VNIVERSIDAD NACIONAL AVTÓNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRIA Y DOCTORADO EN INGENIERIA

FACULTAD DE INGENIERIA

MODELADO DE LA RED DE COMUNICACIÓN INALÁMBRICA PARA EL SOPORTE DE VoIP EN LA LINEA 1 DEL STC METRO.

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN INGENIERIA

INGENIERIA ELECTRICA - TELECOMUNICACIONES

P R E S E N T A:

JESÚS ALEJANDRO FLORES RAMIREZ

TUTOR:

DR. VICTOR RANGEL LICEA

2012

JURADO ASIGNADO:

Presidente:	DR. RAMÓN GUTIÉRREZ CASTREJÓN
Secretario:	DR. JAVIER GÓMEZ CASTELLANOS
Vocal:	DR. VÍCTORRANGEL LICEA
1$^{er.}$ Suplente:	DR. MIGUEL MOCTEZUMA FLORES
2$^{do.}$ Suplente:	DR. VÍCTORGARCÍA GARDUÑO

Lugar donde se realizó la tesis: MÉXICO, D.F.

TUTOR DE TESIS:

DR. VICTOR RANGEL LICEA

_____

FIRMA

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 y a mi hijo Alejandro,
por ser mis nuevos compañeros,
por impulsarme a alcanzar mis metas y
por estar a mi lado en todo momento.

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

Jesús Alejandro

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México por brindarme una excelente formación académica, profesional y humana.

Al posgrado de Ingeniería de la UNAM por abrirme sus puertas y permitirme extender mis conocimientos.

Al Doctor Víctor Rangel Licea por ser el guía en la realización de este trabajo de tesis, por su comprensión y apoyo recibido.

Al Dr. Víctor García Garduño, Dr. Miguel Moctezuma Flores, Dr. Javier Gómez Castellanos y Dr. Ramón Gutiérrez Castrejón, por brindarme sus conocimientos y su apoyo en estos años.

Gracias a la DGAPA-UNAM por el apoyo otorgado para la realización de este trabajo a través del proyecto PAPIIT IN108910 “Diseño de algoritmos de reservación de capa cruzada en redes móviles y mesh de banda ancha”.

Gracias al CONACYT por el apoyo brindado a través del proyecto 105279 “Diseño de técnicas de reservación de capacidad de redes BWA móviles”.

Jesús Alejandro

INDICE DE CONTENIDO

INDICE DE FIGURAS

Capitulo 2

Capitulo 3

Capitulo 4

Capitulo 5

Capitulo 6

INDICE DE TABLAS

Capitulo 3

Capitulo 4

Capitulo 6

CAPÍTULO 1

Introducción

1.1 Antecedentes

El Sistema de Transporte Colectivo Metro (STC Metro)[1], es un organismo público descentralizado cuya tarea principal es el transporte masivo de personas en el Distrito Federal y una pequeña parte de sus alrededores. La red del STC Metro es un conjunto de 11 líneas que acumulan un total de 175 estaciones de las cuales 106 son estaciones subterráneas, 53 superficiales y 16 elevadas.

El servicio es prestado los 365 días del año y a través de sus 240 km. de longitud, el STC logra transportar a más de 4.8 millones de usuarios diariamente, utilizando para ello alrededor de 355 trenes que funcionan con energía eléctrica.

Este gran sistema de transporte colectivo cuenta con personal de seguridad propio y es auxiliado por elementos de seguridad pública, sin embargo los usuarios superan en número a los elementos de seguridad considerablemente. Por esta razón el STC es escenario diario del abuso a los propios usuarios y el ambulantaje.

El STC utiliza una red de comunicaciones basada en telefonía cableada, la cual ya no satisface sus necesidades y es causa de contratar una costosa red de telefonía celular para un sector muy limitado. Esto ocasiona dejar incomunicado a un gran número de personal y técnicos que requieren de este servicio.

[1] Todas las abreviacionestécnicas están incluidas en el apartado “glosario”.

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. Características que les han permitido ser más cómodos y transportarles con facilidad.

Para contrarrestar el problema actual del deficiente sistema de comunicaciones del STC, se tiene planeado implementar una red para la transmisión de voz, datos y video que utilice el estándar IEEE 802.11. Esta tecnología define las características de una WLAN (Wireless Local Area Network), la cual permite la trasmisión de información de manera inalámbrica desde un par hasta decenas de metros.Este tipo de red inalámbrica utiliza las bandas de frecuencia de uso libre del espectro radioeléctrico ubicadas alrededor de 2.4 y 5 GHz.

Existen distintas versiones del estándar de comunicaciones IEEE 802.11 (WiFi). Dos de las más importantes son la versión*g*, que es la más popular en nuestros días y la versión *e*, la cual logra que las WLAN proporcionen QoS (Quality of Service) para datos, voz y video.

En los últimos años el desarrollo de las redes de comunicaciones ha crecido a pasos agigantados, logrando así, que las redes de comunicaciones puedan implementar la transmisión de voz en tiempo real usando el protocolo IP (Internet Protocol).

El transmitir voz sobre redes que utilizan el protocolo IP recibe el nombre de VoIP (Voiceover IP) o voz sobre IP. A diferencia de la transmisión de voz mediante la conmutación de circuitos eléctrico-electrónicos como el que utiliza el servicio de telefonía local, VoIP transmite paquetes de voz a través de una red de conmutación de paquetes. Este mecanismo tiene dos ventajas considerables sobre la transmisión de voz utilizando la conmutación de circuitos [3]:

- ✓ Ahorro en el costo en la transmisión de voz a larga distancia. Ya que no importa qué tan lejos se encuentren los dispositivos que entablan comunicación.

- ✓ Costo reducido de inversión. Debido a que los servicios de voz y datos se soportan sobre la misma red y no hay que contratar dichos servicios por separado.

1.2 Definición del problema

El sistema actual de comunicaciones del STC Metro ya no satisface del todo sus necesidades, en su momento la red de telefonía cableada era suficiente para brindar el servicio de transmisión de voz.

Sin embargo, en nuestros días el STC Metro demanda un sistema de comunicaciones propio que cubra sus necesidades en cuanto a la transmisión fiable, rápida y en todo momento no solo de voz, también de datos, imágenes y video.

El STC Metro necesita brindar más seguridad a sus usuarios, monitorear sus instalaciones de forma remota para detectar, evitar e identificar a las personas que realicen actividades ilícitas dentro de su infraestructura. Asimismo, necesita disminuir las fallas y los accidentes dentro de su red de transporte, como también brindar auxilio de manera inmediata a quién así lo requiera.

Este sistema de transporte cuenta con el apoyo de personal altamente capacitado para atender cualquiera de los incidentes mencionados anteriormente. No obstante tiene un gran problema. Debido a que posee una enorme infraestructura no tiene forma inmediata de saber si algún suceso se presenta en túneles, estaciones, andenes, pasillos y sobre todo carece de algún medio eficiente para alertar a su personal y usuarios.

La comunicación utilizando radiofrecuencia se limita principalmente por las características de la propagación de las ondas en el medio en el que viajan. La red del STC Metro consta en su mayoría de una estructura de metal cubierta con concreto, lo que se aproxima a un medio de propagación de guía de onda circular y rectangular.

Dentro de los túneles del metro las ondas de radiofrecuencia se propagan por reflexión múltiple o multitrayectoria lo que les ocasiona desfase y atenuación, como consecuencia de estos fenómenos se presenta la pérdida de información.

En resumen, el STC Metro necesita de una red de comunicación que esté al alcance de todo su personal, que sea eficiente, que sea de bajo costo tanto de implementación como de mantenimiento, que sea fácil de operar y sobre todo que sea de su propiedad.

1.3 Objetivos y metas

Se persigue como objetivo el modelar la red de comunicación para la línea uno del Sistema de Transporte Colectivo Metro, y así obtener el comportamiento esperado del throughput, retardo y utilización de los enlaces al transportar distintos tipos de tráfico como son: voz sobre IP, datos y video.

Asimismo, se pretende proporcionar un modelo que permita saber, entre otras cosas, la cantidad de tiempo necesaria para que un usuario se cambie de un AP (Access Point) a otro punto de acceso que se encuentre dentro del mismo dominio. Esto se conoce como un Handoff de capa 2.

Del mismo modo, se pretende proporcionar un segundo modelo que permita saber, entre otros aspectos, la cantidad de tiempo necesaria para que un dispositivo se cambie de un AP a otro AP que no se encuentre dentro del mismo dominio. Esto se conoce como un Handover de capa 3.

1.4 Contribuciones

Esta tesis proporciona una descripción del funcionamiento y comportamiento real del protocolo de comunicaciones IEEE 802.11. Modela el comportamiento de la red de comunicaciones basada en un ambiente de propagación vehicular. La cual soporta entre otras cosas QoS, VoIP y es capaz de llevar a cabo el Handoff de un usuario móvil entre dos APs pertenecientes a un mismo dominio y a diferentes dominios de red, utilizando para ello bandas no licenciadas del espectro radioeléctrico.

Los resultados de esta tesis pueden ser tomados en cuenta para el diseño e implementación de la red de comunicación inalámbrica para el soporte de VoIP en la línea 1 del STC metro.

1.5 Estructura de la tesis

El contenido del presente trabajo se organiza como sigue: en el segundo capítulo se describe lo que hasta el momento se ha publicado en fuentes de información confiables acerca de redes inalámbricas de área local, desempeño del estándar IEEE 802.11 en espacios abiertos / cerrados y propagación de ondas de radiofrecuencia en túneles.

Por su parte, el tercer capítulo muestra el funcionamiento y características del estándar de comunicaciones IEEE 802.11, igualmente este capítulo describe las versiones IEEE 802.11 g e IEEE 802.11 e.

Asimismo, el capítulo cuatro presenta el modelo de red que permitió estimar elcomportamiento del throughput, retardo y utilización de los enlaces al transportar distintos tipos de tráfico como son: voz, datos y video. En este apartado también se muestran los modelos que se utilizaron para saber el tiempo mínimo que se necesitó para el Handoff de capa 2 y 3, así como la descripción de las pruebas de análisis para el Handover de ambas capas.

En el capítulo cinco se muestran los resultados obtenidos tanto de los modelos de red como de las pruebas de análisis.

El sexto capítulo se dedica a las conclusiones, es aquí donde se discuten los resultados obtenidos del capítulo cinco y se determina si los tiempos de Handoff conseguidos son buenos para las aplicaciones requeridas.

Finalmente en la última sección se encuentran las referencias utilizadas en este trabajo y el glosario que contiene un repertorio de palabras con su explicación.

CAPÍTULO 2

Conceptos básicos

Las redes inalámbricas han mostrado su eficiencia en el transporte de datos desde ya hace varios años, se les puede utilizar para el transporte de información con una distancia de separación que va desde metros hasta kilómetros.

Múltiples son los elementos que las componen y vastas sus técnicas de operación, sin embargo, algunos de ellos son necesarios y básicos para el funcionamiento de la red.

Debido al avance de la tecnología, la búsqueda de su mejoramiento es un proceso continuo. En este apartado se describen los elementos principales que forman parte de una red WLAN que soporta el servicio de VoIP, la clasificación de las redes inalámbricas de acuerdo a su área de cobertura, las posibles técnicas de seguridad y lo que hasta el momento se ha publicado en fuentes de información confiable acerca de redes inalámbricas de área local, desempeño del estándar IEEE 802.11 (WiFi) en espacios abiertos / cerrados y propagación de ondas de radiofrecuencia en túneles.

2.1 Estado del Arte

2.1.1 Dispositivos móviles y fijos

Son los dispositivos finales que le permiten al usuario tener contacto con la red y poder entablar una llamada o el envío de datos. Los dispositivos móviles están conformados por teléfonos celulares con tecnología GSM/CDMA (Global Systemfor Mobile Communications/ CodeDivisionMultiple Access) y teléfonos IP inalámbricos. La figura 2.1 muestra un conjunto de teléfonos IP inalámbricos.

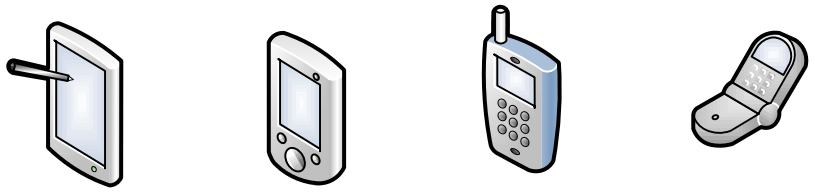


Figura 2.1. Teléfonos IP inalámbricos

Por su parte, los dispositivos fijos se dividen en teléfonos IP duros y suaves. Los teléfonos IP duros tienen una apariencia de un teléfono normal, tienen un puerto Ethernet y no requieren de una PC (Personal Computer) para realizar o recibir una llamada de VoIP.

Los teléfonos IP suaves son computadoras personales con micrófonos, audífonos y un software que les permite entablar una llamada de voz sobre redes IP. A continuación se muestra en la figura 2.2 un teléfono IP duro y uno suave.

Figura 2.2. Teléfonos IP duro y suave

2.1.2 Access Point o punto de acceso

Es un dispositivo electrónico cuya función es propagar una señal electromagnética generalmente en la banda de frecuencia de uso libre o ISM (Industrial, Scientific and Medical). Un Access Point tiene la tarea de crear una región de cobertura de una red inalámbrica y permitirles a los dispositivos el acceso a la red, con una calidad de la señal que hace posible la comunicación.

Las bandas de frecuencia ISM utilizadas internacionalmente son las comprendidas entre los 902 a 928 MHz, 2.4 a 2.4835 GHz y 5.725 a 5.850 GHz. Cabe resaltar que para el uso de estas frecuencias no se requiere de una licencia o permiso. En la figura 2.3 se muestra la representación gráfica de un AP.

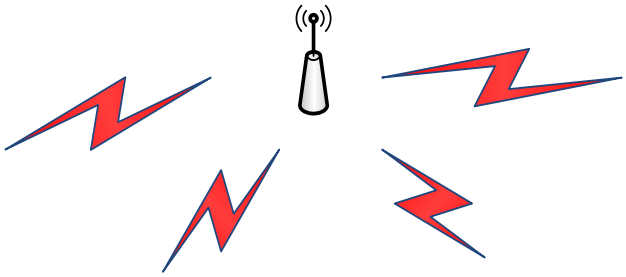


Figura 2.3. Punto de Acceso (AP)

2.1.3 RADIUS server

RADIUS son las siglas correspondientes al Servicio de Autenticación Remota de Usuarios (RemoteAuthentication Dial-In User Server) y es un protocolo que brinda las funciones de AAA, las cuales se refieren a la Autenticación, Autorización y Conteo-Registro.

La primera de las funciones (Autenticación) se refiere a verificar la identidad del dispositivo que quiere conectarse a la red, es decir, "*que demuestre ser quien dice ser*". Lo anterior se logra mediante la presencia de credenciales como un usuario y una contraseña.

La Autorización es la función que permite al usuario que se encuentra dentro de la red, a desempeñar o llevar a cabo sólo aquellas tareas para las cuales goza de privilegio de acceso.

Finalmente, la función de Conteo-Registro permite realizar una bitácora en la que se encuentran almacenadas todas las tareas que llevó a cabo el usuario dentro de la red y la duración en tiempo que el usuario estuvo conectado a ésta.En la figura 2.4 se muestra la representación gráfica de un servidor RADIUS.

Figura 2.4. RADIUS server

2.1.4 Proceso de Handoff o Handover

Cuando un dispositivo móvil pierde conectividad con el actual AP que le brinda servicio, lleva a cabo un proceso de Handoff o Handover. Este proceso consiste en cambiarse a un canal de otro AP vecino que tenga una buena intensidad de señal, lo que le permita continuar en comunicación.

Si el dispositivo móvil se cambia a un AP el cual se encuentra dentro de la misma LAN (Local Area Network) que el AP anterior, entonces se lleva a cabo un Handoff de capa 2 y el dispositivo móvil no cambia de dirección IP [16]. La figura 2.5 ilustra el Handoff de capa 2.

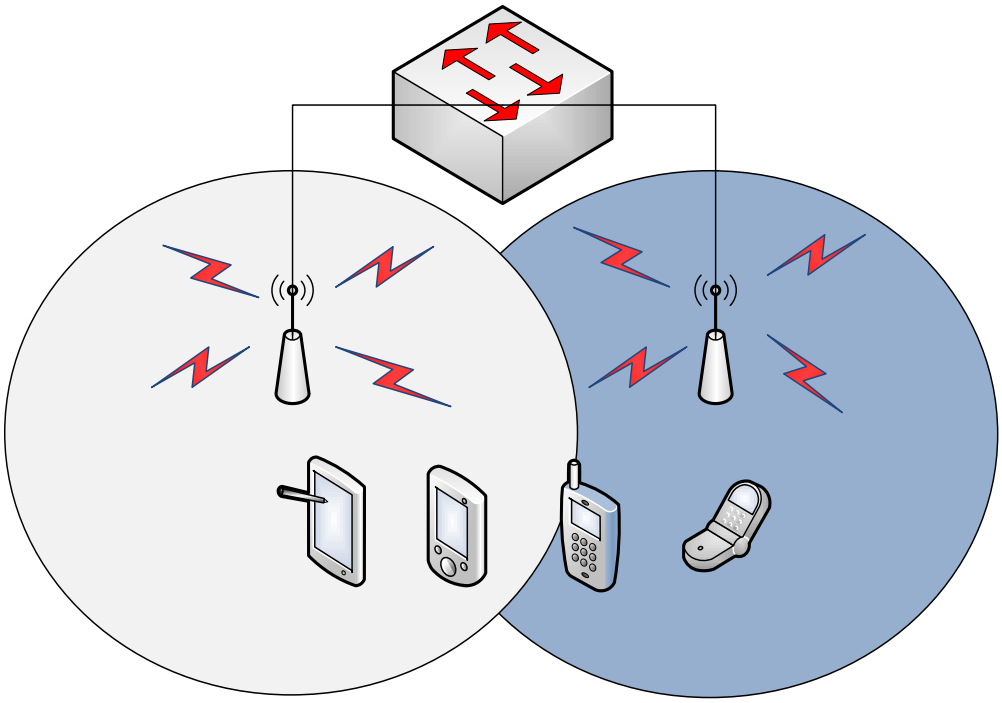


Figura 2.5. Handoff de capa 2

Si el dispositivo móvil cambiara a un AP de una LAN diferente. Entonces se lleva a cabo un Handoff de capa 3 y el dispositivo cambia de dirección IP. A continuación la figura 2.6 muestra un Handoff de capa 3.

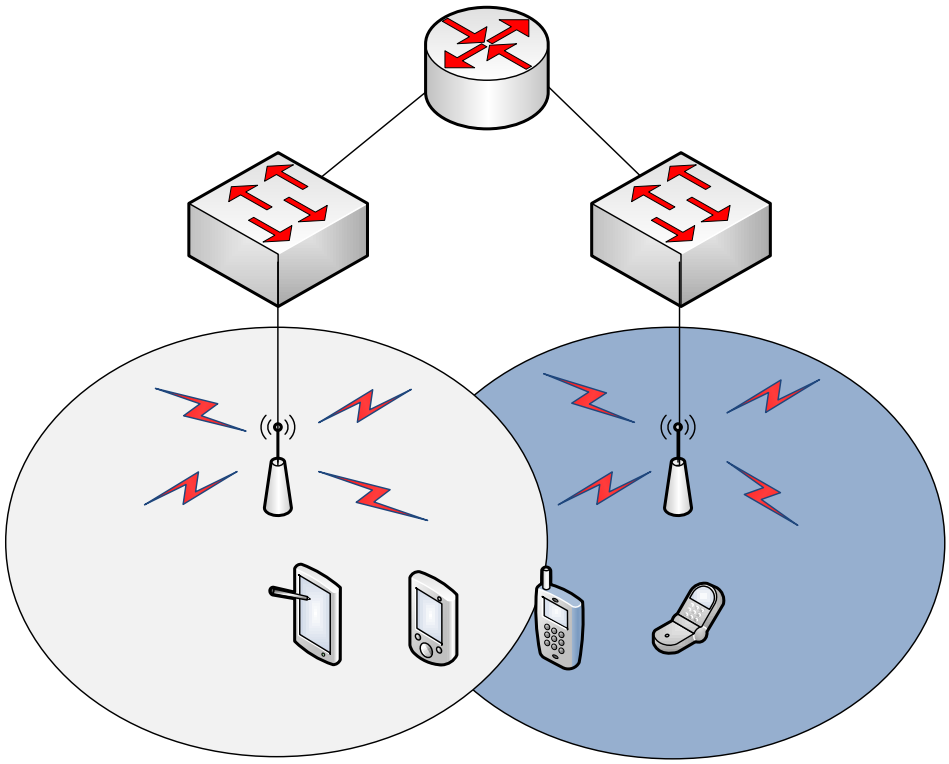


Figura 2.6. Handoff de capa 3

El proceso de Handoff en el estándar IEEE 802.11 consiste de tres etapas: escaneo, autenticación y asociación.

La etapa de escaneo se lleva a cabo una vez que el RSSI (ReceiveSignalStrengthIndicator) es menor que un cierto umbral y ello imposibilita una buena comunicación entre el dispositivo móvil y el AP. Lo cual ocasiona la pérdida de paquetes y en el peor de los casos rompiendo por completo el enlace de comunicación entre los dos dispositivos.

Esta etapa de escaneo consiste en averiguar cuál de los 11 canales que soporta el estándar de comunicaciones IEEE 802.11 g, o cuales de sus tres canales no superpuestos ofrecen un mayor RSSI en los puntos de acceso vecinos.

El escaneo se lleva a cabo en dos formas: escaneo pasivo y el escaneo activo. En el primero de ellos el dispositivo móvil se sintoniza en uno de los canales y espera la escucha de una trama *Beacon,* este tipo de trama la transmite el AP cada 100 ms a todos los dispositivos móviles que se encuentran dentro de su región de cobertura.

La trama *Beacon* anuncia entre otras cosas el SSID (Service Set IDentifier) o nombre de la red, fecha y hora, las tasas de transmisión soportadas y el conjunto de parámetros FH (FrequencyHopping) o DS (DirectSequence) del espectro disperso.

La técnica del escaneo pasivo tiene una gran desventaja, ya que en el peor de los casos el dispositivo móvil deberá esperar 100 ms para escuchar un *Beacon*, lo que incrementará el tiempo de latencia.

La otra técnica del proceso de escaneo es la activa y en ella el dispositivo móvil en lugar de esperar la escucha de un *Beacon,* inmediatamente en cuanto se cambia de canal le envía al AP una trama *proberequest,* en la que solicita el SSID y las tasas soportadas por el AP en cuestión.

Como respuesta a la trama anterior, el punto de acceso envía instantáneamente una trama *probe response frame* al dispositivo móvil indicándole en ésta el intervalo *Beacon*, el SSID, las tasas soportadas y el conjunto de parámetros FH o DS del espectro disperso. Se ha descubierto que tan solo la etapa de escaneo oscila entre los 300 y 1000 ms [7].

La segunda etapa del proceso de Handoff es la Autenticación y es en la cual el dispositivo móvil trata de probar su identidad enviando una trama de autenticación al AP, el cual responde con un mensaje de aceptación o rechazo por no gozar de privilegio de acceso a la red. El proceso de Autenticación dura como máximo 10 ms.

La última etapa es la de Asociación y se llega a ésta tras una autenticación exitosa. Durante esta etapa el dispositivo móvil le envía al AP una trama *re-associationrequest*mediante la cual pregunta por la dirección MAC (Medium Access Control) del AP con la cual el dispositivo móvil está asociado, el SSID de la red, las tasas soportadas y le indica al AP cada cuanto tiempo se coloca en modo activo para escuchar un *Beacon*.

Como repuesta a la última trama, el AP le envía al dispositivo móvil una trama de *reassociationreply* mediante la cual le envía un identificador de asociación o de dispositivo móvil, además le indica las tasas soportadas de transmisión de datos y si la trama de solicitud fue procesada con éxito o no.

El tiempo aproximado en la etapa de Asociación es de máximo 10 ms, después de que una asociación es llevada con éxito el AP le brinda los recursos requeridos al dispositivo móvil.

Sumando el tiempo de las tres etapas que forman parte del proceso de Handoff, acumulan una latencia de 300 a 500 ms.

En [8] han propuesto llevar a cabo una sincronización entre Puntos de Acceso y dispositivos móviles con respecto al tiempo utilizado por el NTP (Network Time Protocol). De esta manera se plantea que los AP transmitan tramas *Beacon* en sus canales y los dispositivos móviles se cambien a éstos en el tiempo esperado por la escucha de dicha trama.

Así, los dispositivos móviles estarían llevando a cabo un escaneo pasivo pero se cambiarían de canal justo en el momento en que el AP transmite la trama *Beacon*y ello reducirá en aproximadamente 100 ms el tiempo de Handoff.

Aunque esta idea es una buena propuesta, no se considera como solución en el presente trabajo debido a que esta técnica refleja una dificultad muy grande para lograr la sincronización entre los dispositivos.

En [7] como han identificado que la etapa de escaneo es la que introduce el mayor tiempo de latencia en el proceso de Handoff, han propuesto llevarla a cabo en un segundo plano.Así, se plantea realizar la etapa de escaneo mientras aún el dispositivo móvil se encuentra asociado al actual AP y permitirle descubrir canales con un buen RSSI de los AP vecinos antes de que pierda conexión con el AP vigente.

De esta manera la etapa de escaneo puede ser eliminada en el proceso de Handoff y a esta técnica le llaman "*rápida búsqueda en segundo plano* (fastbackgroundscan)". Utilizando esta técnica han hecho pruebas con un chipset Atheros 5212 y han encontrado que el cambio de canal toma alrededor de 4 ms.

En este mismo artículo mencionan que debido a que se lleva a cabo un escaneo activo, el dispositivo móvil envía inmediatamente una trama *proberequest*al AP y máximo espera 8 ms para recibir una trama *probe response frame* por parte del mismo. En caso de que el dispositivo móvil no reciba la trama de respuesta del nuevo AP, le toma otros 4 ms cambiarse al canal con el que estaba asociado al anterior AP. De tal forma que en total, el proceso de escaneo en segundo plano tiene una duración de 16 ms en búsqueda de un canal.

La técnica anterior es buena, sin embargo, no es el equipo con el que se contaba en el laboratorio y el que se tiene es configurable hasta cierto punto.

En [12] los autores proponen hacer una modificación en una de las etapas del proceso de Handoff, ellos proponen hacer un cambio en la etapa de "escaneo" y con ello minimizar la pérdida de conectividad que experimenta un nodo móvil cuando se encuentra entre dos Puntos de Acceso. En este documento se considera que un nodo móvil decide que es tiempo de buscar que otro AP le provea el servicio cuando experimenta una perdida continua de paquetes y de "*Beacon*s", así como una baja SNR (SignaltoNoise Ratio) o un bajo nivel de RSSI por parte del AP al que se encuentra actualmente conectado.

En el mismo documento apoyándose del software *OPNET Modeler,* se evalúa el desempeño de la versión a del estándar IEEE 802.11 al simular el comportamiento de una red de 9.5 km de longitud con AP situados cada 300 m que utilizan la banda de 5 GHz. Las adaptaciones en la etapa de "escaneo" del proceso de Handoff que se hacen son las siguientes:

1.- Se ocupa el valor de RSSI medido a cada instante y conforme a un umbral es usado para decidir si es momento de iniciar el proceso de Handoff o no. Si el umbral es mayor que la sensibilidad mínima del receptor, entonces se tiene un tiempo de sobra (antes que se pierda conexión con el AP actual) para *pre-procesar* datos del proceso de Handoff.

2.- Se ocupa el valor de RSSI medido a cada instante para comparar la intensidad de señal entre dos AP vecinos, si el móvil recibe un RSSI menor que un umbral establecido del AP actual, entonces se inicia el proceso de Handover.

3.- Se implementan tiempos de espera (timeouts) para validar la actividad de un AP conforme al tiempo y así evitar disociaciones o re-asociaciones cíclicas entre dos AP, a esto se le llama el efecto ping-pong o el efecto flip-flop.

Con los cambios hechos en la etapa de "escaneo" del proceso de Handoff, los resultados a los que llegaron se muestran a continuación:

1.- El nodo móvil permanece más tiempo conectado a un AP y ello elimina el fenómeno de flip-flop.

2.- El retardo por el intercambio de datos o retardo de comunicación (delay) disminuye de 0.10 segundos a 0.45 ms.

3.- El periodo de desconexión entre AP disminuye hasta los 50 ms.

4.- La única desventaja es que debido a que el nodo móvil permanece conectado a un AP demasiado tiempo teniendo a su vez la posibilidad de cambiarse a otro AP vecino, el trafico descartado (data dropped) se incrementa hasta un promedio de 1500 bits/segundo. Este resultado daña la robustez de la red.

Esta nueva idea de modificar la etapa de escaneo puede ser útil en el modelo de simulación que se plantea implementar en el desarrollo de este trabajo, sin embargo, se tienen que modificar los parámetros ya que el tráfico descartado es demasiado para la aplicación principal que es la trasmisión de voz.

2.1.5 Propagación de la señal dentro del túnel

La forma de propagación dominante en los túneles es la reflexión múltiple y es por ello que la señal que llega al receptor lo hace por múltiples trayectorias.

En [6] se muestra un modelo que permite calcular las pérdidas de propagación en túneles rectangulares contemplando las irregularidades dentro del túnel como paredes no completamente lisas, presencia de raíles y catenarias, de tal forma que los resultados arrojados por dicho modelo son adecuados para las secciones en donde el túnel no es ideal. Este modelo se hizo en base a un análisis de los modos de propagación que se presentan en una guía de onda rectangular.

Dicho modelo presenta buenas aproximaciones a la realidad sobre todo en zonas en las que la antena receptora se encuentra a 100 metros de distancia o más de la antena receptora. Los resultados arrojados por el modelo son inexactos en zonas donde las antenas se encuentran con una distancia de separación inferior a los 100 metros.

Este modelo puede ayudar al presente trabajo a simular el comportamiento de la propagación de las ondas de radiofrecuencia dentro del túnel.

En la ciudad de Bilbao se ha puesto en operación un sistema privado de telefonía móvil digital cuya principal característica es la utilización de un cable radiante colocado sobre el riel en el cual viajan los trenes, este sistema lleva por nombre TETRA [11].

Dentro del túnel el cable radiante proporciona cobertura de señal a los trenes, éstos llevan en la parte superior frontal una antena que les permite la comunicación. Ya en las estaciones, la señal es provista por una serie de antenas que trabajan en conjunto para lograr comunicarse con los trenes en operación.

Esta red de comunicación con cable radiante fue implementada sobre una de las líneas que componen la red de transporte público del metro de Bilbao, esta línea consta de 17 estaciones distribuidas en un total de 22 km de longitud. Usando un conjunto de cuatro frecuencias no traslapables que se encuentran en la banda de 410 MHz a 430 MHz, se proporciona comunicación a dos tipos de terminales móviles: terminales de tren y terminales individuales de usuario.

El cable radiante que se utiliza en esta red tiene un factor de atenuación de 0.039 dB/m. Las ventajas que involucra su uso son el proporcionar una cobertura de señal uniforme a lo largo del túnel y su sencillo mantenimiento.

Este último documento puede ser útil al presente trabajo ya que muestra el factor de atenuación de un cable radiante que tiene buenos resultados en la transmisión inalámbrica de datos y que ya está en uso en una red completamente operacional.

2.2 Redes inalámbricas

Una red inalámbrica es un conjunto o grupo de dispositivos que intercambian información mediante ondas electromagnéticas y utilizan como medio de transmisión al aire. Las redes inalámbricas cuyos dispositivos presentan movilidad se denominan redes inalámbricas móviles.

A continuación se presenta una clasificación de las redes inalámbricas con respecto a su región de cobertura.

2.2.1 WPAN (Wireless Personal Area Network)

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 PDA (Personal Digital Assistant). Las tecnologías en WPAN son el Bluetooth y Home RF.

2.2.2 WLAN (Wireless Local Area Network)

Es una red inalámbrica de área local cuya cobertura es de unas decenas 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 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 datos a través de mensajes de RTS (RequesttoSend) y CTS (Clear toSend). 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.

2.2.3 WMAN (Wireless Metropolitan Area Network)

Es una red inalámbrica que brinda cobertura en 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.

2.2.4 WSN (Wireless Sensor Network)

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 en 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 el RFID (Radio FrequencyIDentification).

2.2.5 WWAN (Wireless Wide Area Network)

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.

Las tecnologías en WWAN son GSM, GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunications System) y EDGE (Enhanced Data Rates for GSM Evolution).

