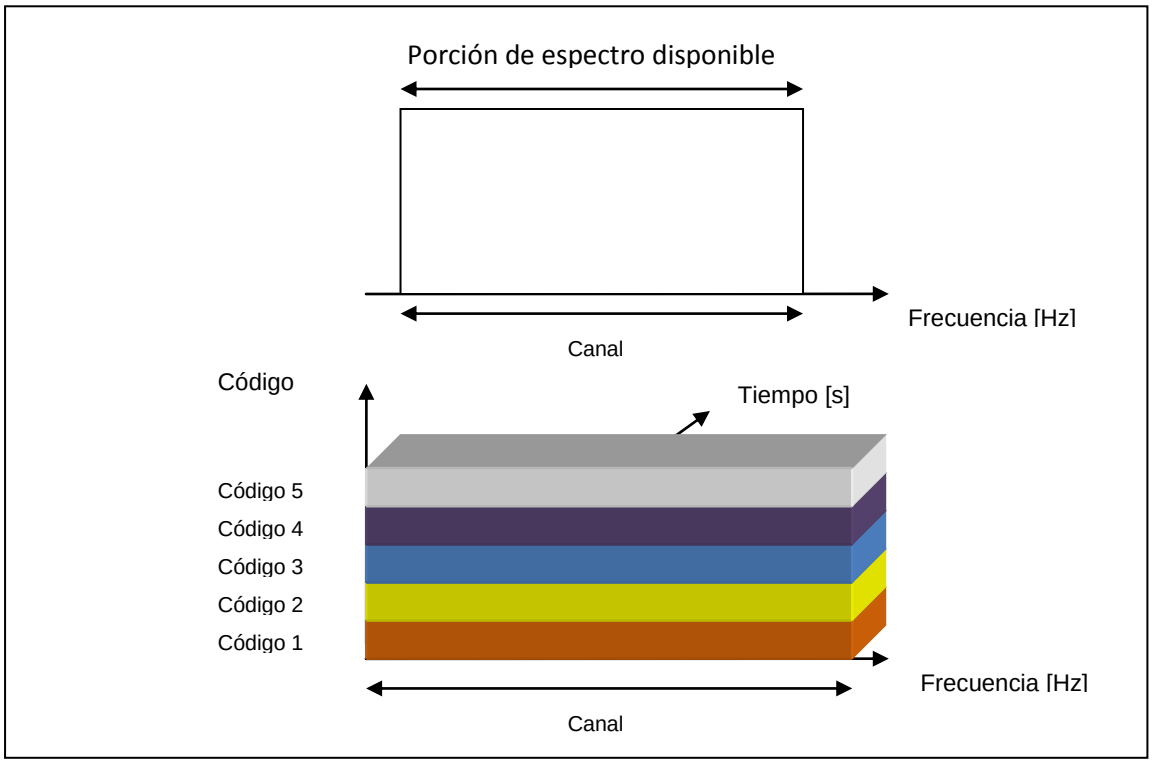


Figura 3.- Esquema del Acceso Múltiple por División de Código.

- Multiplexación por División de Frecuencias Ortogonales (OFDM)

Esta es una técnica que divide la porción del espectro disponible en un conjunto de portadoras o canales. A diferencia de FDM no necesita de bandas de guarda entre portadoras y éstas se pueden traslapar ya que son ortogonales, es decir, la frecuencia central de cada portadora coincide con los nulos de las otras portadoras, por esta razón no hay interferencia en el punto central de la portadora y se tiene un mejor aprovechamiento del espectro.

Cada una de las terminales transmite su información segmentada a través de un conjunto de portadoras o canales y la cantidad de portadoras que se le asignan es proporcional a la cantidad de información que envía [3].

A continuación se ilustra esta técnica de acceso al medio.

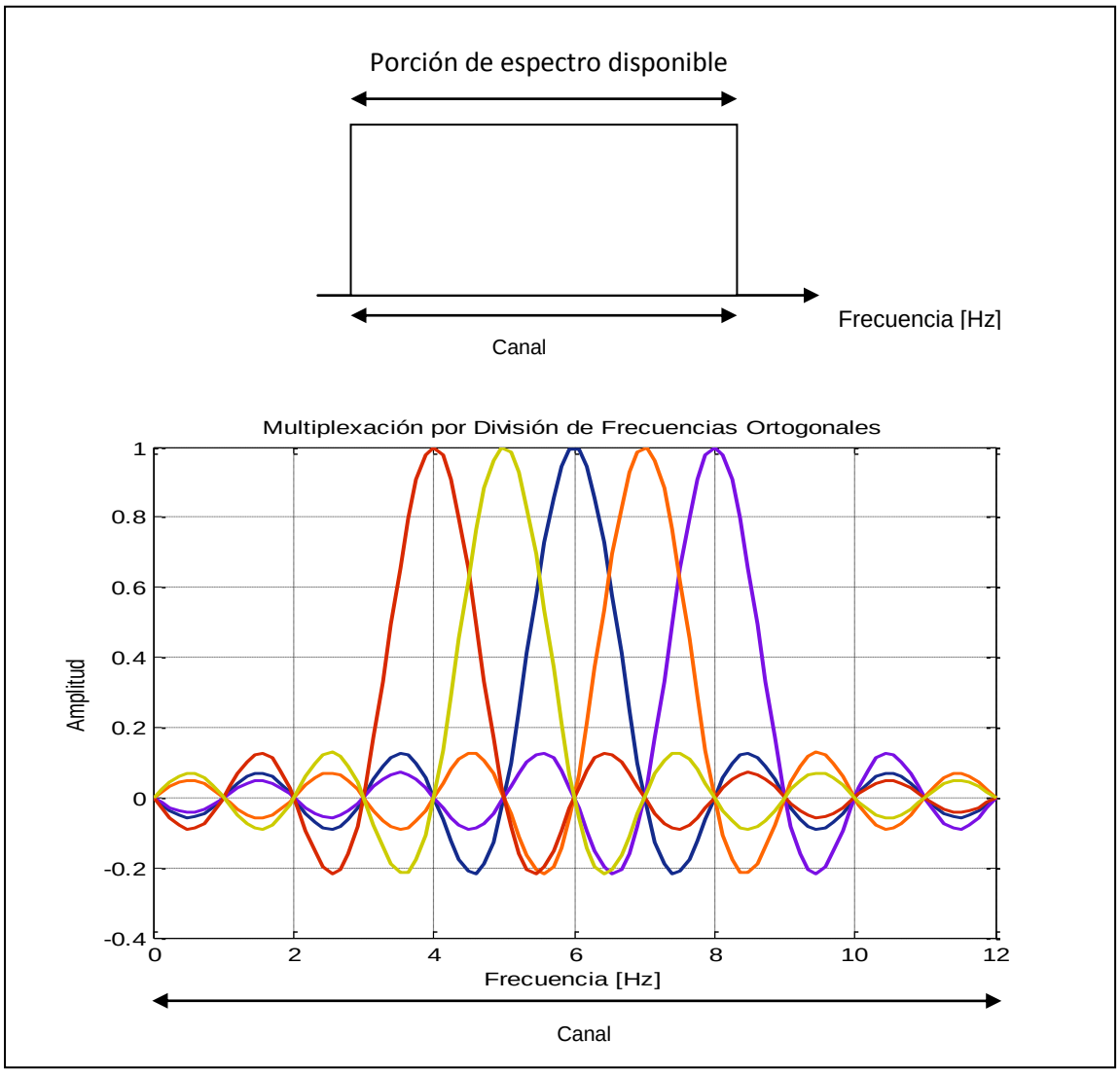


Figura 4.- Esquema de la Multiplexación por División de Frecuencias Ortogonales.

2.2. Control de Acceso al Medio (MAC)

A nivel MAC, el control de acceso al medio es por dos maneras: la Función de Coordinación Distribuida (DCF) y la Función de Coordinación Puntual (PCF), esta última utiliza un Punto de Acceso como controlador central y se basa en DCF.

La Función de Coordinación Distribuida se utiliza en redes ad hoc, en las cuales el único requisito es que al menos existan dos terminales que se

encuentren dentro del rango de cobertura de la señal. La siguiente figura muestra la red ad hoc más simple:

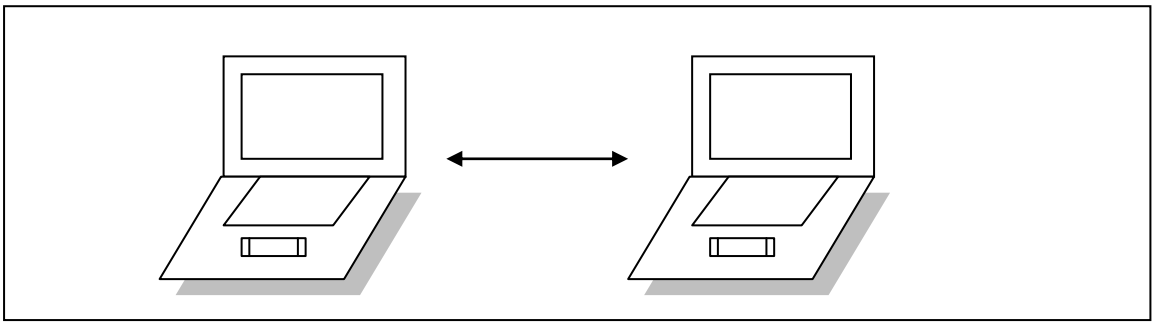


Figura 5.- Configuración de una red ad hoc, no necesita ningún tipo de gestión administrativa.

DCF emplea el algoritmo de Acceso Múltiple por Detección de Portadora con Evasión de Colisiones (CSMA/CA), el cual funciona de la manera siguiente: cuando una terminal desea transmitir escucha el canal y si lo encuentra libre se espera un tiempo denominado Espacio Entre Trama (IFS) y vuelve a sensar el canal, si lo encuentra libre entonces transmite.

Al terminar su transmisión liberará el canal y otras estaciones podrán tener acceso a éste; sin embargo antes de transmitir se esperan otro tiempo IFS y si el canal se encuentra libre generan un tiempo aleatorio de espera. La terminal que tenga el menor tiempo de espera volverá a sensar el canal y si lo encuentra libre entonces transmitirá. Las terminales restantes se abstendrán de transmitir mientras se concluye la transmisión actual.

DCF emplea tres tipos de IFS para dar prioridad de acceso al medio a los elementos de la red. El primer tipo de IFS es el tiempo más corto y se denomina Espacio Corto Entre Trama (SIFS), su duración es de 16 µs y es utilizado por una terminal cuando emite un Acuse de Recibo de trama (ACK), cuando solicita Permiso Para Enviar una trama (RTS) o cuando responde a un sondeo hecho por el AP [5].

El segundo tipo de IFS se denomina Espacio Corto Entre Trama de la PCF (PIFS), el cual es utilizado por el Punto de Acceso cuando emite un sondeo.

El tercer y último tipo de IFS se denomina Espacio Corto Entre Trama de la DCF (DIFS) y es utilizado por una terminal que desea transmitir.

Para disminuir la probabilidad de que dos o más terminales tengan nuevamente una colisión se usa el algoritmo Exponencial Backoff. Este es un algoritmo en el que las terminales en colisión transmiten en un tiempo aleatorio dentro de un

rango de tiempo que crece de manera exponencial después de cada colisión. Lo anterior se realiza con la finalidad de disminuir la probabilidad de colisión entre estas terminales.

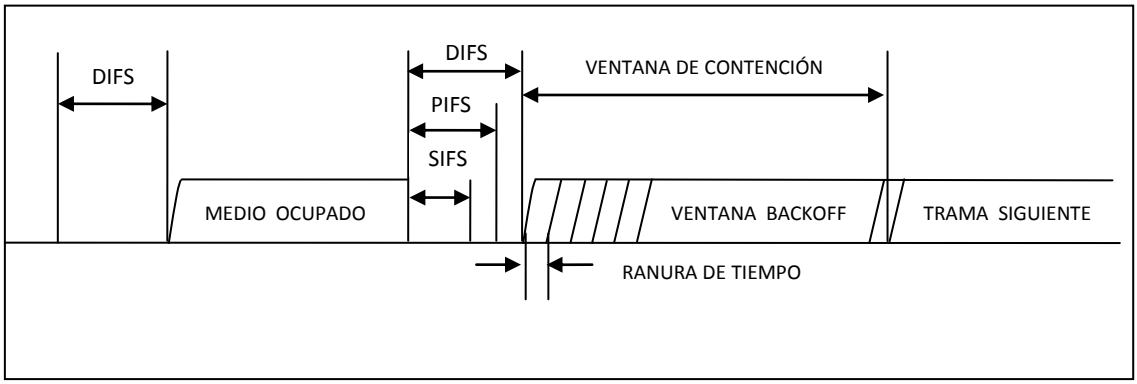


Figura 6.- Método básico de acceso al medio empleando DCF.

En la Función de Coordinación Puntual, las terminales móviles acceden a la red mediante un Punto de Acceso, esto se puede observar en la siguiente figura:

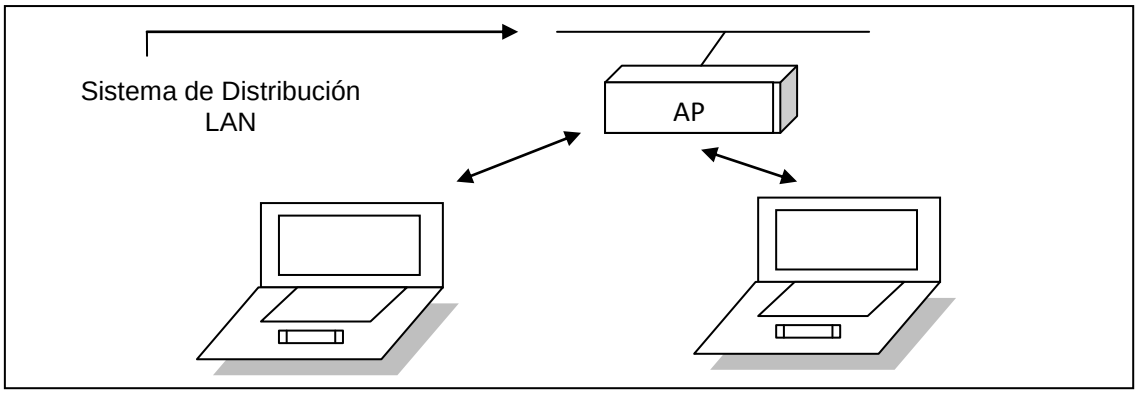


Figura 7.- Configuración de una red con Infraestructura, los nodos acceden a la red mediante Puntos de Acceso.

En esta técnica el AP se encuentra conectado a la red y mediante el uso de PIFS realiza un sondeo y se adueña del medio impidiendo el tráfico mientras recibe respuesta. Las terminales consultadas responden usando un SIFS y después se compite por el acceso al medio utilizando DCF. Esto se hace para que el AP no mantenga siempre ocupado el canal y permita a las terminales (las no controladas por el AP) acceder al medio para realizar su transmisión, posteriormente el AP vuelve a hacer un sondeo utilizando un PIFS.

