ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Análisis Comparativo de las Tecnologías WI-FI y WIMAX; Aplicaciones y Servicios"

TESIS DE GRADO
Previo a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Arellys Eloísa Briones Estébanez

Nadia Yadira Gracia Cedeño

GUAYAQUIL – ECUADOR

Año: 2006

AGRADECIMIENTOS

Agradezco de manera especial al Ing. Cesar Yépez F, por aceptar ser nuestro director de tesis y guiarnos con todos sus conocimientos desde el primer día, gracias por permitirnos invadir su oficina y obtener todos los beneficios de ella, gracias por su paciencia y el tiempo dedicado, solo con su apoyo pudimos haber cumplido esta meta, gracias Inge!

Al director de nuestra carrera el Dr. Boris Ramos S. y a los miembros del Tribunal de tesis, gracias por sus contribuciones, apoyo e interés en este trabajo.

Al Ing. Carlos Nieto, Director de Setel - Guayaquil, gracias por el tiempo, la información y las facilidades que nos brindó para que este trabajo pudiera ser culminado.

A la Ing. Viviana Gaona, gracias por estar con nosotras al realizar las pruebas de campo, fueron parte principal de esta Tesis.

A nuestro amigo el Ing. Carlos Perez, gracias por ayudarnos y tomarse el tiempo de leer y corregir este trabajo, todas sus sugerencias hicieron mas productiva nuestra tesis, gracias Carlin!

Agradezco primeramente a DIOS por las gracias y bendiciones que me ha concedido, y poner en mi camino a todas aquellas personas que me han ayudado y que colaboraron de una forma u otra en la culminación de mi carrera.

Gracias en especial a mí querido Ing. CÉSAR YÉPEZ por su dedicación desinteresada a este trabajo y por guiarnos durante todo este tiempo. A todo el personal de VIA COMUNICACIONES que supieron hacernos sentir bienvenidas y nos permitieron compartir su espacio de trabajo. A los Ingenieros CARLOS NIETO y VIVIANA GAONA de SETEL que compartieron con nosotras su experiencia. A mi estimado Ing. CARLOS PÉREZ quien colaboró con sus conocimientos y su tiempo, ayudándonos a mejorar. A mi amiga y compañera de tesis ARELLYS BRIONES por su constancia y paciencia infinita.

Un agradecimiento muy especial al Ing. CHRISTIAN LETAMENDI por su apoyo incondicional durante el transcurso de mi carrera universitaria.

Y por último pero más importante a mi familia, los seres que han estado conmigo en mis altas y bajas, a mis padres por su eterno apoyo y comprensión, siendo ellos mi razón de vivir y a mi hermana de quien estoy muy orgullosa y de quien espero tantos éxitos como pueda ella lograr.

Mil gracias a todos, les aseguro que sin su apoyo no estaría donde me encuentro hoy.

De todo corazón GRACIAS.

Nadia

Siempre soñé con el día que escribiría esta página, pensaba a quien agradecería tanta dicha, no se si olvidé a alguien por eso agradezco a todas las personas que una u otra forma me ayudaron a cumplir esta meta que espero sea el comienzo de muchas mas. Pero a quien no puedo olvidar de agradecer es a Dios, gracias por darme el regalo tan hermoso de vivir y sentirte siempre a mi lado, gracias por ponerme en los lugares adecuados y rodearme de personas maravillosas que me han dado tanta felicidad y muchísimas razones para agradecer estar viva. Gracias Flaco por todo!

Arellys

A nuestras queridas Secretarias de la Facultad de Eléctrica, la Sra. Narcisa Briones y la Sra. Gissella Correa, gracias por su paciencia a nuestra insistencia en los trámites pertinentes a esta Tesis.

A mi Papo y a mi Omi, gracias ha ellos existo, gracias por no dejarme desertar en mis sueños, gracias por el apoyo en estos años de estudios, gracias por todos sus sacrificios que me hicieron posible llegar a esta meta y convertirme en alguien digno de ustedes, gracias de todo corazón padres míos, este logro es también de ustedes.

A las razones de mi vida, mis ñañas Johissy y Katiusca, gracias por darme un ejemplo a seguir, gracias por estar en los momentos que mas necesité y por toda la ayuda y retadas que me dieron (que fueron muchas), ya que me ayudaron a ser una mejor persona, gracias ñañas las adoro muchísimo!

A mi godo, gracias vida por estar conmigo en todo el trayecto de la realización de esta tesis, gracias por escucharme y ser mi apoyo cuando estaba con problemas, gracias por todas las palabras de aliento cuando mas las necesitaba, toda mi vida te agradeceré por haber estado allí, gracias amor!.

A mi amiga con la cual realicé este trabajo, gracias Nayito, por ponerle muchas ganas y llegar juntas a esta meta, gracias a tu familia por acogerme en tantas amanecidas, gracias por tanto aguante que sé no ha sido fácil, pero valió la pena…… ¡ lo logramos amiguis!.