2.3 Seguridad en redes inalámbricas

2.3.1 Método SSID

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

Cualquier usuario que desee conectarse a una red debe conocer el SSID para comunicarse con el AP y tener acceso a dicha red. El AP continuamente difunde este identificador de una manera automática mediante un tipo de trama especial llamada "*Beacon*" a todos los dispositivos que se encuentran dentro de su rango de cobertura.

Como una técnica de seguridad se deshabilita la difusión del SSID en el AP, de esta manera no se anuncia el nombre de la red y sólo las terminales que lo conocen pueden comunicarse con el AP y conectarse. Sin embargo, esta técnica dificulta que los usuarios configuren y conecten a la red inalámbrica.

2.3.2 Método MAC

Hoy en día la mayoría de los AP son configurables y ello les permite almacenar así como administrar una tabla que contiene las direcciones MAC de los usuarios que gozan del privilegio de acceso a la red.

La desventaja que presenta esta técnica de seguridad es que la mayoría de los AP que se encuentran en el mercado no poseen la habilidad de redistribuir los cambios hechos en sus tablas de direcciones MAC. Por ello se tienen que administrar de forma manual y de la misma manera borrar o agregar cualquier dirección MAC en cada uno de los AP pertenecientes a la red.

Durante el proceso de autenticación los usuarios envían sus direcciones MAC al AP y éste las compara con su tabla de direcciones MAC para decidir si gozan o no del privilegio de acceso a la red. En este intercambio de mensajes otro usuario malintencionado puede usar un capturador de tráfico o *sniffer* para obtener una de las direcciones MAC válidas y utilizarla posteriormente para que el AP le permita la conexión a la red.

2.3.3 Método WEP

Es el acrónimo de Privacidad Equivalente a Cableado (WiredEquivalentPrivacy). En esta técnica de seguridad se utiliza una clave compartida entre los usuarios y los AP.

En este modo de seguridad se utiliza al algoritmo de encriptación RC4, éste se compone de un Vector de Inicialización (IV o clave WEP) y de una clave (clave secreta). El primero de ellos se genera al momento de transmitir una trama, es distinto en la transmisión de cada frame y tiene una longitud de 24 bits. El segundo de ellos (la clave) se asigna de forma manual, es estática y tiene una longitud 40 bits [1].Otra técnica que utiliza el mismo principio de funcionamiento pero utilizando una clave de 40 a 104 bits se denomina WEP - 2.

Al momento de transmitir una trama se calcula el CRC de 32 bits y se genera el Vector de Inicialización al cual se le añade la clave secreta, posteriormente se genera una secuencia pseudoaleatoria de la misma longitud que el CRC de 32 bits y se realiza la operación XOR u OR exclusiva entre la secuencia pseudoaleatoria y el CRC de 32 bits. Con ello se encripta la información del tipo y subtipo de la trama que se está enviando.

La trama transmitida lleva en el campo "*cuerpo de la trama*" el Vector de Inicialización y la información cifrada. El usuario destino al recibir esta trama crea la misma secuencia pseudoaleatoria con el IV y la clave secreta. Finalmente para descifrar la información se lleva a cabo la función XOR entre la secuencia pseudoaleatoria creada por el receptor y la información encriptada que recibió en el frame.

En nuestros días existen numerosos softwares que capturan los paquetes transmitidos en una red y tienen la capacidad de descifrar la clave secreta que viaja en los frames cifrados, ello permite que una terminal pueda conectarse a la red de forma clandestina.

2.3.4 Método WPA

WPA son las siglas correspondientes al Acceso Protegido Wi-Fi (Wi-Fi Protected Access) y surge como respuesta a las debilidades que presenta WEP. Este método de seguridad continúa utilizando como algoritmo de encriptación a RC4 pero con la diferencia de que ahora ocupa un Vector de Inicialización de 48 bits. La clave secreta que se ocupa en WPA es una clave de 128 bits y se genera de forma dinámica para cada usuario.

El método WPA usa el estándar IEEE 802.1 X para controlar el acceso a la red mediante puertos y un RADIUS server para realizar las funciones de autenticación, autorización y conteo. La primera función es para verificar la identidad de los usuarios, la segunda para permitirle a un usuario desempeñar sólo las funciones que le fueron otorgadas dentro de la red y la tercera para llevar un registro del tiempo que un usuario ha estado conectado a la red.

La técnica de seguridad WPA también puede operar de una manera semejante a WEP utilizando una Clave Inicial Compartida (PreShared Key - PSK) entre los usuarios y los AP pertenecientes a la red, sin embargo, al utilizar esta variante de WPA disminuye su eficacia de seguridad puesto que presenta las mismas debilidades de la técnica WEP.

2.3.5 Método WPA-2

El estándar IEEE 802.11 i es comúnmente conocido como WPA - 2, esta técnica de seguridad es compatible con su predecesor WPA y utiliza el Estándar de Cifrado Avanzado (AES) como algoritmo de encriptación el cual es extremadamente seguro. WPA -2 además de operar en redes que soportan IEEE 802.11 también puede ser implementada en redes ad-hoc.

Esta técnica de seguridad inalámbrica es la más reciente y opera de dos maneras, la primera de ellas es utilizando una clave inicial compartida entre los AP y los usuarios para autenticarlos (WPA2-Personal) y la segunda es mediante la implementación de un servidor de autenticación para permitir el acceso de los usuarios a la red (WPA2-Empresa).

2.4 Protocolo IP móvil

Cuando un usuario forma parte de una red éste se puede localizar mediante su dirección IP, la cual es formada por un conjunto de 32 bits representados en 4 grupos de 8 bits y separados por un punto. Cada grupo de una dirección IP está representado en forma decimal.

El valor de cada octeto puede variar entre 0 y 255, ya que son el mínimo y máximo valor decimal que se puede representar con un conjunto de 8 bits.

Si el usuario permanece conectado a la red puede enviar y recibir información, pero, ¿qué pasa si este usuario es móvil y en su trayectoria decide conectarse a otra red?

Para solucionar el problema de mantener conexión con un usuario móvil cuando se encuentre en otra red, el IETF (Internet EngineeringTaskForce) propuso en Agosto del año 2002 un protocolo para soporte de movilidad IP (Mobile IP), el cual estableció como RFC 3344.

Este protocolo permite que un usuario móvil se pueda mover a través de distintas redes o subredes y pueda ser alcanzable al mantener siempre su dirección IP inicial. En la figura 2.7 se representa un Handoff de un usuario móvil entre distintas redes.

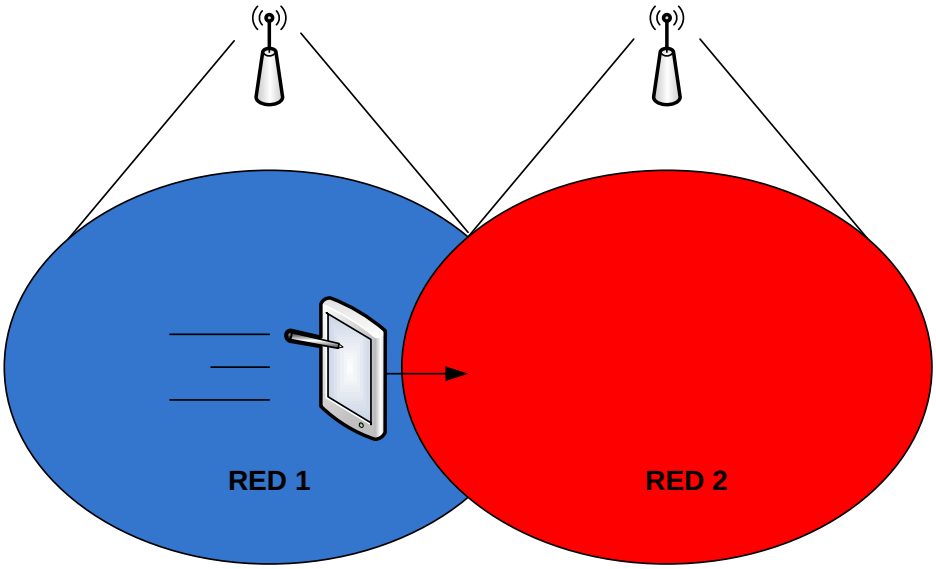


Figura 2.7. Handoff de un usuario móvil entre distintas redes

Para poderse comunicar con el usuario móvil cuando se encuentre en otra red, el protocolo define los siguientes elementos de red y términos [13].

HOME AGENT.- Es un router que se encuentra conectado a la red donde el usuario móvil adquirió su dirección IP original. Es el encargado de transmitir los datagramas destinados al usuario móvil a la red donde este usuario se encuentre de visita, es por ello que mantiene información de la localización actual del usuario móvil.

FOREIGN AGENT.- Router conectado en la red en la que el usuario móvil se encuentra de visita que recibe los paquetes enviados por el *Home Agent*y los entrega al usuario móvil. Este router realiza la función de *Gateway* cuando el usuario móvil desea enviar paquetes desde la red en la que se encuentra de visita a cualquier otro destino.

TUNEL.- Trayectoria virtual que un datagrama encapsulado por el *Home Agent*sigue para ser desencapsulado en el otro extremo por un *ForeignAgent* y así poder ser entregado al usuario móvil en la red en que se encuentre de visita.

HOME NETWORK.- Red en la cual el usuario móvil adquiere su dirección IP inicial.

HOME ADDRESS.- Dirección IP que el usuario móvil adquiere inicialmente cuando se encuentra conectado a una red *Home Network*.

CARE OF ADDRESS.- Dirección IP que el usuario móvil adquiere cuando se encuentra de visita en una red. El *Home Agent*mantiene una asociación entre la dirección *Home Address* y la dirección *Care of Address* de un nodo móvil a fin de saber su correcta ubicación.

En la figura 2.8 se muestra la relación entre los elementos que conforman IP móvil.

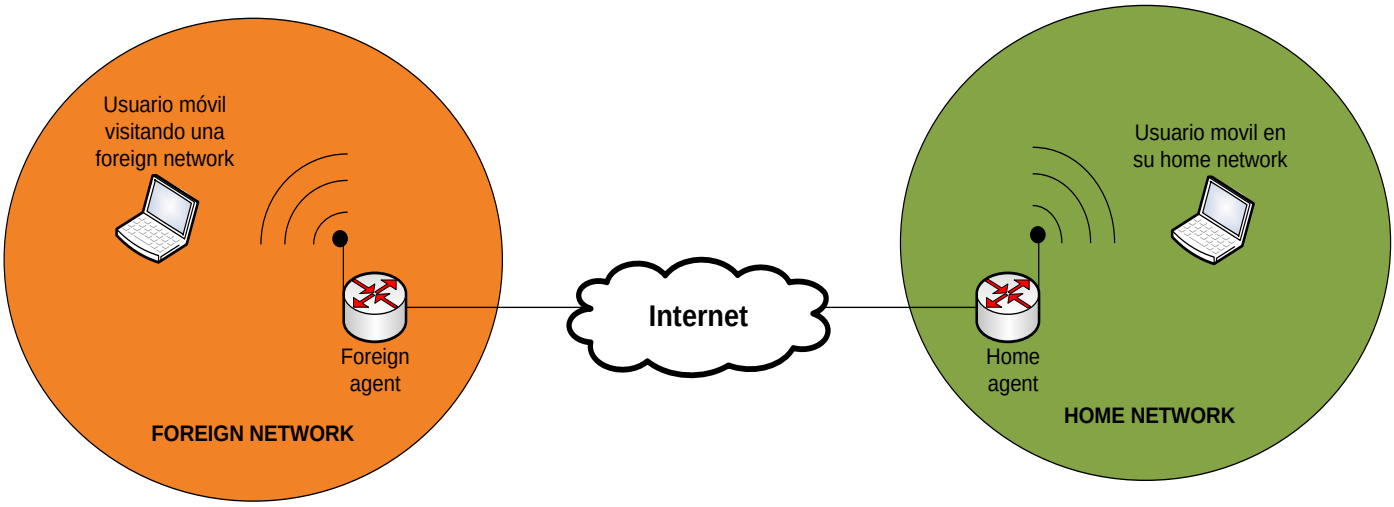


Figura 2.8. Relación entre los elementos que conforman IP móvil

El protocolo IP móvil se compone de tres etapas las cuales se describen a continuación [20].

Descubrimiento de Agentes.

En esta etapa tanto el *Home Agent*como el *ForeignAgent* anuncian sus servicios en la red mediante mensajes de IRDP (Internet RouterDiscoveryProtocol). Los mensajes IRDP se envían de forma periódica y contienen información que permite saber si un Agente está operando como *Home Agent*o como *ForeignAgent* y los servicios que soportan.

Un usuario móvil que está al alcance de una red vecina puede esperar hasta que reciba un mensaje IRDP o puede enviar un mensaje "*agentsolicitation*" para pedir información del Agente más cercano. Es mediante este proceso que un usuario móvil puede determinar si se encuentra conectado a su *Home Network* o se encuentra de visita en otra red.

Registro.

En el momento en que un usuario móvil recibe un mensaje IRDP anunciando que proviene de un *ForeignAgent* y la intensidad de señal de su *Home Agent*es muy baja, entonces comienza el periodo de registro.

En esta etapa el usuario móvil recopila la información acerca de su *Care of address*y *Home address* la cual envía a través del *ForeignAgent* hacia el *Home Agent*para solicitarle a éste último una petición de registro a través del mensaje "*registrationrequest*".

El *Home Agent*autentica la petición de registro del usuario móvil y lo asocia con su *Care of address*. Además crea un túnel con el *ForeignAgent* por el cual enviará los paquetes destinados al usuario móvil y envía el mensaje "*registrationreply*" al *ForeignAgent* como confirmación de la petición de registro.

El *ForeignAgent* revisa la validez del mensaje "*registrationreply*", coloca al usuario móvil en su lista de visitantes y crea el túnel con el *Home Agent*.

Túnel.

Cuando el usuario móvil se encuentra ya sea en su *Home Network* o de visita en alguna otra red, envía paquetes a otro usuario utilizando su dirección *Home address* como la dirección IP fuente. Esto se traduce a que el usuario destino no se percata si el usuario móvil se encuentra en su *Home network* o en alguna otra red.

Por el contrario, cuando el usuario destino desea enviar paquetes al usuario móvil lo hace colocando como IP destino la dirección *Home address* del usuario móvil. Si el usuario destino y el usuario móvil se encuentran en la misma red, el envío no involucra el paso del paquete a través de un túnel y la transferencia sucede como en cualquier LAN. Pero si el usuario destino y el usuario móvil no se encuentran en la misma red, el paquete es capturado por el *Home Agent* y reenviado por éste a través del túnel utilizando como IP destino la dirección *Care of address* del usuario móvil. En el otro extremo del túnel el paquete es interceptado por el *ForeignAgent* y dirigido al usuario móvil. En este sentido, el túnel sirve para permitir el paso de paquetes encapsulados y desencapsularlos cuando llegan al final del túnel donde los espera el *ForeignAgent*.

El protocolo más común para encapsular los paquetes que viajan a través del túnel en una red IP es el GenericRoutingEncapsulation (GRE) del cual es propietario CISCO y definido en el RFC 2784.

En la figura 2.9 se ilustra la trayectoria que los paquetes siguen entre los elementos de IP Móvil a fin de ser entregados al usuario destino y móvil.

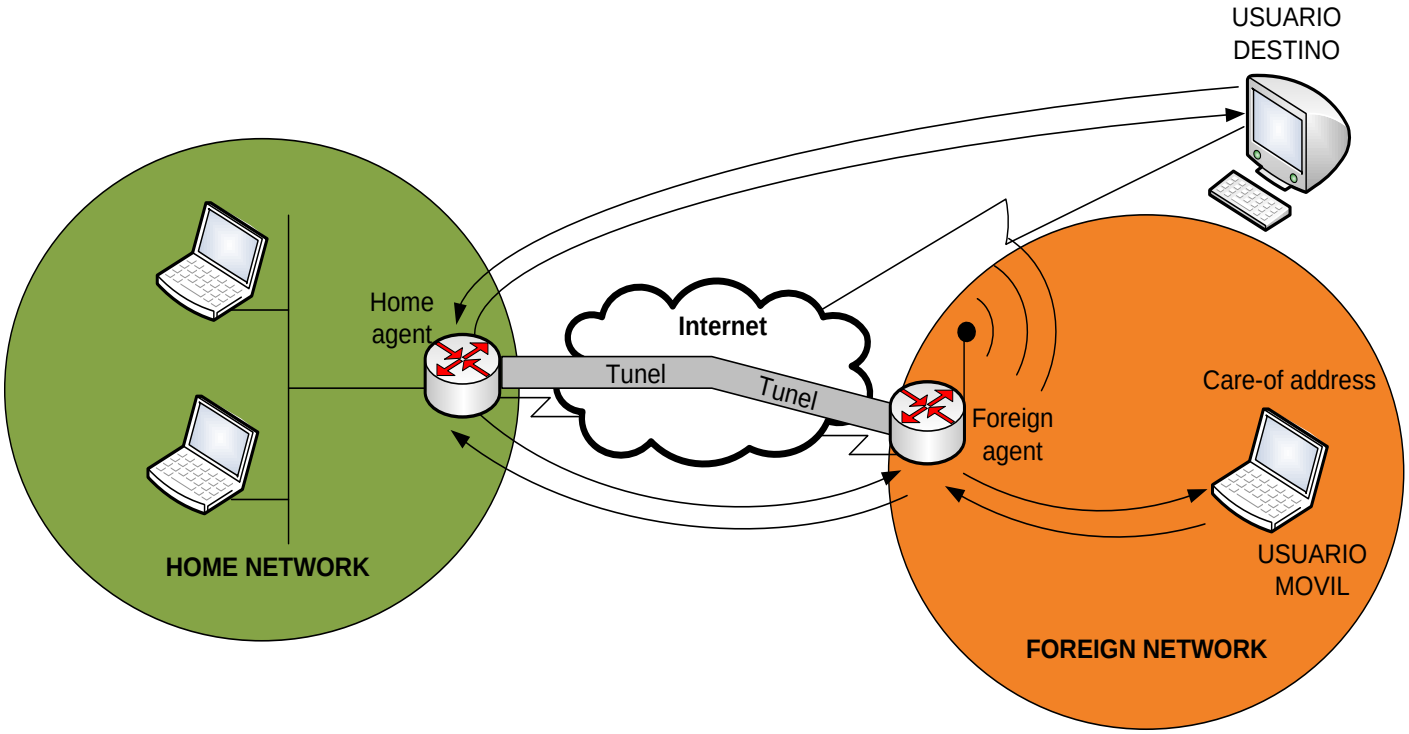


Figura 2.9Trayectoria que los paquetes siguen entre los elementos de IP Móvil a fin de ser entregados al usuario destino y móvil.

CAPÍTULO 3

Protocolo de comunicaciones IEEE 802.11

Para que una comunicación sea adecuada y entendible debe existir un ente que rija el funcionamiento y la manera de comunicarse, así como entre los seres humanos existen lenguas para darse a entender, en las redes WLAN existe el protocolo de comunicaciones IEEE 802.11 que estandariza la forma en que dos o más dispositivos inalámbricos se comunican.

En este capítulo se muestra el funcionamiento y características del estándar de comunicaciones IEEE 802.11, asimismo, se presentan las particularidades de sus dos versiones ocupadas en el presente trabajo. Por una parte se muestra la versión IEEE 802.11 gla cual es la versión más utilizada por dispositivos inalámbricos en nuestros días y por otra parte la versión IEEE 802.11 ela cual logra que las redes WLAN proporcionen QoS para paquetes de voz y video sobre el tráfico de datos.

3.1 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 bandasde 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.

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.

En la tabla 3.1 se muestra como el estándar 802.11 maneja el siguiente código para los siguientes bits:

Bit	Código										
1	-1	+1	-1	-1	+1	-1	-1	-1	+1	+1	+1
0	+1	-1	+1	+1	-1	+1	+1	+1	-1	-1	-1

Tabla 3.1. Representación de los bits 0 y 1 con su código correspondiente de 11 chips

En la figura 3.1 se muestra un ejemplo al transmitir y recibir los bits de información 0110 utilizando DSSS:

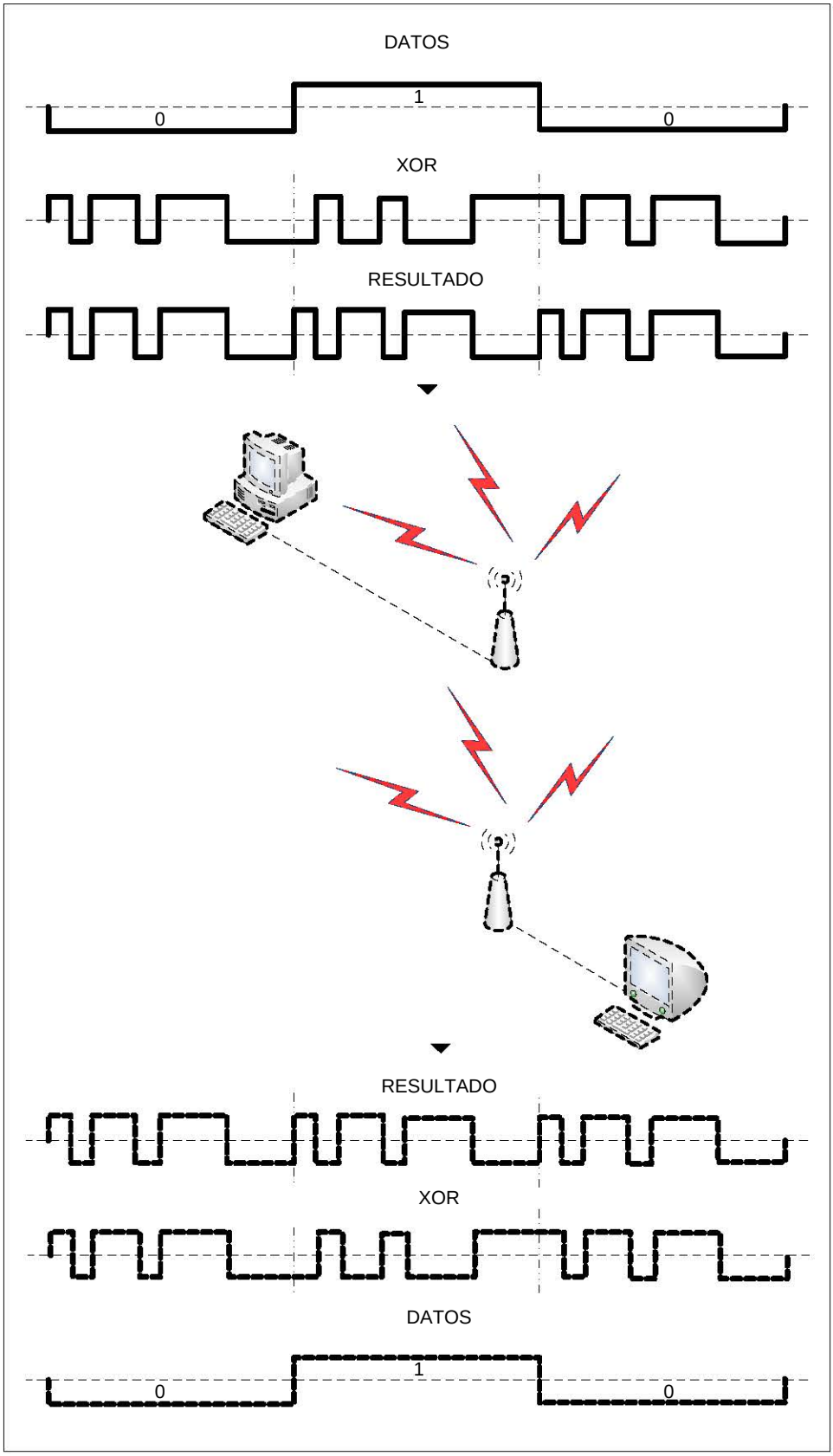


Figura 3.1. Ejemplo al transmitir y recibir los bits de información 0110 utilizando DSSS

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

La figura 3.2 muestra el modo de operación del Espectro Disperso por Salto de Frecuencia:

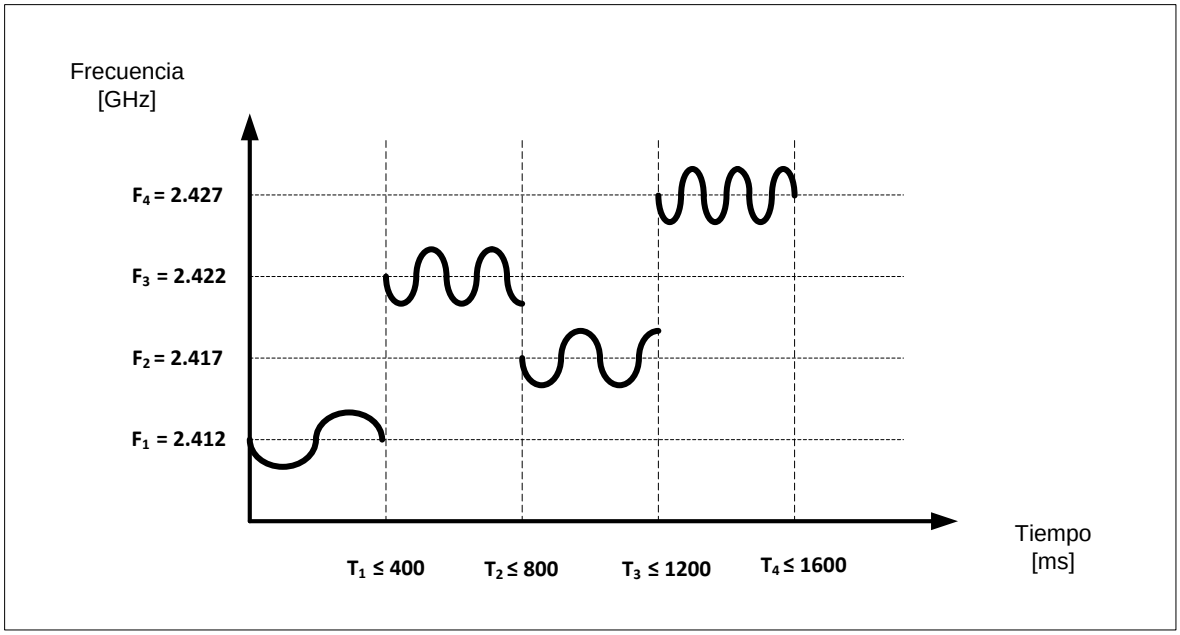


Figura 3.2. Modo de operación del Espectro Disperso por Salto de Frecuencia

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.

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.

La figura 3.3 muestra la representación del Acceso Múltiple por División de Código.

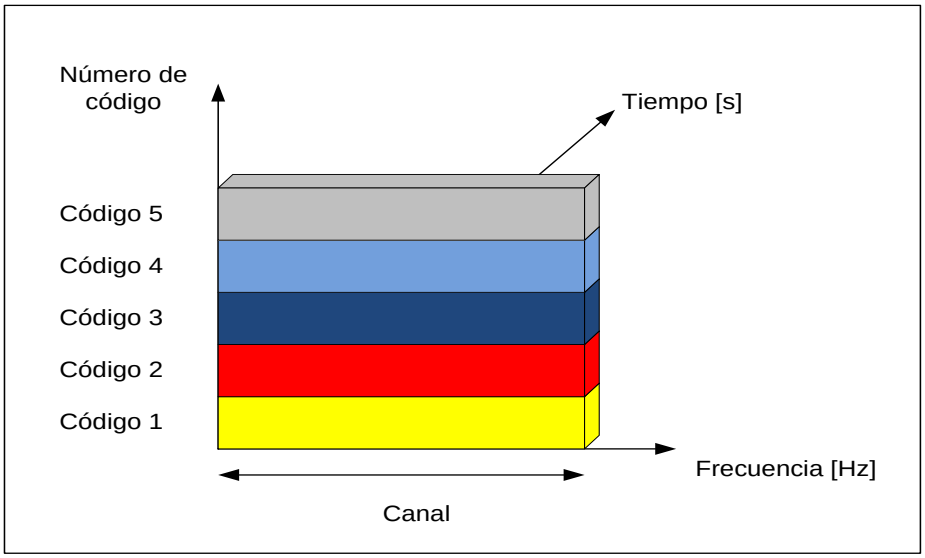


Figura 3.3. Representación del Acceso Múltiple por División de Código

- 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.

En la figura 3.4 se muestra esta técnica de acceso al medio:

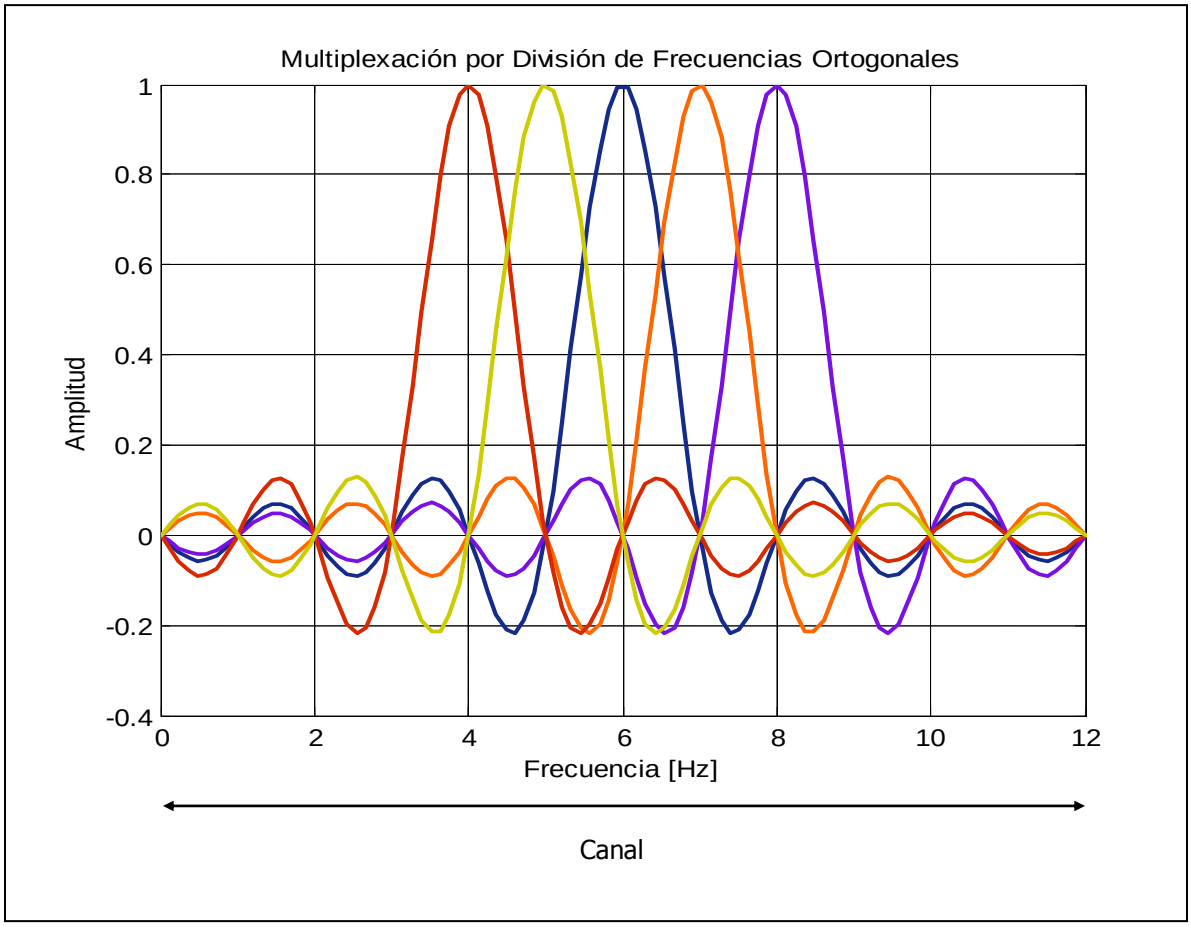


Figura 3.4. Multiplexación por División de Frecuencias Ortogonales

3.2 Formato de la trama MAC

E la figura 3.5 muestra el formato de la trama MAC en el estándar IEEE 802.11 [10].