2.2.1. Formato de la trama MAC

La siguiente figura muestra el formato de la trama MAC en el estándar IEEE 802.11 [8]:

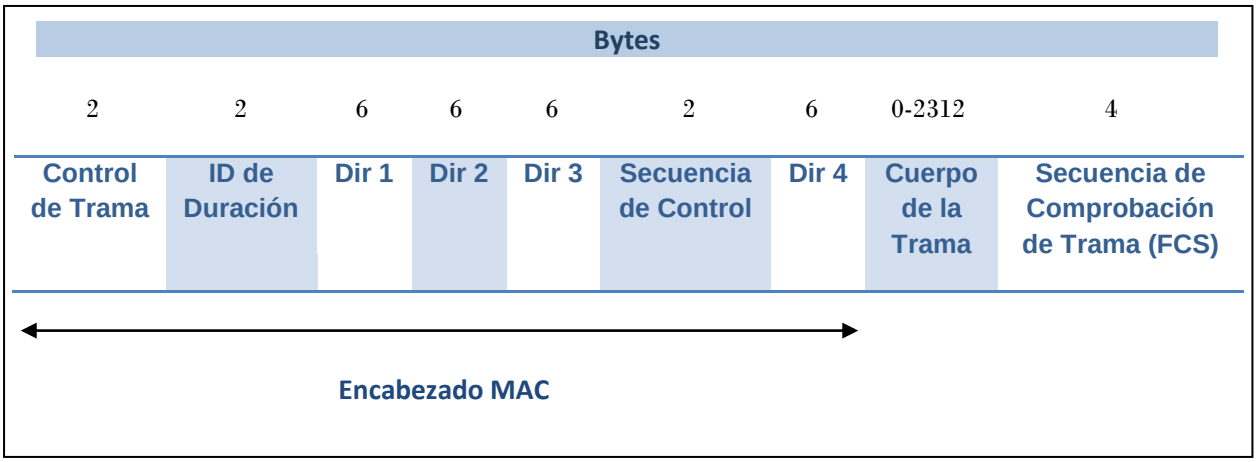


Figura 8.- Campos de la trama MAC de IEEE 802.11

A continuación se explica la función de cada campo de la trama:

- **Control de Trama**

Este campo está compuesto por los siguientes subcampos:

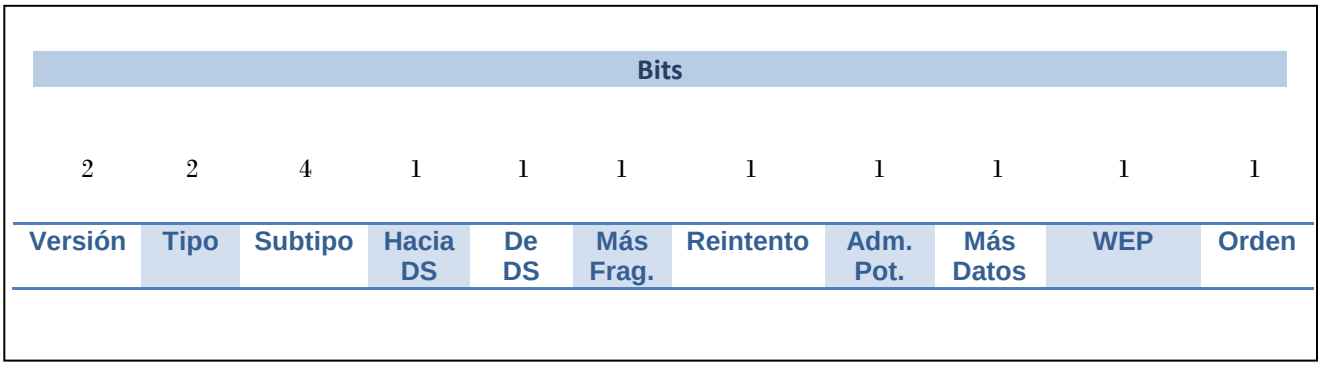


Figura 9.- Subcampos del campo de control de IEEE 802.11

Versión: Este campo especifica la versión del estándar IEEE 802.11 que se está utilizando.

Tipo: Aquí se especifica el tipo de la trama y esta puede ser de control, administración o datos.

Control.-Este tipo de tramas colabora en la entrega de las tramas de datos.

Administración.- Estas tramas sirven para organizar las comunicaciones entre los elementos de la red.

Datos.- Estas tramas transportan la información.

Abajo se muestra una tabla especificando el tipo de trama de acuerdo a la combinación de los dos bits de este subcampo.

Combinación		Tipo de Trama
0	0	Administración
0	1	Control
1	0	Datos
1	1	Reservada

Tabla 1.- Tipos de trama y su combinación correspondiente.

Subtipo: Este campo especifica el subtipo del tipo de trama. A continuación se mencionan los subtipos de cada tipo de trama.

Administración

Estas tramas se encargan de mantener la comunicación entre las terminales y los AP.

Dentro de las tramas de administración tenemos las siguientes:

- Solicitud de asociación.- Estas tramas las envían las terminales para iniciar el proceso de comunicación con el AP.
- Respuesta de asociación.- Este tipo de tramas las envían los puntos de acceso y en ellas se informa si el AP acepta o rechaza la solicitud de asociación. En caso de aceptarla, la misma trama contiene información sobre las tasas de transmisión así como el Identificador de Conjunto de Servicio (SSID), el cual es un código que contienen los paquetes de una red y los identifican como miembros de la misma.

- Solicitud de reasociación.- Estas tramas son enviadas por las terminales cuando se encuentran asociadas a un AP y desean cambiarse a otro AP de la misma red.

- Respuesta de reasociación.- En este tipo de tramas el AP al que la terminal se desea cambiar, responde si acepta o rechaza la solicitud de reasociación.

- Beacon.- Estas tramas son enviadas periódicamente por los AP a las terminales que se encuentran dentro de su área de cobertura y en éstas se especifica la información de la red a la cual pertenecen.

- Disociación.- Esta trama es enviada por las terminales que se encuentran dentro de la región de cobertura de un AP para finalizar la comunicación.

- Autenticación.- Estas tramas son enviadas de las terminales al AP y por medio de ellas se puede conocer la identidad de las terminales. Hay dos maneras de realizar la autenticación; la primera es cuando las terminales envían las tramas y el AP acepta o rechaza la conexión; la segunda es cuando el AP tiene que comprobar si la terminal tiene la llave correcta, para ello le envía un texto el cual la terminal debe cifrar con su clave y devolverla al AP, si el texto se cifra con la llave correcta entonces el AP permite la conexión.

- Desautenticación.- Este tipo de tramas son enviadas entre las terminales y su función es anunciar el fin de la comunicación entre las mismas.

Control

Las tramas de control se encargan de la entrega de las tramas de datos.

Dentro de las tramas de control tenemos las siguientes:

- Sondeo de ahorro de energía (Power Save-Poll).- Este tipo de trama la envía una terminal que se encuentra en modo de ahorro de energía a otra terminal que contiene al AP, solicitando que este último le envíe una trama a la terminal que se encuentra en modo de ahorro de energía.

- Solicitud para enviar (Request to Send).- Esta trama se envía cuando una terminal quiere transmitir una trama de datos a otra

terminal. Cuando las terminales vecinas escuchan esta solicitud se abstienen de transmitir, lo que reduce las colisiones.

- Permiso para enviar (Clear to Send).- Este tipo de trama es enviada por la terminal receptora (la que recibió la solicitud para enviar) a la terminal transmisora para indicarle que puede enviar la trama de datos.

- Acuse de recibo (Acknowledge).- Esta trama la envía la terminal receptora a la transmisora y su función es confirmar la recepción de la trama de datos.

- Fin del periodo libre de contención (CF-End).- Esta trama anuncia a las terminales el fin de un periodo libre de contención.

- Confirmación de la trama CF-End (CF-End+CF-Ack).- Con esta trama se confirma el fin del periodo libre de contención y las terminales compiten por el acceso al canal.

Datos

Este tipo de tramas contienen la información.

Dentro de las tramas de datos se encuentran:

- Datos + CF-Ack.- Esta trama contiene los datos y proporciona un acuse de recibo de datos anteriores. Esta trama sólo puede ser usada durante el periodo libre de contenciones.

- Datos + CF-Poll.- Esta trama es utilizada por el AP para entregarle datos a una terminal. Esta trama sólo puede ser usada durante el periodo libre de contenciones.

- Datos + CF-Ack + CF-Poll.- Esta trama contiene las dos tramas anteriores y sólo puede ser usada durante el periodo libre de contenciones.

- Datos.- Esta trama puede usarse para transportar datos y puede utilizarse tanto en el periodo de contención como en el libre de contenciones.

- Función nula.- Esta trama la transmite una terminal a un AP indicándole que se pondrá en modo de ahorro de energía.

Las siguientes tramas realizan las mismas funciones que las anteriores, pero sin transportar datos.

- CF-Ack
- CF-Poll
- CF-Ack + CF-Poll

En la tabla se muestran las posibles combinaciones para el subtipo de trama.

Tipo		Subtipo				Significado
0	0	0	0	0	0	Solicitud de asociación
0	0	0	0	0	1	Respuesta de asociación
0	0	0	0	1	0	Solicitud de reasociación
0	0	0	0	1	1	Respuesta de reasociación
0	0	0	1	0	0	Solicitud de sondeo
0	0	0	1	0	1	Respuesta de sondeo
0	0	0	1	1	0	Reservada
0	0	0	1	1	1	Reservada
0	0	1	0	0	0	Beacon
0	0	1	0	0	1	Indicación de mensaje de anuncio de tráfico
0	0	1	0	1	0	Disociación
0	0	1	0	1	1	Autenticación
0	0	1	1	0	0	Desautenticación
0	0	1	1	0	1	Reservada
0	0	1	1	1	1	Reservada
0	1	0	0	0	0	Reservada
0	1	1	0	0	1	Reservada
0	1	1	0	1	0	PS-Poll
0	1	1	0	1	1	RTS
0	1	1	1	0	0	CTS
0	1	1	1	0	1	ACK
0	1	1	1	1	0	CF-End

0	1	1	1	1	1	CF-End + CF-Ack
1	0	0	0	0	0	Datos
1	0	0	0	0	1	Datos + CF-Ack
1	0	0	0	1	0	Datos + CF-Poll
1	0	0	0	1	1	Datos + CF-Ack + CF-Poll
1	0	0	1	0	0	Función nula (sin datos)
1	0	0	1	0	1	CF-Ack (sin datos)
1	0	0	1	1	0	CF-Poll (sin datos)
1	0	0	1	1	1	CF-Ack + CF-Poll (sin datos)
1	0	1	0	0	0	Reservada
1	0	1	1	1	1	Reservada
1	1	0	0	0	0	Reservada
1	1	1	1	1	1	Reservada

Tabla 2.- Subtipos de trama y su combinación correspondiente.

Hacia el Sistema de Distribución (DS): Es un campo que se pone en 1 cuando las terminales envían la trama de datos a un DS. Este campo se pone en 0 en las otras tramas.

De DS: Es un campo que se pone en 1 cuando las terminales reciben la trama de datos de un DS. Este campo se pone en 0 en las otras tramas.

La tabla muestra el significado de las combinaciones de los dos campos anteriores:

Hacia DS	De DS	Significado
0	0	La trama es enviada de una terminal a otra terminal
0	1	La trama de datos proviene del sistema de distribución
1	0	La trama de datos es enviada al sistema de distribución
1	1	La trama es enviada de un AP a otro AP

Tabla 3.- Significado de los subcampos Hacia DS y De DS del campo de control.

Más fragmentos: Este campo se pone en 1, es decir, se activa si se quiere indicar que se espera otro fragmento y es usado en las tramas de administración o datos.

Reintento: Este campo se activa cuando se indica que la trama es una retransmisión.

Administración de Potencia: Cuando este campo se activa indica que la terminal móvil pasará al modo de ahorro de energía. Por el contrario, cuando este campo se desactiva o se pone en 0, indica que la terminal pasará al modo activo y trabajará normalmente.

Más datos: Si este campo se activa, entonces el AP tiene tramas pendientes por enviar a una terminal que se encuentra en modo de ahorro de energía.

WEP: Este campo se activa cuando la información del campo “cuerpo de la trama” de tramas del tipo de datos o de autenticación ha sido cifrada por el algoritmo WEP, el cual se describe más adelante.

Orden: Este campo se activa cuando las tramas de datos o fragmentos se transmiten con la clase de servicio de ordenamiento estricto, esta clase de servicio se proporciona a las terminales que no pueden aceptar cambios de ordenamiento entre tramas unicast (trama dirigida a una terminal en particular) y multicast (trama dirigida a un grupo de terminales).

- **Duración/ID**

Este campo tiene dos funciones. Por un lado es el Identificador Asociado (AID) de la terminal móvil en las subtramas “sondeo de ahorro de energía” de las tramas de control; por otro lado es el valor del periodo que se ha asignado una estación para abstenerse de transmitir cuando ha escuchado una trama RTS o CTS.

- **Dirección 1**

Este es el campo que especifica la dirección del destino de la trama. Si la trama va hacia el sistema de distribución, esta dirección corresponde al AP, de lo contrario, es la dirección de la terminal final.

- **Dirección 2**

En este campo se especifica la dirección del dispositivo que está transmitiendo la trama. Si la trama viene del sistema de distribución, esta dirección es la del AP, de lo contrario, es la dirección de la terminal que transmite la trama.

- **Dirección 3**

Este es el campo que especifica la dirección de la terminal que transmitió la trama cuando ésta proviene del sistema de distribución, de lo contrario, indica la dirección de la terminal destino cuando la trama se dirige al sistema de distribución.

- **Secuencia de control**

Este campo se conforma de otros dos campos: número de fragmento y número de secuencia. El primero es un campo de 12 bits que especifica el número de fragmento de una misma trama. El segundo es un campo de 4 bits que especifica el número de trama de una secuencia de tramas [14].

- **Dirección 4**

Campo que especifica la dirección del AP que transmite la trama a otro AP cuando estos forman parte de un sistema de distribución inalámbrico.

- **Cuerpo de la trama**

Este campo tiene una longitud de 0 a 2312 bytes y contiene la información del tipo y subtipo de trama que se está enviando.

- **Secuencia de comprobación de trama (FCS)**

Aquí se analiza si la trama fue dañada durante el transporte, es decir, se verifica si la trama llegó íntegra a su destino final o fue modificada durante el transporte de la misma.

La secuencia de comprobación de trama se calcula mediante un Código de Redundancia Cíclica (CRC) de 32 bits usando los bits de los campos del encabezado MAC y del cuerpo de la trama. El mecanismo es el siguiente:

1.- Una vez que se tiene la cadena de bits de los campos anteriores, se le añade 32 ceros a la derecha llamados “bits de redundancia”.

2.- Se toman los coeficientes del siguiente polinomio generador de orden 32 [2].

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

La cadena de bits correspondiente a los coeficientes del polinomio generador resulta:

100000100110000010001110110110111

3.- Se efectúa la división binaria:

Cociente

Cadena de bits correspondiente a los coeficientes del polinomio generador | Cadena de bits de los campos del encabezado MAC, cuerpo de la trama y 32 bits de redundancia

Residuo

Se realiza enseguida la siguiente resta binaria:

Cadena de bits de los campos del encabezado MAC, cuerpo de la trama y 32 bits de redundancia − Residuo

Finalmente la cadena de bits resultante de la operación anterior se envía a la estación receptora.

4.- Al recibir esta cadena, la estación receptora la divide entre la misma cadena de bits correspondiente a los coeficientes del polinomio generador de orden 32. Si el residuo de la división es “cero”, la trama no habrá sido modificada durante el transporte, lo que indica que no contendrá errores. Por el contario si existe un residuo como resultado de la división, indicará que la trama contiene al menos un error.

A continuación se muestra un ejemplo de cómo se calcula el CRC de 32 bits suponiendo que los bits de los campos del encabezado MAC y del cuerpo de la trama son 10110110:

1. Se le añaden los bits de redundancia:

10110110000000000000000000000000000000000

2. Los coeficientes del polinomio generador resultan:

100000100110000010001110110110111

3. Se efectúa la división binaria:

```
                                           10110010
100000100110000010001110110110111 | 1011011000000000000000000000000000000000
                                   10110001101110010101011011000010
```

Ahora se realiza la siguiente resta binaria:

1011011000000000000000000000000000000000 - 10110001101110010101011011000010

La siguiente cadena es la que se envía al receptor:

1011010101001110010001101010100100111110

4.- Al llegar al receptor la cadena anterior, se realiza la siguiente división binaria:

```
                                           10110010
100000100110000010001110110110111 | 1011010101001110010001101010100100111110
                                                                          0
```

La trama recibida no tiene errores debido a que el residuo de la división anterior es cero.