A todos mis amigos que en cada materia sufrieron igual que yo en este largo camino universitario, en especial a ustedes Chiney y Jorge Luis gracias por ser mis amigos y ser tan incondicionales.

DEDICATORIAS

A mis padres,
A mis hermanas y
A Ñaña Toya

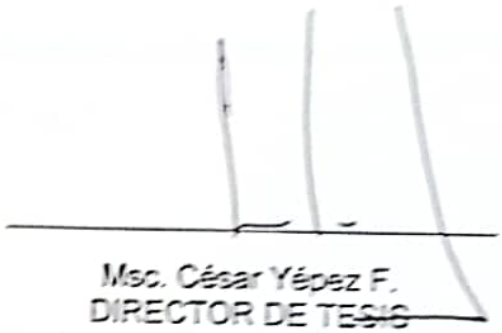
Arellys

A mis padres y
A mi hermana

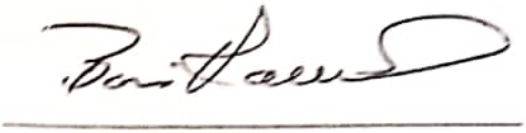
Nadia

TRIBUNAL DE GRADUACIÓN

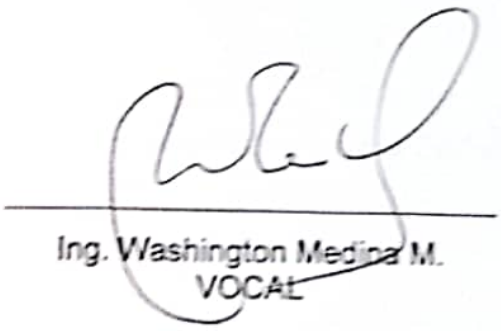
Ing. Holger Cevallos U.
SUB-DECANO DE LA FIEC
PRESIDENTE



Msc. César Yépez F.
DIRECTOR DE TESIS



Ing. Boris Ramos S.
VOCAL



Ing. Washington Medina M.
VOCAL

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

Arellys Eloísa Briones Estébanez

Nadia Yadira Gracia Cedeño

RESUMEN

El presente trabajo realizará comparaciones entre las dos tecnologías inalámbricas existentes actualmente de área local y metropolitana como lo son Wi-Fi y WIMAX respectivamente.

El análisis comparativo de los aspectos teóricos será realizado entre los estándares IEEE 802.11 e IEEE 802.16 y sus respectivas variantes con la finalidad de determinar en que puntos uno es superior a otro.

El análisis comparativo de los aspectos prácticos entre estas dos tecnologías será obtenido de las pruebas realizadas con equipos reales o en su defecto con pruebas de laboratorio.

Al término del estudio esperamos concluir cual de estas dos tecnologías tiene más propiedades y características en las mismas aplicaciones y servicios.

INDICE GENERAL

CAPITULO 2

ACRÓNIMOS

ACK :Acuse de Recibo

ADSL :Línea de Abonado Digital Asimétrica

AES :Estándar de Encriptación Avanzada

AH :Autenticación de Cabecera

AK :Clave de Autorización

AP :Punto de Acceso

ASK :Modulación por Desplazamiento de Amplitud

ATM :Modo de Transferencia Asíncrono

BER :Tasa de Bits Erróneos

BH :Backhaul

BHM :Backhaul Máster

BHS :Backhaul Esclavo

BPSK :Modulación por Desplazamiento de Fase Binario

BS :Estación Base

BSS :Grupo de Servicios Básicos

CBC :Cipher Block Chaining

CCK	**:**Clave de Código Complementario
CDMA	**:**Acceso Múltiple por División de Código
CHI	**:**Contenedor del Certificado de Identidad
CHPK	**:**Contenedor del Certificado de Clave Pública
CID	**:**Identificador de Conexión
CMR	**:**Conferencia Mundial de Radiocomunicaciones
COFDM	**:**Multiplexación por División Ortogonal de Frecuencia Codificada
CONATEL	**:**Consejo Nacional de Telecomunicaciones
CPE	**:**Equipo Local de Cliente
CSMA/CA	**:**Acceso Múltiple con Escucha de Portadora y Evasión de Colisiones
CSMA/CD	**:**Acceso Múltiple con Escucha de Portadora y Detección de Colisiones
CSMA	**:**Acceso Múltiple con Escucha de Portadora
CTS	**:**Permiso para enviar
DAMA	**:**Acceso Múltiple Asignado por Demanda
DES	**:**Estándar de Encriptación de Datos
DFT	**:**Transformada Discreta de Fourier