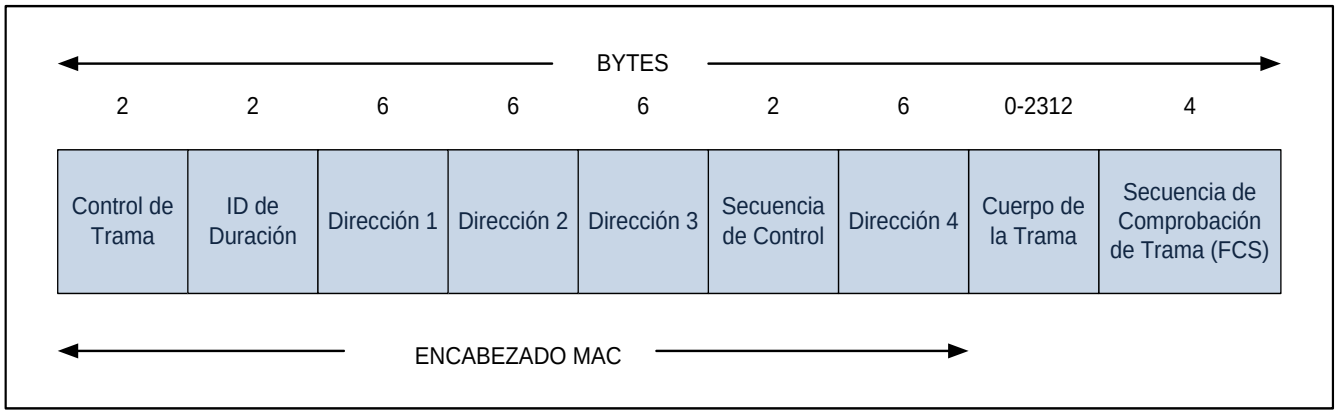


Figura 3.5. Formato de la trama MAC en el estándar IEEE 802.11

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

- **Control de Trama**

La figura 3.6 muestra los subcampos del campo control de trama.

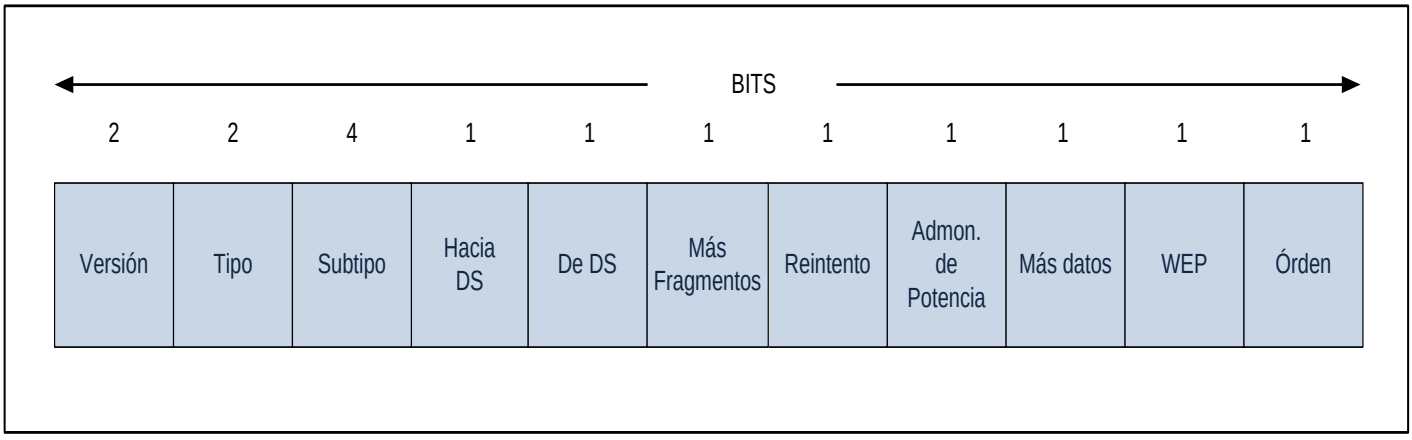


Figura 3.6. Formato del campo Control de Trama

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 la tabla 3.2 que especifica 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 3.2. 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 (PowerSave-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 (RequesttoSend).- 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 toSend).- 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 3.3 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 3.3. Posibles combinaciones para el subtipo de trama

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 3.4 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 3.4. 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.

- **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”.

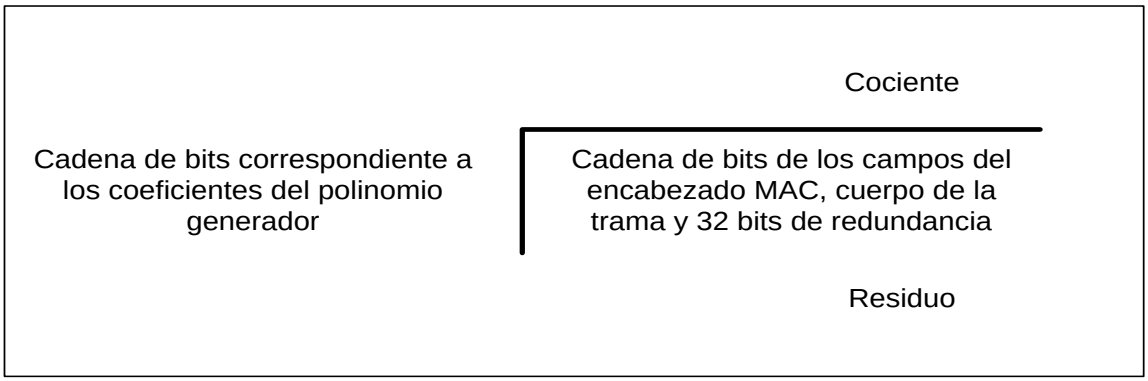
2.- Se toman los coeficientes del siguiente polinomio generador de orden 32.

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

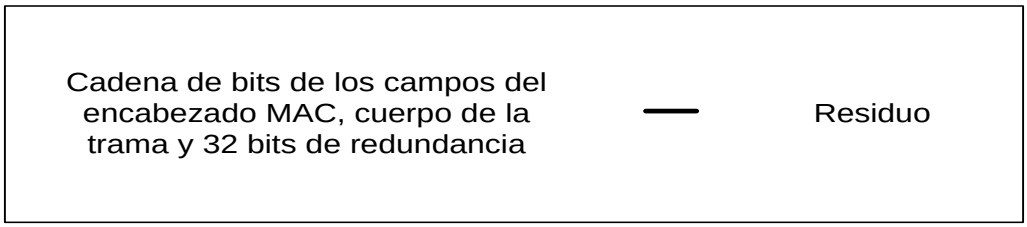
La cadena de bits correspondiente a los coeficientes del polinomio generador resulta:

100000100110000010001110110111

3.- Se efectúa la división binaria:



Se realiza enseguida la siguiente resta binaria:



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.

3.3 Protocolo de comunicaciones IEEE 802.11 g

A través de los años y conforme a las necesidades de comunicación que se requieren, se han hecho una serie de modificaciones sobre el estándar de comunicaciones IEEE 802.11 y ello ha ocasionado la publicación de distintas versiones de éste.

Hoy en día, la versión g del estándar IEEE 802.11 es la más utilizada. Esto es debido a que desde el año de su publicación (2003) han existido en el mercado numerosos dispositivos que lo soportan y hasta la fecha, está más que comprobado su funcionamiento y eficiencia.

La versión g de este estándar utiliza la banda no licenciada de 2.4 GHz y específicamente opera en el intervalo de frecuencias de 2.4 a 2.483 GHz. A continuación se muestra en la tabla 3.5 las principales características de esta versión del estándar:

Modulación	OFDM y DSSS
Tasa de transmisión mínima [MHz]	11
Tasa de transmisión máxima [MHz]	54
Número total de canales	11
Número de canales no superpuestos	3
Radio de cobertura en interiores [m]	35
Radio de cobertura en exteriores [m]	140
Beneficios	Compatibilidad con la versión b del estándar IEEE 802.11, buena tasa de transferencia y su frecuencia de operación impide que sus ondas sean fácilmente absorbidas por objetos.
Desventajas	Interferencia ocasionada por otros dispositivos que ocupan la misma banda de frecuencia como teléfonos inalámbricos, hornos de microondas y el bluetooth.

Tabla 3.5 Principales características del estándar IEEE 802.11 g

La figura 3.7 que se muestra a continuación representa los 11 canales y sus frecuencias correspondientes inicial, central y final.

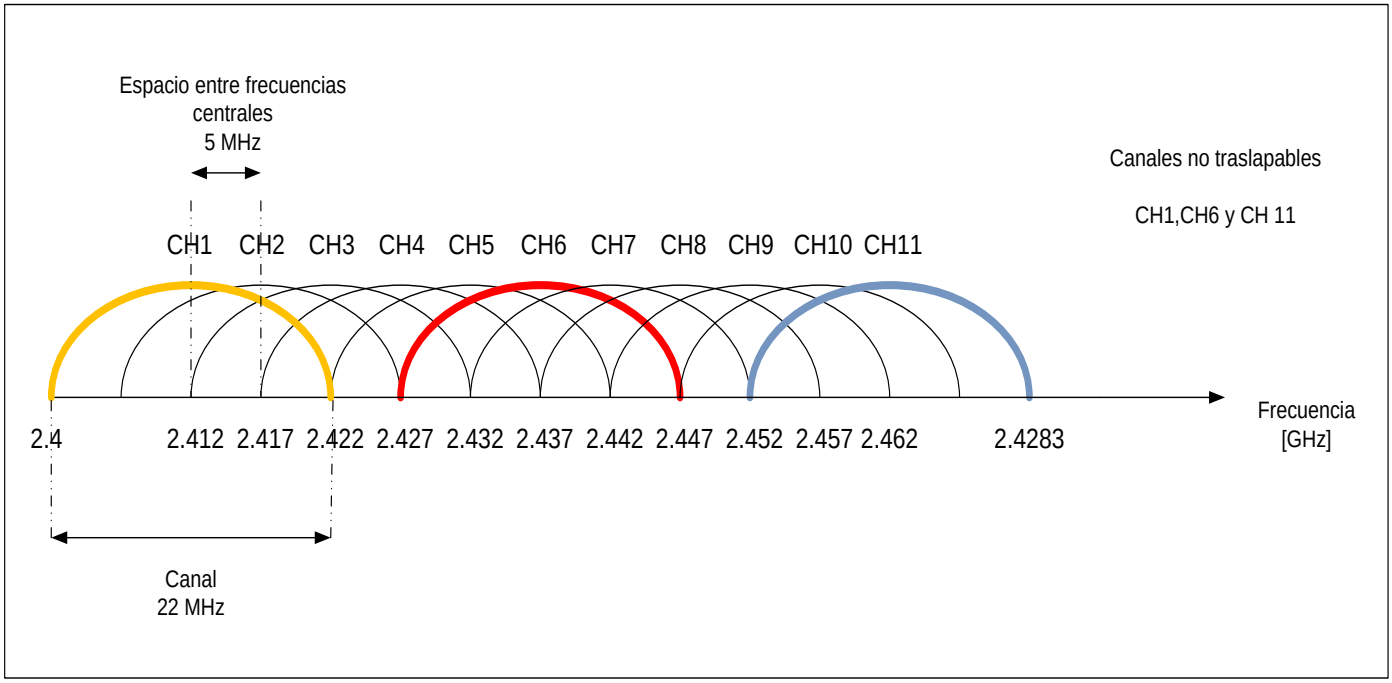


Figura 3.7. Representación de los 11 canales y sus frecuencias correspondientes inicial, central y final

Un Punto de Acceso que soporta esta versión del estándar puede ser configurado en cualquiera de los once canales anteriores, si dos AP se encuentran operando dentro de una misma área y en un mismo canal pueden causarse interferencia entre sí. Para solucionar lo anterior, se recomienda que se configuren ambos Puntos de Acceso en canales que tengan al menos 5 canales de separación.

En el caso de tener tres o más Puntos de Acceso dentro del mismo escenario planteado anteriormente, se evita la interferencia al usar los canales 1,6 y 11, ya que estos canales se encuentran espaciados 25 MHz y tienen 5 canales de separación entre sí.

3.4 Protocolo de comunicaciones IEEE 802.11 e

La versión e del estándar se publicó en el año 2005 y su objetivo es proporcionar Calidad de Servicio (QoS) para datos, voz y video en una WLAN.

A continuación se muestra en la figura 3.8 el formato de la trama MAC que utiliza el estándar de comunicaciones IEEE 802.11 e para brindar Calidad de Servicio [4].

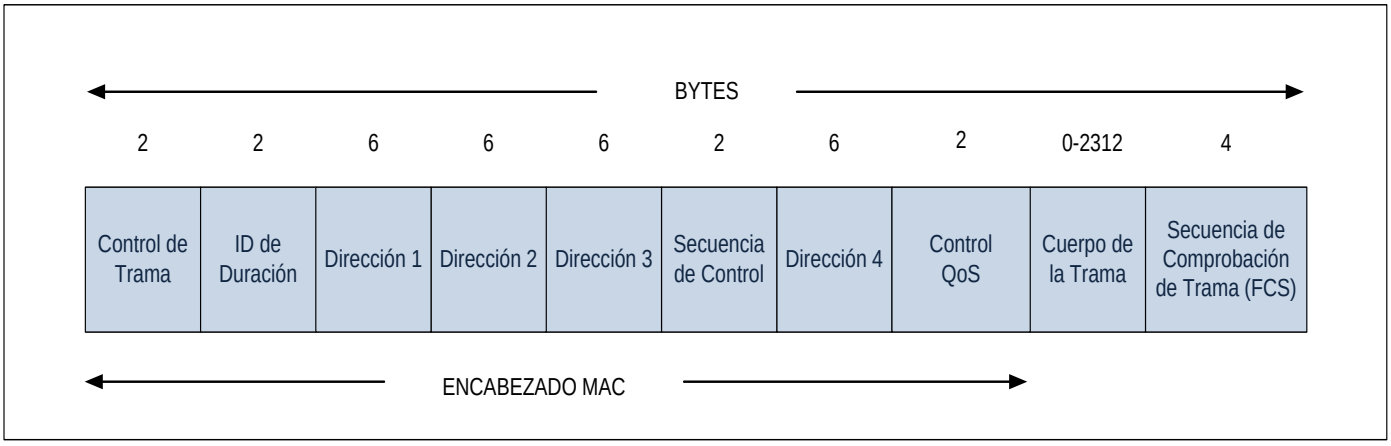


Figura 3.8. Formato de la trama MAC que utiliza el estándar de comunicaciones IEEE 802.11 e

Como se puede observar, la trama que utiliza la versión e del estándar IEEE 802.11 es la misma que utiliza la versión g, excepto que la versión e le añade un campo más (Control QoS) de 16 bits para poder priorizar el tráfico.

IEEE 802.11 e realiza modificaciones en el subnivel MAC de la capa de Enlace de Datos para poder administrar y darle prioridad al tráfico de distintas aplicaciones dentro de una WLAN. Esta versión especifica los métodos de acceso al medio para así brindar hasta ocho clases de servicio diferentes mapeadas en cuatro categorías de acceso: background, besteffort, video y tráfico de voz.

Los mecanismos de acceso al medio que IEEE 802.11 e utiliza son el Acceso al Canal Distribuido Mejorado (EDCA - *EnhancedDistributedChannel Access*) y el Acceso al Canal Controlado HCF (HCCA - *HCF ControlledChannel Access*). Ambos pertenecientes a la Función de Coordinación Hibrida (HCF) que mezcla las funciones DCF y PCF [5].

El EDCA es un mecanismo basado en contienda y el HCCA en un mecanismo en el cual el Punto de Acceso controla el tráfico hacia y desde los dispositivos móviles.

En el momento en que un paquete con prioridad llega a la capa MAC, éste se encapsula en un frame y refleja la misma prioridad en el encabezado de la trama MAC. El paquete trae consigo uno de los 16 Identificadores de Tráfico (TID) que la capa superior coloca para diferenciar a las unidades de datos que pasa a la capa MAC (MSDU), el cual indica que necesita algún tipo de QoS. Si se está ocupando la función EDCA, ocho de esos identificadores (0 - 7) anuncian una categoría de tráfico que es una etiqueta que indica una prioridad de usuario (UP) y refleja una preferencia por su entrega sobre otros paquetes en el mismo enlace. Este primer conjunto de identificadores son mapeados en cuatro categorías de Acceso (CA). Si se ocupa el método HCCA, este identificador toma los valores de 8 a 15 y refleja un tipo de trafficstream (TS) [9].

El mapeo entre los identificadores y las categorías de acceso se muestra en la tabla 3.6:

Prioridad	Categoría de acceso (AC)	Tráfico/Designación
1	0	BestEffort
2	0	BestEffort
0	0	BestEffort
3	1	Video Probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

Tabla 3.6. Mapeo de prioridad de usuario a categoría de acceso[15].

Una vez que los paquetes son mapeados en las cuatro categorías de acceso, cada uno de ellos pasa a un buffer de datos correspondiente a una de las cuatro categorías de acceso donde es almacenado en cola. Cada uno de estos buffer tiene su propio intervalo de ContentionWindow (CW) de Backoff y su tiempo AIFS (el cual se explica más adelante).

La figura 3.9 muestra el proceso general desde que un paquete se recibe en capa MAC hasta su intento por transmitirse:

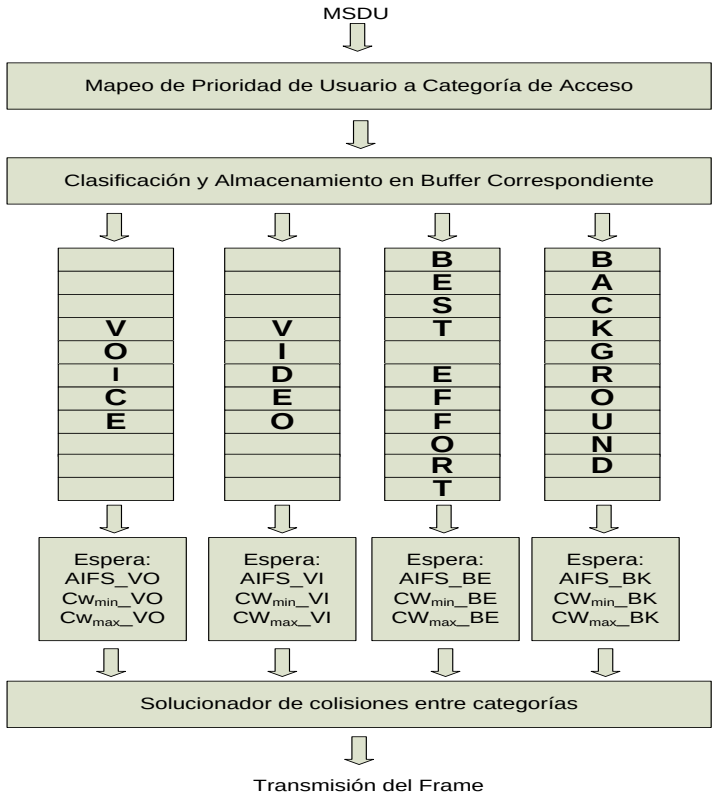


Figura 3.9 Proceso general desde que un paquete se recibe en capa MAC hasta su intento por transmitirse

Si el contador de backoff en dos o más colas de categoría de acceso está por terminar de manera simultánea, se escoge la trama de la cola con mayor prioridad para ser transmitida y las colas restantes pero involucradas en este aspecto asumen que ocurrió una colisión e incrementan el tamaño de su ventana de backoff.

Para administrar el control de acceso al medio usando el método EDCA, el estándar IEEE 802.11 e define un nuevo espacio entre tramas llamado ArbitrationInterframeSpace (AIFS) que sería un tanto equivalente al tiempo DIFS si se ocupa al estándar IEEE 802.11 sin calidad de servicio. AIFS brinda un orden de prioridad de acceso al canal a cada una de las cuatro categorías de acceso anteriores y se define mediante la siguiente ecuación:

$$AIFS\ [AC] = AIFSN\ [AC] * aSlotTime + aSIFSTime$$

Donde AIFSN es el acrónimo de ArbitrationInterframeSpaceNumber, el cual es un número entero que ayuda a que los frames de las colas con mayor prioridad accedan al canal antes que los framesde otrascolas que no son sensibles al retardo. Los valores de Slot Time y SIFS Time son definidos por capa Física

A continuación se muestra en la tabla 3.7 que representa los valores recomendados de AIFSN por el estándar así como sus correspondientes valores mínimo y máximo de la ventana de backoff.

AC	AIFSN	CW_{min}	CW_{max}
AC_BK	7	aCW_{min}	aCW_{max}
AC_BE	3	aCW_{min}	aCW_{max}
AC_VI	2	$(aCW_{min}+1)/2-1$	aCW_{min}
AC_VO	2	$(aCW_{min}+1)/4-1$	$(aCW_{min}+1)/2-1$

Tabla 3.7 Valores recomendados de AIFSN y CW por el estándar IEEE 802.11 e

Como se puede observar en la tabla anterior, las colas de voz y video tienen el mismo valor de AIFSN y ello hace que ambas parezcan tener la misma prioridad de acceso al canal. Sin embargo, se logra una ligera prioridad en la cola de tráfico de voz sobre la cola de tráfico de video al escogerse en la primera de estas colas una ventana de backoff más pequeña que en la segunda, tal como lo muestran las columnas de Cwmin y Cwmax.

Con base en lo anterior, enseguida se muestra en la figura 3.10 la nueva forma de control de acceso al medio que utiliza la versión e del estándar IEEE 802.11

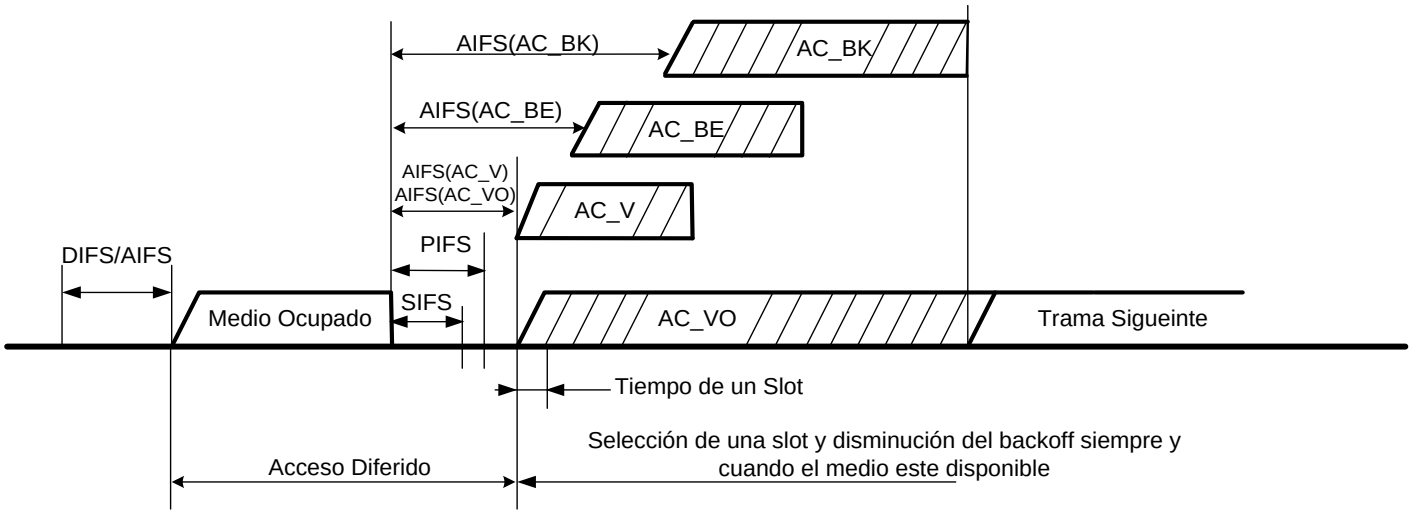


Figura 3.10 Nueva forma de control de acceso al medio que utiliza la versión IEEE 802.11 e

Se puede observar que el método de acceso al canal es muy semejante al que el estándar ha utilizado desde sus inicios, sin embargo, el tiempo AIFS permite que los frames de las colas accedan al canal en el siguiente orden: primero voz y video, segundo besteffort y tercero background.

CAPÍTULO 4

Modelado de la red

A fin de evaluar el desempeño de las versiones g y e del estándar de comunicaciones IEEE 802.11, así como estimar el comportamiento del throughput, retardo y utilización de los enlaces tanto en un escenario físico como en uno simulado, en este capítulo se muestran las distintas topologías de red que se implementaron con el objetivo de obtener y analizar el comportamiento de un Handover de capa 2 y 3 en una red que soporta VoIP.

4.1 Implementación del modelo de simulación e instrumental

En esta sección se describe tanto la topología de red física como la implementada en el simulador y las diferentes pruebas que se realizaron en éstas.

4.1.1 Modelo instrumental

Antes de montar la red física que permitiera probar el desempeño del equipo de voz sobre IP con el que se contaba, se procedió a realizar una serie de pruebas con una red inalámbrica ya puesta en operación que se tenía en el Departamento de Telecomunicaciones.

Esta red consta de 3 AP Linksys WAP54G, que como su nombre lo indica operan en la banda no licenciada de 2.4 GHz. y un RADIUS server le apoya brindando las funciones de Autenticación, Autorización y Conteo-Registro de los usuarios que se conectan a la red.

Cada uno de los AP pertenece a la red 192.168.4.0 con una máscara de 255.255.255.0 y una dirección de broadcast de 192.168.4.255. Estas características hacen que los tres AP pertenezcan al mismo segmento, sin embargo, cada uno de ellos anuncia un nombre de red o SSID distinto. La tabla 4.1 relaciona a cada uno de los AP con su SSID.

Nombre	SSID	Dirección IP
AP TELECOM.1	Telecomunicaciones 1	192.168.4.6 /24
AP TELECOM.2	Telecomunicaciones 2	192.168.4.4 /24
AP TELECOM.3	Telecomunicaciones 3	192.168.4.2 /24

Tabla 4.1 Relación entre cada AP y su SSID

A continuación se muestra en la figura 4.1 un diagrama que representa la ubicación de cada uno de los AP WAP54G en el piso del Departamento de Telecomunicaciones y en la tabla 4.2 se muestran las distancias que los separan.

Nombre	Distancia [m]
AP TELECOM.1 - AP TELECOM.3	44.34
AP TELECOM.2 - AP TELECOM.1	30.18
AP TELECOM.3 - AP TELECOM.2	21.84

Tabla 4.2 Distancia entre los APsWAP54G en el piso del Departamento de Telecomunicaciones

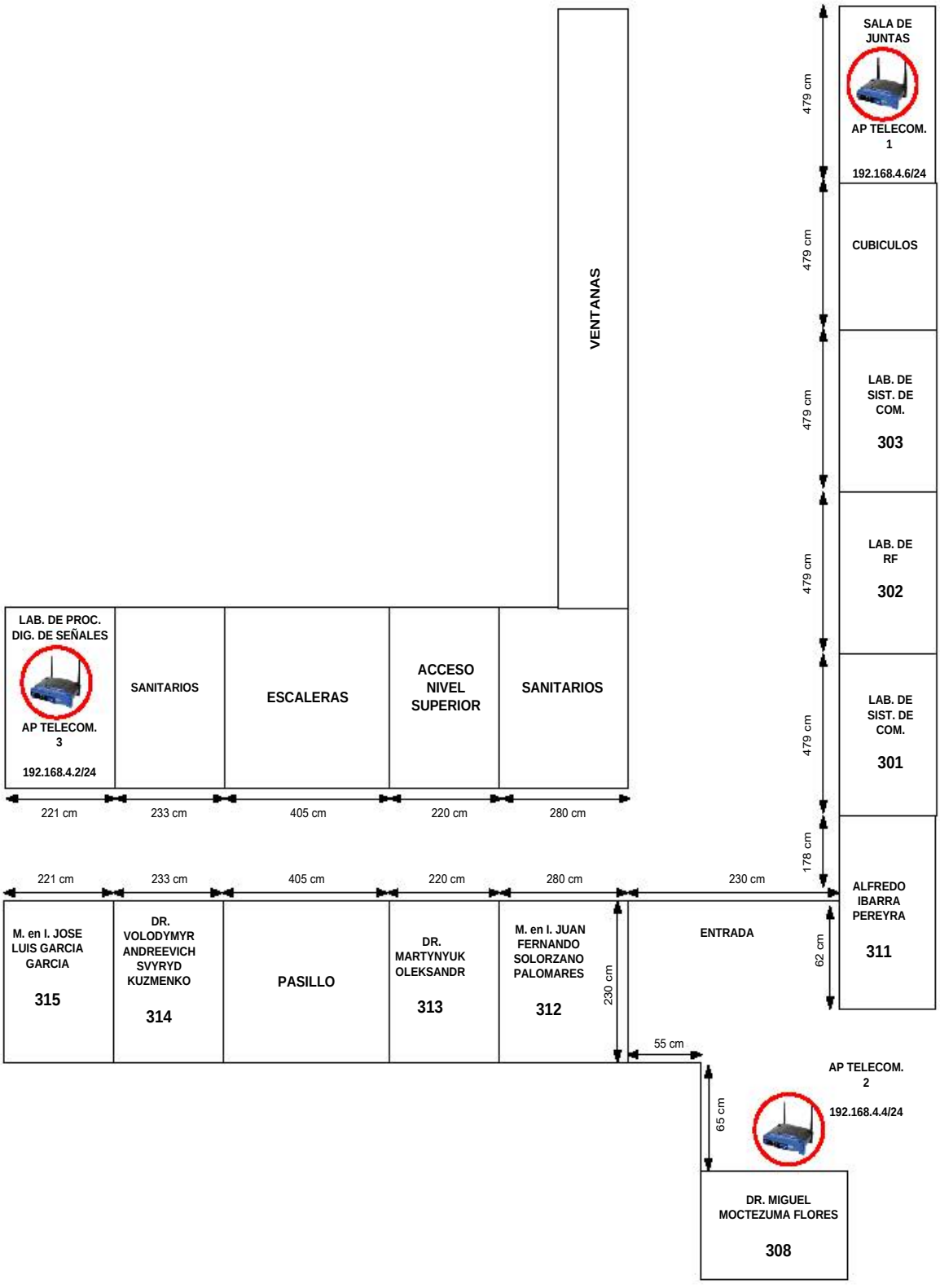


Figura 4.1 Diagrama que representa la ubicación de cada uno de los AP WAP54G en el piso del Departamento de Telecomunicaciones

Después de registrarme y darme de alta como usuario de la red, se procedió a realizar una captura de tráfico con el software Wireshark con el objetivo de conocer los paquetes que se intercambiaban entre los AP y una laptop mientras se llevaba a cabo una descarga de un video de Internet.

La misma prueba sirvió para dar a conocer el tiempo empleado en la autenticación de un usuario en un intento por realizar un Handoff o Handover en esta red. A continuación se muestra en la figura 4.2 un esquema resultante de la captura de tráfico de un intento de Handoff con los AP Telecomunicaciones 1 y 3.

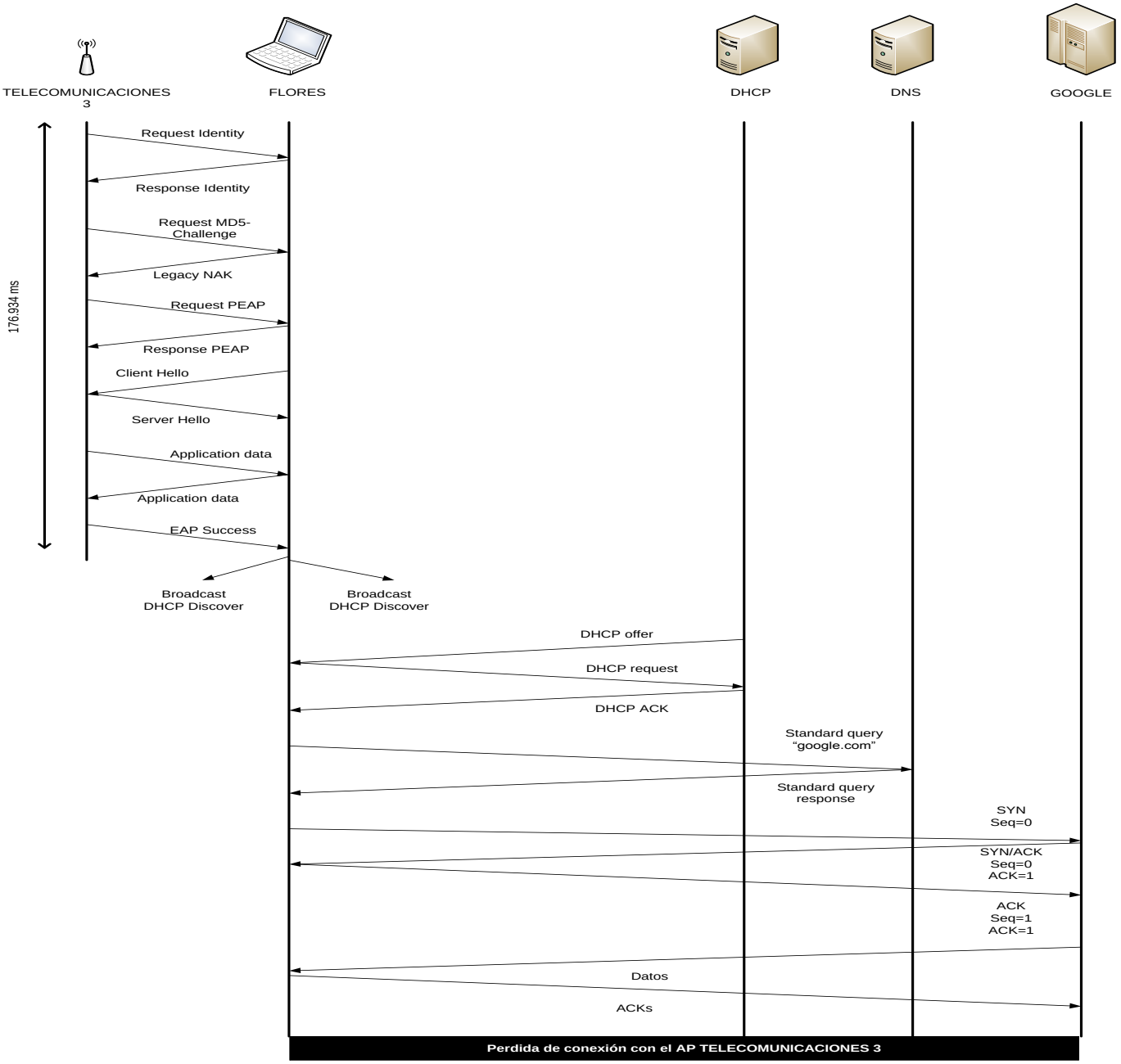


Figura 4.2 Esquema resultante de la captura de tráfico de un intento de Handoff con los AP Telecomunicaciones 1 y 3

Como se puede observar en el esquema anterior, no fue posible realizar el Handoff, ya que se pierde la conexión con el AP TELECOMUNICACIONES 3 antes que se conecte con el AP TELECOMUNICACIONES 1. Si bien ambos AP están en el mismo segmento de red, deben tener el mismo SSID para que el Handoff sea posible.