2.3. Versiones del protocolo de comunicaciones IEEE 802.11

La siguiente tabla muestra las características de las principales versiones del estándar IEEE 802.11

Versión	Año en que se publicó	Frecuencia de operación [GHz]	Capa Física	Capa MAC	Tasa de transmisión mínima [Mbps]	Tasa de transmisión máxima [Mbps]	Número de canales	Radio de cobertura [m]	Tipo de modulación	Comentarios
Legacy	1997	2.4	DSSS FHSS	CSMA/ CA	1	2	----	100	DBPSK DQPSK	Esta es la versión original del estándar y se encuentra en desuso.
IEEE 802.11 a	1999	5.15 - 5.25 5.25 - 5.35 5.725-5.825	OFDM	CSMA/ CA	6	54	12 8 → red inalámbrica 4→conexión punto- punto Canal 36→5180 [MHz] Canal 44→5220 [MHz] Canal 52→5260 [MHz] Canal 60→5300 [MHz]	120	BPSK QPSK 16-QAM	No tiene interferencias producidas por dispositivos de uso cotidiano en la banda de 2.4 GHz como los teléfonos inalámbricos y hornos de microondas, pero por su alta frecuencia sus ondas son fácilmente absorbidas y por ello se necesita de un mayor número de AP en la red. En la actualidad es posible encontrar dispositivos que soporten esta versión. El ancho de banda de la señal es de 22 MHz, por ello los canales 36, 44, 52 y 60 no causan interferencia entre si ya que se encuentran espaciados 40 MHz.
IEEE 802.11 b	1999	2.4 – 2.483	CDMA	CSMA/ CA	5.5	11	11 8 → red inalámbrica 3→conexión punto- punto Canal 1 → 2412 [MHz] Canal 6 → 2437 [MHz] Canal 11→ 2462[MHz]	140	DQPSK QPSK	Por su frecuencia de operación sus ondas alcanzan a propagarse a una mayor distancia por lo que necesita de un menor número de AP. Esta versión es compatible con la versión original y sufre interferencias de teléfonos inalámbricos, hornos de microondas y el bluetooth, ya que operan en la misma banda de frecuencia. El ancho de banda de la señal es de 22 MHz, por ello los canales 1,6 y 11 no causan interferencia entre si ya que se encuentran espaciados 25 MHz. En la actualidad existe una gran variedad de dispositivos que soportan esta versión.
IEEE 802.11 g	2003	2.4 -2.483	OFDM	CSMA/ CA	19	54	11 8 → red inalámbrica 3→conexión punto- punto Canal 1 → 2412 [MHz] Canal 6 → 2437 [MHz] Canal 11→ 2462[MHz]	140	BPSK QPSK 16 - QAM 64 - QAM	Es compatible con la versión 802.11 b y sufre las mismas interferencias. Con el uso de OFDM se pueden tener mayores tasas de transmisión ya que no se producen errores por efecto de multitrayectoria y hasta la fecha es la versión 802.11 más utilizada.

Tabla 4.- Características principales de las versiones del estándar IEEE 802.11 empleadas para comunicaciones de las WLAN [1], [2], [3], [13]

En seguida se muestra un listado de las versiones del protocolo de comunicaciones IEEE 802.11 [10]:

IEEE 802.11 d

Dado que las frecuencias de operación de IEEE 802.11 no son permitidas en algunos países, esta versión se publicó en el 2001 para admitir que distintos dispositivos se comuniquen conforme a las bandas de frecuencia permitidas de la región donde operan.

IEEE 802.11 e

Este estándar se publicó en el año 2005 y su objetivo es lograr que las WLAN proporcionen Calidad de Servicio (QoS) para datos, voz y video.

IEEE 802.11 f

Esta es una recomendación que se publicó en el año 2003 para permitir la interoperabilidad de distintas marcas de AP, de esta manera, la terminal puede moverse entre varios AP pertenecientes a la misma red y de distintas marcas sin perder conexión.

IEEE 802.11 h

Esta versión se publicó en el año 2003 y su función es implementar en los AP de las WLAN que operan en 5 GHz, las funciones de Control de Potencia de Transmisión (TPC) y la Selección de Frecuencia Dinámica (DFS). La primera se refiere a utilizar la mínima potencia de transmisión para el usuario más lejano y la segunda para seleccionar el canal en el que se produzca la mínima interferencia con otros sistemas, por ejemplo radares meteorológicos y satélites.

IEEE 802.11 i

Estándar publicado en el 2004 cuyo propósito es incrementar la seguridad en las WLAN mediante mejorados métodos de encriptación y procesos de autenticación. Esta versión usa IEEE 802.1 x para autenticar a los usuarios y el Estándar de Cifrado Avanzado (AES) como método de encriptación.

IEEE 802.11 k

Este es un esbozo publicado en enero del 2008, propone la administración de recursos y con ello una mejora en el tráfico en la red. Utilizando esta versión, se detectará el AP con mejor señal y brindará servicio a su máxima capacidad a las terminales que lo soliciten, aquellas terminales que el AP ya no alcance a dar servicio, serán asistidas por los AP restantes de la red.

IEEE 802.11 p

Este es un borrador conocido como Acceso Inalámbrico de Ambiente Vehicular (WAVE) que se pretende terminar en este año y cuyo objetivo es brindar comunicación inalámbrica entre vehículos en movimiento con una velocidad de hasta 200 km/hr y con una distancia de hasta 1000 metros de separación. Los dispositivos que soporten esta tecnología utilizarán la banda de 5 GHz.

IEEE 802.11 r

Es un esbozo para permitir que una terminal pueda cambiarse de AP (handoff) de manera rápida, segura y sin perder conexión. Con este estándar se pretende que los protocolos de seguridad de la red identifiquen a la terminal en el nuevo AP en menos de 50 ms.

IEEE 802.11 s

Es un esbozo que se pretende terminar este año y su objetivo es definir una arquitectura y un protocolo para las redes inalámbricas mesh (redes inalámbricas de topología de malla implementadas sobre una WLAN), ya que cada fabricante toma en cuenta un protocolo para decidir la mejor trayectoria que tomará el paquete dentro de una red mesh.

IEEE 802.11 w

Esta versión aún está en desarrollo y su objetivo es brindar mayor seguridad en las WLAN mejorando los métodos de encriptación y procesos de autenticación establecidos en IEEE 802.11 i.

Asimismo, la versión aplicará estas técnicas de seguridad no sólo en las tramas de datos sino también en las tramas de administración de la red.

2.4. Seguridad en redes inalámbricas

Basta con que una terminal tenga buena recepción de la señal del AP para que tenga acceso a la red, sin embargo, la mayoría de las veces la información que se maneja en ésta es importante y confidencial. Es por ello que el tema de la seguridad en redes inalámbricas es sumamente importante ya que le permitirá el acceso sólo a aquellas terminales que gocen de este privilegio.

2.4.1. SSID

El Identificador de Conjunto de Servicio (SSID) o nombre de la red, es un código de 32 caracteres alfanuméricos que contienen los paquetes de una red y los identifican como miembros de la misma.

La terminal debe conocer el SSID para comunicarse con el AP y tener acceso a la red. Por su parte, el AP continuamente difunde este identificador de una manera automática a todas las terminales que se encuentran dentro de su rango de cobertura. No obstante, como una técnica de seguridad esta función se puede deshabilitar en el AP para que no difunda el SSID y sólo las terminales que lo conozcan se puedan comunicar con éste.

Esta técnica dificulta que los usuarios configuren y se conecten a la red inalámbrica.

2.4.2. MAC

Esta técnica permite que los AP tengan almacenada una tabla de direcciones MAC de las terminales que tienen permiso de acceso a la red.

No es muy recomendable utilizar esta técnica de seguridad ya que en cada AP de la red se tiene que dar de alta o baja y de forma manual la MAC de cada terminal.

Cuando una terminal con permiso de acceso a la red le envía su MAC al AP para comprobar que goza de tal privilegio, otra terminal puede capturarla usando un *sniffer* y después usarla para que el AP la reconozca como válida y le permita el acceso a la red.

2.4.3. WEP

Privacidad Equivalente a Cableado (WEP) es una técnica de seguridad que utiliza una misma clave para las terminales y para los AP, la cual debe ser escrita manualmente en cada uno de ellos.

WEP[1] utiliza RC4 como algoritmo de encriptación, el cual está compuesto de un Vector de Inicialización (IV o clave WEP) y de una clave (clave secreta). El vector de inicialización es generado al momento de transmitir una trama, debe ser distinto para cada una de ellas y tiene una longitud de 24 bits, la clave es asignada de forma manual, es estática y tiene una longitud 40 bits [6], [12].

Al transmitir una trama, se calcula el CRC de 32 bits y se genera el IV al cual se le añade la clave, con esta unión se genera una secuencia pseudoaleatoria de la misma longitud que el CRC de 32 bits, posteriormente se realiza una XOR entre la secuencia pseudoaleatoria y el CRC de 32 bits para encriptar la información del tipo y subtipo de la trama que se está enviando.

La trama lleva en el campo "cuerpo de la trama" el IV y la información encriptada, cuando llega a su destino la terminal que la recibe genera la misma secuencia pseudoaleatoria con el IV y la clave. Posteriormente se realiza una XOR entre la secuencia pseudoaleatoria y la información encriptada que recibió, logrando así descifrar la información.

La desventaja de esta técnica es que en la actualidad existe un software llamado Airsnort que captura los paquetes que se envían en la red; si se logra capturar de 5 a 10 millones de paquetes encriptados, esta herramienta puede descifrar la clave y tener acceso a la red.

2.4.4. WPA

Acceso Protegido Wi-Fi (WPA) es una técnica de seguridad que surge después que se analizaron las debilidades de WEP. Esta técnica sigue utilizando RC4 como algoritmo de encriptación con la variante de que maneja un IV de 48 bits, genera una clave de 128 bits de forma dinámica para cada terminal y la distribuye de forma automática en la red.

WPA usa IEEE 802.1 x para controlar el acceso a la red mediante puertos y un servidor de autenticación (RADIUS server), el cual realiza las funciones de autenticación, autorización y contabilidad. La primera función es para verificar la identidad de la terminal, la segunda para permitirle desempeñar dentro de la

[1] Existe una variante de esta técnica de seguridad llamada WEP2, que extiende la longitud de la clave de 40 a 104 bits manteniendo la longitud del IV.

red sólo las funciones que le fueron otorgadas y la tercera para llevar un registro del tiempo que ha estado conectado a la red.

WPA también puede operar de una manera semejante a WEP utilizando una Clave Inicial Compartida (PSK) entre las terminales y los AP, sin embargo, una gran desventaja de utilizar esta técnica de seguridad es que mediante el software Aircrack-ng se pueden capturar los paquetes que se envían en la red y descifrar la clave.

2.4.5. WPA2

Es el nombre comercial de IEEE 802.11i, es compatible con WPA y utiliza el Estándar de Cifrado Avanzado (AES) como algoritmo de encriptación, el cual es extremadamente seguro.

WPA2 es la técnica de seguridad más reciente y opera de dos maneras: utilizando una clave inicial compartida entre los AP y las terminales para autenticarlas (WPA2-Personal) o utilizando un servidor de autenticación para permitir el acceso de las terminales a la red (WPA2-Empresa).

Esta técnica de seguridad también puede ser implementada en redes ad-hoc.

Resumen del capítulo.

En este capítulo se han descrito las características a nivel capa Física y MAC del estándar de comunicaciones IEEE 802.11, asimismo, se han mostrado las técnicas de acceso múltiple al medio que emplean las terminales para tener acceso al canal de transmisión.

Este capítulo también contempla la descripción de la función que desempeña cada uno de los campos que forman la trama MAC, así como las distintas versiones del estándar IEEE 802.11 y las técnicas de seguridad que se emplean en las redes inalámbricas.

3. Protocolo de comunicaciones IEEE 802.11 N

A continuación se muestran las características principales de IEEE 802.11 N

Año en que se publicó	2006
Frecuencia de operación [GHz]	2.4 y 5
Capa Física	OFDM - MIMO
Capa MAC	CSMA/CA
Tasa de transmisión mínima [Mbps]	54
Tasa de transmisión máxima [Mbps]	300
Número de canales	15 13 → 5 GHz 2 → 2.4 GHz
Radio de cobertura [m]	300
Tipo de modulación	BPSK QPSK 16 – QAM 64 - QAM

Tabla 5.- Características principales del protocolo de comunicaciones IEEE 802.11 N

Esta es la versión más reciente del estándar IEEE 802.11, surge como una respuesta a la necesidad de incrementar la velocidad de transmisión de datos, calidad de la señal y radio de cobertura de las redes WLAN. El primer borrador fue aprobado en enero del año 2006, el segundo a principio del año 2007 y aún no se ha convertido en un estándar, sin embargo, hay una gran variedad de equipos que ya lo soportan.

IEEE 802.11 N trabaja en las bandas de frecuencia de 2.4 y 5 GHz, lo que lo hace compatible con las versiones a, b y g. En la primera banda de frecuencia usa un ancho de banda de canal de 20 MHz y en la segunda usa un ancho de banda de canal de 40 MHz, lo que indica que al utilizar esta última banda de frecuencia aumenta al doble la tasa de transmisión.

Las redes que soportan este nuevo protocolo de comunicaciones también pueden brindar servicio a las terminales que manejan estándares anteriores, sin embargo, la eficiencia de la red se puede ver afectada si al menos existe una de estas terminales que demande el servicio al AP. La terminal conectada a esta red aumentará ligeramente su tasa de transferencia pero no podrá utilizar algunas de las funciones del protocolo IEEE 802.11 N.

Este protocolo de comunicaciones hace algunos cambios en la capa Física y en la capa MAC al estándar de comunicaciones IEEE 802.11. En capa Física utiliza una combinación de OFDM y Múltiples Entradas/Múltiples Salidas (MIMO).

Con la finalidad de aumentar la posibilidad de comunicación la tecnología MIMO emplea varias antenas tanto en el transmisor como en el receptor. Si un objeto impide que la señal llegue a una de las antenas las otras restantes pueden recibirla.

Para un mejor rendimiento de la red se recomienda que las antenas del transmisor y receptor se encuentren separadas $\lambda/2$, es decir, 0.0625 m para la banda de 2.4 GHz y 0.03 m para la banda de 5 GHz [9].

MIMO emplea las siguientes cuatro técnicas (a veces sólo unas de ellas) para lograr un mayor rendimiento de la red [15]:

- Combinación de Relación Máxima (MRC)
- Codificación Espacio-Temporal por Bloques (STBC)
- Multiplexado por División Espacial (SDM)
- Formación de haces de transmisión (TxBF)

Combinación de Relación Máxima (MRC)

En la técnica MRC se utilizan múltiples antenas en el receptor y cada una de ellas recibe la señal de forma separada, posteriormente se suman todas las recepciones de la señal que llegaron a cada una de las antenas y de esta manera se logra incrementar la Relación Señal a Ruido (SNR).

A continuación se muestra una representación de esta técnica:

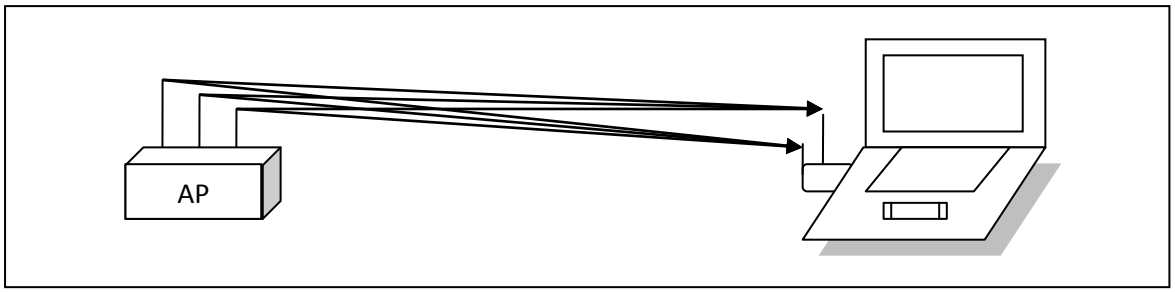


Figura 10.- Esquema del funcionamiento de la técnica MRC.