En el esquema anterior también se puede observar que tan solo el tiempo empleado en autenticar al usuario antes de asignarle una dirección IP es de 176.934 ms, este tiempo rebasa la latencia de la voz sobre IP que es de 150 ms.

Al momento de perder la conexión con el AP TELECOMUNICACIONES 3 automáticamente se inicia el restablecimiento de conexión a la misma red, pero debido a que se recibe una mejor señal del AP TELECOMUNICACIONES 1 el usuario móvil se conecta a éste. En la figura 4.3 se observa un esquema que muestra la captura de tráfico y su tiempo empleado en la autenticación.

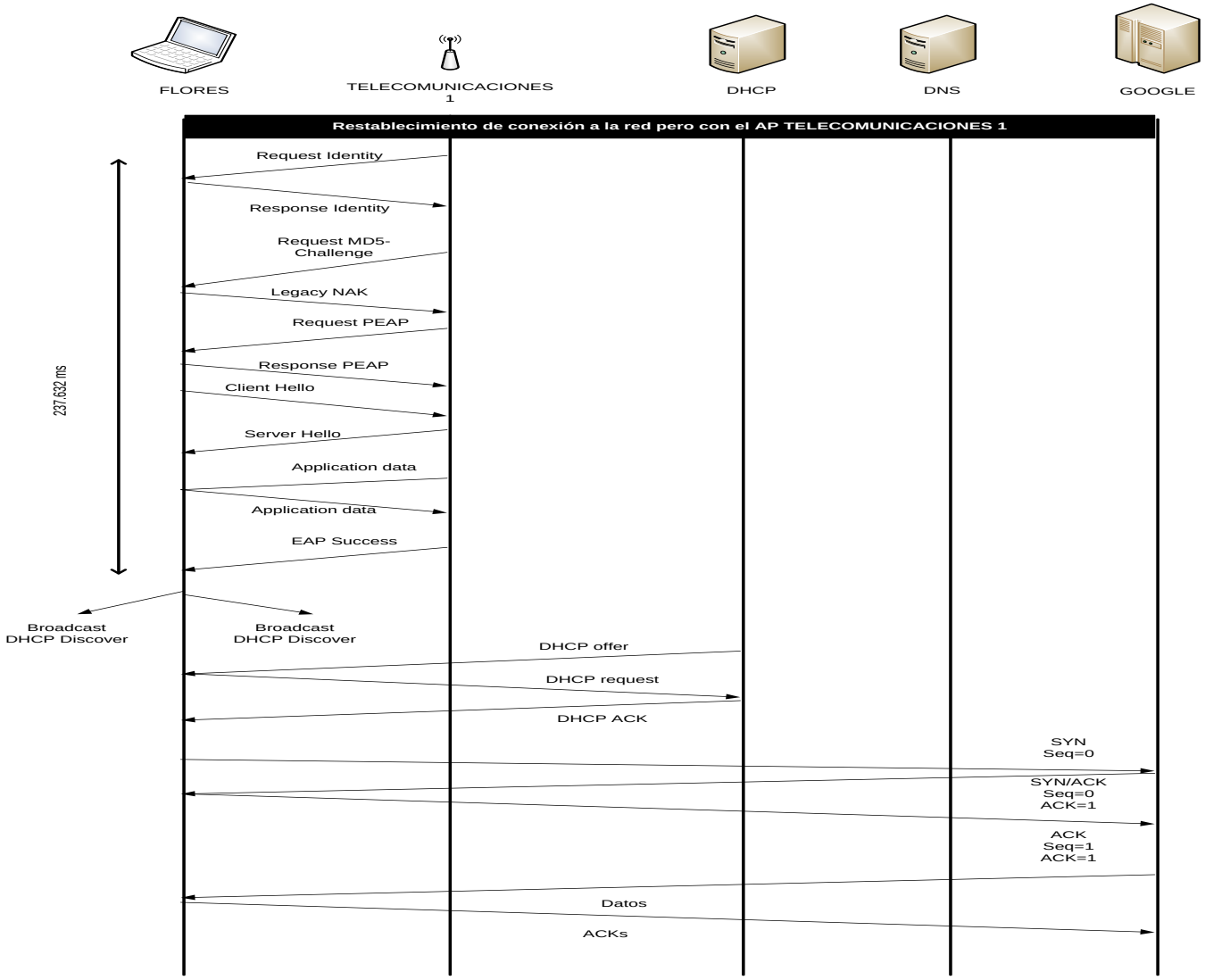


Figura 4.3 Esquema que muestra la captura de tráfico y su tiempo empleado en la autenticación

Se puede observar en la figura 4.3 que el tiempo empleado en autenticar al mismo usuario es de 237.632 ms. Nuevamente se rebasa el tiempo contemplado para la latencia en VoIP.

Tomando como referencia las capturas de tráfico anteriores, se elaboró otro esquema donde se le añaden los tiempos teóricos establecidos en el estándar[2] para lograr el acceso al canal utilizando las variantes del espacio entre tramas (IFS). Dicho esquema se observa en la figura 4.4.

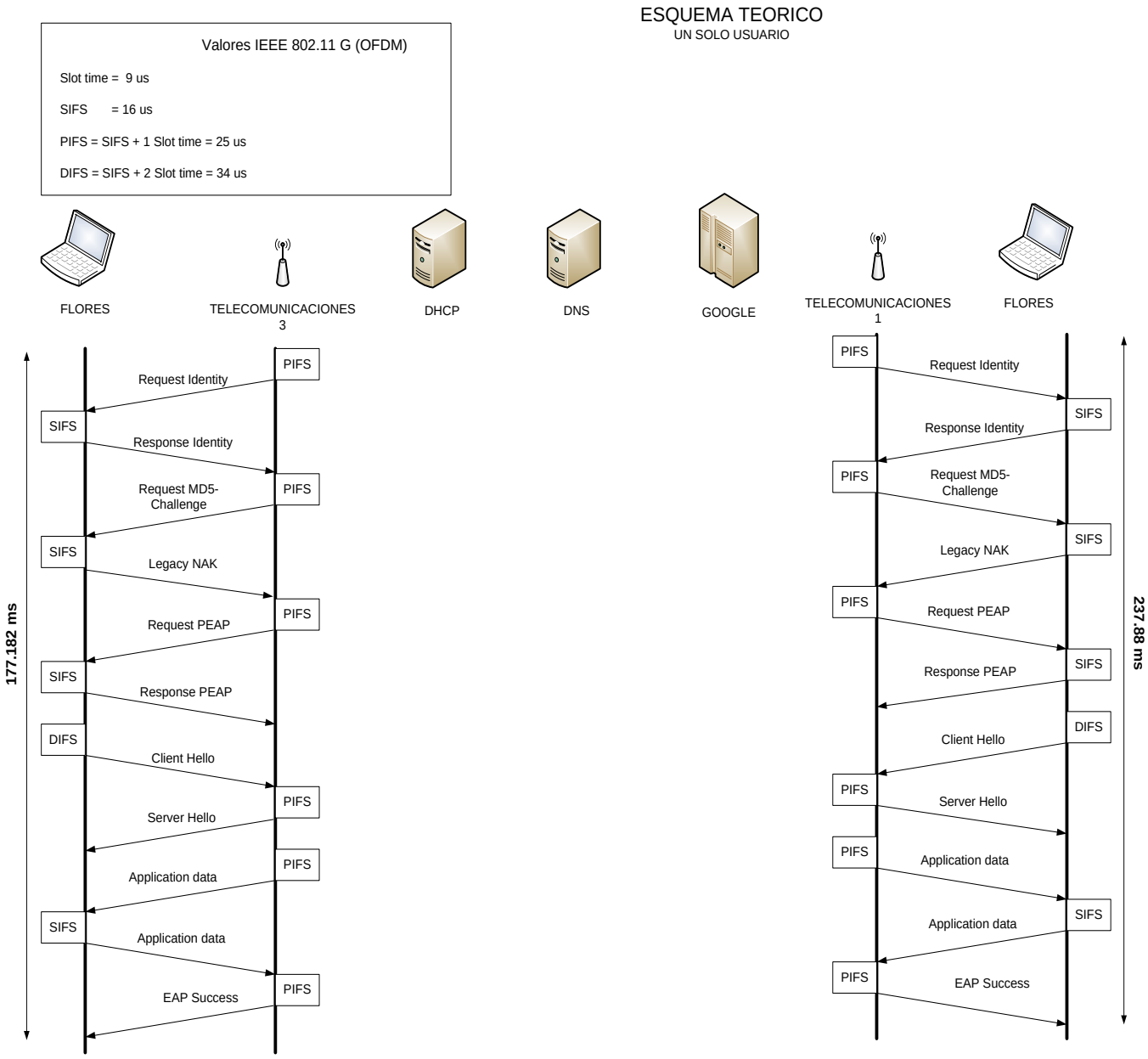


Figura 4.4 Esquema donde se añaden los tiempos teóricos establecidos en el estándar

[2] IEEE 802.11, ***Information technology -Telecommunications and information exchange between systems- Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications***, Second edition 2005, pp. 298

Con el esquema de la figura 4.4 podemos observar que nuevamente se autentica por doble vez al mismo usuario al conectarse a otro AP perteneciente a la misma red, incrementando así la latencia por arriba de los 150 ms que se considera como máxima para evitar una comunicación entre cortada. En consecuencia se concluye que esta red implementada con los AP WAP54G no es adecuada para el soporte de VoIP.

Como resultado se optó por implementar y configurar una red con equipo que soportara voz sobre IP y sobre ésta se realizaron las pruebas que permitieron lograr un Handoff de capa dos y tres.

En seguida se muestra en la tabla 4.3 la lista de equipo que se requirió para implementar la red de soporte de VoIP:

EQUIPO	Descripción
Cisco WIP 310	Teléfono IP inalámbrico que opera en la banda no licenciada de 2.4 GHz y es compatible con la versión b y g del estándar IEEE 802.11. Soporta llamadas de voz sobre IP y calidad de servicio (IEEE 802.11 e).
Hp LAPTOP dv2625 / Hp LAPTOP compaq nc6220	Dispositivo conectado a la red con dos funciones principales. Por una parte se le ocupa para configurar y administrar a cada uno de los dispositivos pertenecientes a la red y por otra parte sirve como usuario móvil al ejecutar la aplicación del softphone X-LITE para iniciar y recibir llamadas en la red de VoIP.
Linksys SPA 400	Gateway Telefónico que permite la interconexión de la red de VoIP con la Red Telefónica Pública Conmutada (PSTN), soporta hasta cuatro líneas telefónicas análogas en sus puertos RJ11 y puede almacenar hasta 32 cuentas de buzón de voz para registrar saludos, contestadora, menús entre otros.
Linksys SPA 9000 – IP PBX	Central Telefónica Privada que soporta el protocolo IP para administrar las llamadas internas, entrantes y salientes que operan sobre una red de datos. Puede operar hasta con 16 teléfonos IP conectados más los dos teléfonos análogos que se le conecten. Registra a cada uno de los usuarios de la red y les asigna un número de identificación (ID) con el que pueden ser localizados por otros usuarios. Trabaja con distintos codificadores de voz como G.711, G. 723, G.726 y G.729.

Linksys SPA 901	Teléfono IP sin display gráfico que conectado a un IP PBX mediante un cable de red y conectores RJ45 es capaz de realizar y recibir llamadas de voz sobre IP.
Linksys SPA 922	Teléfono IP que conectado a un IP PBX mediante un cable de red y conectores RJ45 es capaz de realizar y recibir llamadas de voz sobre IP. Este teléfono posee las características de altavoces, conferencia, transferencia de llamadas y un display gráfico de alta resolución que indica entre otras cosas su número de identificación (ID) o extensión en la red de VoIP y el ID del dispositivo de la llamada entrante.
Linksys WRP 400	Router inalámbrico que opera con la versión g del estándar IEEE 802.11, tiene dos puertos telefónicos y cuatro Fast Ethernet. Soporta llamadas de voz sobre IP, calidad de servicio (QoS), maneja distintos algoritmos de codificación de la voz y brinda seguridad inalámbrica WEP, WPA así como WPA2.
ROUTER CISCO SERIES 2600	Elemento de interconexión de redes y direccionamiento de paquetes en la red de voz sobre IP. Este router modular posee dos interfaces Fast Ethernet y un puerto de consola para poder administrarlo.
Softphone X-LITE	Software que simula las funciones de un teléfono IP convencional. Instalado en una computadora puede hacer y recibir llamadas de otros softphones o teléfonos IP. Este software en particular permite llamadas de voz, video y mensajes instantáneos.
SWITCH ETHERNET	Dispositivo de interconexión que en cada uno de sus puertos define un dominio de colisión. Se encarga de gestionar y administrar las tramas de los dispositivos que se encuentran conectados a éste. El dispositivo soporta Ethernet y FastEthernet.
TELEFONO ANALOGO	Dispositivo fijo que convierte señales acústicas a señales eléctricas y viceversa. Sirve para realizar y recibir llamadas de voz dentro y fuera de la red de VoIP conectándose mediante un cable telefónico con conectores RJ11.

Tabla 4.3 Lista de equipo que se requirió para implementar la red deVoIP

Inicialmente se utilizó el teléfono WIP 310 para saber el comportamiento que tiene un teléfono de VoIP inalámbricoy la calidad de la llamada que ofrece. Asimismo, este dispositivo se utilizó para conocer las ventajas de un equipo que soporta QoS sobre los teléfonos convencionales de VoIP.

El teléfono WIP 310 demostró su buen funcionamiento al realizar y recibir llamadas de VoIP correctamente, sin embargo, se decidió no utilizarlo en el desarrollo de las pruebas debido a que no es capaz de soportar un Handoff de capa 2 y 3 [18] [19].

En consecuencia, se optó por utilizar el softphone X-LITE que instalado en una laptop se utilizó como usuario móvil para hacer y recibir llamadas de voz en la red de voz sobre IP. En la figura 4.5 se muestra la representación gráfica de la red para llevar a cabo un Handover de capa 2.

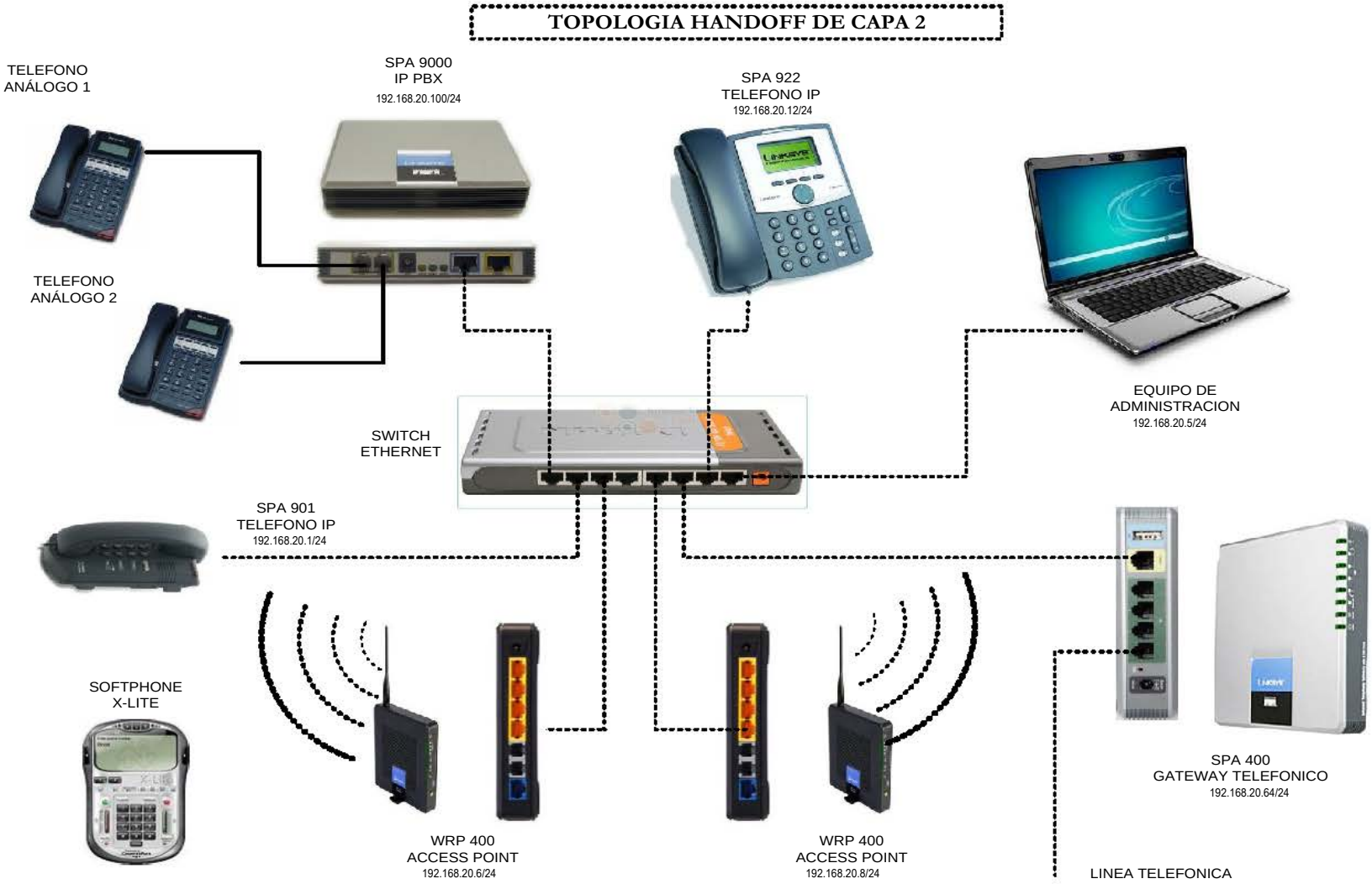


Figura 4.5Representación gráfica de la red para llevar a cabo un Handover de capa 2

En la figura 4.5 se puede observar que cada uno de los elementos pertenece a la red 192.168.20.0 con una máscara de 255.255.255.0 y una dirección de broadcast 192.168.20.255, estas características les permiten intercomunicarse entre sí sin la necesidad de un enrutador debido a que todos los elementos se encuentran en la misma red.

Las líneas punteadas representan un cable de red UTP categoría 5 terminado con conectores RJ45 mientras que las líneas continuas representan un cable telefónico terminado con conectores RJ11.

La laptop que funciona como equipo de administración al estar conectada a la red ya sea mediante un cable o conectada de forma inalámbrica mediante alguno de los AP, sirve para administrar remotamente a cada uno de los elementos que conforman la red de VoIP. Una vez terminada la administración de los equipos, se ejecuta la aplicación del softphone X-LITE sobre esta laptop, para que juntos simulen ser un teléfono IP capaz de soportar roaming.

Los dos AP WRP 400 se encuentran separados aproximadamente 31 metros uno del otro en un ambiente INDOOR, esta fue la máxima distancia que se les pudo separar debido a que necesitan una conexión de voltaje AC para su funcionamiento. Sin embargo, esta distancia de separación no fue suficiente para lograr un Handover debido a que a los 31 metros aun se registraba un buen nivel de intensidad de señal y SNR del AP con el que el usuario móvil se había conectado inicialmente. Por tal razón como no se podían modificar las características del terreno donde se implementó la red de manera física, se decidió rodear al AP con estructuras metálicas que disminuyeran el nivel de intensidad de señal y SNR a los 31 metros y así el usuario móvil decidiera conectarse al AP vecino.

La configuración que se muestra en la figura 4.5 se implementa con la intención de que se lleve a cabo un Handoff de capa 2, esto debido a que la dirección IP de los dos AP WRP 400 pertenecen a la misma red LAN 192.168.20.0, contienen el mismo default gatewaycuya dirección es 192.168.20.254 y ambos anuncian el mismo SSID de la red que lleva por nombre "***Redalejovoip***".

También es importante comentar que los dos AP WRP 400 utilizan los canales 1 y 11 que especifica la versión g del estándar IEEE 802.11, es decir, trabajan en los canales cuya frecuencia central está en 2.412 y 2.462 MHz respectivamente.De esta manera, al elegir los canales lo más separados se evita que se genere interferencia entre canales adyacentes. Los dos AP transmiten con una potencia promedio de 63 mW, o lo que es lo mismo, 18 dBm con una ganancia de antena de 2 dBi [2].

Todas y cada una de las llamadas de voz se realiza utilizando el codificador de voz G.711. En la tabla 4.4 se muestra la relación entre el nombre del elemento de la red y su Identificador único.

Elemento	Número de Identificador (ID) o número de extensión
Cisco WIP 310	108
Hp LAPTOP dv2625 - Softphone X-LITE	111
Hp LAPTOP compaq nc6220 - Softphone X-LITE	113
Linksys SPA 901	104
Linksys SPA 922	109
TELEFONO ANALOGO 1	105
TELEFONO ANALOGO 2	107

Tabla 4.4 Relaciónentre el elemento de la red de VoIP con su Identificador único

La topología de red que se observa en la figura 4.6 muestra la representación gráfica de los elementos que se tuvieron que implementar y configurar para llevar a cabo un Handoff de capa 3. Esta topología de red es similar a la utilizada en el Handover de capa 2, sin embargo, en esta red se agrega un Router Cisco Series 2600 puesto que necesita encaminar o direccionar paquetes de dos redes distintas, una de ellas es la red 192.168.20.0, y la otra es la red 192.168.20.128, ambas con una máscara de 255.255.255.128

Por simplicidad se decidió dejar la central telefónica IP PBX con su misma dirección IP y sólo cambiarle la máscara, de esta manera el IP PBX pertenece a la red 192.168.20.0/25

Cada uno de los AP WRP 400 utiliza DHCP [14] para asignar direcciones IP válidas a los usuarios que desean conectarse. Se configura al AP perteneciente a la red 192.168.20.0 cuya dirección IP es 192.168.20.6/25 para que comience la asignación de direcciones IP en 192.168.20.30/25 y que las asigne de manera continua hasta completar un número máximo de usuarios igual a 20, de esta manera la última dirección IP disponible que este AP puede asignar es la 192.168.20.49/25. Por su parte el AP perteneciente a la red 192.168.20.128 cuya dirección IP es 192.168.20.131/25 se programa para que empiece a asignar direcciones a partir de 192.168.20.150/25 y que con un máximo de 20 usuarios pueda asignar la última dirección IP disponible cual es 192.168.20.169/25.

En esta configuración de red como en la configuración para realizar un HO de capa 2 se utiliza WEP como método de seguridad inalámbrica. Asimismo en ambas topologías se habilita el soporte de WMM como una forma de implementación de Calidad de Servicio (IEEE 802.11 e). WMM son las siglas de WiFi Multimedia y brinda prioridad al tráfico de voz, audio y video sobre el transporte de datos en las redes WiFi, lo anterior se realiza en base a cuatro categorías de acceso.

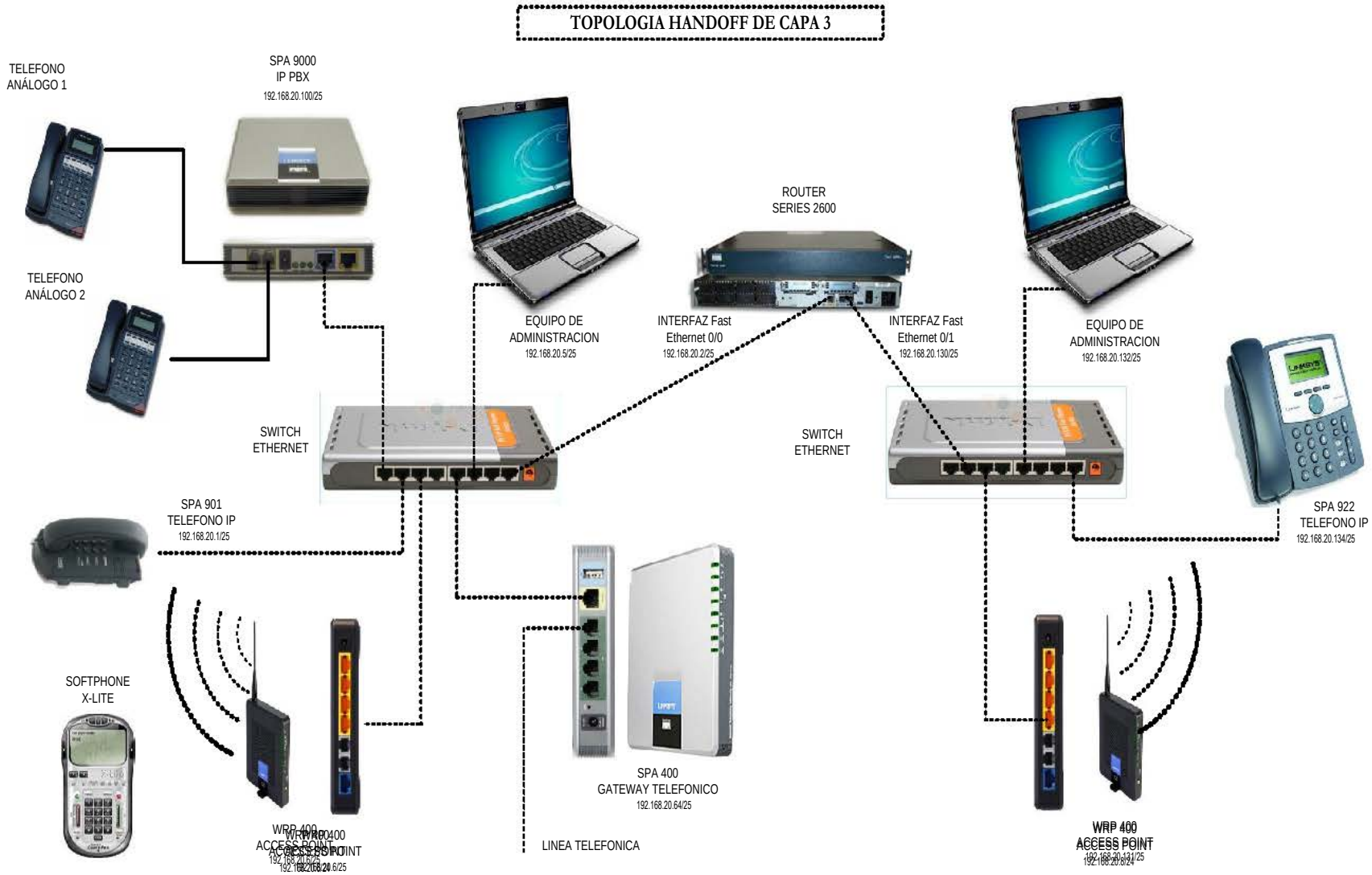


Figura 4.6 Representación gráfica de los elementos que se tuvieron que implementar y configurar para llevar a cabo un Handoff de capa 3.

La primer categoría y con la más alta prioridad es el *tráfico de voz*. La segunda categoría y con una prioridad inferior es el *tráfico de video*. La tercera prioridad y con una prioridad más baja es el tráfico etiquetado como *besteffor*t, este es el tráfico generado por dispositivos que no soportan QoS pero su tráfico es afectado por altos retardos tal como el navegar por Internet. La última categoría con la prioridad más baja de todas es el tráfico etiquetado como *background*que es el tráfico no afectado por una alta latencia como la transferencia e impresión de datos.

Con el fin de que los usuarios conectados a cualquiera de las dos redes mediante un cable o a través de alguno de los dos AP pudieran tener conexión con los elementos de la red vecina, por una parte, se configuró elRouter Cisco Series 2600, tal como se muestra en el apéndice A.1 y por otra parte, se configuró en cada uno de los AP una ruta estática hacia la red ajena. Esta ruta estática se especificó mediante la dirección IP de la red, su máscara y el default Gateway tal como lo muestran las figuras 4.7 y 4.8.

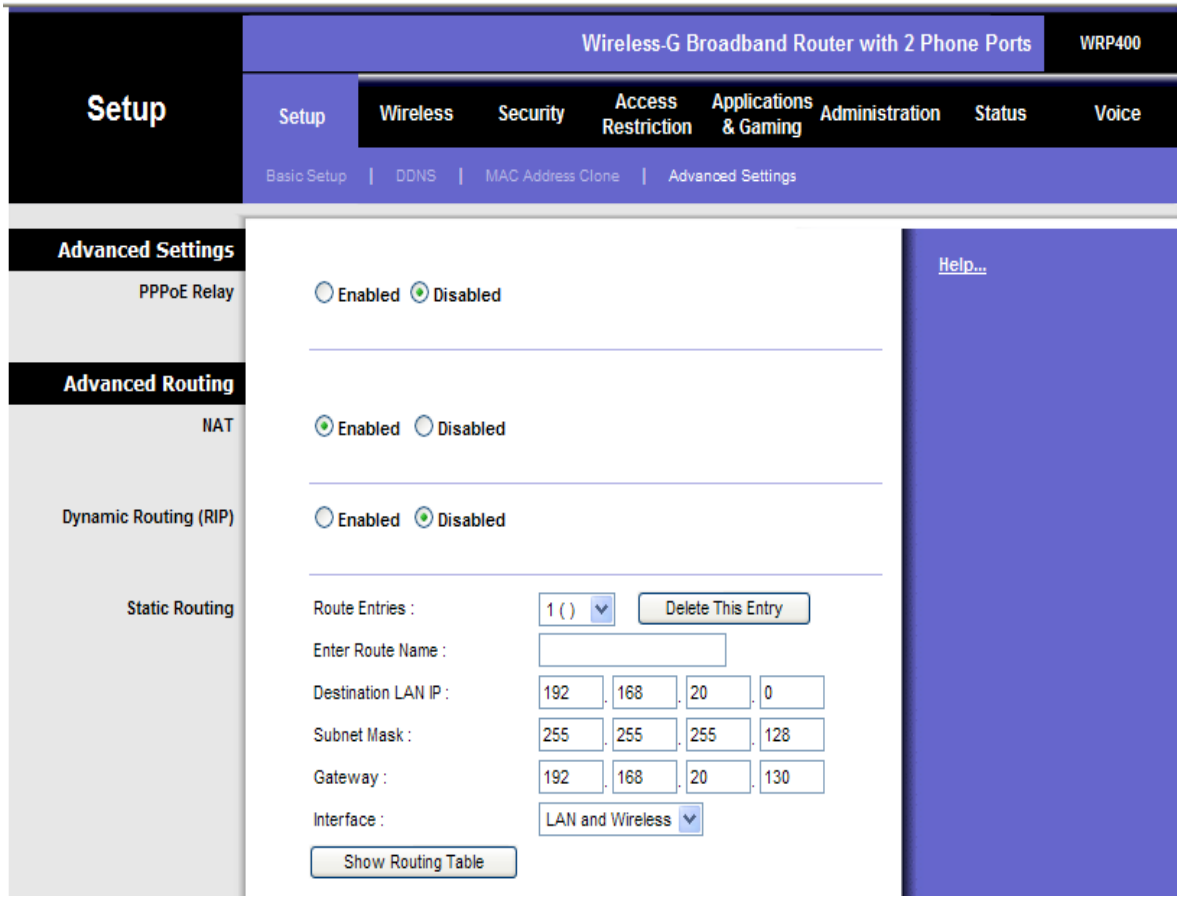


Figura 4.7Configuración de la ruta estática hacia la red 192.168.20.0 en el AP WRP 400 con dirección IP 192.168.20.131/25

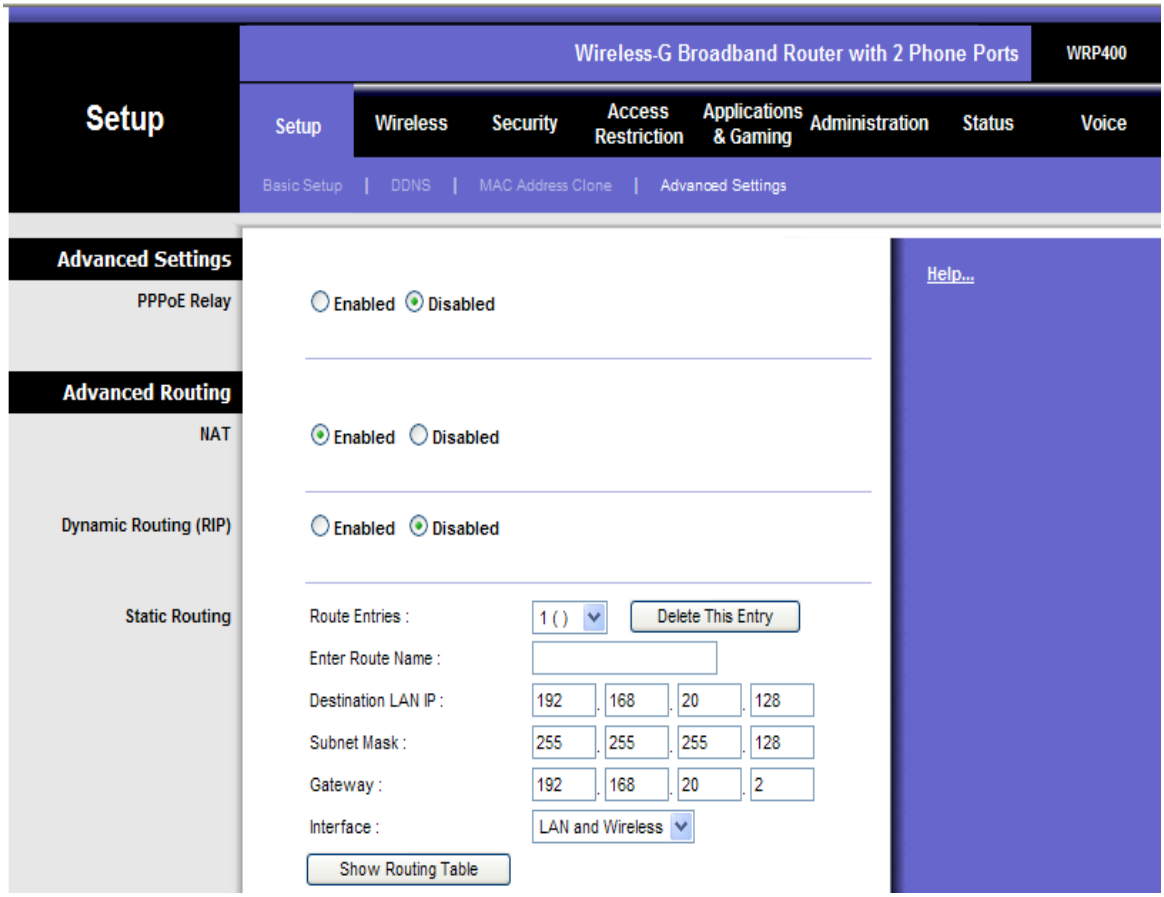


Figura 4.8Configuración de la ruta estática hacia la red 192.168.20.128 en el AP WRP 400 con dirección IP 192.168.20.6/25

La figura 4.9 muestra de manera física a la red que se implementó para llevar a cabo las pruebas de Handoff de capa 2 y 3.

Figura 4.9Red que se implementó para llevar a cabo las pruebas de Handoff de capa 2 y 3.

4.1.2 Modelo de simulación

La figura 4.10 muestra la topología de red que se implementó en el simulador de redes OPNET Modeler[21].

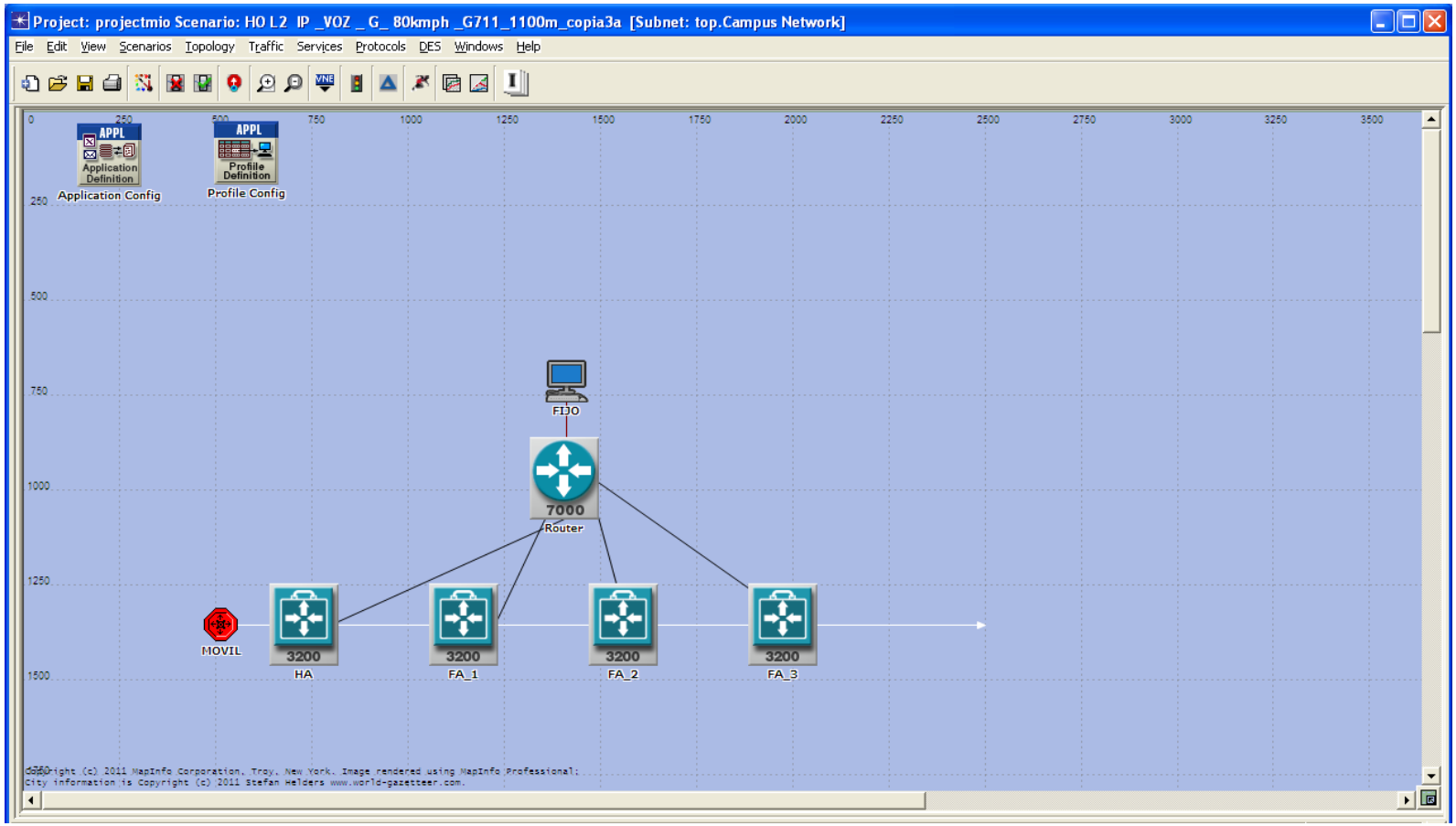


Figura 4.10 Topología de red que se implementó en el simulador de redes OPNET Modeler

La red consta de un usuario fijo, un router, un Home Agent, tres ForeignAgent y un usuario móvil.

El usuario móvil (MOVIL) es una subnet que consta de un router móvil (MR) y de un ordenador fijo (CLIENTE). En esta configuración el MR es sólo para brindarle conexión inalámbrica al CLIENTE. La figura 4.11 muestra la relación entre estos tres elementos de red.

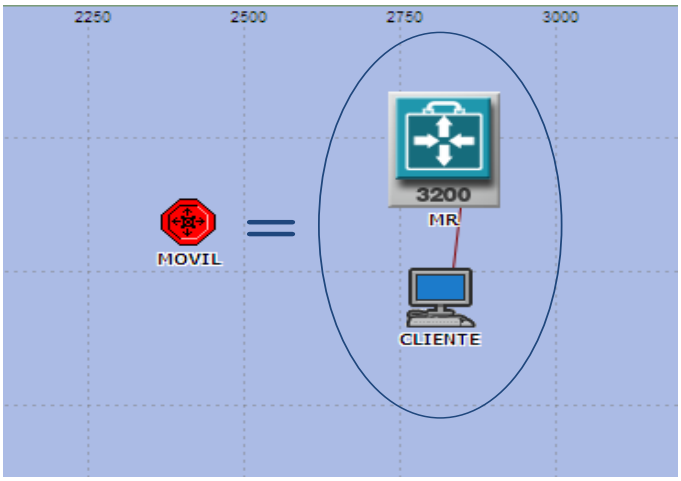


Figura 4.11Elementos que componen la subnet móvil

Se configura la aplicación de tráfico de voz G.723, la cual es soportada por los usuarios fijo y móvil. El códec de voz G.723 envía 33 frames de voz por segundo y cada uno con una longitud de 20 bytes, logrando de esta manera un data rate o tasa de transferencia de 5.33 kbps. En seguida se muestra el cálculo para obtener este data rate:

$$\left(\frac{1\ frame}{30\ ms}\right)\left(\frac{1000\ ms}{1\ s}\right)\left(\frac{20\ bytes}{frame}\right)\left(\frac{8\ bits}{1 byte}\right) = 5333.3333\ bps$$

Los elementos inalámbricos que son el usuario móvil, el HA y los tres FA tienen las siguientes características:

Soportan la versión g del estándar IEEE 802.11
Tienen una tasa de transmisión máxima de 54 Mbps.
Utilizan una potencia de transmisión de 18 dBm, lo que es igual a 63.0957 mW

En la tabla 4.5 se muestran los elementos que fueron configurados en los AP:

Nombre	BSSID	Canal de operación
HA	0	1
FA_1	1	6
FA_2	2	11
FA_3	3	1

Tabla 4.5Configuración de los AP

Al usuario móvil se le configura una trayectoria rectilínea con una velocidad de 22.2222 m/s, lo que es equivalente a 80 km/h y es la velocidad promedio a la que se mueve el tren del STC Metro.

En este modelo de red se implementa el protocolo Mobile IP a fin de que se puedan rutear los paquetes al usuario móvil a pesar de que éste se encuentre conectado en una red vecina y asociado a un ForeignAgent.

La tabla 4.6 muestra las direcciones IP de los elementos involucrados en Mobile IP de este modelo de simulación:

Nombre	DIRECCIÓN IP
CLIENT - MOBILE NODE	192.168.6.5/24
MOBILE ROUTER – MOBILE NODE	192.168.8.2/24
HOME AGENT	192.168.8.1/24

Tabla 4.6 Direcciones IP de los elementos involucrados en Mobile IP

Además de lo anterior, a este modelo de red se le configuró un ambiente de propagación vehicular cuyo Pathloss se calcula mediante la siguiente ecuación [17] [21].

$$PL[dB] = 40\,(1 - 4x10^{-3}h_{bs})log_{10}\left(\frac{R}{1x10^{3}}\right) - 18log_{10}h_{bs} + 21log_{10}\left(\frac{f}{1x10^{6}}\right) + 80 + s$$

Donde:

h_{bs} se refiere a la altura en metros a la que está puesto el AP con respecto al nivel del suelo.

R representa la distancia en metros entre el usuario móvil y el AP.

f expresa la frecuencia de operación en Hz.

s se utiliza para representar el valor de shadow fading.

Para obtener el valor de SNR se emplearon las siguientes ecuaciones [17].

$$Prx\ [dBm] = PIRE\ [dBm] + Grx\ [dBi] - PL\ [dB]$$

Donde:

Prx representa la potencia recibida.

$EIRP$ expresa la potencia isotrópica radiada efectiva.

Grx es la ganancia de la antena de recepción.

$$EIRP\ [dBm] = Ptx[dBm] + Gtx[dBi] - Lc[dB]$$

Donde:

Ptx representa la potencia de transmisión.

Gtx expresa la ganancia de la antena de transmisión .

Lc son las perdidas del cable y conectores .

$$N[dBm] = 10log_{10}(T * BW * k_0) + N_f[dB] + 30$$

Donde:

N representa el ruido térmico.

T denota la temperatura en grados kelvin.

BW expresa el ancho de banda en Hz .

k_0 es la constante de Boltzmann cuyo valor es $1.38x10^{-23}\ J/k$

N_f figura de ruido en el receptor.

$$SNR[dB] = Prx[dBm] - N[dBm]$$

Donde

SNR representa la cantidad de la relación señal a ruido.

Finalmente se le configuró a este modelo de simulación un valor de Bit Error Rate (BER) con respecto al tipo de modulación empleada, la cual es DPSK.

La figura 4.12 muestra la relación entre el BER y el SNR que se obtiene utilizando la modulación DPSK .

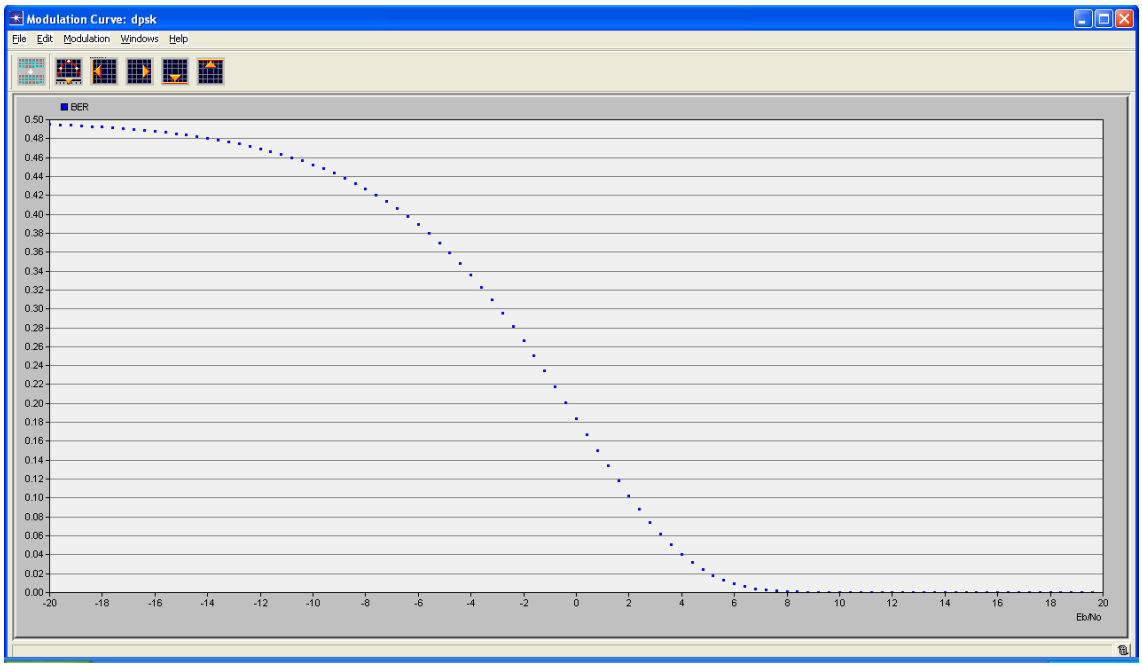


Figura 4.12 Relación entre el BER y el SNR con modulación DPSK [21].

Haciendo un zoom sobre esta gráfica, se puede observar que para un BER alrededor de $1x10^{-6}$ corresponde un valor de SNR igual a 11.2 dB, tal como lo muestra la figura 4.13.

.

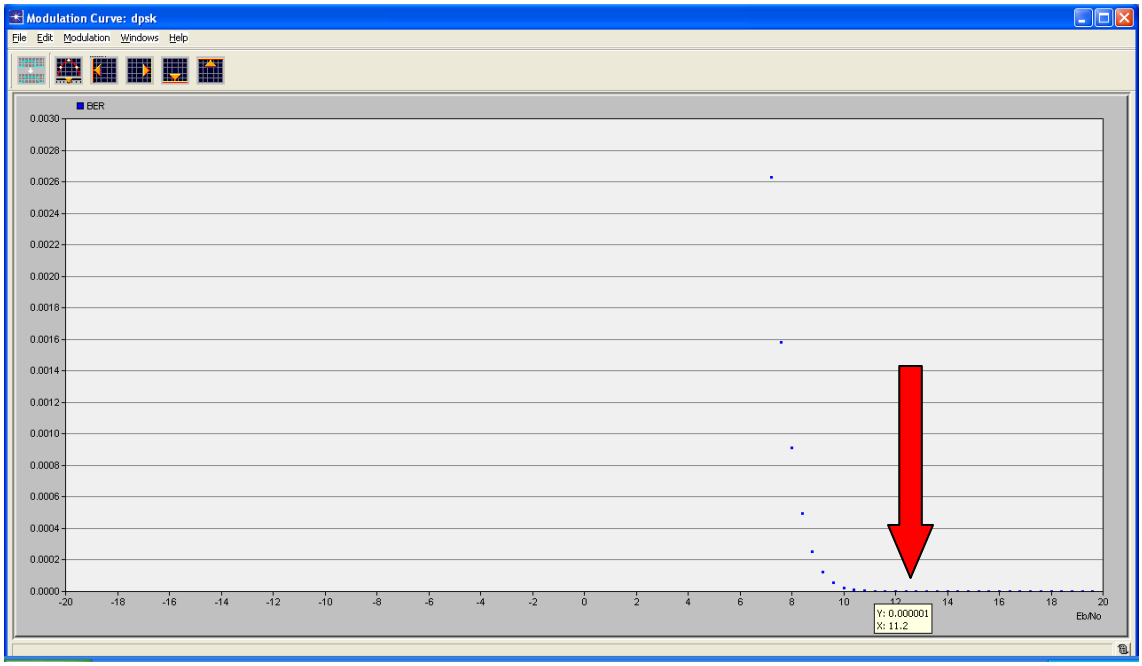


Figura 4.13 Zoom en la gráficade modulación dpsk donde se muestra la relación entre el BER y SNR [21].

Utilizando los siguientes valores:

$$h_{bs} = 4\ m$$
$$R = 233\ m$$
$$f = 2411000000\ Hz$$
$$s = 8\ dB$$
$$Lc = 2\ dB$$
$$Gtx = 10\ dB$$
$$Ptx = 18\ dBm$$
$$Grx = 10\ dB$$
$$BW = 22000000\ Hz$$
$$N_f = 2\ dB$$
$$T = 290\ K$$

El resultado de las ecuaciones es el siguiente:

$$PL[dB] = 40\ [1 - 4x10^{-3}(4)]log_{10}\left(\frac{233}{1x10^{3}}\right) - 18log_{10}(4) + 21log_{10}\left(\frac{2411000000}{1x10^{6}}\right) + 80 + 8$$

$$\boxed{PL[dB] = 123.2881}$$

$$EIRP\ [dBm] = 18[dBm] + 10[dBi] - 2[dB]$$

$$\boxed{EIRP\ [dBm] = 26}$$

$$Prx\ [dBm] = 26\ [dBm] + 10\ [dBi] - 123.2881\ [dB]$$

$$\boxed{Prx\ [dBm] = -87.2881}$$

$$N[dBm] = 10log_{10}[(290)(22000000)(1.38x10^{-23})] + 2[dB] + 30$$

$$\boxed{N[dBm] = -98.5530}$$

$$SNR[dB] = -87.2881[dBm] + 98.5530[dBm]$$

$$SNR[dB] = 11.2649$$

Por lo tanto, conforme a los datos anteriores y a las ecuaciones vistas en esta sección, se tiene que cada AP tiene un radio de región de cobertura de aproximadamente 233 metros para que a esta distancia se tenga un SNR de 11.2 dB.Tomando en cuenta que para llevarse a cabo un Handover se necesita un traslape del 15, 20 y hasta un 30% entre regiones de cobertura de AP vecinos, se coloca una distancia de separación de 431 m entre AP adyacentes.

4.2 Pruebas de análisis

4.2.1 Pruebas sobre el modelo instrumental

En este apartado se muestran las capturas de tráfico obtenidas en las numerosas pruebas de Handoff de capa 2 y 3. Estas capturas se realizan con el Software Wireshark [22], el registro de intensidad de señal y SNR se obtienen del Software Network Stumbler[23] y se corrobora el cambio de AP así como de dirección IP en su caso con los datos que arroja el comando *ipconfig/all* del Símbolo de Sistema de Windows XP.

4.2.1.1 Pruebas de Handover de Capa 2

La figura 4.14 muestra la captura de tráfico que se obtuvo al realizar una llamada desde el Softphone con número de Identificación 111 (usuario móvil) al Softphone con número de extensión 113 (usuario fijo). Esta llamada se realizó utilizando la topología para un Handover de capa 2 y considerando que al usuario móvil se le asignó la dirección IP estática 192.168.20.10/24 y al usuario fijo la IP 192.168.20.50/24.

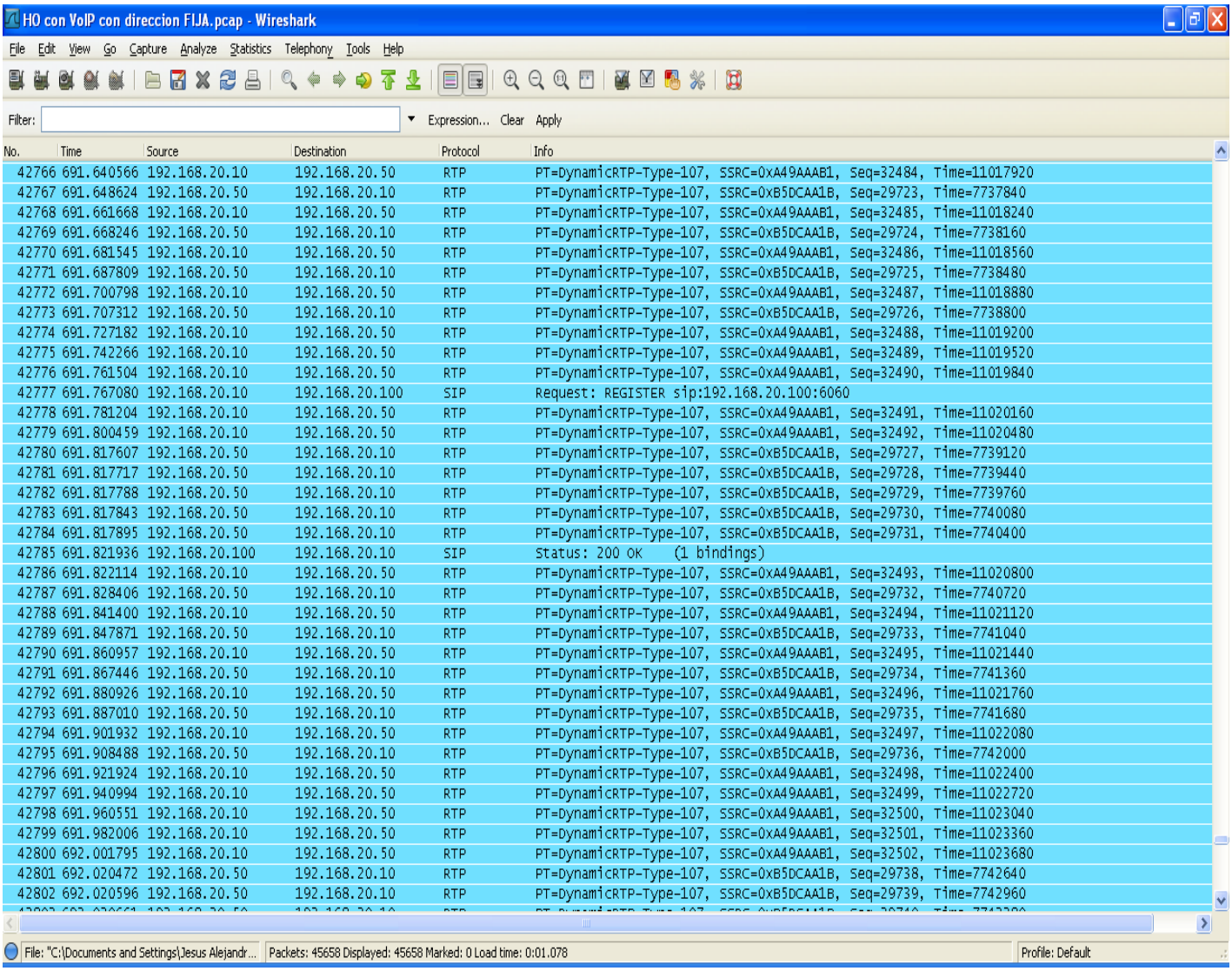


Figura 4.14 Captura de tráfico en Handoff de capa 2 con dirección IP fija en el usuario móvil.

La figura 4.15 muestra la intensidad de señal que recibimos del AP al cual estamos conectados y el valor de SNR, éstos son -28 dBm y 72 dB respectivamente con un valor de ruido igual a -100 dBm. En la misma imagen se puede observar que en la columna de *Channel* abreviada como *Chan*el software Network Stumbler coloca un asterisco (*) para indicar que estamos conectados a ese Access Point.

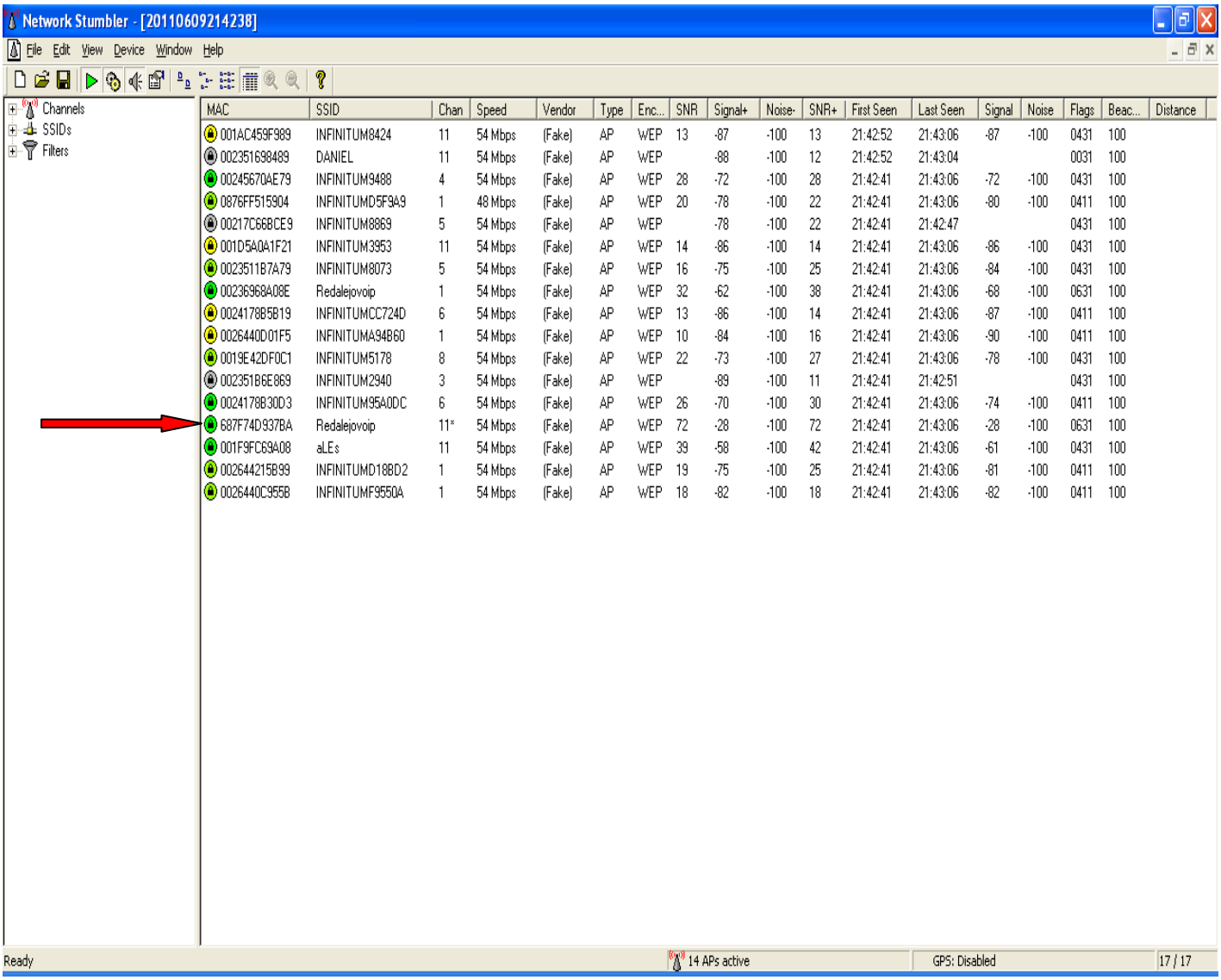


Figura 4.15Intensidad de la señal que se recibe del AP inicial

Con la llamada entre los softphones en curso y al caminar desde donde se encontraba el AP inicial hacia el nuevo AP, se registran lo siguientes datos que se muestran en la figura 4.16:

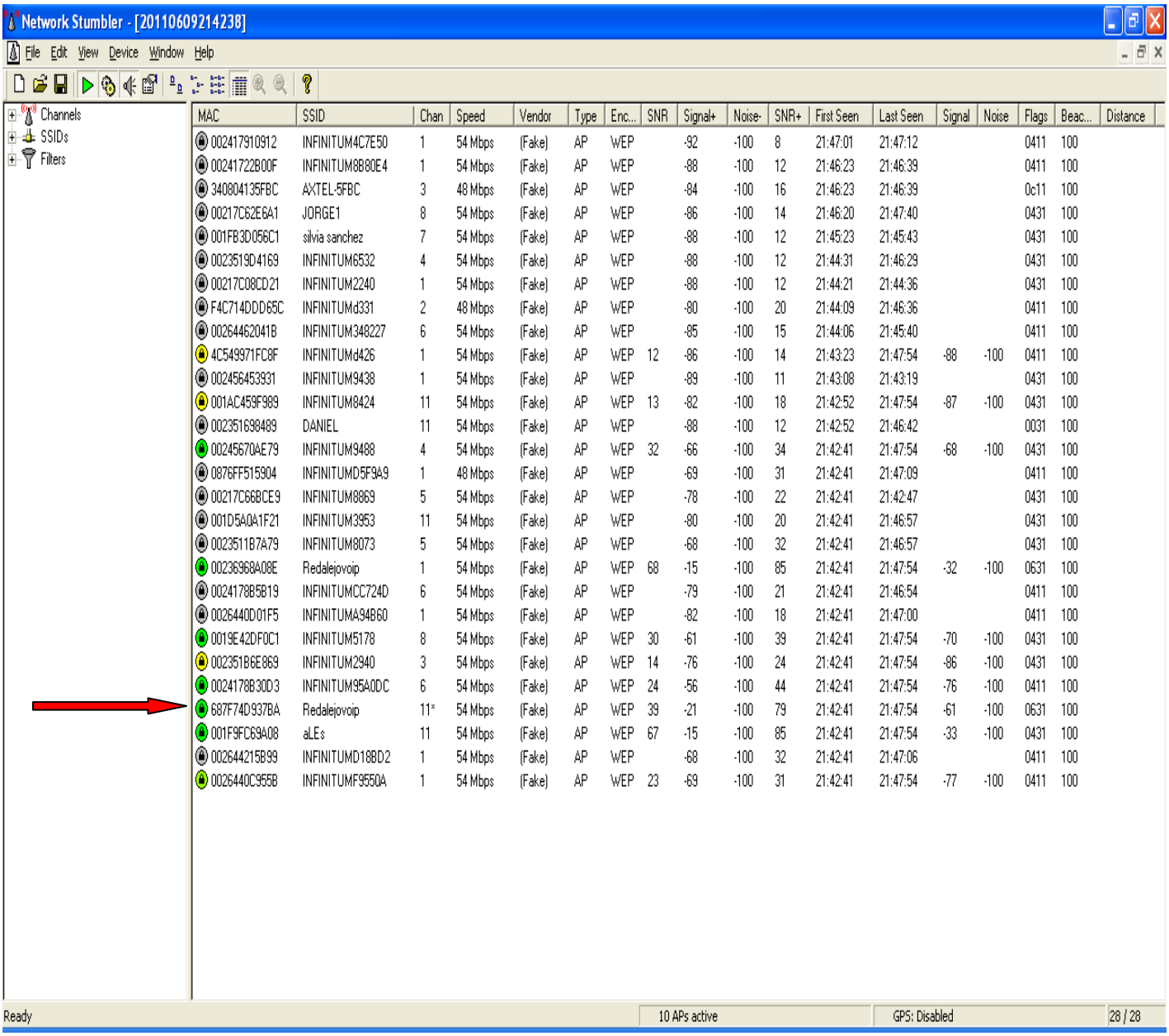


Figura 4.16 Datos obtenidos cuando el usuario móvil esta junto al nuevo AP

Se puede observar en la imagen anterior que estando junto al nuevo AP el usuario móvil no decide cambiarse a éste, ello es debido a que recibe una intensidad de señal igual a -61 dBm y un SNR de 39 dB. Para que se lleve a cabo un Handover por parte del usuario móvil se colocan estructuras metálicas alrededor del AP que opera en el canal 11 del estándar y con ello se obliga a disminuir la intensidad de señal en 11 dBm.