Codificación Espacio-Temporal por Bloques (STBC)

STBC se utiliza cuando el número de antenas de transmisión es mayor que el número de antenas de recepción. Esta técnica transmite distintas copias codificadas de una misma secuencia de datos desde cada una de las antenas del transmisor hacia cada una de las antenas del receptor, éste último decodifica todas las señales recibidas y las combina para obtener la mayor parte de la información de la señal transmitida y aumentar la SNR.

IEEE 802.11 N usa el código Alamouti como código base. En seguida se muestra la matriz de codificación para el caso más simple, en el cual se involucran dos antenas para transmitir y una para recibir dos símbolos consecutivos s_1 y s_2.

$$X = \begin{pmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{pmatrix}$$

Las filas de la matriz representan los símbolos transmitidos por cada una de las antenas y las columnas representan distintos instantes de transmisión.

A continuación se muestra la representación del caso más simple de esta técnica:

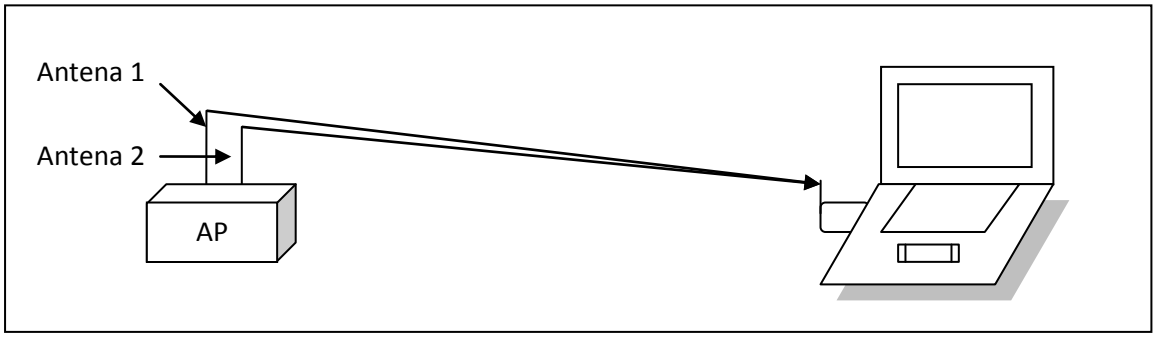


Figura 11.- Esquema del funcionamiento de MIMO y STBC.

En el tiempo t_1 la antena 1 transmite el símbolo s_1 y la antena 2 transmite el símbolo s_2. En el tiempo t_2 la antena 1 transmite el símbolo $-s_2^*$ y la antena 2 transmite el símbolo s_1^*.

Multiplexado por División Espacial (SDM)

SDM es la técnica más usada en MIMO, la cual divide la información en paquetes más pequeños y los transmite por las distintas antenas disponibles multiplexándolos en un mismo canal y al mismo tiempo.

A continuación se muestra una representación de esta técnica:

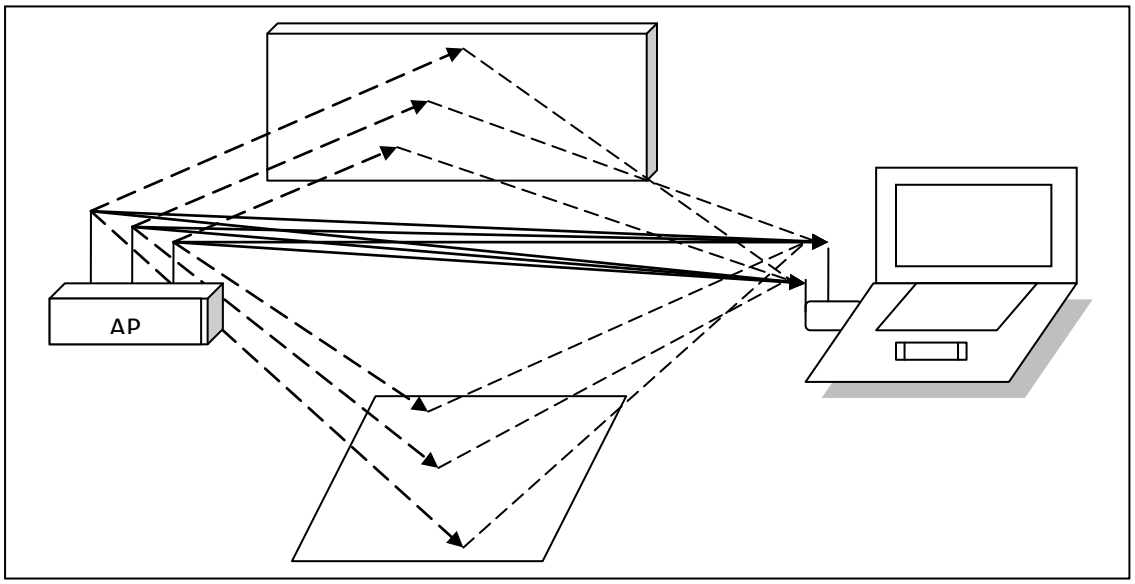


Figura 12.- Esquema del funcionamiento de MIMO y SDM.

En la figura anterior se puede observar que las señales directas y reflejadas por múltiples objetos son captadas por cada una de las antenas del receptor.

MIMO con SDM ocupa el fenómeno de multitrayectoria (distintos caminos que toma la señal debido a la reflexión de la misma sobre algunos objetos) para incrementar la tasa de transmisión y distancia de propagación, lo que le permite reducir el número de AP de la red.

Actualmente los AP que soportan las versiones a y g del estándar IEEE 802.11 se separan de 15 a 21 metros. Los AP que manejan el protocolo IEEE 802.11 N y que brindan servicio sólo a las terminales que también soportan este protocolo se separan entre 20 y 25 metros, es por ello que utilizando el protocolo IEEE 802.11 N se reduce el número de AP en la red.

Esta técnica en lugar de discriminar las señales de multitrayectoria envía paquetes de información por las señales reflejadas que llegan al receptor con buena intensidad.

Formación de haces de transmisión (TxBF)

Esta técnica se puede utilizar cuando SDM no funciona del todo bien, ya que permite que la transmisión de cada una de las antenas de un AP sea dirigida en la dirección de una terminal y viceversa, es decir, que la transmisión de cada una de las antenas de una terminal sea dirigida en dirección de un AP.

Utilizando TxBF se incrementa la SNR y se tienen mayores tasas de transmisión.

A continuación se muestra una representación de esta técnica:

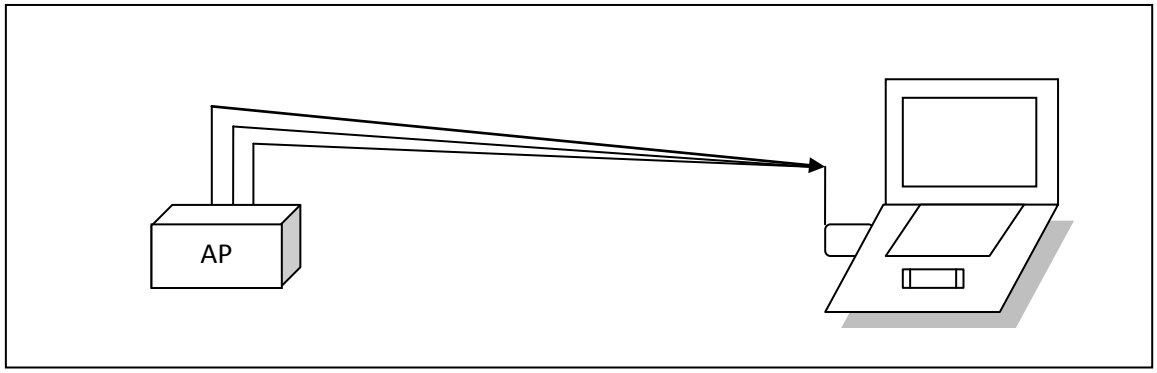


Figura 13.- Esquema del funcionamiento de TxBF.

A diferencia de los estándares anteriores, a nivel MAC el protocolo de comunicaciones IEEE 802.11 N envía múltiples tramas en un solo paquete. Por paquete se envían los ACK de las mismas [9], esto ayuda a reducir el número de encabezados y el tiempo de procesamiento de los elementos de la red.

Las tramas se agrupan sólo si son de la misma prioridad y cada una contiene su propia dirección fuente, dirección destino y longitud.

El paquete de confirmación de tramas especifica las tramas no recibidas y solicita la retransmisión de las mismas.

Este protocolo de comunicaciones define el Espacio Inter Trama Reducido (RIFS) como el tiempo que una misma terminal tiene que dejar pasar antes de volver a transmitir otra trama. Su duración es de 2 µs (8 veces menor que SIFS) y debe ser utilizado por una misma terminal.

La siguiente figura muestra el esquema del método de acceso al medio utilizando IEEE 802.11 N.

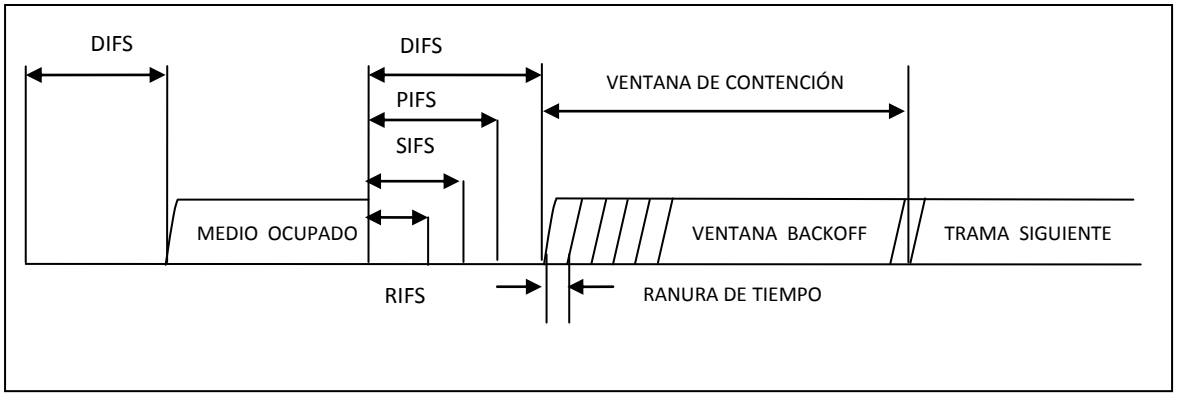


Figura 14.- Método básico de acceso al medio empleando DCF en IEEE 802.11 N

Las terminales que usan MIMO al entrar al modo de ahorro de energía pueden desactivar todas sus antenas salvo una que posteriormente recibirá la trama de reactivación por parte del AP.

Para lograr una mayor seguridad en las redes que soportan IEEE 802.11 N, los AP y las terminales pueden utilizar WPA2 como técnica de seguridad.

Resumen del capítulo

Este capítulo se ha enfocado a describir las características a nivel capa Física y MAC que han logrado que el protocolo de comunicaciones IEEE 802.11 N brinde un mayor rango de cobertura y una mayor tasa de transmisión.

Los dos parámetros anteriores son de gran utilidad para los usuarios y debido a ello se tiene demasiado interés en el protocolo.

El capítulo siguiente muestra una serie de pruebas que permiten conocer el comportamiento real del protocolo de comunicaciones IEEE 802.11 N y compararle con la versión IEEE 802.11 G, cual es la más utilizada en nuestros días.

4. Maqueta de pruebas

4.1. Descripción

Con el fin de estudiar el comportamiento del Estándar IEEE 802.11 N se creó la red inalámbrica LabN y se realizaron pruebas de comunicación entre un router que desempeñaba la función de un AP y una terminal móvil con un adaptador para esta tecnología.

Las pruebas se realizaron en un ambiente de propagación mixto, es decir, en un terreno con regiones donde había obstáculos que impedían el paso de la señal y con zonas en las que los dispositivos tenían LOS.

Se llevaron a cabo 3 pruebas: la primera de ellas consistió en medir con un software la intensidad de la señal, la SNR y la tasa de transmisión que se tenían en la terminal a una distancia de 10, 50 y 100 metros con respecto al AP. La segunda consistió en medir la tasa de transmisión al efectuar una comunicación entre la terminal y el AP usando el Protocolo de Transferencia de Archivos (FTP). La tercera en registrar la posición de cada una de las antenas en el AP para la cual se tenía la máxima tasa de transmisión entre la terminal y el AP.

Con el fin de contrastar los resultados arrojados usando la versión N del estándar IEEE 802.11 se realizaron las mismas pruebas pero usando la red inalámbrica INFINITUM6532 que utiliza la versión G del mismo estándar.

Primera prueba

A fin que el AP y la terminal tuvieran una mejor LOS, se colocó el AP sobre la marquesina de una casa a una altura de 2.40 metros con respecto al nivel del suelo, la única desventaja fue que en este lugar había un anuncio con estructura metálica que impedía el paso de la señal.

Se conectó la terminal móvil a la red y cuando la terminal se encontraba en un punto de prueba se iniciaba la descarga de un video desde www.youtube.com y se tomaban las lecturas correspondientes. El software que se utilizó para tomar las lecturas de la intensidad de la señal y la SNR fue Network Stumbler® versión 0.4.0. Para tomar la lectura de la tasa de transmisión en la capa Física se utilizó el estado de la conexión.

A continuación se muestra una descripción física del lugar donde se realizó la primera de las pruebas:

Figura 15.- Ubicación del lugar de pruebas y regiones de cobertura.