De la manera anterior se registra el cambio de AP cuando el usuario móvil tiene una intensidad de señal igual a -72 dBm y un SNR de 28 dB, estas características se pueden observar en la figura 4.17:

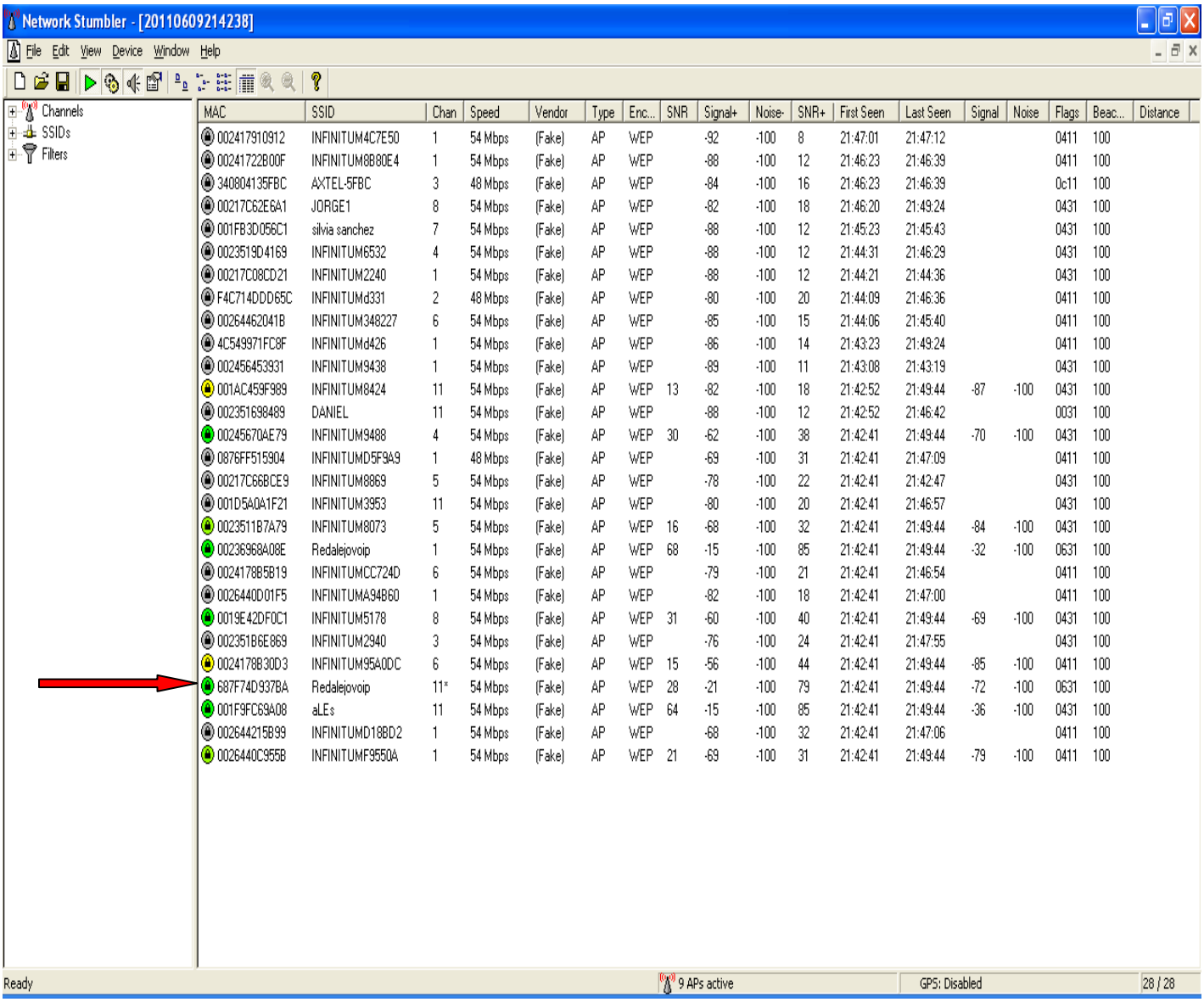


Figura 4.17 Datos obtenidos del AP anterior cuando se coloca la estructura metálica.

Inmediatamente el software Network Stumbler coloca en la columna de *Chan* un signo positivo (+) al AP que abandona y coloca un asterisco junto al AP al cual se encuentra conectado. Esto se puede ver en la figura 4.18:

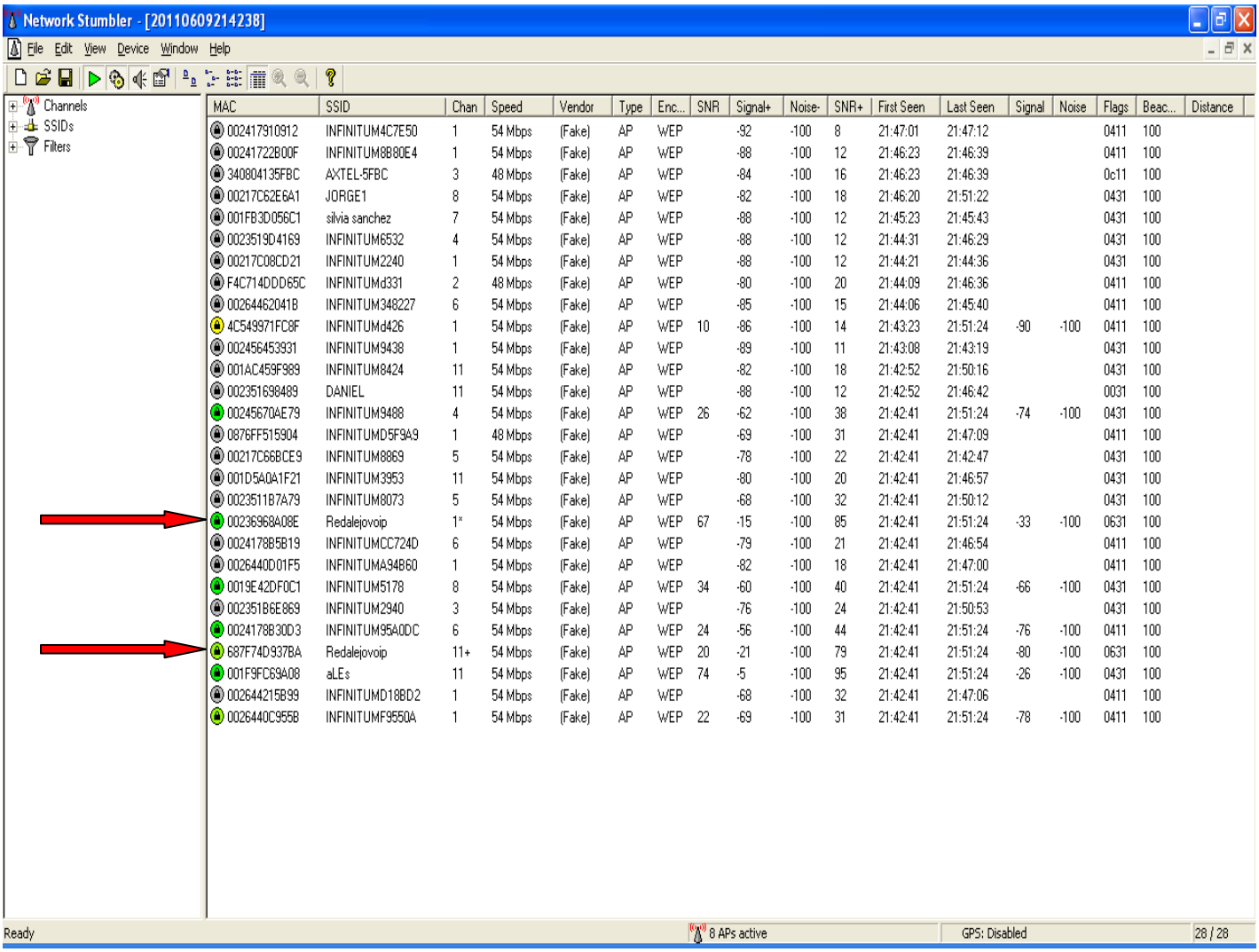


Figura 4.18. Datos obtenidos al cambiar del AP anterior al AP nuevo.

Durante todo el proceso se obtiene periódicamente la dirección IP del usuario móvil, la cual se muestra en la figura 4.19:

Figura 4.19 Dirección IP del usuario móvil.

Como se puede observar la dirección IP no cambia en todo el proceso, y se lleva a cabo un Handover de capa 2 exitoso al cambiarse el usuario móvil entre dos AP pertenecientes a la misma red sin finalizar o terminar la llamada en curso.

Posteriormente se realizó una prueba similar a la anterior pero habilitando la asignación automática de dirección IP en el usuario móvil. Con ello se obtuvo la siguiente captura de tráfico que se muestra en la figura 4.20:

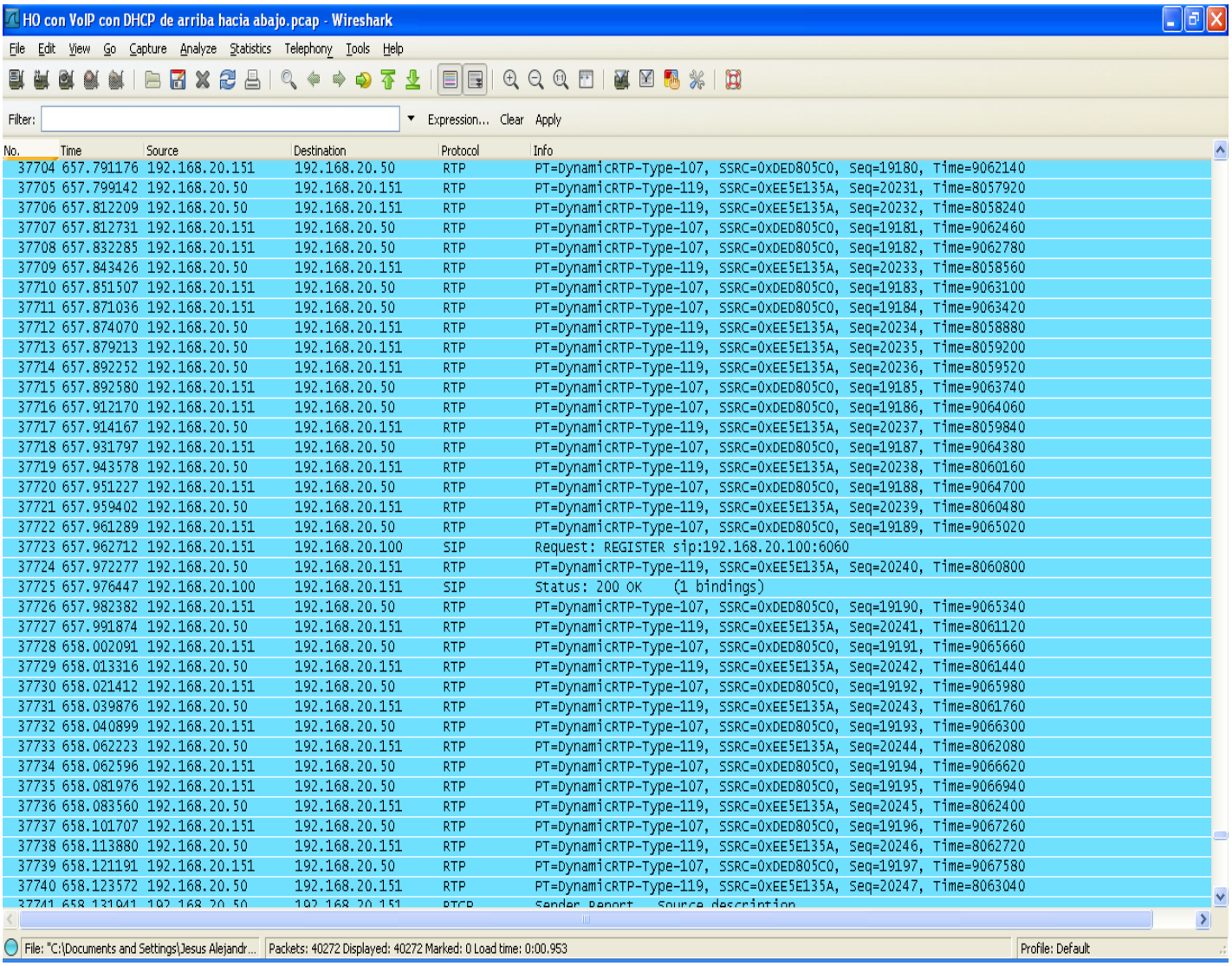


Figura 4.20Captura de tráfico habilitando la asignación automática de dirección IP en el usuario móvil

Como se puede visualizar en la figura 4.20, el usuario móvil adquiere la dirección 192.168.20.151/24 conectado al primer AP WRP 400 mientras que el usuario fijo mantiene la misma dirección IP 192.168.20.50/24. Se puede corroborar la dirección IP del usuario móvil visualizando el campo de *Dirección IP* de la figura 4.21:

Figura 4.21 Nueva dirección adquirida del usuario móvil

La figura 4.22 muestra que junto al primer AP el usuario móvil registra un valor de intensidad de señal de -28 dBm, un SNR de 72 dB y un ruido de -100 dBm:

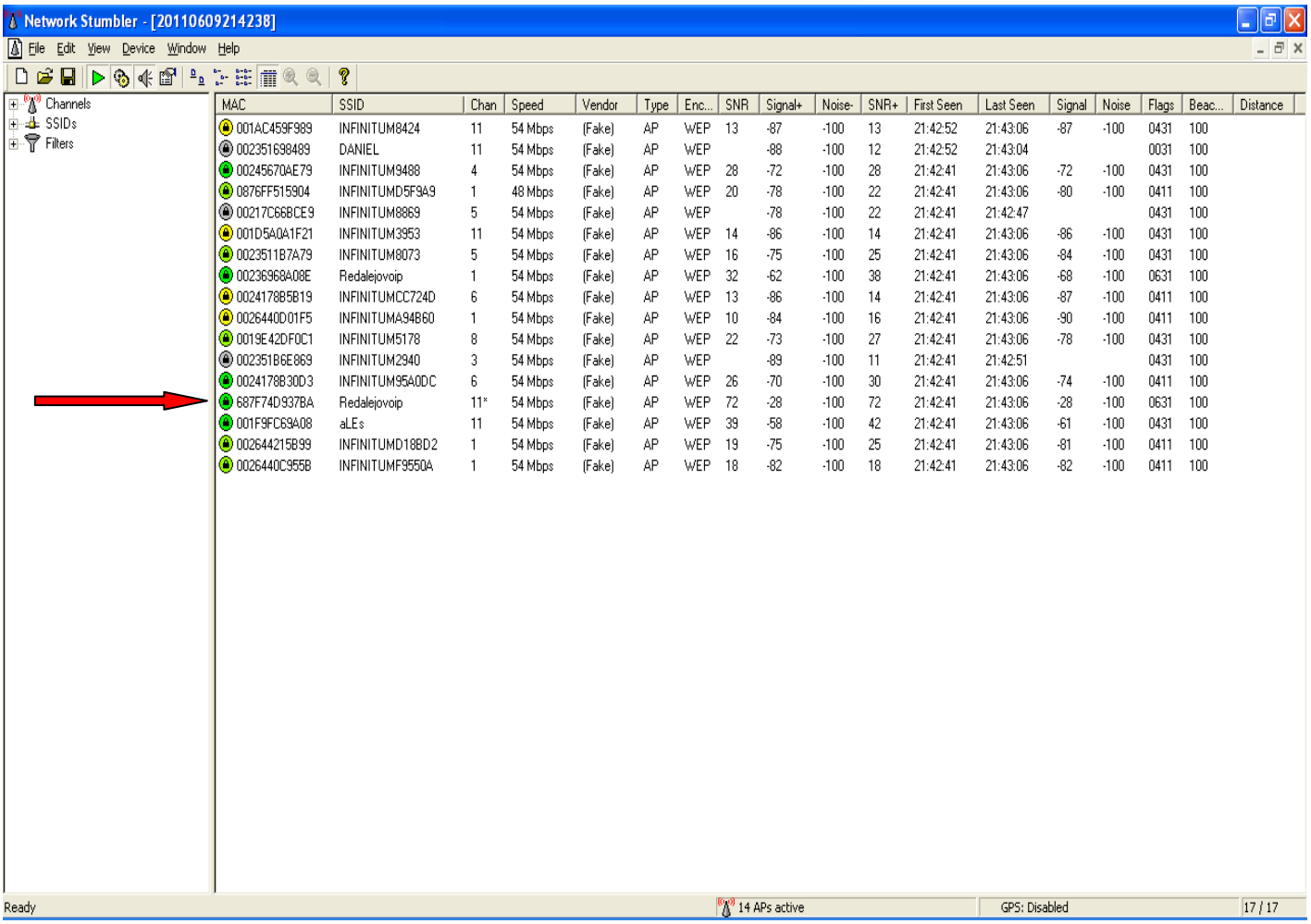


Figura 4.22. Valores obtenidos del usuario móvil en el AP nuevo.

Después de llegar caminando con el usuario móvil al otro AP WRP 400, se sigue la misma técnica para obligar a que se lleve a cabo el cambio de Access Point. Este cambio ocurre cuando el usuario móvil registra del primer AP un valor de intensidad de señal igual a -71 dBm y un SNR de 29 dB, cuando el móvil se conecta al segundo AP se recibe de éste una intensidad de señal igual a -24 dBm y un SNR de 76 dB, durante el proceso el valor del ruido permanece constante igual a -100 dBm. Lo anterior se puede observar en la figura 4.23:

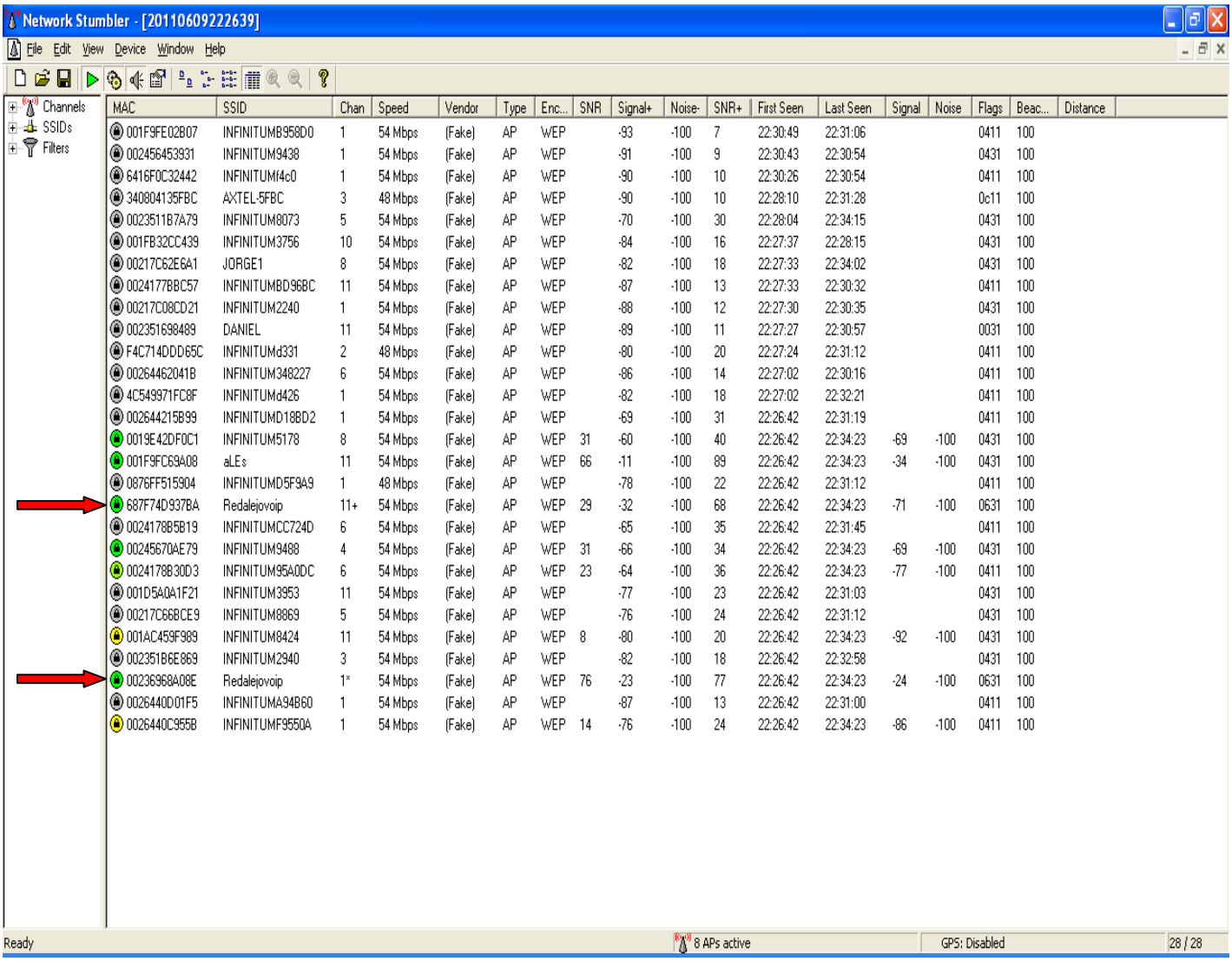


Figura 4.23 Valores de SNR e intensidad de la señal del AP anterior y AP nuevo.

Al término de este proceso se registró que el usuario móvil nunca cambió su dirección IP que había adquirido desde un inicio mediante DHCP. Esto es lo que se esperaba puesto que se trata de un Handover de capa 2. La figura 4.24 muestra que el campo de Dirección IP no cambia con respecto al obtenido en el inicio de esta prueba:

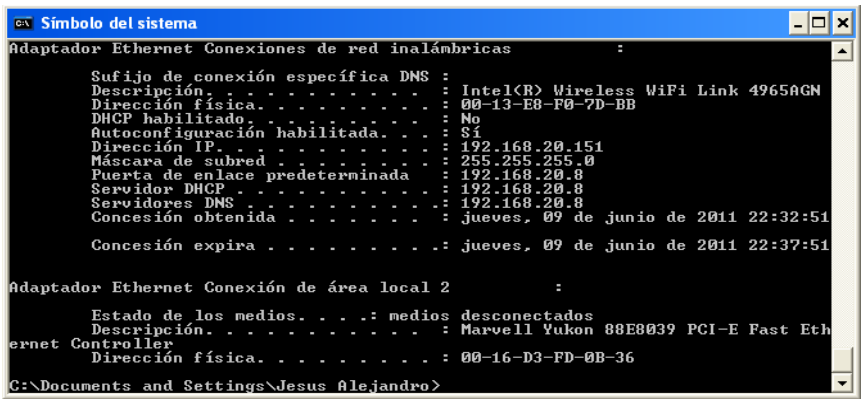


Figura 4.24 Dirección IP del usuario móvil

Las pruebas realizadas indican que en un Handoff de capa 2 una vez que el usuario móvil se autentica con el primer AP y obtiene una dirección IP válida en la red, la conserva durante y después del proceso de Handover.

El Handoff de capa 2 se lleva a cabo de una manera *transparente* dado que durante el proceso de Handover de capa 2 el usuario móvil no obtiene una nueva dirección IP ni vuelve a autenticarse con el nuevo AP.

4.2.1.2 Pruebas de Handover de Capa 3

Para llevar a cabo esta sección de pruebas se utilizó la topología para un Handoff de capa 3 y se realizó una llamada desde el Softphone con número de Identificación 111 (usuario móvil) al Softphone con número de extensión 113 (usuario fijo). Aeste último se le asignó la dirección IP estática de 192.168.20. 5/24 mientras que el usuario móvil obtuvo su dirección IP mediante DHCP. La figura 4.25 muestra la captura de tráfico en el momento en que se lleva a cabo el Handover mientras se mantiene activa la llamada entre softphones.

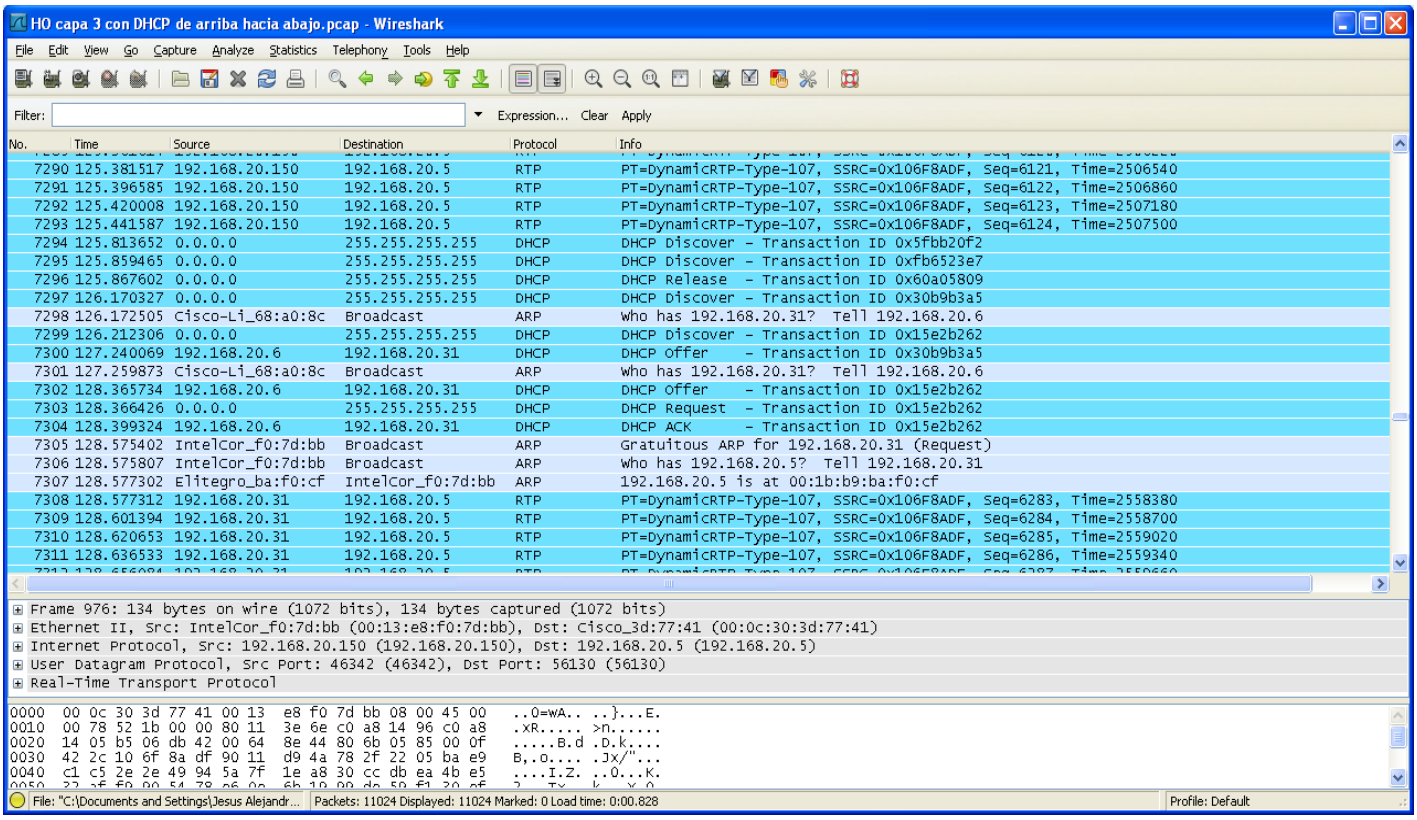


Figura 4.25 Captura de tráfico en Handoff de capa 3 con WMM y DHCP habilitados en el usuario móvil.

Es importante comentar que la captura de tráfico anterior se realizó teniendo habilitado el campo de WMM, es decir, se habilitó la función de Calidad de Servicio en redes WiFi.

La figura 4.26 muestra la dirección IP del usuario móvil que obtuvo mediante DHCP al conectarse con el primer o anterior AP WRP 400:

Figura 4.26 Dirección IP del usuario móvil que obtuvo mediante DHCP al conectarse con el primer AP.

Se puede observar en la figura 4.24 que estando asociado al primer o anterior AP con dirección IP 192.168.20.131/25 perteneciente a la red 192.168.20.128, el usuario móvil adquiere automáticamente la dirección IP 192.168.20.150/25.

Durante el proceso de Handover, el usuario móvil se asocia al segundo o nuevo AP con dirección IP 192.168.20.6/25 perteneciente a la red 192.168.20.0 y adquiere mediante DHCP la dirección IP 192.168.20.31/25. Lo anterior se puede observar en los campos de Puerta de enlace predeterminada, Máscara de subred y Dirección IP de la figura 4.27.

Figura 4.27 Dirección IP del usuario móvil que obtuvo mediante DHCP al conectarse con el nuevo AP.

Es relevante comentar que la llamada se mantuvo activa durante y después del proceso de Handoff, el cual para este caso, en que se mantuvieron habilitadas las funciones WMM y DHCP, tuvo una duración de 3.1557 segundos, tal como se muestra en la sección 5.1 “Análisis del modelo de instrumentación para el Handoff de capa 3”.

La figura 4.28 muestra la captura de tráfico en un Handover de capa 3, manteniendo la misma dirección IP estática en el usuario fijo y haciendo un mapeo de dirección MAC a dirección IP mediante DHCP reservado para el usuario móvil. De esta manera, el segundo AP al reconocer al usuario móvil con dirección MAC 00:13:E8:F0:7D:BB, le asigna durante el proceso de Handoverla dirección IP 192.168.20.31/25 establecida en su tabla de mapeo.

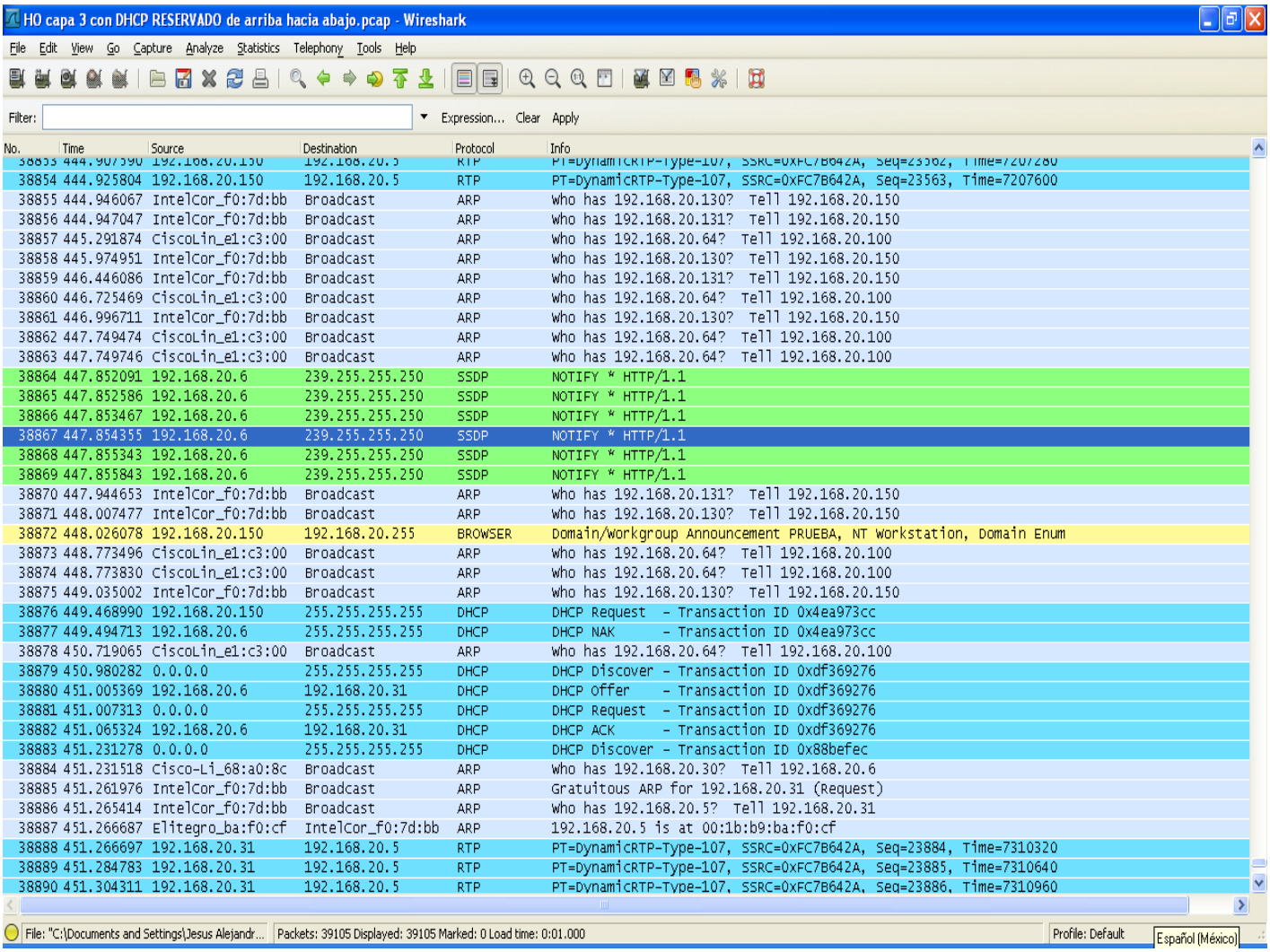


Figura 4.28 Captura de tráfico en Handoffde capa 3 con WMM y DHCP reservado.

Es importante comentar que en esta prueba se sigue habilitando el campo de WiFi Multimedia (WMM); sin embargo, una vez finalizado el proceso de Handover y habiendo adquirido el usuario móvil la nueva dirección IP, la llamada automáticamente se finaliza. El proceso de Handover con esta configuración tiene una duración total de 6.3408 segundos, tal como se muestra en apartado 5.1 “Análisis del modelo de instrumentación para el Handoff de capa 3”.

Finalmente se probó el no habilitar el campo de WMM para que no se implementara QoS y dejar habilitado la asignación de dirección IP mediante DHCP para el usuario móvil. Se continúa asignando la dirección IP estática 192.168.20.5/25 para el usuario fijo y de esta manera se logra la captura de tráfico que se muestra en la figura 4.29:

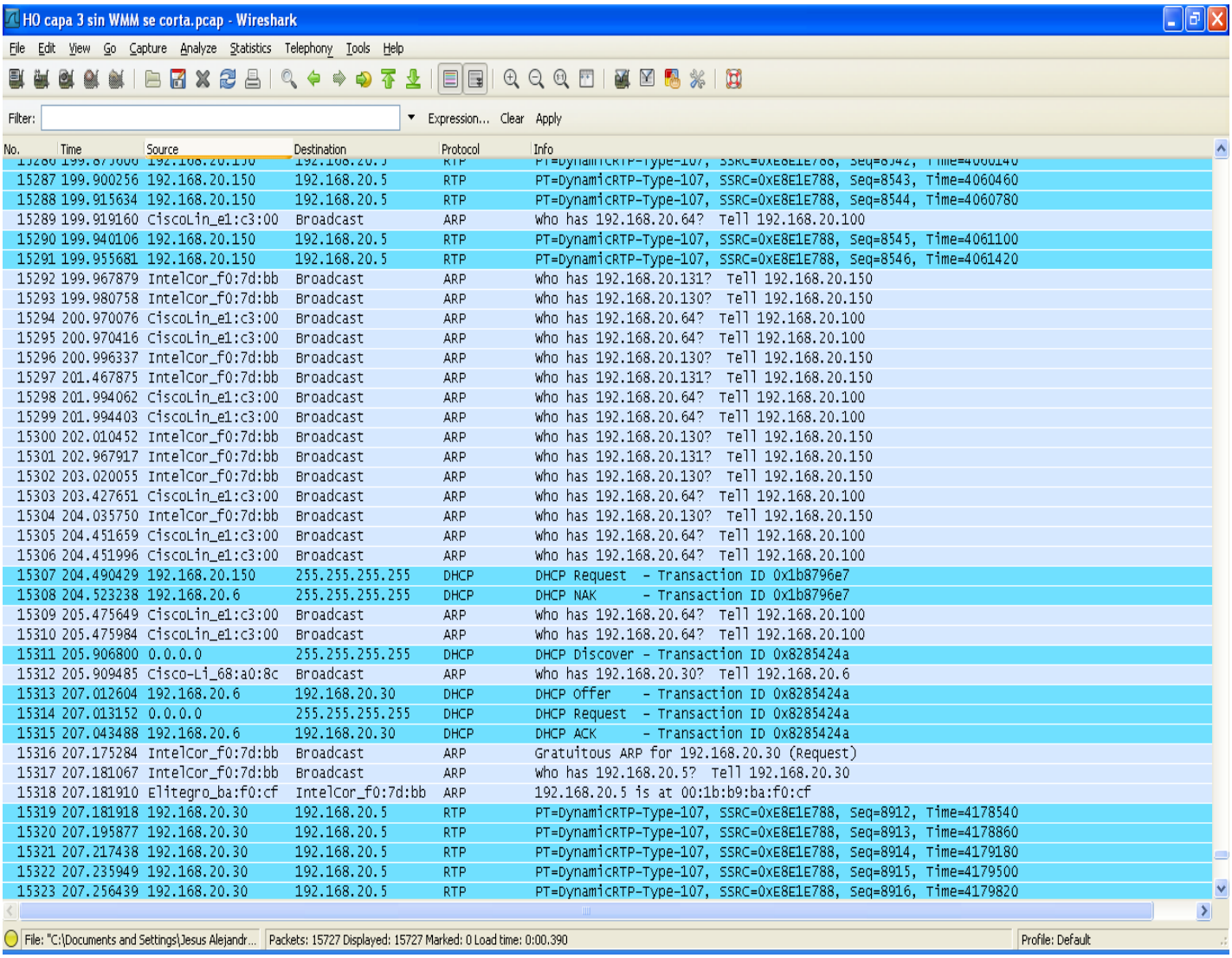


Figura 4.29 Captura de tráfico en Handoff de capa 3 sin WMM y DHCP habilitado para el usuario móvil.

Se puede observar en la captura de la Figura 4.29, que inicialmente el usuario móvil al estar conectado al primer AP obtiene la dirección IP 192.168.20.150/25 y durante el proceso de Handover obtiene la dirección IP 192.168.20.30/25 del segundo AP, no obstante, segundos después la llamada se finaliza de forma automática como sucedió con el caso anterior.

Para este caso en que no se habilitó la función WMM y el usuario móvil obtuvo su dirección IP a través de DHCP, se obtuvo una duración en el proceso de Handover de 7.2662 segundos.

CAPÍTULO 5

Resultados

En este capítulo se muestran los resultados obtenidos tanto en las simulaciones de los modelos de red hechos con OPNET Modeler, asícomo en las pruebas físicas hechas con el equipo instrumental.

5.1 Análisis del modelo de instrumentación para el Handoff de capa 2

Como se pudo observar en la realización de las pruebas correspondientes a este apartado, el Handover de capa 2 se realizó exitosamente por lo que se deduce que la topología de red implementada para realizar este Handoff es adecuada.

Asimismo, los resultados de las pruebas para este Handover indican que se trata de un Handoff “suave”. Esto debido a que se realizó el Handover entre los dos AP WRP400 pertenecientes al mismo segmento de red y en todo el proceso se mantuvo la llamada activa.

Es importante resaltar que las pruebas muestran que el Handover de capa 2 se lleva a cabo de una forma *transparente,* ya que el usuario móvil nunca cambió su dirección IP durante ni después del proceso de Handoff de capa 2, ni volvió a autenticarse con el nuevo AP. Siempre conservó su dirección de red que obtuvo de forma dinámica mediante el servicio de DHCP y de forma estática a través de una asignación manual.

5.2Análisis del modelo de instrumentación para el Handoff de capa 3

Los resultados que arrojan las pruebas correspondientes al Handover de capa 3 indican que la topología de red implementada para realizar este Handoff es adecuada. Lo anterior se debe, principalmente, a que teniendo a cada uno de los AP WRP 400 en una red diferente, se pudo lograr que el usuario móvil pudiera cambiarse de AP y por lo tanto de red manteniendo en todo momento la llamada activa.

La figura 5.1 muestra el esquema de señalización que se creó a partir de la captura de tráfico realizada con WireShark para el caso en el que se activó la característica WMM y el usuario móvil obtuvo su dirección IP a través de DHCP.

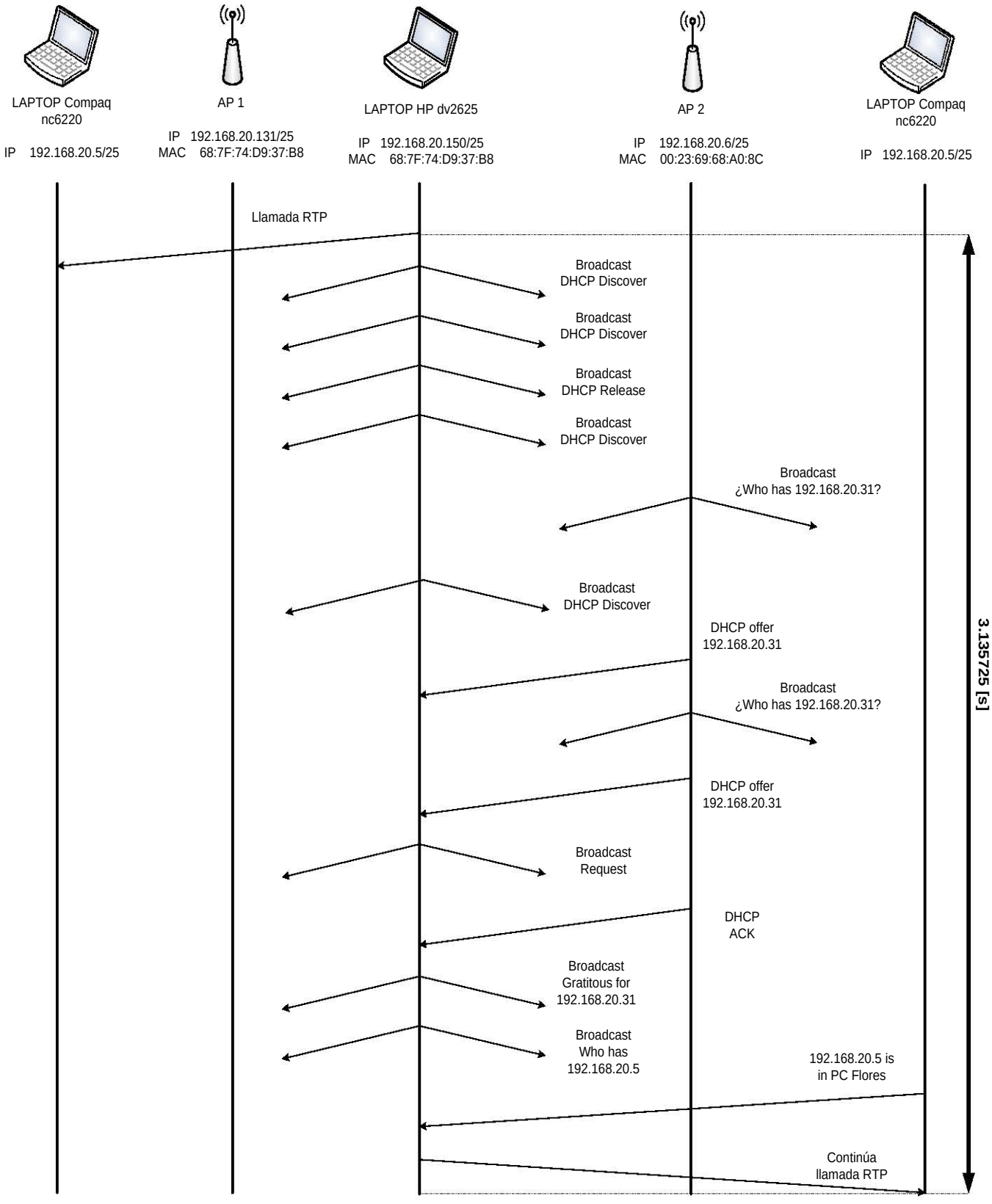


Figura 5.1 Esquema de señalización a partir de la captura de tráfico de WireShark

Como se puede ver en la figura anterior la llamada de VoIP se mantiene activa durante todo el proceso de Handover. En la figura 5.1 se muestra que a partir de la captura del último paquete de voz que envía el usuario móvil al usuario fijo utilizando el protocolo RTP (Real-Time Protocol), se inicia el proceso de Handover de capa 3 el cual tiene una duración de 3.1557 segundos.

Este tiempo supera por mucho la latencia de los paquetes de voz que es de 150 ms. Sin embargo, debido a que la llamada se mantuvo activa antes y después del proceso de Handover, se entiende que se trata de un Handoff “suave”.

En la figura 5.1 se muestra que durante el proceso de Handover, el usuario móvil se cambió de la dirección IP 192.168.20.150/25 a la dirección IP 192.168.20.31/25. Lo anterior indica que el usuario móvil logró cambiarse de red y con ello efectuó el Handover de capa 3.

La figura 5.2 muestra el esquema de señalización que se creó a partir de la captura de tráfico en el caso en que se activó la característica WMM, pero el usuario móvil obtiene su dirección IP a través de DHCP reservado.

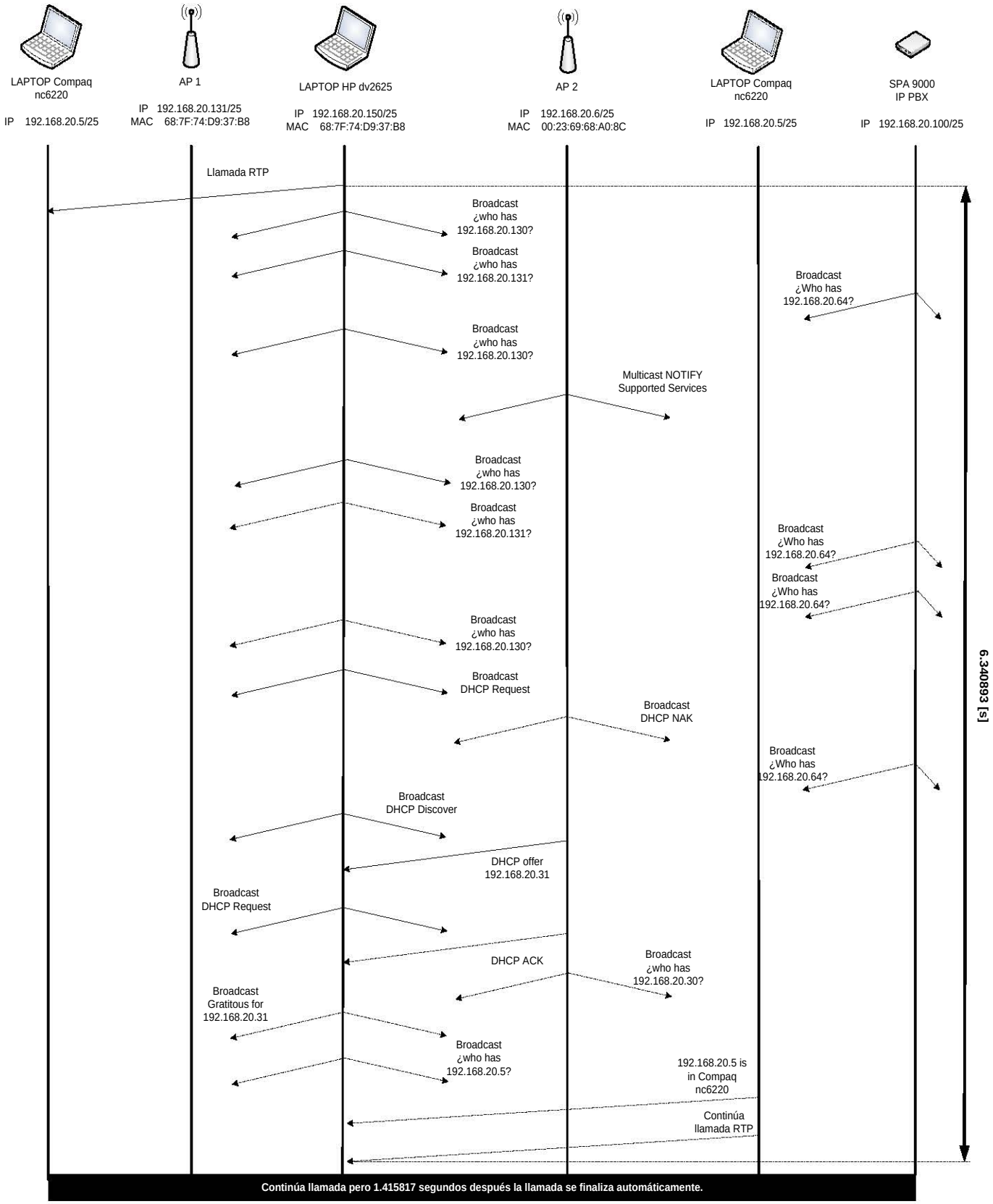


Figura 5.2 Esquema de señalización con WMM y una IP asignada mediante DHCP reservado.

La figura 5.2 muestra que el proceso de Handover de capa 3 en estas condiciones tiene una duración de 6.3408 segundos, incrementándose al doble que en el caso anterior.

En el diagrama de la figura 5.2 se observa el mapeo de dirección MAC a dirección IP que el AP 2 efectúa sobre el usuario móvil, es decir, al reconocer la dirección MAC 00:13:E8:F0:7D:BB le asigna la dirección IP 192.168.20.31/25.

Es importante comentar que en esta configuración de red, 1.4158 segundos después que haber terminado el proceso de Handover la llamada de voz se finaliza automáticamente. Por lo que se concluye que no es bueno tener una tabla de mapeo de direcciones MAC a direcciones IP y que lo más recomendable es que el direccionamiento se haga en función del servicio de DHCP.

5.3Análisis del modelo de simulación para el Handoff de capa 2 y capa 3

Los resultados obtenidos a través de la topología de red que se implementó en el simulador de redes OPNET Modeler son los siguientes.

La figura 5.3 muestra los paquetes recibidos por el usuario móvil. En esta figura se puede observar que el móvil recibe sólo durante 7 segundos los 33 frames por segundo que especifica el códec de voz G.723.

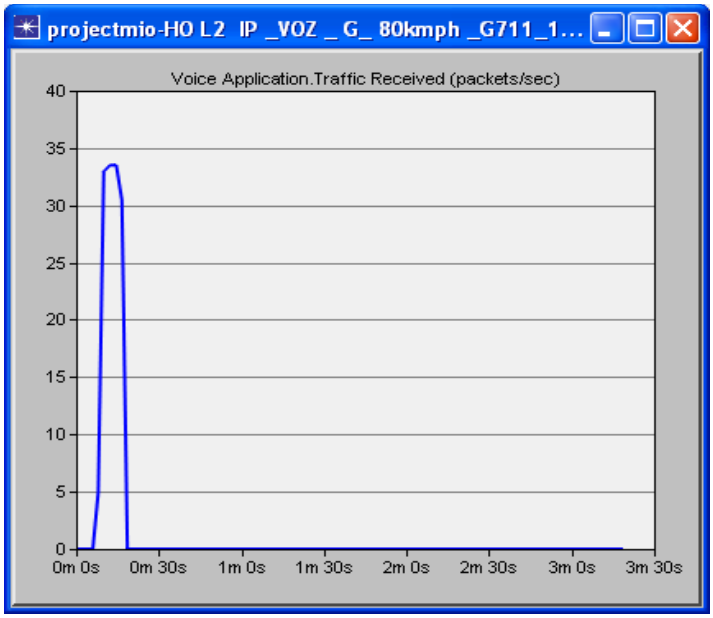


Figura 5.3 Paquetes recibidos por el usuario móvil

Es importante mencionar que este tráfico recibido es proveniente sólo del *Home Agent* y que el usuario móvil al recorrer su trayectoria no se puede conectar a ForeignAgent alguno.

La figura 5.4 muestra el retardo, el cual no supera los 150 ms establecidos como máximo para un paquete de voz. Podemos concluir que al menos el retardo es adecuado.

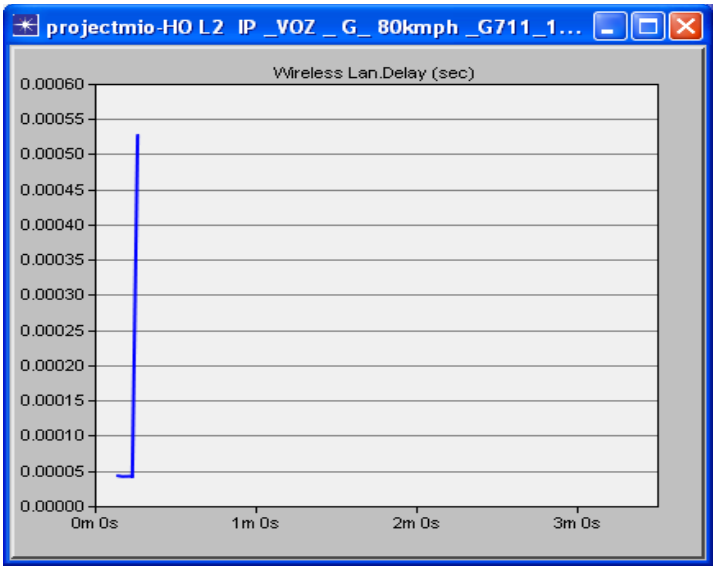


Figura 5.4 Retardo

La figura 5.5 muestra los paquetes enviados por el usuario fijo hacia el usuario móvil. Esta figura expresa que sí se están enviando los 33 frames por segundo que especifica el códec de voz G.723.

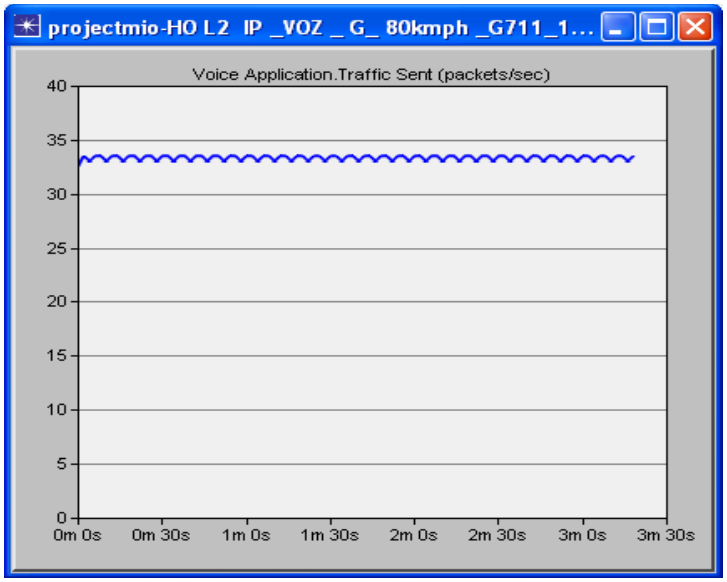


Figura 5.5 Paquetes enviados por el usuario fijo hacia el usuario móvil.

Debido a que el usuario móvil al recorrer su trayectoria no se puede conectar a ForeignAgent alguno, conesta misma topología de red se logra imprimir en la consola del simulador OPNET Modeler los valores de Pathloss, Potencia recibida y SNR. A fin de comprobar que los valores obtenidos con el simulador sean correctos, éstos se calculan de forma simultánea en Excel. Posteriormente, los datos obtenidos por ambos medios se grafican y comparan, los resultados se observan en las figuras 5.6, 5.7 y 5.8

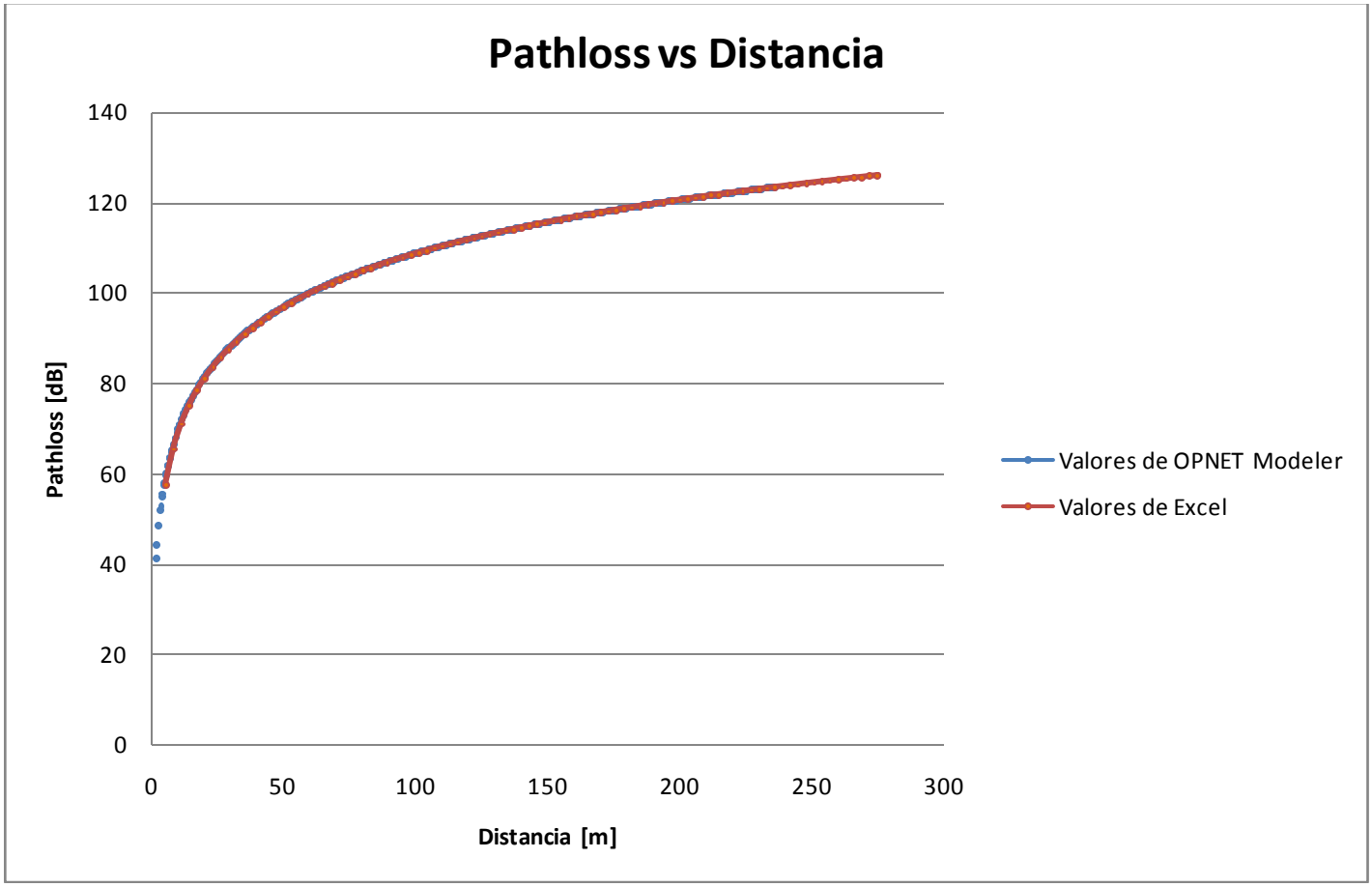


Figura 5.6 Pathloss obtenido a partir de los valores de OPNET Modeler y Excel

Se puede observar que las curvas de la gráfica anterior son muy semejantes, sin embargo, existe una pequeña diferencia al inicio de éstas la cual se debe principalmente a la distancia inicial que hay entre el usuario fijo y el *Home Agent*. Por una parte se tiene una distancia de separación de 1.9 metros en el modelo de red de OPNET modeler, mientras que en Excel esta misma distancia son 5 metros.

La figura 5.7 muestra la potencia que el usuario móvil recibe del *Home Agent*a lo largo de su trayectoria. Se puedeobservar nuevamente que las dos curvas de esta figuraobtenidas a partir de los valores de OPNET Modeler y Excel son muy parecidas, sin embargo, muestran el mismo efecto en su inicio debido a la diferencia en la distancia de separación que se comentó anteriormente.

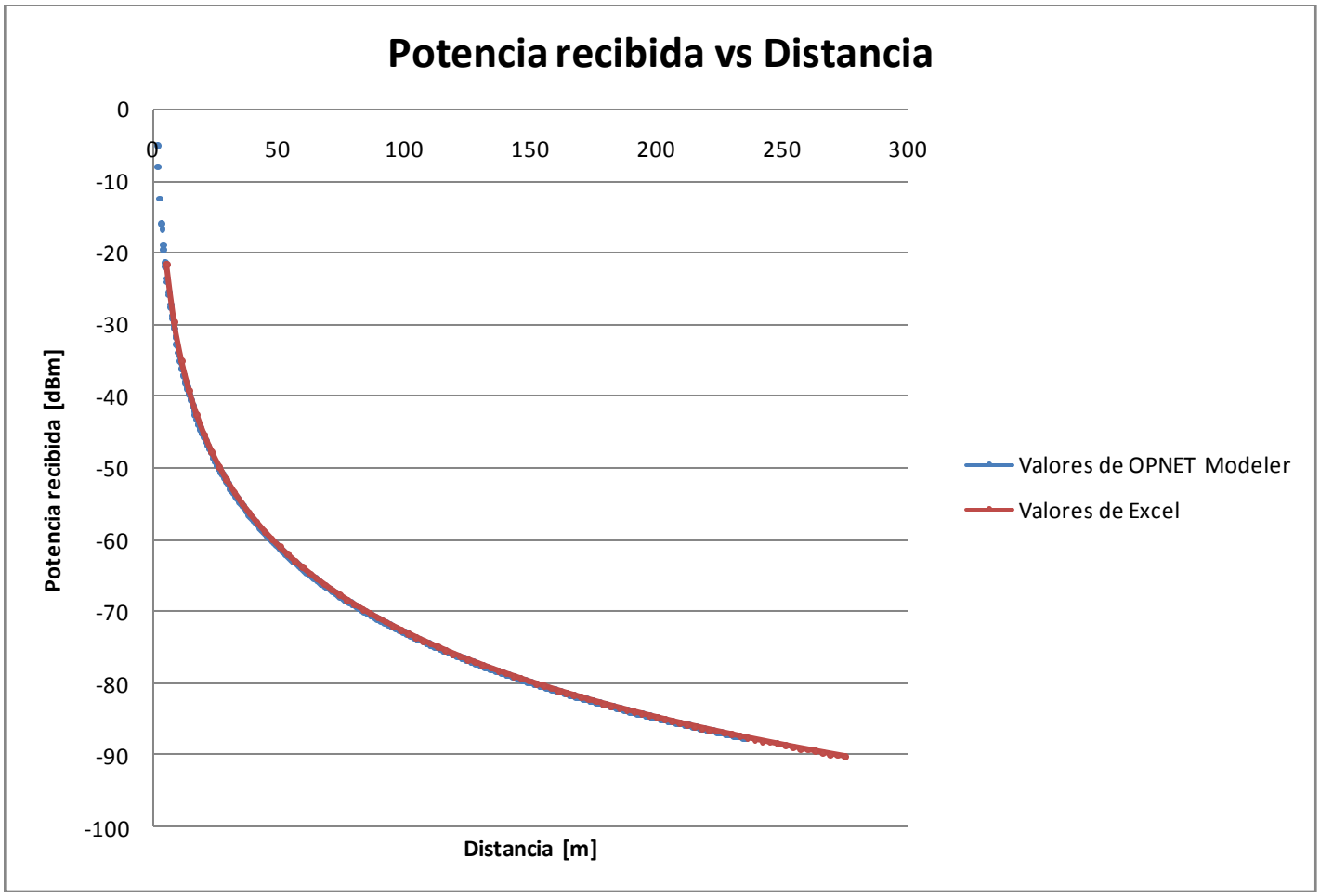


Figura 5.7 Potencia recibida creadacon los valores de OPNET Modeler y Excel

Por su parte la figura 5.8 muestra el valor de la Relación Señal a Ruido (SNR) que el usuario móvil registra durante el recorrido de su trayectoria. Ambas curvasde esta figura son muy parecidas entre sí y las dos registran un SNR de aproximadamente 11.2 dB.