Las siguientes dos figuras muestran las lecturas hechas por Network Stumbler® y el estado de la conexión a las redes LabN e INFINITUM6532 usando IEEE 802.11 N e IEEE 802.11 G respectivamente:

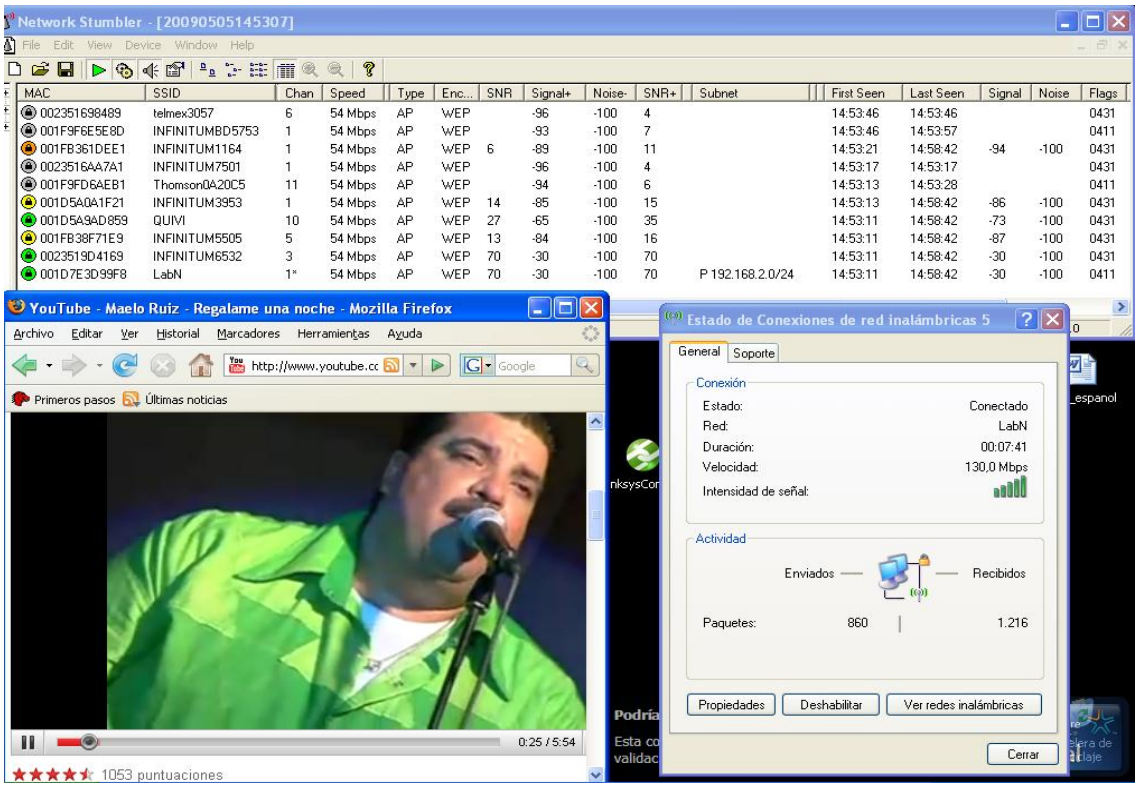


Figura 16.- Toma de lecturas en la red LabN usando Network Stumbler® y el estado de la conexión

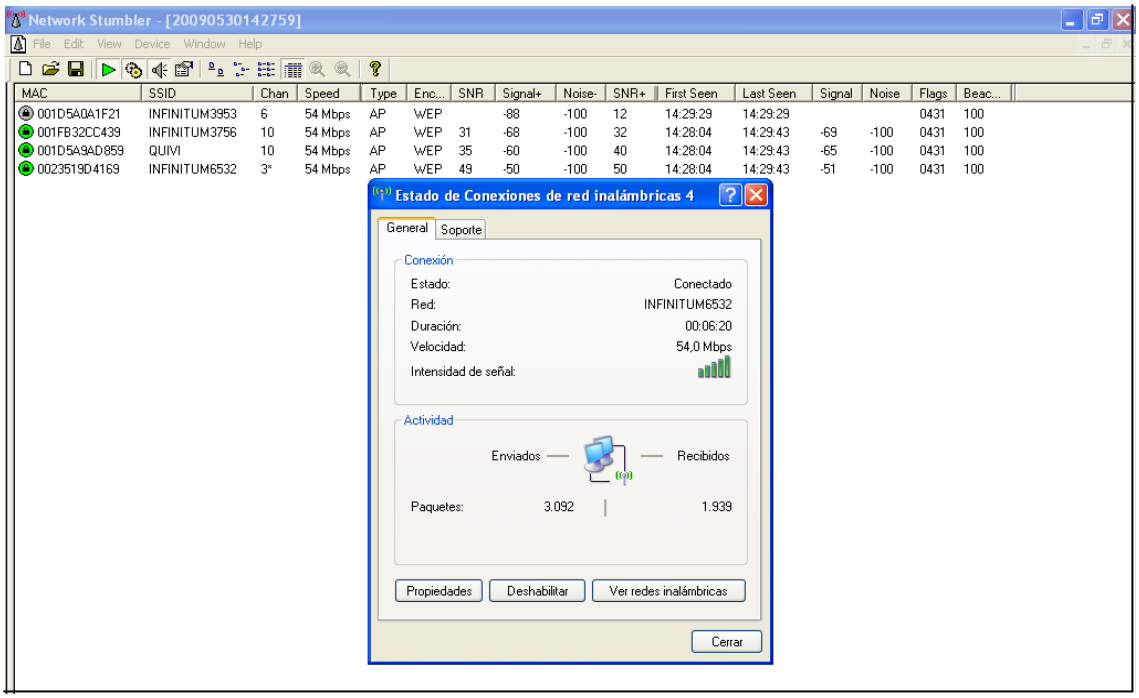


Figura 17.- Toma de lecturas en la red INFINITUM6532 usando Network Stumbler® y el estado de la conexión

Las dos figuras siguientes muestran la ubicación de los puntos de prueba utilizando las redes LabN e INFINITUM6532 respectivamente.

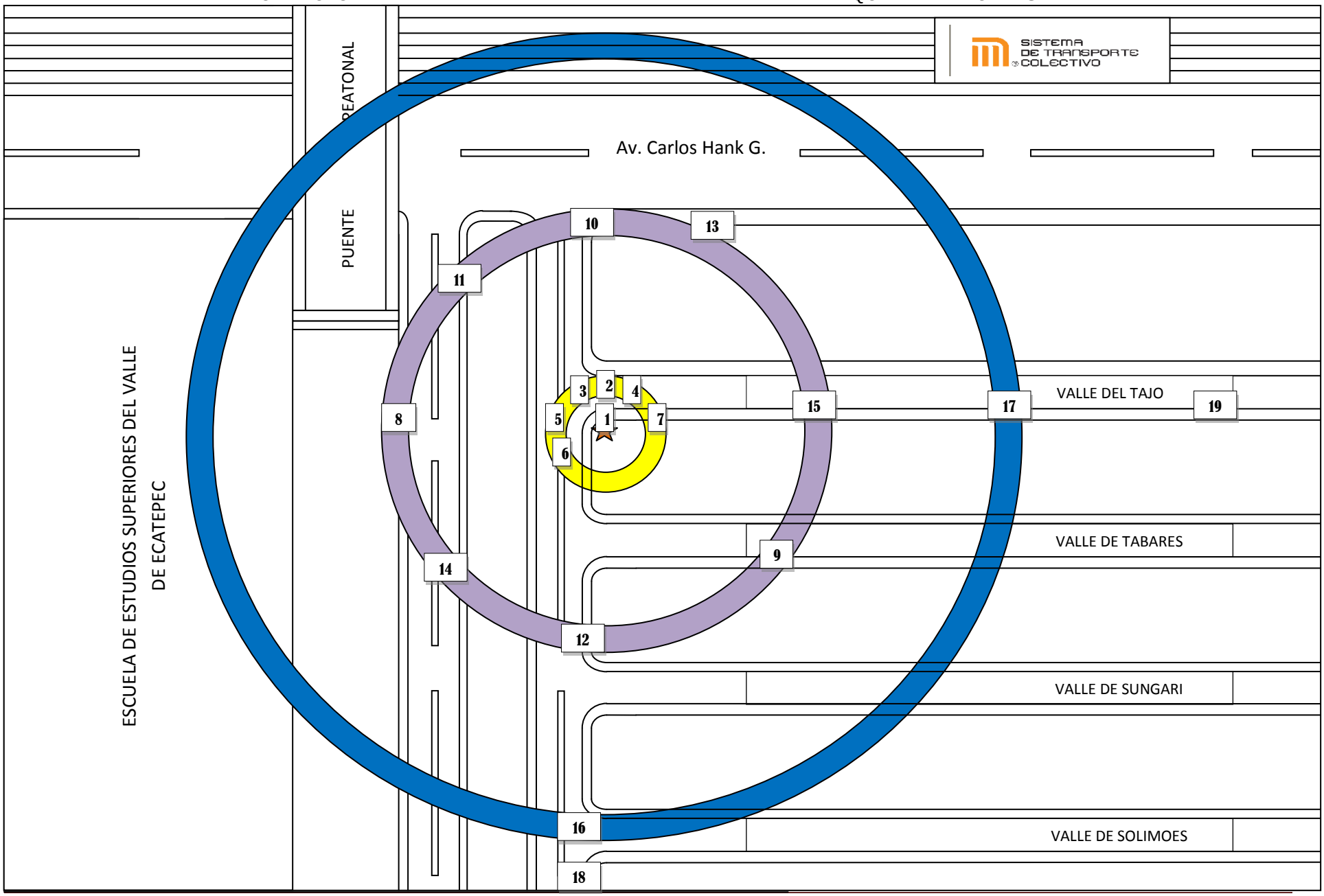


Figura 18.- Mapa del lugar de pruebas, regiones de cobertura y puntos de prueba utilizando la red LabN que soporta IEEE 802.11 N

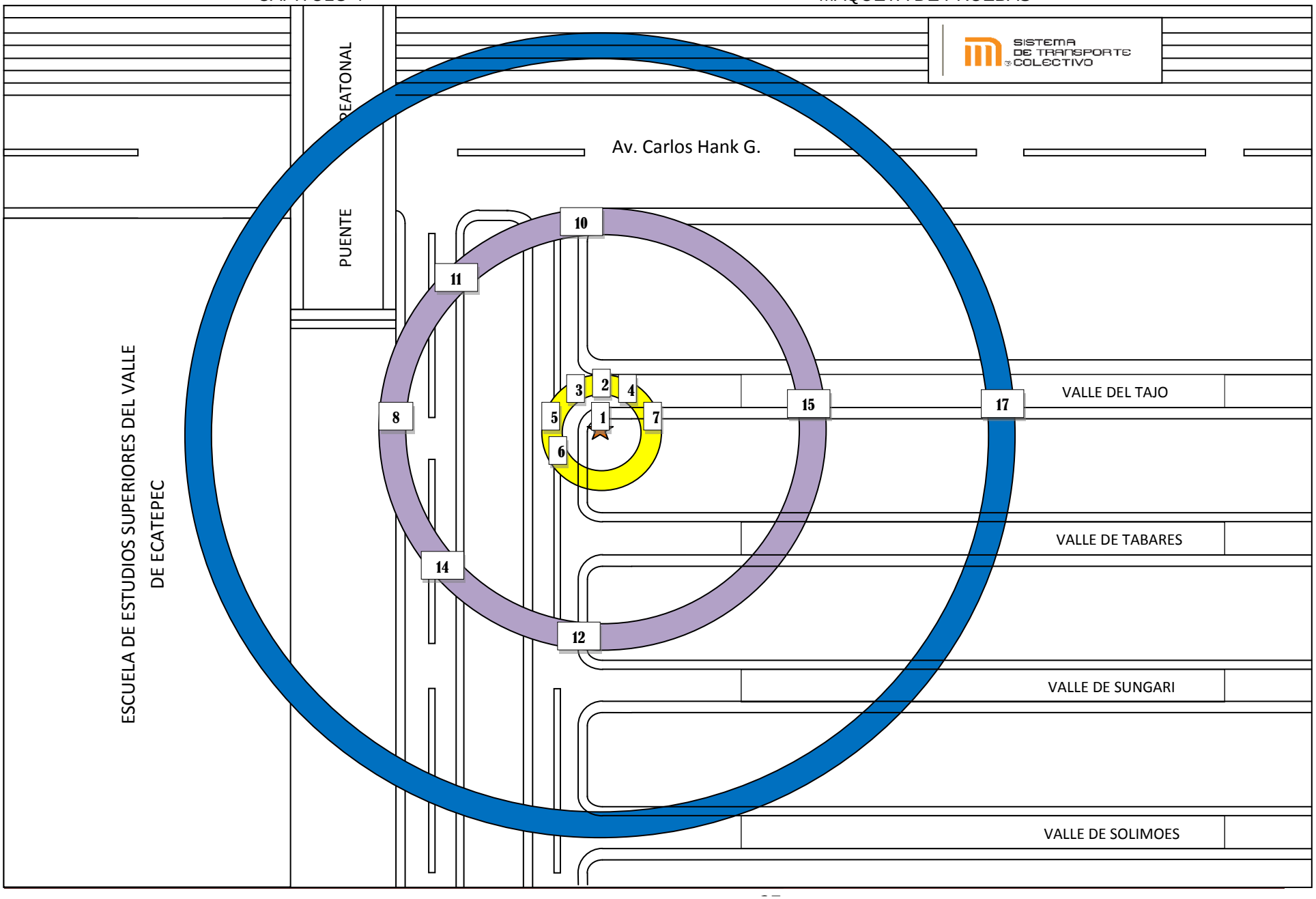


Figura 19.-Mapa del lugar de pruebas, regiones de cobertura y puntos de prueba utilizando la red INFINITUM6532 que soporta IEEE 802.11G

Segunda prueba

Para medir la tasa de transmisión en la capa Aplicación del modelo TCP/IP se configuró un servidor con una cuenta de usuario anónima usando el software Win FTP Server versión 2.4.0. En el servidor se colocó el archivo vts_01_2.vob de 1.0737 GB, el cual se transmitió a la terminal utilizando FTP.

La siguiente figura muestra la pantalla principal del servidor:

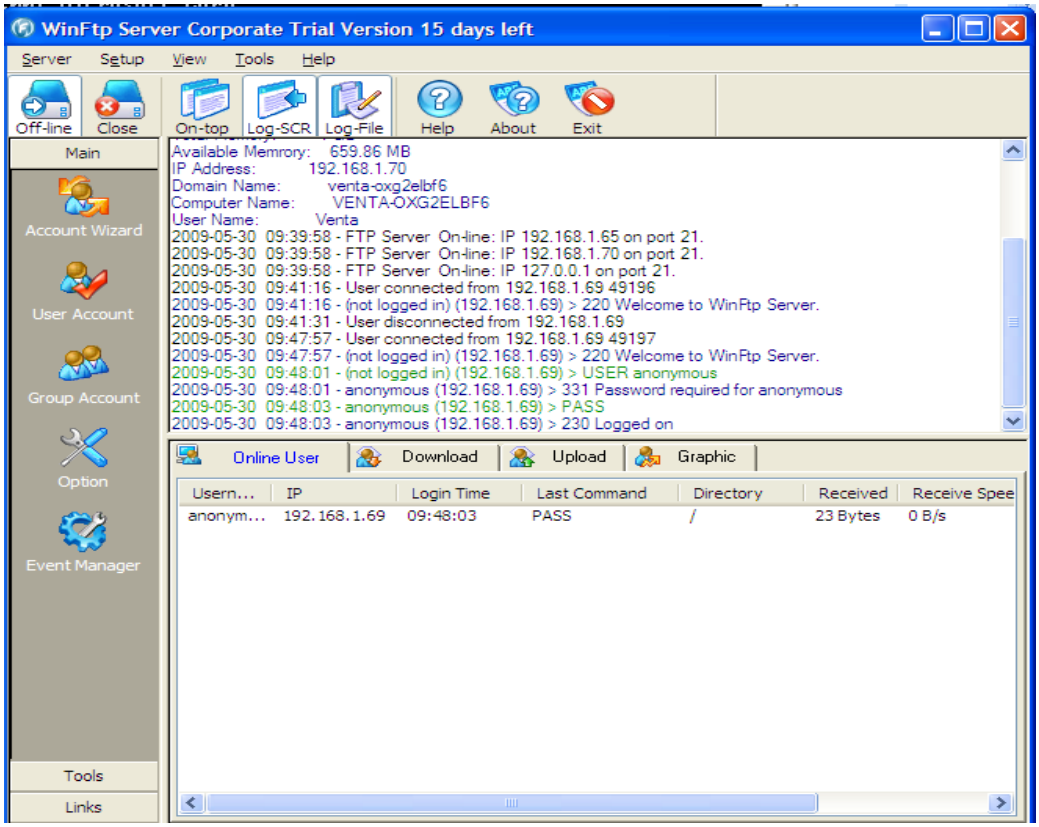
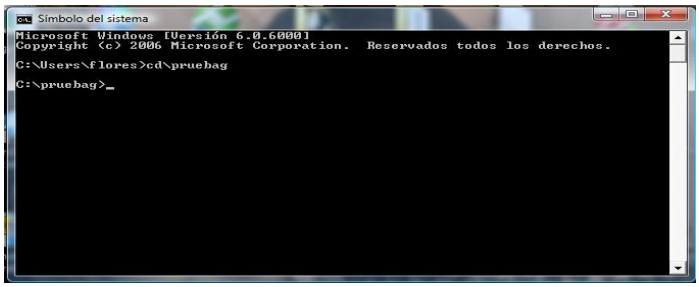


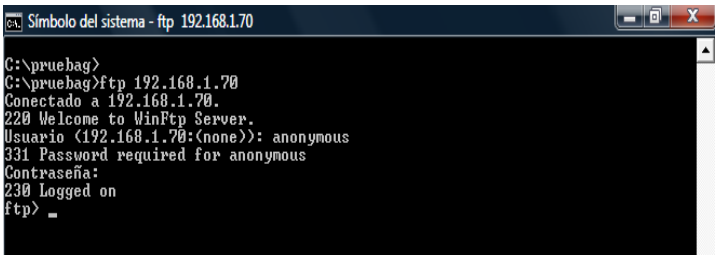
Figura 20.- Ventana de comandos del servidor WinFtp.

Para facilitar la transmisión del archivo se desactivó el firewall de Windows y se creó en la raíz de la carpeta C:\ de la terminal, una carpeta llamada *pruebag*, la cual sirvió de almacén para el archivo transmitido.

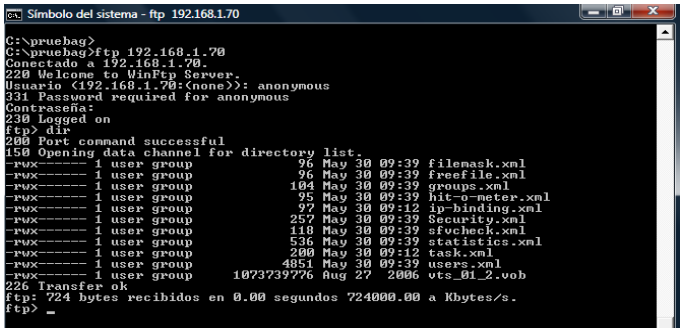
Estando en el símbolo del sistema (MS-Dos) se tecleó el comando *cd\pruebag* para acceder a la carpeta.



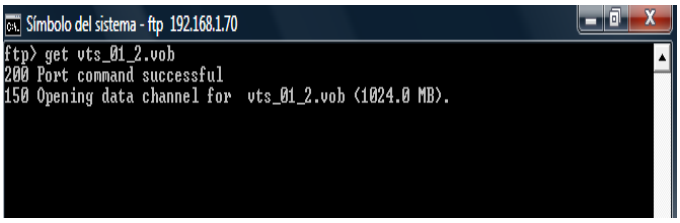
Posteriormente se accedió al servidor mediante el comando *ftp 192.168.1.70* esta dirección es la dirección IP del servidor. Como se había configurado una cuenta anónima se introdujo como usuario *anonymous* y sin contraseña. En seguida el servidor mandó el mensaje *Logged on*, lo que indicó que la terminal estaba conectada.



Se tecleó el comando *dir* para que el servidor mostrara el contenido de su directorio.



Se observó que efectivamente contenía el archivo que se deseaba transmitir a la terminal, por lo que se tecleó el comando *get vts_01_2.vob* para iniciar su transferencia.



Tercer prueba

Se deseaba saber en qué posición de cada una de las antenas del AP se lograba la máxima tasa de transmisión en capa Física. Para ello se movían las antenas a distintas posiciones mientras se monitoreaba la tasa de transmisión en el estado de la conexión y se realizaba la descarga de un video de www.youtube.com

5. Resultados

Primera prueba

Los resultados de la primera prueba usando IEEE 802.11 N se muestran en la siguiente tabla:

PUNTO DE PRUEBA	DISTANCIA [m]	SEÑAL [dB]	SNR	TASA DE TRANSMISIÓN [Mbps]
1	2.4	-30	70	130
2	10	-48	52	130
3	10	-61	39	117
4	10	-49	50	130
5	10	-68	32	104
6	10	-73	27	104
7	10	-61	39	130
8	50	-70	30	117
9	46	-82	18	26
10	50	-74	26	104
11	50	-71	29	117
12	50	-75	25	78
13	50	-64	36	13
14	50	-75	25	78
15	50	-60	40	130
16	100	-71	29	26
17	100	-70	30	78
18	116.6	-90	10	13
19	150	-64	36	13

Tabla 6.- Lecturas de intensidad de la señal, SNR y tasa de transmisión correspondientes a una distancia del punto de acceso utilizando IEEE 802.11 N

Los puntos de prueba 18 y 19 se tomaron con la finalidad de encontrar la máxima distancia de cobertura que brinda el AP que soporta IEEE 802.11 N.

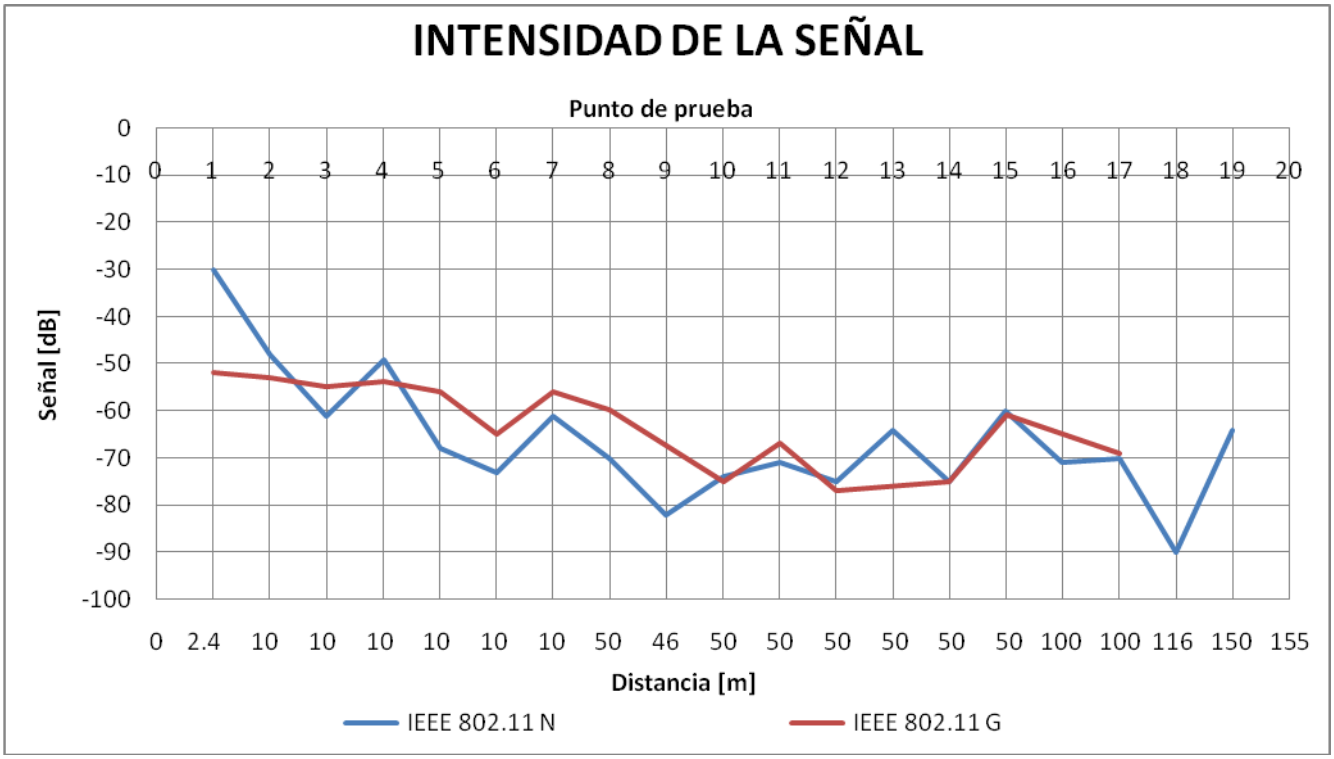
Se manejan los mismos puntos en ambas tablas a fin de poder compararlos uno a uno, no se tiene registro de algunos de éstos en la red INFINITUM6532 ya que en ellos la señal era muy débil y no se tenía conexión.

Los resultados de la primera prueba usando IEEE 802.11 G se muestran en la tabla de abajo:

PUNTO DE PRUEBA	DISTANCIA [m]	SEÑAL [dB]	SNR	TASA DE TRANSMISIÓN [Mbps]
1	2.4	-52	48	54
2	10	-53	47	54
3	10	-55	45	36
4	10	-54	49	54
5	10	-56	44	36
6	10	-65	35	36
7	10	-56	44	54
8	50	-60	40	32
10	50	-75	25	25
11	50	-67	33	36
12	50	-77	23	18
14	50	-75	25	22
15	50	-61	39	36
17	100	-69	31	18

Tabla 7.- Lecturas de intensidad de la señal, SNR y tasa de transmisión correspondientes a una distancia del punto de acceso utilizando IEEE 802.11 G

La siguiente gráfica muestra la intensidad de la señal de los puntos de prueba de las redes LabN e INFINITUM6532:

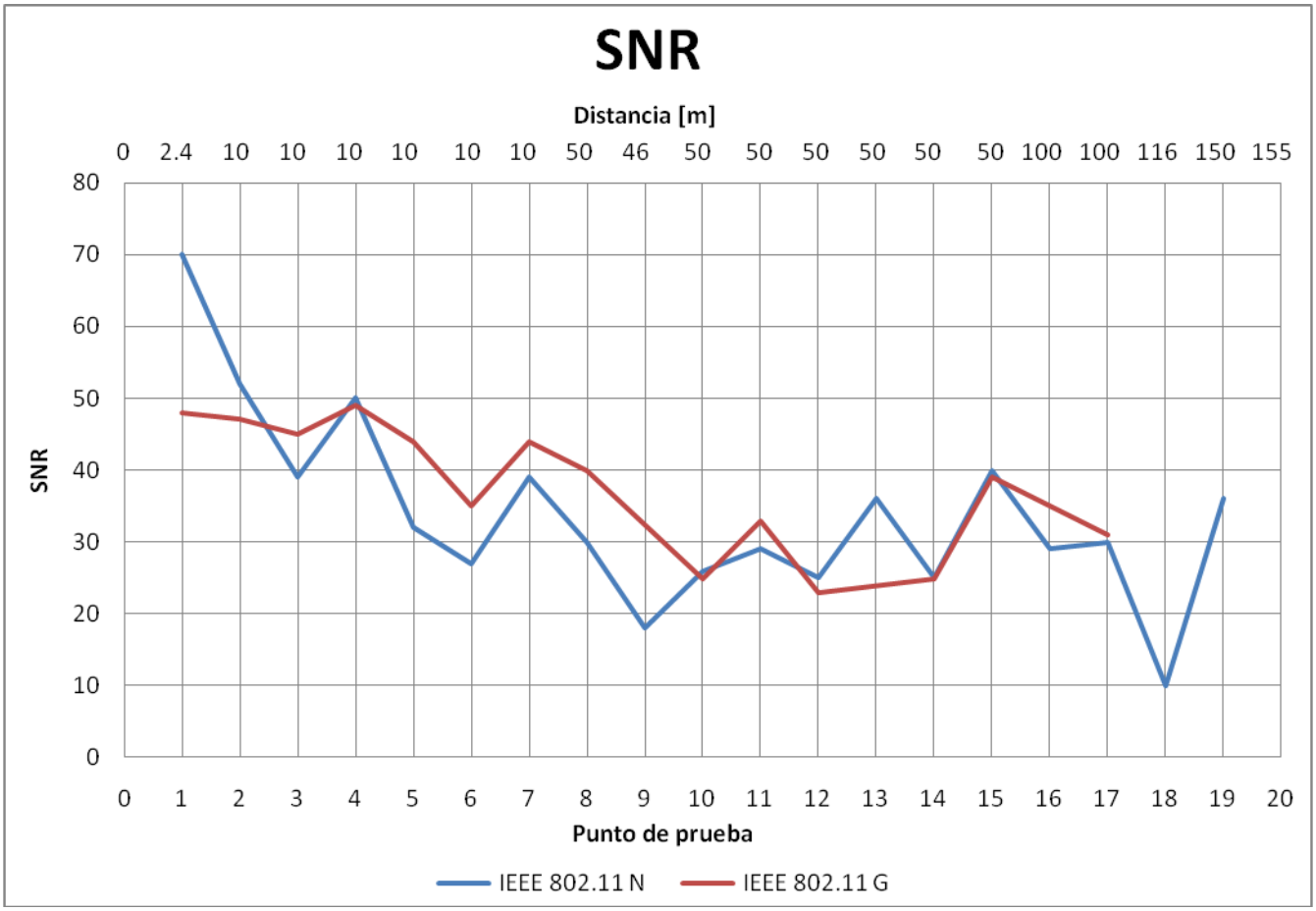


Gráfica 1.- Intensidad de la señal utilizando IEEE 802.11 G e IEEE 802.11 N

La gráfica anterior muestra que la intensidad de la señal es mayor para los puntos de prueba de la red INFINITUM6532, sin embargo, la región de cobertura disminuye notablemente al reflejarse la señal por presencia de un obstáculo, ya que no se pudo tener conexión en los puntos de prueba 9, 13 y 16.

En la misma gráfica se puede observar que utilizando la red LabN la región de cobertura no se ve tan afectada por la reflexión de la señal debida a la presencia de obstáculos, ya que se pudo tener conexión en los puntos de prueba 9, 13, 16 e incluso en el punto 18. El punto 19 muestra que con la tecnología que soporta IEEE 802.11 N se puede tener conexión a la red a una distancia máxima de 150 metros.

La siguiente gráfica muestra la SNR de los puntos de prueba de las redes LabN e INFINITUM6532:



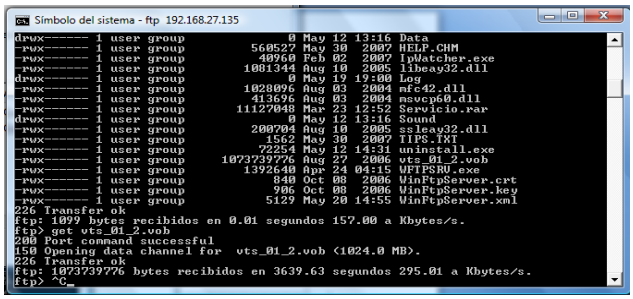
Gráfica 2.- SNR utilizando IEEE 802.11 G e IEEE 802.11 N

Existe una relación directamente proporcional entre la intensidad de la señal y la SNR, es por ello que sus gráficas son muy parecidas. En la gráfica de la intensidad de la señal se observa que en general la señal tiene una mayor

intensidad cuando se utiliza el estándar IEEE 802.11 G, lo que se refleja en un incremento en la SNR. Parecería que el estándar IEEE 802.11 G puede brindar mayores tasas de transmisión y una mayor cobertura que el protocolo IEEE 802.11 N, pero no es así. Hay que recordar que el protocolo IEEE 802.11 N utiliza las señales que se consideran perjudiciales para enviar información, en otras palabras, ocupa las señales de multitrayectoria para incrementar la tasa de transmisión y distancia de propagación.

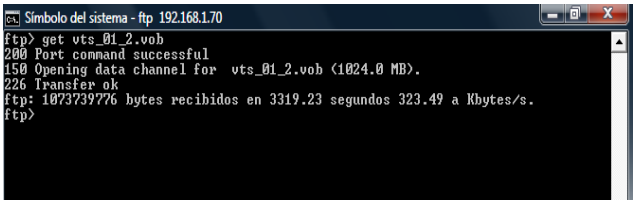
Segunda prueba

La tasa de transmisión en la capa de Aplicación utilizando la red LabN se muestra a continuación:



$$Tasa\ de\ transmisión = \frac{(1073739776)(8)}{3639.63}\left[\frac{bits}{s}\right] = 2.3601\left[\frac{Mbits}{s}\right]$$

La tasa de transmisión en la capa de Aplicación utilizando la red INFINITUM6532 se muestra en seguida:



$$Tasa\ de\ transmisión = \frac{(1073739776)(8)}{3319.23}\left[\frac{bits}{s}\right] = 2.5879\left[\frac{Mbits}{s}\right]$$

Los resultados de esta prueba no son los esperados, ya que indican que la transmisión de archivos utilizando FTP es más rápida sobre la red INFINITUM6532 que soporta IEEE 802.11 G en comparación con la red LabN que trabaja con IEEE 802.11N, no obstante, ambos resultados nos indican que la tasa de transmisión de archivos utilizando FTP en una WLAN es de aproximadamente 2 Mbps.