Hay que recordar que por el tipo de modulación que se está utilizando, a un valor de SNR igual a 11.2 dB corresponde un valor de Bit Error Rate (BER) igual a $1x10^{-6}$.

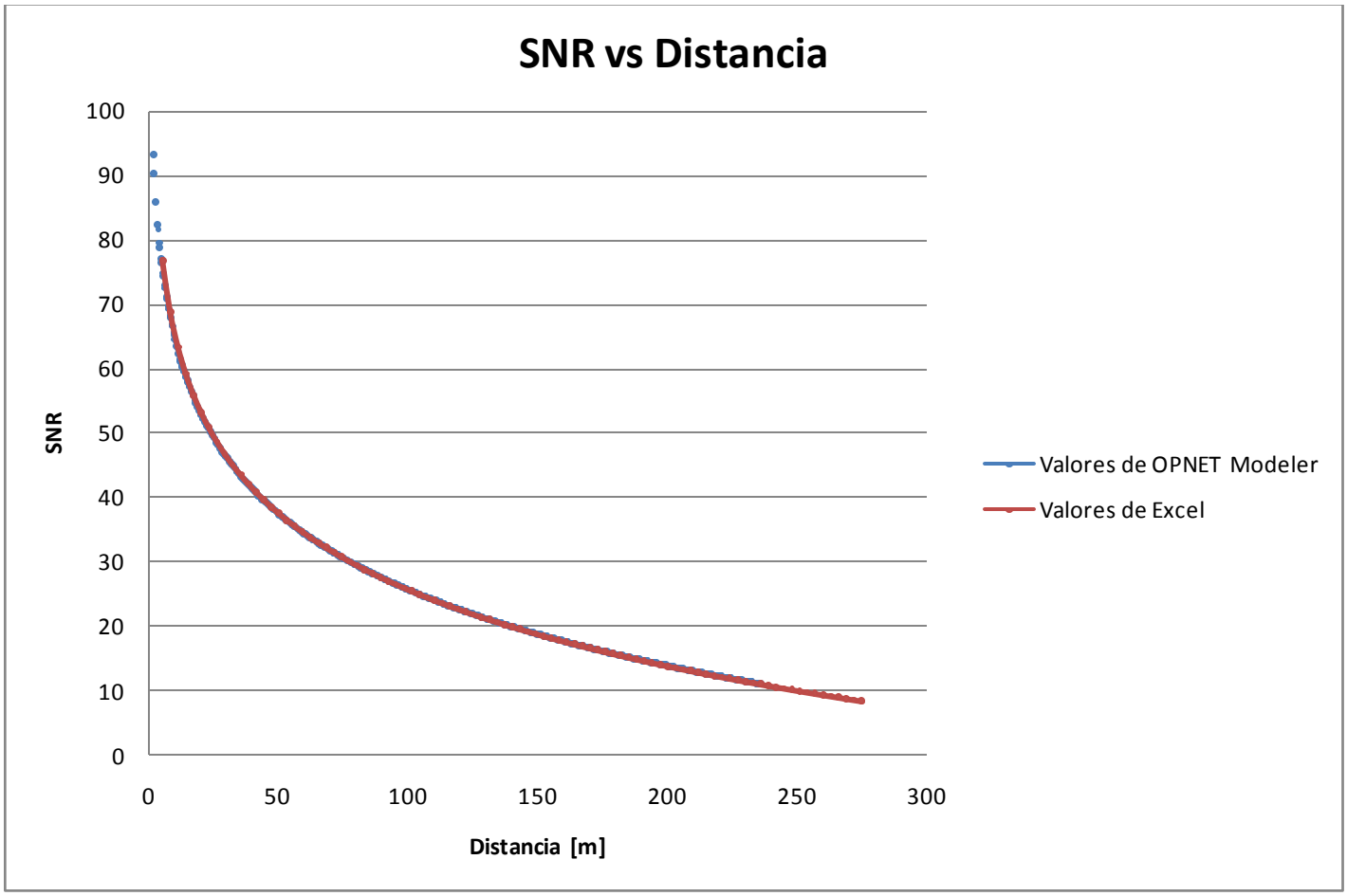


Figura 5.8SNR creado con los valores obtenidos en OPNET Modelery Excel

Las graficas de Pathloss, Potencia recibida y SNR indican que los valores del simulador OPNET Modeler son correctos. La figura 5.8 muestra que a una distancia de 233 m se tiene un SNR de 11.2 dB, condiciones que indican que el usuario móvil se encuentra en la región de cobertura del AP vecino (ForeignAgent 1) y sin embargo no se ha cambiado a éste.

CAPÍTULO 6

Conclusiones

El equipo de VoIP puede soportar un Handover de capa 2 y 3 sin terminar la llamada en curso, ello se traduce a que con estos dispositivos de red se puede llevar a cabo un Handoff suave.

Para llevarse a cabo un Handover de capa 2 y 3 con el equipo de VoIP suministrado es necesario entre otras cosas el habilitar las funciones de WMM.

En un Handoff de capa 2 una vez que el usuario móvil se autentica con el primer AP y obtiene una dirección IP válida en la red, la conserva durante y después del proceso de Handover. El Handoff de capa 2 se lleva a cabo de una manera *transparente*dado que durante el proceso de Handover de capa 2 el usuario móvil no obtiene una nueva dirección IP ni vuelve a autenticarse.

El tiempo empleado para llevar a cabo un Handoff de capa 3 con el equipo utilizado en el presente trabajo es de 3.1557 segundos. Durante el proceso de Handover de capa 3, el usuario móvil obtiene una nueva dirección IP perteneciente al segmento de la red en la que se encuentra de visita, pero no vuelve a autenticarse.

Si se desea realizar un handover de capa 2 y 3 utilizando el equipo de voz sobre IP empleado en este trabajo, la mejor manera de asignar direcciones IP a los usuarios es mediante un servidor DHCP.

El equipo utilizado en el presente trabajo es de carácter comercial, de bajo costo y por ello de bajo rendimiento, estas características lo hacen apto para operar en una red pequeña. Para implementar la red de VoIP de gran dimensión en la línea 1 del STC Metro se deben optimizar los tiempos de Handoff de capa 2 y 3, para ellose necesita usar equipo más sofisticado pero de un costo más elevado como son servidores Proxy SIP, centrales telefónicas privadas IP PBX, Gateways telefónicos, múltiples controladores Wireless LAN para una mejor administración de los APy dispositivos móviles con una mayor capacidad de procesamiento. Con ayuda del equipo anterior se lograrían tiempos de Handoveracordes al tiempo de latencia máximo para paquetes de VoIP que es de 150 ms.

El softphone X-LITE puede soportar un Handoff de capa 2 y 3, por lo que instalado en una computadora, ya sea o no portátil, puede ser un buen teléfono IP para distribuir entre el personal de una empresa, sin que ello implique el gasto de inversión en equipo nuevo.

El softphone X-LITE funciona adecuadamente en los procesos de Handover por lo que sería una buena opción el instalarlo y ejecutarlo en otros dispositivos que presenten una mayor movilidad y comodidad para un usuario por ejemplo en un teléfono inteligente o Smartphone.

El modelo de simulación, a pesar de arrojar los mismos valores de Pathloss, Potencia recibida y SNR que los calculados en Excel, no se comporta de la misma manera ni de la forma esperada. Por tal razón, parte de los objetivos no fueron completados en su totalidad dejándose como trabajo a futuro.

6.1 Trabajo futuro

Se puede complementar tanto el modelo de simulación como el instrumental al añadirle la característica de utilizar cable radiante. La tabla 6.1 muestra las características más relevantes de un conjunto de cables radiantes que se consideran como opción para ser implementados en la red.

Marca Cable Radiante	Modelo	Pérdida de Acoplamiento C95 a 6m [dB]	Pérdida Longitudinal [dB/100m]	Diámetro [pulgadas]	Instalación
Radiaflex	**RCF12-50**	87	15.3	1/2	Autosoportado 5-10 cm
Radiaflex	**RCF78-50**	85	8.3	7/8	Autosoportado 5-10 cm
Radiaflex	**RCF114-50**	95	6.19	1 1/4	Autosoportado 5-10 cm
Radiaflex	**RCF158-50**	95	4.65	1 5/8	Autosoportado 5-10 cm
nuTract	**TRC1250**	79	7.9	1 1/4	Sobre la pared o techo
Silec Cable	**C000012NGP**	75	34	1/2	Autosoportado 8-10 cm
Silec Cable	**C000078NGP**	77	14.5	7/8	Autosoportado 8-10 cm
Silec Cable	**C000114NGP**	77	11.5	1 1/4	Autosoportado 8-10 cm
Silec Cable	**C000158NGP**	77	7.4	1 5/8	Autosoportado 8-10 cm
Leaky Cables	**WBLCX-10D**	77	15.3	1/2	Autosoportado 8-10 cm
Leaky Cables	**WBLCX-20D**	83	7.4	1	Autosoportado 8-10 cm

Tabla 6.1 Características más relevantes de los cables radiantes [16]

En la tabla anterior la columna de *Pérdida de acoplamiento*se refiere a las pérdidas que experimenta la señal al serinsertada al sistema de cable radiante proveniente del usuario móvil, a una distancia de separación entre éstos de 6 metros. La columna referente a *Pérdida longitudinal* es la pérdida por unidad de distancia que experimenta la señal al viajar a través del cable radiante.

Asimismo, la figura 6.1 obtenida de [16] muestra la relación de la intensidad de la señal recibida que tiene cada uno de los cables radiantes a una cierta distancia.

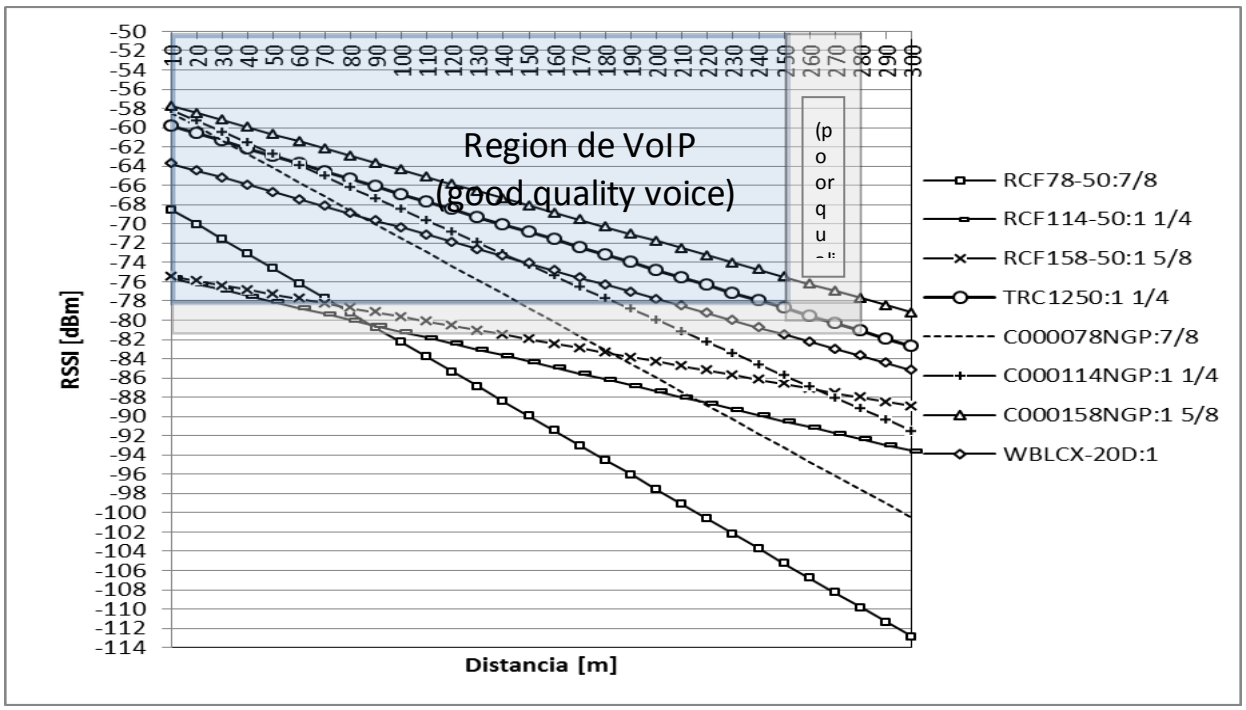


Figura 6.1Potencia recibida contra distancia para el conjunto de cables radiantes anterior

Para que un cable radiante pueda ser utilizado en aplicaciones de VoIP, debe tener una potencia de recepción entre los -50 y -78 dBm. Con lo anterior se concluye que el cable que muestra el mejor comportamiento para el envío de paquetes de VoIP es el C0000158NGP de la compañía Silec Cable, seguido del cable TRC1250 de la empresa nuTract.

Debido al alto costo del primer cable el cual es superior a los $60 USD por metro, finalmente se considera como opción al cable radiante TRC1250 ya que tiene un comportamiento de propagación similar al anterior pero su costo es de $38.86 USD.

APÉNDICE A

A.1 Programación de Router Cisco Series 2600

```
VoIP#show running-config
Building configuration...

Current configuration : 922 bytes
!
version 12.3
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
!
hostname VoIP
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Bk5/$hq7Lu/d9/R9lB0j3hhf8C/
!
no network-clock-participate slot
no network-clock-participate wic 0
noaaa new-model
ip subnet-zero
ipcef
!
!
noip domain lookup
!
!
```

```
!
!
!
interface FastEthernet0/0
ip address 192.168.20.2 255.255.255.128
duplex auto
speed auto
!
interface Serial0/0
noip address
shutdown
no fair-queue
!
interface FastEthernet0/1
ip address 192.168.20.130 255.255.255.128
duplex auto
speed auto
!
interface Serial0/1
noip address
shutdown
!
ip http server
ip classless
!
!
banner login ^C !!! ROUTER Redalejovoip ACCESO RESTRINGIDO !!! ^C
!
line con 0
passwordredvoip
logging synchronous
login
line aux 0
linevty 0 4
passwordredvoip
login
linevty 5 15
passwordredvoip
login
!
!
end
```

A.2 Programación en OPNET

A.2.1 Pipeline WLAN_POWER

```
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

	double		altura,shadow;		//Declaración de variables de tipo doble

	double		Lc, Ptx, Gtx, EIRP, Grx,rcvd_power1, path_loss1;

	double		dist;

	double		rcvd_power11;

	int		mod_src, nod_src;		//Declaración de variables de tipo entero

	char		NAME [20];//Declaración de variable de tipo cadena de longitud 20 caracteres

	double		tx_x,tx_y,tx_z,rx_x,rx_y,rx_z;		//Declaración de variables de tipo doble

	double		DIST_START, DIST_END,distancia;

	double		straight_line_distance;

	double		src_latitude,src_longitude,src_altitude,src_xpos, src_ypos,src_zpos;

	double		des_latitude,des_longitude,des_altitude,des_xpos, des_ypos,des_zpos;

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
```

```
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

if (op_prg_odb_ltrace_active ("GEO"))                                   // Se coloca una traza de nombre GEO

{

        mod_src = op_pk_creation_mod_get (pkptr);                       // Se obtiene el ID del modulo que creó el paquete

        nod_src = op_topo_parent (mod_src);                             //Se obtiene el ID del nodo padre del módulo que creó el paquete

        op_ima_obj_attr_get (nod_src, "name", NAME);                    // Se obtiene elnombre del nodo padre

                if (strcmp (NAME, "HA") ==0 ||strcmp (NAME, "FA_1") ==0 )   // Condicional de comparación de cadenas

                        {

                                printf ("\n\t El nombre de quien envio el paquete es [%s]", NAME);   // Se imprime el nombre del nodo padre que envía el paquete

                                tx_x = op_td_get_dbl (pkptr, OPC_TDA_RA_TX_GEO_X);   // Obtención de la coordenada geocéntrica “x” del transmisor

                                tx_y = op_td_get_dbl (pkptr, OPC_TDA_RA_TX_GEO_Y);   // Obtención de la coordenada geocéntrica “y” del transmisor

                                tx_z = op_td_get_dbl (pkptr, OPC_TDA_RA_TX_GEO_Z);   // Obtención de la coordenada geocéntrica “z” del transmisor

                                rx_x = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_GEO_X;    // Obtención de la coordenada geocéntrica “x” del receptor

                                rx_y = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_GEO_Y);   // Obtención de la coordenada geocéntrica “y” del receptor

                                rx_z = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_GEO_Z);   // Obtención de la coordenada geocéntrica “z” del receptor

                                distancia = sqrt(pow(tx_x-rx_x,2)+pow(tx_y-rx_y,2)+pow(tx_z-rx_z,2));   //Obtención de la distancia entre transmisor y receptor
                                                                                                        //mediante el uso de la ecuación de distancia

op_ima_obj_pos_get (nod_src,&src_latitude,&src_longitude,&src_altitude,&src_xpos, &src_ypos,&src_zpos);   //Obtención de latitud, longitud, altitud y posiciones en x,y,z
                                                                                                          //correspondientes al transmisor

op_ima_obj_pos_get (5,&des_latitude,&des_longitude,&des_altitude,&des_xpos, &des_ypos,&des_zpos);   //Obtención de latitud, longitud, altitud y posiciones en x,y,z
                                                                                                    //correspondientes al receptor, el número 5 corresponde al ID
```

```
                                                                    //del módulo “wlan_port_rx_1_0” del nodo padre “MR”.
                                                                                        //No siempre es el mismo y se debe leer en el depurador.

straight_line_distance =prg_geo_lat_long_distance_get (src_latitude,src_longitude,src_altitude,des_latitude,des_longitude,des_altitude);          // Se calcula la distancia entre
                                                                                                                                                    //transmisor y receptor en
                                                                                                                                                  //línea recta y en metros usando  la
                                                                                                                                                // función prg_geo_lat_long_distance_get


printf("\n\t DISTANCIA1 [%f] \t DISTANCIA2 [%f] \t TIME (%g) \t\n",straight_line_distance, distancia, op_sim_time());   //Se imprime la distancia obtenida por ambos métodos
                                                                                                                                                    // y se comparan entre si. Se imprime también el
                                                                                                                                                    //tiempo de simulación.


                                }

}

if (op_prg_odb_ltrace_active ("DIST"))                                                                                                              // Se coloca una traza de nombre DIST

{

        mod_src = op_pk_creation_mod_get (pkptr);                                                                                                   // Se obtiene el ID del modulo que creó el paquete

        nod_src = op_topo_parent (mod_src);                                                                                                 //Se obtiene el ID del nodo padre del módulo que creó el paquete

        op_ima_obj_attr_get (nod_src, "name", NAME);                                                                                                // Se obtiene el nombre del nodo padre

                if (strcmp (NAME, "HA") ==0 ||strcmp (NAME, "FA_1") ==0 )                                                                           //Condicional de comparación de cadenas

                {


                        printf("\n\t El nombre de quien envioel paquete es [%s]", NAME);                                                       //Se imprime el nombre del nodo padre que envía el paquete

                        DIST_START = op_td_get_dbl (pkptr, OPC_TDA_RA_START_DIST);//Se obtiene la distancia entre en el transmisor y receptor en
                                                                                                                                                    //el instante que comienza la transmisión del paquete

                        DIST_END = op_td_get_dbl (pkptr, OPC_TDA_RA_END_DIST);//Se obtiene la distancia entre en el transmisor y receptor en
```

```
                                                                                                        //el instante que finaliza la transmisión del paquete

                printf("\n\t DIST START [%f]  \t DIST END [%f] \t  TIME (%g) \t\n",DIST_START, DIST_END,op_sim_time());          //Se imprimenambasdistanciasobtenidas
                                                                                                                                //anteriormente así como el tiempo de
                                                                                                                                //simulación y se comparan
                }

}

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/


altura = 4;                                                                                             //Asignación de la altura del AP (estación base)

shadow = 8;                                                                                     //Asignación del valor de Shadow Fading

path_loss1 = 40 * (1-(0.004 * altura)) * log10 (prop_distance/1000) - 18 *log10 (altura) + 21 * log10 (tx_center_freq / 1000000) + 80 + shadow;          // Cálculo de Pathloss en dB

path_loss = pow (10.0, path_loss1 / 10.0);                                                              //Cálculo de Pathloss en Watts

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

if (op_prg_odb_ltrace_active ("PATHLOSS"))                                                              // Se coloca una traza de nombre PATHLOSS

{

        mod_src = op_pk_creation_mod_get (pkptr);                                                       // Se obtiene el ID del modulo que creó el paquete
```

```
	nod_src = op_topo_parent (mod_src);  // Se obtiene el ID del nodo padre del módulo que creó el paquete

	op_ima_obj_attr_get (nod_src, "name", NAME);                                    // Se obtiene el nombre del nodo padre


		if (strcmp (NAME, "HA") ==0 | |strcmp (NAME, "FA_1") ==0 )          //Condicional de comparación de cadenas


		{

			printf ("\n\t El nombre de quien envio el paquete es [%s]", NAME);          //Se imprime el nombre del nodo padre que envía el paquete

			dist = op_td_get_dbl (pkptr, OPC_TDA_RA_END_DIST);                    //Se obtiene la distancia entre el transmisor y el receptor en
                                                                                      //el momento en que finaliza la transmisión del paquete

			printf("\n\t distes \t %f \t PATHLOSS [dB] es \t %f \t \t TIME (%g)\t\t\n",dist, path_loss1,op_sim_time() );          //Se imprime la distanciaobtenida
                                                                                                                                  //anteriormente, el pathloss y el
                                                                                                                                //tiempo de simulación

		}

}
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

tx_ant_gain = 15;                                                  // Se asigna la ganancia de la antena de transmisión a un valor de 15dBi

rx_ant_gain = 15;                                                  // Se asigna la ganancia de la antena de recepción a un valor de 15dBi

op_td_set_dbl (pkptr, OPC_TDA_RA_RX_GAIN, rx_ant_gain);            //Se coloca el valor de la ganancia de la antena de recepción en los
                                                                       //parámetros del paquete.

op_td_set_dbl (pkptr, OPC_TDA_RA_TX_GAIN, tx_ant_gain);            //Se coloca el valor de la ganancia de la antena de transmisión en
                                                                       //los parámetros del paquete.
```

```
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/

Lc = 2 ;                                                                    //Se le asignan perdidas por conectores de 2 dB

Ptx = (10 *log10 (op_td_get_dbl (pkptr, OPC_TDA_RA_TX_POWER)))+ 30;         // Se obtiene la potencia recibida en watts y se
                                                                                    //se convierte a dBm.

Gtx = tx_ant_gain;                                                                  // Se reasigna la ganancia de la antena de
                                                                                    //transmisión a una nueva variable

EIRP = Ptx +  Gtx - Lc;                                                             //Se calcula laPotencia Isotrópica
                                                                                    //Radiada Efectiva (PIRE) en dBm

Grx = rx_ant_gain;                                                                  // Se reasigna la ganancia de la antena de
                                                                                    //recepción a una nueva variable

rcvd_power1 =  EIRP + Grx - path_loss1 ;                                            // Se calcula la potencia recibida  en dBm

rcvd_power = pow (10.0,(rcvd_power1 - 30)  / 10.0);                         // Se convierte la potencia recibida de dBm a watts


if (op_prg_odb_ltrace_active ("RCVDPOWER"))                 // Se coloca una traza de nombre PATHLOSS

{

        dist = op_td_get_dbl (pkptr, OPC_TDA_RA_END_DIST);//Se obtiene la distancia entre el transmisor y el receptor
                                                                                    //al finalizar la transmisión del paquete

        rcvd_power11 = op_td_get_dbl (pkptr, OPC_TDA_RA_RCVD_POWER);                //Se obtiene la potencia recibida en watts

        printf("\n\t DIST es \t%f \t RCVDPOWER [W]  ES \t %E \t  RCVDPOWER [dBm]  ES \t %f \t \t TIME (%g)\t\t\n",dist,rcvd_power11, rcvd_power1, op_sim_time());
```

```
                                                                                    //Se imprime la distancia obtenida, la potencia recibida
                                                                                    //en watts y en dBm así como el tiempo de simulación

        op_pk_print_options (pkptr, OPC_PK_PRINT_ALL);//Se imprimen todos los parámetros del paquete recibido

}
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&*/
```

A.2.2 Pipeline DRA_SNR

```
/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/

double          SNRatio, rcvd_power1, noise_figure, BW, noiseN ;                    //Declaración de variables de tipo doble

double          dist, snr13;

double          reciv, reciv1;

int             mod_src, nod_src;                                                   //Declaración de variables de tipo entero

char            NAME [20];                                                  //Declaración de variable de tipo cadena de longitud 20 caracteres

/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/


/*&&&&&&&&&&&.....LINEAS QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
```

```
/*&&&&&&&&&&&.....LINEA S QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEA S QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/


    rcvd_power1 = (10 *log10 (rcvd_power))+ 30 ;                    // Valor de la potencia recibida en  dBm

    noise_figure = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_NOISEFIG);   // Valor de la FIGURA DE RUIDO en dB

    BW = op_td_get_dbl (pkptr, OPC_TDA_RA_RX_BW);                   // Obtiene el valor del ancho de banda

    noiseN = 10 *log10 (290 * BW * (1.38E-23)) + noise_figure + 30 ; // Valor del ruido térmico en dBm

    SNRatio = rcvd_power1 - noiseN;                                 // Valor de SNR en dB



    op_td_set_dbl (pkptr, OPC_TDA_RA_SNR,SNRatio);                  // Asignación del valor de SNR en dB al paquete


    if (op_prg_odb_ltrace_active ("MODULO"))                        //Colocación de la traza “MODULO”
    {
        mod_src = op_pk_creation_mod_get (pkptr);                   //Obtención del ID del modulo que creó el paquete
        nod_src = op_topo_parent (mod_src);                         //Obtención del ID del nodopadre del módulo que creó el paquete

        op_ima_obj_attr_get (nod_src, "name", NAME);                //Obtención del nombre del nodopadre
            if (strcmp (NAME, "HA") ==0 ||strcmp (NAME, "FA_1") ==0 ) //Condicional de comparación de cadenas
            {
```

```
                    printf ("\n\t El nombre de quien envio el paquete es [%s]", NAME);          //Impresión en pantalla del nombre del nodo padre

                    snr13 = op_td_get_dbl (pkptr, OPC_TDA_RA_SNR);                            //Obtención del SNR del frame que arribó

                    dist = op_td_get_dbl (pkptr, OPC_TDA_RA_START_DIST);                      //Obtención de la distancia de separación entre el transmisor
                                                                                              //y el receptor [m]

                    reciv= op_td_get_dbl (pkptr, OPC_TDA_RA_RCVD_POWER);                      //Obtención de la potencia recibida del frame que arribó [W]

                    reciv1= (10*log10(reciv))+30;                                             //Conversión de la potencia recibida a [dBm]

                    op_pk_print_options (pkptr, OPC_PK_PRINT_ALL);                            //Impresión de todos los parámetros del frame que arribó

    printf("\n\t Distancia [m] entre Tx y Rx es\t %f \t SNR [dB] ES \t %f \t POTENCIA RCVD [dBm]\t %f \t \t TIME (%g) \t \t\n",dist,snr13,reciv1, op_sim_time());

                                                                                              //Impresión en pantalla de la distancia, SNR, potencia recibida y tiempo de simulación

                }

    }


/*&&&&&&&&&&&.....LINEA S QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEA S QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
/*&&&&&&&&&&&.....LINEA S QUE PONGO YO .....&&&&&&&&&&&&&&&&&&&&&*/
```

A.3 Programación en MATLAB

A.3.1 Multiplexado por División de Frecuencias Ortogonales (OFDM)

```
clearall
clearscreen
x1 = linspace(0,12);
y1 = sinc(6-x1);
plot(x1,y1,'r')
holdon
x2 =linspace(0,12) ;
y2 = sinc(8-x2);
plot(x2,y2,'b')
holdon
x3 = linspace(0,12);
y3 = sinc(7-x3);
plot(x3,y3,'m')
holdon
x4 =linspace(0,12) ;
y4 = sinc(4-x4);
plot(x4,y4,'k')
holdon
x5 =linspace(0,12) ;
y5 = sinc(5-x5);
plot(x5,y5,'g')
holdon
gridon
title('Multiplexación por División de Frecuencias Ortogonales')
xlabel('Frecuencia [Hz]')
ylabel('Amplitud')
```

Glosario

802.11 Familia de estándares que especifica una interfaz aérea entre dos clientes inalámbricos o entre un cliente inalámbrico y un Punto de Acceso, es para tecnologías de redes WLAN y fue desarrollada por la IEEE.

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

AP Punto de Acceso, es un dispositivo cuyo papel es crear una red inalámbrica y permitirles 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 de Detección de Portadora con Evitación 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 grupos de 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 e	Estándar de comunicaciones inalámbricas que desarrolla las especificaciones técnicas para proporcionar Calidad de Servicio (QoS) al tráfico de datos, voz y video en una WLAN.
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 802.15	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.
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.
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 parautilizar 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.
VoIP	Tecnología que transmite paquetes de voz a través de una red de conmutación de paquetes usando el protocolo IP.
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 unas decenas 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.

WMM Son las siglas de WiFi Multimedia y brinda prioridad al tráfico de voz, audio y video sobre el transporte de datos en las redes WiFi

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, red 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.

Referencias

[1] Cisco Systems, Inc. Academia de Networking de Cisco Systems. ***Guía del primer año. CCNA® 1 y 2***. Terceraedición. Madrid. Pearson Educación, 2004, pp. 160-161.

[2] Cisco Systems. ***WRP400 Wireless-G Broadband Router with 2 Phone Ports – User Guide***. 2009, pp. 132.

[3] Daniel Minoli, et. al. ***Delivering Voice over IP Networks***. United States of America. Jhon Wiley & Sons, 1998, pp.17-19.

[4] David Tung Chong Wong, et. al. ***Wireless Broadband Networks.*** New Jersey. Wiley, 2009, pp 407- 408.

[5] Fernando Andreu, et. al.***Redes WLAN Fundamentos y Aplicaciones de Seguridad.*** España. Marcombo, 2006, páginas 25 – 26.

[6] Francisco J.Alonso-Caballero, et. al.***Aplicación rigurosa del análisis modal al cálculo de propagación en túneles.*** IEEE. 2007

[7] Gurpal Singh, et. al.***Multimedia Ready Handoff Technique for 802.11 Networks.*** IEEE. 2007.

[8] I.Rmani, et. al.***Syncscan: Practical Fast Handoff for 802.11 Infrastructure Networks***. IEEE. Marzo 2005.

[9] IEEE Computer Society. ***Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements***. New York. IEEE, 2005.

[10] IEEE Computer Society.***Information technology -Telecommunications and information exchange between systems- Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications***. Segundaedición. New York. IEEE, 2005.

[11] Javier Morgardei, et. al.***Planificación y verificación de instalación de la red Tetra en el metro de Bilbao***, IEEE. 2005.

[12] Mohamed Kassab, et. al.***IEEE 802.11a performance for infrastructure-to-train communications in an underground tunnel***, IEEE. 2006.

[13] Nokia Research Center. ***Request for Comments 3344 - IP Mobility Support for IPv4***. C. Perkins, Agosto 2002.

[14] Ralph Droms. ***Request for Comments 2131 - Dynamic Host Configuration Protocol.*** Bucknell University, Marzo 1997.

[15] Sunghyun Choi, et. al. ***IEEE 802.11 e Contention – Based Channel Access (EDCF) Performance Evaluation.*** IEEE. 2005

[16] Victor Rangel Licea, et. al.***Propuesta para el sistema deradiocomunicación para la línea 1 del metro del STC basado en un sistema inalámbrico de banda ancha***. Convocatoria 2009-1: FOMIX CONACYT-GDF. México, 2009, pp.6-7, 19.

[17] Victor RangelLicea.Modelos de Propagación. En: ***Redes Inalámbricas de Banda Ancha***, México, Junio 2009. pp. 13-14, 17.

[18] https://supportforums.cisco.com/thread/2021772/

[19] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10033/ps10041/data_sheet_c78-502697.html

[20] http://www.cisco.com/en/US/docs/ios/solutions_docs/mobile_ip/mobil_ip.html#wp1030412

[21] http://www.opnet.com

[22] http://www.wireshark.org

[23] http://stumbler.net