La razón del comportamiento anterior es debido a que se realizó la prueba de transmisión de FTP utilizando la red LabN y al mismo tiempo otros usuarios estaban utilizando el ancho de banda del canal pues sus terminales tenían integradas tarjetas de red que podían recibir la señal. Por el contrario, al momento de realizar la misma prueba con la red INFINITUM6532 sólo se tenía la terminal que se uso para dicha prueba, lo que provocó que hubiera una mayor tasa de transmisión.

Tercera prueba

- Protocolo de comunicaciones IEEE 802.11 N

Después de haber colocado las antenas del AP en diferentes posiciones y haber obtenido la tasa de transmisión en cada una de ellas, se observó que la máxima tasa de transmisión era de 270 Mbps y se tenía dentro de un radio de 0.3 m alrededor del AP para cualquiera de las dos siguientes configuraciones de las antenas:

Figura 21.- Posición vertical del AP, posición de sus antenas y tasa de transmisión.

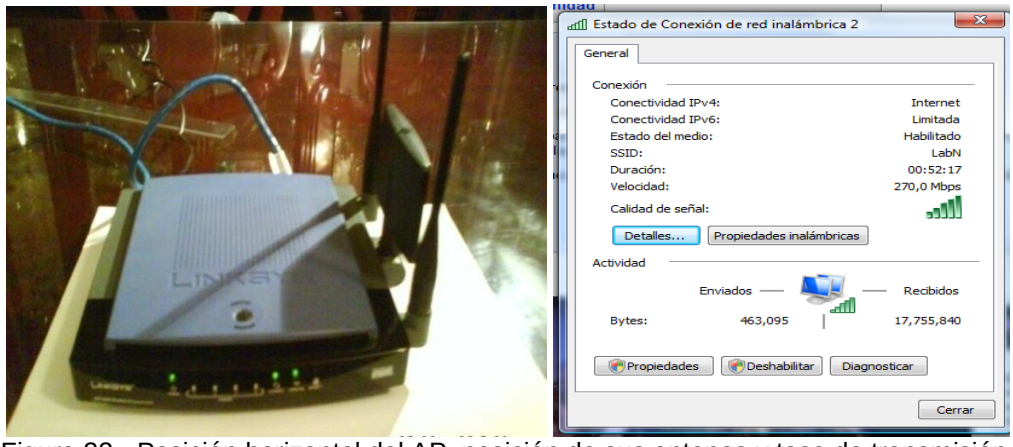


Figura 22.- Posición horizontal del AP, posición de sus antenas y tasa de transmisión.

Se observó que existe una ligera ventaja al utilizar la posición horizontal del AP ya que los dispositivos tienen una mejor LOS y la tasa de transmisión no varía al desplazar la terminal dentro del radio de cobertura de 0.3 metros.

La máxima tasa de transferencia fue de 270 Mbps debido a que la prueba se realizó con línea de vista entre el transmisor y el receptor. El protocolo de comunicaciones IEEE 802.11 N utiliza las reflexiones de la señal en distintas trayectorias para aumentar la tasa de transmisión y la distancia de propagación.

Como se puede observar en las fotografías anteriores, los objetos (a excepción de la mesa) se encontraban mínimo a una distancia de 1.5 m y si colocáramos múltiples objetos reflejantes a una distancia menor y en todas direcciones, seguramente las señales reflejadas tendrían un menor tiempo de retardo y una mayor intensidad dado que no recorrerían una larga distancia, de esta manera se aumentaría la tasa de transmisión hasta los 300 Mbps.

- Estándar de comunicaciones IEEE 802.11 G

La máxima tasa de transmisión que se tuvo con el AP que soporta esta versión fue de 54 Mbps y no se pudo manipular la posición de su antena debido a que se encontraba en su interior.

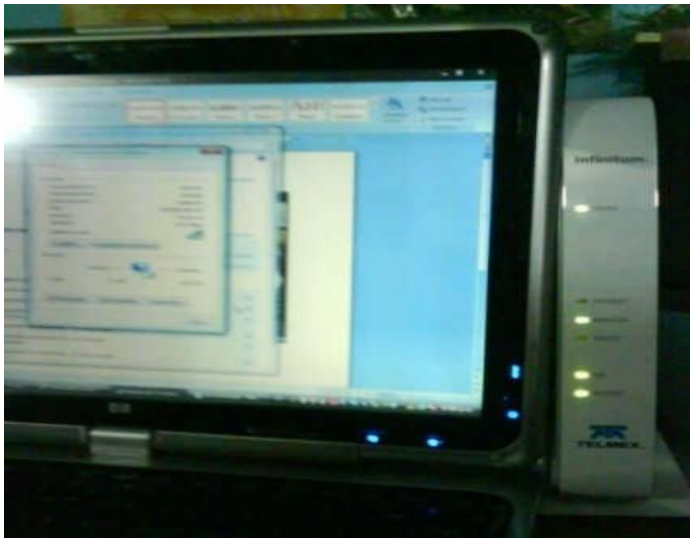
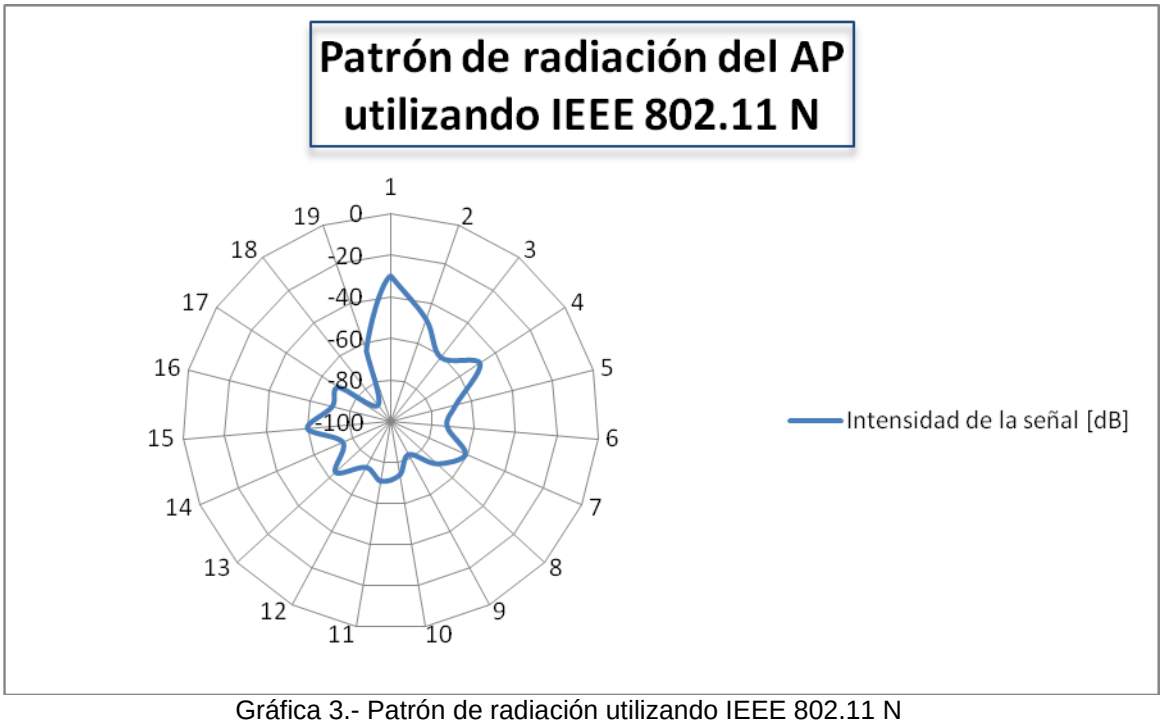


Figura 23.- Posición vertical del AP que soporta IEEE 802.11 G

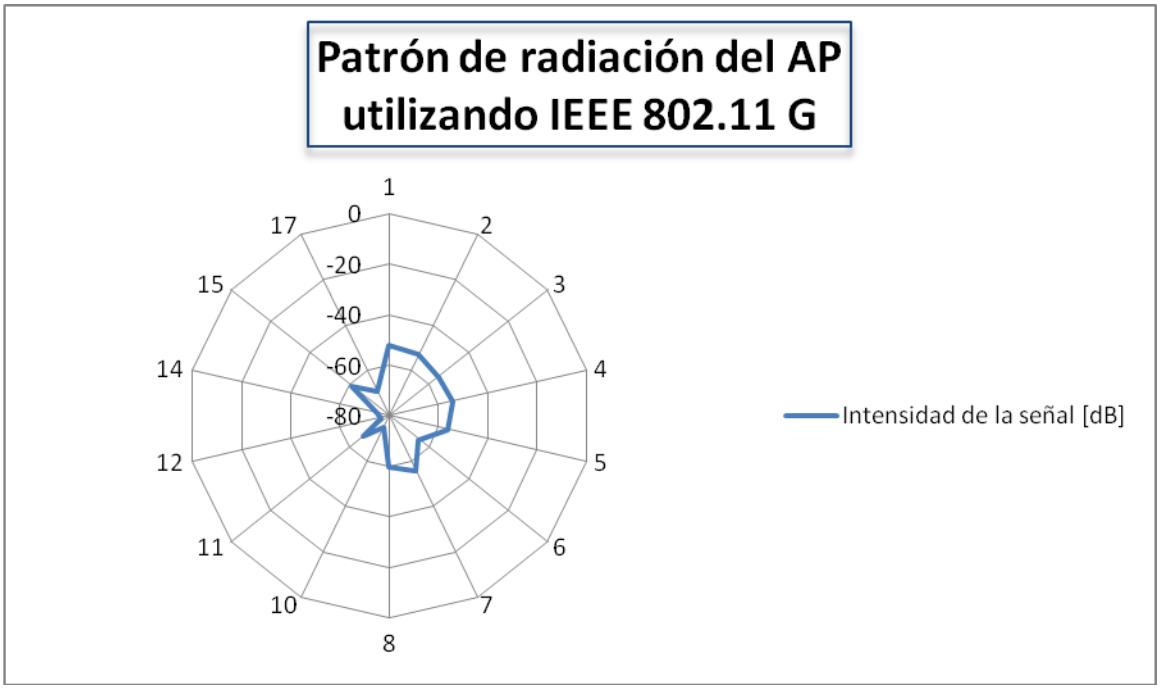
La ventaja de utilizar la versión N del estándar IEEE 802.11 es que debido a que se tiene un mayor número de antenas, se puede aumentar hasta 5 veces la tasa de transmisión que se tiene con la versión G.

5.1. Gráfica del patrón de radiación

A continuación se muestran las gráficas de los patrones de radiación de los AP que soportan las versiones N y G del estándar IEEE 802.11



Gráfica 3.- Patrón de radiación utilizando IEEE 802.11 N



Gráfica 4.- Patrón de radiación utilizando IEEE 802.11 G

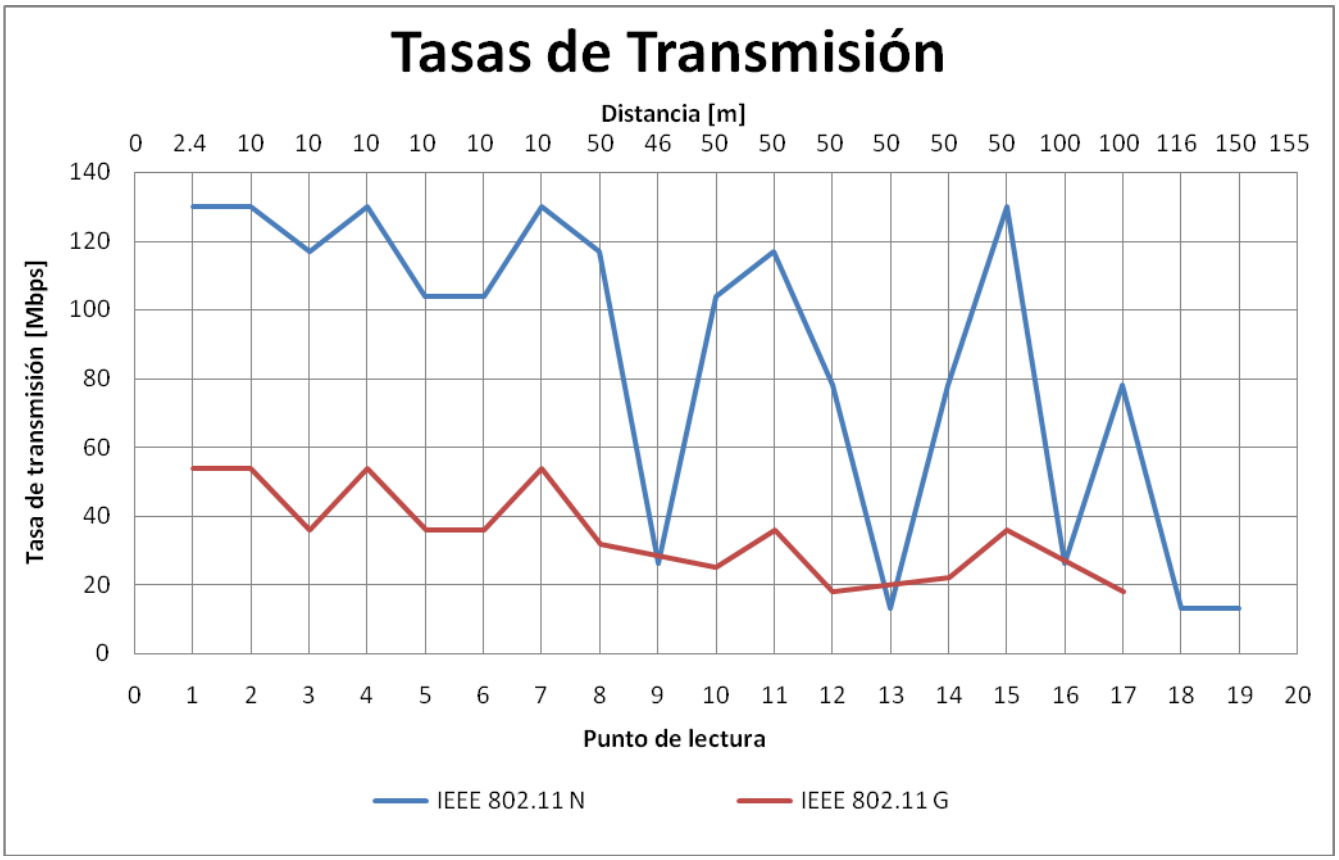
Ambos patrones de radiación no se muestran uniformes debido a los obstáculos que desviaban o impedían el paso de la señal.

Comparando ambos patrones de radiación se observó que la intensidad de la señal en el punto de prueba 1 es mucho mayor si se usa IEEE 802.11 N, además que la señal se propaga a una mayor distancia si se usa este protocolo.

Por el contrario, se observó que en general el estándar IEEE 802.11 G ofrece una mejor intensidad de la señal dentro de un radio de cobertura de 10 m que el protocolo N del mismo estándar.

5.2. Gráfica de tasa de transmisión

Enseguida se muestran las gráficas de la tasa de transmisión en capa Física de las redes LabN e INFINITUM6532 que soportan las versiones N y G del estándar IEEE 802.11 respectivamente:



Gráfica 5.- Tasas de transmisión en capa Física utilizando IEEE 802.11 G e IEEE 802.11 N

La gráfica anterior indica que la tasa de transmisión que proporciona la versión N del estándar 802.11 en cada uno de los puntos de prueba es al menos 2.4 veces mayor que la que brinda IEEE 802.11G, debido a que se usa un mayor número de antenas para la transmisión de información y se emplea la técnica MIMO para aprovechar las reflexiones de la señal.

6. Conclusiones

6.1. Contribuciones

Esta tesis proporciona una descripción del funcionamiento y comportamiento real del protocolo de comunicaciones IEEE 802.11 N que tiene hasta este momento. Asimismo, muestra su desempeño en cuanto a tasas de transmisión y distancias de propagación con respecto al estándar de comunicaciones IEEE 802.11 G.

6.2. Conclusiones generales

Al comparar los resultados de las pruebas de intensidad de la señal, SNR, tasa de transmisión en capa Física y tasa de transmisión en capa de Aplicación realizadas con los dispositivos que soportan el estándar IEEE 802.11 G y el protocolo IEEE 802.11 N, se observó que aunque la intensidad de la señal y la SNR sean mayores al utilizar el estándar IEEE 802.11 G, el protocolo IEEE 802.11 N permite una mayor área de cobertura y un incremento en la tasa de transmisión ya que utiliza la tecnología MIMO para dividir la información y transmitirla por sus antenas, y aprovecha las señales de multitrayectoria con buena intensidad para transmitir paquetes de información.

El comportamiento del protocolo IEEE 802.11 N es mejor que el estándar IEEE 802.11 G, sin embargo, el costo de los dispositivos que soportan el protocolo de comunicaciones IEEE 802.11 N es elevado porque no existe mucha demanda en éstos.

Actualmente los dispositivos que soportan el protocolo de comunicaciones IEEE 802.11 N son hasta 5 veces más rápidos que los dispositivos que soportan el estándar IEEE 802.11 G y no tardará mucho en darse a conocer el borrador final de esta versión, lo que llevará a su estandarización y seguramente sólo habrá cambios en el software de los dispositivos que lo soportan, es por ello que no es riesgoso adquirirlos en este momento.

La nueva versión del estándar IEEE 802.11 tiene como objetivo brindar al usuario la opción de obtener mayores tasas de transmisión, mayor seguridad y una mayor región de cobertura, reduciendo así el número de puntos muertos (áreas sin cobertura) tanto en el hogar como en la empresa y por nada pretende sustituir los dispositivos que soportan versiones anteriores, ya que es compatible con ellos.

7. Anexos

7.1. Glosario

IEEE 802.11 Familia de estándares que especifican las características a nivel capa Física y MAC para una WLAN.

Ad hoc Modo de operación de una red inalámbrica en la que no hay AP, para que las terminales se puedan comunicar tienen que estar dentro de su rango de cobertura.

AP Punto de Acceso, es un dispositivo cuyo papel es crear una red inalámbrica y permitir a las terminales que se encuentran dentro de su área de cobertura el acceso a la red.

Bluetooth Tecnología que usa la frecuencia de 2.4 GHz para brindar conexión inalámbrica de corto alcance entre laptops, teléfonos inalámbricos y otros. Pertenece al estándar IEEE 802.15.

CDMA Acceso Múltiple por División de Código, es una técnica de acceso múltiple al medio, en la cual las terminales móviles usan la totalidad del espectro disponible durante todo el tiempo gracias a que cada una usa un código ortogonal.

CRC Código de Redundancia Cíclica, es un método utilizado para verificar errores en una trama que ha sido transmitida.

CSMA/CA Acceso Múltiple por Detección de Portadora con Evasión de Colisiones. Algoritmo que define el estándar IEEE 802.11 cuando se usa DCF.

DCF Función de Coordinación Distribuida, es la forma de control de acceso al medio donde no hay AP y se usa CSMA/CA como protocolo de acceso aleatorio al medio.

DFS Selección de Frecuencia Dinámica, es una función implementada en los AP que operan en 5 GHz para seleccionar el canal, en el cual se produzca la mínima interferencia con otros sistemas de comunicaciones.

DIFS Espacio Corto Entre Trama de la Función de Coordinación Distribuida.

Dirección MAC Dirección de Control de Acceso al Medio, identificador de la tarjeta de red que consiste en un conjunto de 48 bits agrupados en cuatro y representados en forma hexadecimal. Los primeros 6 dígitos identifican al fabricante y los últimos 6 identifican a la tarjeta en particular.

DSSS Espectro Disperso por Secuencia Directa, es una técnica para el esparcimiento de la potencia de la señal sobre una banda de frecuencias y consiste en generar una cadena de 11 bits por cada bit de información.

ETSI Instituto Europeo de Normas de Telecomunicaciones, es una asociación sin fines de lucro que se encarga de la estandarización de las tecnologías de la información en Europa.

FDMA Acceso Múltiple por División de Frecuencia, es una técnica de acceso múltiple al medio y consiste en que la porción de espectro disponible se divide en bandas más pequeñas y cada una de estas es asignada a un usuario para que transmita.

FHSS Espectro Disperso por Salto de Frecuencia, es una técnica para el esparcimiento de la potencia de la señal sobre una banda de frecuencias y consiste en transmitir en una frecuencia durante un intervalo de tiempo y posteriormente cambiarse de frecuencia para seguir transmitiendo.

Fragmento Porción o parte de una trama. La fragmentación es empleada para aumentar la probabilidad de que las tramas lleguen sin errores a su destino.

FTP Protocolo de Transferencia de Archivos, protocolo de la capa de Aplicación del modelo TCP/IP que permite la transferencia de archivos de todo tipo entre terminales remotas.

GPRS Servicio General de Paquetes vía Radio, brinda la transmisión de información mediante la conmutación de paquetes a usuarios GSM.

GSM Sistema Global para las Comunicaciones Móviles, es un estándar para teléfonos móviles digitales que brinda los servicios de voz, datos, mensajes de texto y acceso a internet.

Handoff Proceso mediante el cual una terminal móvil se cambia de AP debido a que la potencia y calidad de la señal son insuficientes para la comunicación.

HiperLAN Estándar de comunicaciones inalámbricas desarrollado por la ETSI que contiene las especificaciones técnicas para una WLAN.

HiperMAN Estándar de comunicaciones inalámbricas desarrollado por la ETSI que contiene las especificaciones técnicas para una WMAN.

Home RF Es una tecnología que brinda conexión inalámbrica entre periféricos y computadoras.

IEEE Son las siglas del Instituto de Ingenieros Eléctricos y Electrónicos, es una asociación sin fines de lucro que se encarga de aplicar los avances en las tecnologías de la información.

IEEE 802.11 G Estándar de comunicaciones inalámbricas que desarrolla las especificaciones técnicas para una WLAN, usa la frecuencia de 2.4 GHz y alcanza hasta 54 Mbps.

IEEE 802.11 N	Protocolo de comunicaciones inalámbricas que desarrolla las especificaciones técnicas para una WLAN, usa las frecuencias de 2.4 y 5 GHz y alcanza hasta 300 Mbps.
IEEE 802.15	Estándar de comunicaciones inalámbricas que desarrolla las especificaciones técnicas para una WPAN.
IEEE 802.16	Estándar de comunicaciones inalámbricas que desarrolla las especificaciones técnicas para una WMAN.
LOS	Línea De Vista, este término se refiere a que la trayectoria de la señal que va del transmisor al receptor debe ser directa y no tener obstáculos que impidan su paso.
MIMO	Múltiples Entradas- Múltiples Salidas, tecnología de radiocomunicación que divide la información en paquetes más pequeños y los transmite por distintas antenas multiplexándolos en un mismo canal y al mismo tiempo.
Multitrayectoria	Propagación de la señal por distintas trayectorias debido a la reflexión de la misma sobre algunos objetos.
OFDM	Multiplexación por División de Frecuencias Ortogonales, es una técnica de acceso múltiple al medio, la cual divide la porción del espectro disponible en un conjunto de portadoras o canales a través de los cuales se manda la información segmentada.
PCF	Función de Coordinación Puntual, es la forma de control de acceso al medio donde el AP es el que permite o rechaza el acceso a las terminales.
PDA	Asistente Digital Personal, hoy día se le conoce como Palm. Es una computadora de bolsillo que puede conectarse a una WPAN o incluso a una WLAN.
Periodo de contención	Intervalo de tiempo durante el cual todas las terminales compiten por el acceso al canal para realizar su transmisión.
PIFS	Espacio Corto Entre Trama de la Función de Coordinación Puntual.
Protocolo	Conjunto de reglas que se deben seguir por los elementos de la red para poder comunicarse.
PSK	Clave Inicial Compartida, variante de las técnicas de seguridad WPA y WPA2 en la cual las terminales y los AP utilizan una misma clave.
QoS	Calidad de Servicio, término que se refiere a la garantía de entregar una cantidad de datos en un determinado tiempo.
RADIUS	Servicio de Autenticación Remota de los Usuarios. Protocolo que brinda las funciones de autenticación, autorización y registro del tiempo que las terminales han estado conectadas a la red.
Región de cobertura	Zona dentro de la cual la potencia y calidad de la señal hacen posible la comunicación.

RFID Identificación por Radio Frecuencia, es un sistema que usa las frecuencias que van desde los 125 kHz hasta los 2.4 GHz para transmitir de forma automática la identidad de un objeto.

RTS/CTS Es un mecanismo usado por el estándar 802.11 para reservar el canal y reducir las colisiones entre tramas.

SIFS Espacio Corto Entre Trama.

SNR Relación Señal a Ruido, parámetro que ayuda a conocer la proporción del ruido presente en la señal y se define como el cociente de la intensidad de señal deseada entre la suma de las intensidades de las señales indeseadas o ruido.

SSID Identificador de Conjunto de Servicio o nombre de la red, es un código de 32 caracteres alfanuméricos que contienen los paquetes de una red y los identifican como miembros de la misma.

Tasa de transmisión Cantidad de bits que se transmiten por unidad de tiempo en un sistema de comunicaciones.

TCP/IP Protocolo de Control de Transmisión/Protocolo de Internet, conjunto de protocolos de red que sirven para comunicar terminales de distintas redes y hacerles llegar los datos en orden, sin pérdidas y sin errores.

TDMA Acceso Múltiple por División de Tiempo, es una técnica de acceso múltiple al medio y consiste en que la porción de espectro disponible se divide en pocos canales los cuales son divididos en múltiples ranuras de tiempo y cada una de éstas es asignada a un usuario para que transmita.

Terminal Dispositivo que se puede comunicar con otro o con el AP de forma inalámbrica y usando los recursos de la red.

TPC Control de Potencia de Transmisión, es una función implementada en los AP que operan en 5 GHz para utilizar la mínima potencia de transmisión para el usuario más lejano y evitar interferencias con otros sistemas.

Trama Conjunto de bits que son transmitidos como una unidad.

UMTS Sistema Universal de Telecomunicaciones Móviles, permite aplicaciones en tiempo real en teléfonos móviles y computadoras portátiles en cualquier parte del mundo.

WAVE Acceso Inalámbrico de Ambiente Vehicular, es el nombre para el borrador IEEE 802.11 p, el cual brindará comunicación inalámbrica entre vehículos en movimiento para reducir accidentes y congestionamientos en las carreteras.

WEP Privacidad Equivalente a Cableado, es una técnica de seguridad para redes inalámbricas que utiliza una misma clave para las terminales y para los AP.

Wi-Fi Nombre comercial para el estándar IEEE 802.11. Desarrolla la interoperabilidad entre los productos que lo soportan.

WiMAX Nombre comercial para el estándar IEEE 802.16. Desarrolla la interoperabilidad entre los productos que lo soportan.

WLAN Red de Área Local Inalámbrica, transmite y recibe datos entre sus elementos utilizando ondas electromagnéticas que utilizan el aire como medio de transmisión. Su radio de cobertura es de unos cientos de metros.

WMAN Red de Área Metropolitana Inalámbrica, transmite y recibe datos entre sus elementos utilizando ondas electromagnéticas que utilizan el aire como medio de transmisión. Su radio de cobertura es de varios kilómetros.

WPA Acceso protegido Wi-Fi, es una técnica de seguridad para redes inalámbricas que utiliza una clave diferente para cada terminal, la cual distribuye de forma automática en la red.

WSN Red de Sensores Inalámbrica que contiene un conjunto de dispositivos inalámbricos desplegados en una región para medir una variable en particular, por ejemplo la humedad.

WWAN Red de Área Extensa Inalámbrica, transmite y recibe datos entre sus elementos utilizando ondas electromagnéticas que utilizan el aire como medio de transmisión. Su radio de cobertura es de varios cientos de kilómetros.

XOR OR - exclusiva, función lógica cuya ecuación es:

$$F = X\bar{Y} + \bar{X}Y$$

Zigbee Conjunto de protocolos para comunicaciones inalámbricas en una WSN.

7.2. Router de banda ancha Wireless-N WRT300N

Características:

- Tecnología MIMO
- Compatible con Banda B y G
- Switch 4 Puertos Full-Duplex 10/100, Internet: 1 puerto de 10/100 RJ-45. (ABA) (4 Puertos RJ45 libre + 1 Puerto para línea de entrada)
- Velocidad de Transmisión de 11Mbps, 54Mbps, 108Mbps, 300Mbps.
- Mayor Alcance que los Router Linksys WRT54G
- QoS, puede definir qué velocidad o prioridad se le da a cada aplicación o puertos.
- Filtro por palabras o paginas, puede bloquear para todos o algunos usuarios los sitios que no deben visitar.
- Firewall Interno, protege su red de Instrusos.
- Acepta Conexiones VPN.
- Característica de Seguridad WPA, WPA2, 802.1x, WEP, and Wireless MAC Filtering

7.3. Adaptador para ordenador portátil Wireless-N WUSB300N

Características:

- Éstandares: IEEE 802.11b, IEEE 802.11g, Draft IEEE 802.11n, USB 1.1, USB 2.0
- Puertos: Puerto USB
- LEDs: Power, Link/Act
- Modulación:
  802.11b: CCK, QPSK, BPSK
  802.11g: OFDM
  Wireless-N: BPSK, QPSK, 16-QAM, 64-QAM
- Potencia de transmisión:
  802.11b: 14±1dBm (Typical)
  802.11g: 14±1dBm (Typical)
  Wireless-N: 14±1dBm (Typical)
- Sensibilidad de recepción:
  11Mbps @ -86dBm (Typical)
  54Mbps @ -68dBm (Typical)
  Wireless-N @ -62dBm (Typical)
- Consumo:
  TX: <480mA (Max)
  RX: <390mA (Max)
- Características de Seguridad: WEP, WPA and WPA2 Encryption Security
- Security key bits: Up to 256-bit encryption
- Dimensiones: 57mm x 10mm x 101mm
- Peso: 0.029 kg
- Certificaciones: FCC, Wi-Fi (802.11b/g)
- Temperatura Operativa: 0º C ~ 55º C (32º F ~ 131º F)
- Temperatura almacenaje: -20º C ~ 80º C (-4º F ~ 176º F)

7.4. Referencias

[1] Liljana Gavrilosvska et al. Ad Hoc Networking Towards Seamless Communications. Springer. 2006

[2] Aftab Ahmad. Wireless And Mobile Data Networks. Wiley Interscience. New Jersey 2005

[3] Petros Nicopolitidis et al. Wireless Networks. Wiley Interscience. 2003

[4] Andreas F. Molish. Wireless Communications. Wiley Interscience. 2005

[5] William Stallings. Comunicaciones y redes de computadores. Pearson Educación. Séptima edición. 2004

[6] Cisco Systems, Inc. Academia de Networking de Cisco Systems. Guía del primer año. CCNA® 1 y 2. Tercera edición. Pearson Educación, 2004

[7] Computer Networks. Andrew S. Tanenbaum. Prentice Hall. Third Edition. 1996

[8] 802.11 IEEE Standard for Local and metropolitan area networks. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[9] Thomas Paul and Tokunbo Ogunfunmi. Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amendment. IEEE Circuits and systems magazine. First Quarter 2008.

[10] http://en.wikipedia.org/wiki/802.11

[11] http://technet.microsoft.com/es-es/library/cc784756.aspx

[12] http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf

[13] http://en.wikipedia.org/wiki/List_of_WLAN_channels

[14] http://technet.microsoft.com/en-us/library/cc757419(WS.10).aspx

[15] http://www.arubanetworks.com/pdf/technology/whitepapers/wp_80211n_sp.pdf