DIFS **:**Distribución de Espacio entre Tramas

DOI **:**Dominio de Interpretación

DSL **:**Línea de Abonado Digital

DSSS **:**Secuencia Directa en el Espectro Extendido

EAP **:**Protocolo de Autenticación Extensible

EAP-TLS **:**Seguridad de la Capa de Transporte-EAP

EAP-TTLS **:**Seguridad de la Capa de Transporte con Túnel-EAP

ER **:**Rango Extendido

ESP **:**Encapsulamiento Seguro de la Información Útil

FCC **:**Comisión Federal de Comunicaciones

FDD **:**Duplexación en el Dominio de la Frecuencia

FDM **:**Multiplexado por División en Frecuencia

FDMA **:**Acceso Múltiple por División de Frecuencia

FEC **:**Corrección de Errores en la Recepción

FFT **:**Transformada Rápida de Fourier

FHSS **:**Espectro Extendido por Salto de Frecuencia

FSK **:**Modulación por Desplazamiento de Frecuencia

GPRS **:**Sistema Global de Paquetes Vía Radio

GPS **:**Sistema de Posicionamiento Global

GSM **:**Sistema Global para Comunicaciones Móviles

HMAC **:**Cabecera de la MAC

HSCSD **:**Datos de Alta Velocidad en Circuitos Conmutados

IC **:**Circuito Integrado

ICM **:**Bandas para Aplicaciones Industriales, Científicas y Médicas

IEEE **:**Instituto de Ingenieros Eléctricos y Electrónicos

IETF **:**Grupo de Trabajo sobre Ingeniería de Internet

IKE **:**Intercambio de Claves en Internet

IP **:**Protocolo de Internet

IPSec **:**Protocolo de Seguridad IP

IPv4 **:**IP cuarta versión

IPv6 **:**IP sexta versión

IV **:**Vector de Inicialización

KEK :Generación de Clave de Encriptación

LAN :Rede de Área Local

LOS :Línea de Vista Directa

MAC PDU :Unidad de Protocolo de Datos

MAC :Control de Acceso al Medio

MBWA :Acceso Inalámbrico de Banda Ancha Móvil

MIC :Chequeo de Integridad de Mensaje

MMDS :Servicio de Distribución Multipunto Multicanal

NAV :Vector de Asignación de Red

NLOS :Sin Línea de Vista Directa

OFDM :Multiplexación por División Ortogonal de Frecuencia

OFDMA :Acceso Múltiple por División Ortogonal de Frecuencia

OSI :Modelo de Interconexión de Sistemas Abiertos

PAN :Red de Área Personal

PDC :Celulares Digitales Personales

PEAP :Protocolo de Autenticación Extensible Protegido

PKCS **:**Estándares de Criptografía basado en Clave Pública

PKM **:**Administración de Clave Privada

PMC **:**Canal de Administración Primario

PSK **:**Modulación por Desplazamiento de Fase

QAM **:**Modulación de Amplitud en Cuadratura

QoS **:**Calidad de Servicio

QPSK **:**Modulación por Desplazamiento de Fase en Cuadratura

RFC **:**Petición de Comentarios

RLAN **:**Redes Radioeléctricas de Área Local

R-S **:**Código de Reed-Solomon

RSA **:**Algoritmo de Rivest, Shamir y Adleman

RSN **:**Red de Seguridad Robusta

RSNA **:**Asociación de Redes de Seguridad Robusta.

RSS **:**Potencia de la Señal Recibida

RSSI **:**Intensidad de la Señal de Recepción

RTS **:**Solicitud para Enviar

SA **:**Asociación de Seguridad

SAID **:**Identificador de SA

SCRSCC **:**Código Convolucional R-S por Concatenación Serial

SM **:**Módulo de Suscriptor

SNR **:**Relación entre Señal y Ruido

SNT **:**Secretaría Nacional de Telecomunicaciones

SS **:**Estación de Usuario

SSID **:**Identificador de Conjunto de Servicios

SSL **:**Capa para Conexiones Seguras

TCP/IP **:**Protocolo de Control de Transmisión/Protocolo de Internet

TDD **:**Duplexación en el Dominio del Tiempo

TDM **:**Multiplexación por División en el Tiempo

TDMA **:**Acceso Múltiple por División de Tiempo

TEK **:**Claves de Encriptación de Tráfico

TKIP **:**Protocolo de Integridad de Clave Temporal

TSN **:**Red Transicional de Seguridad

U-NII **:**Infraestructura de Información Nacional Sin Licencia

UTP **:**Par Trenzado sin Blindar

VCS **:**Sensor de Portadora Virtual

VoIP **:**Voz sobre Protocolo de Internet

VPN **:**Red Privada Virtual

WAS **:**Sistemas de Acceso Inalámbrico

WECA **:**Sociedad para la Compatibilidad Ethernet Inalámbrica

WEP **:**Privacidad Equivalente al Cableado

Wi-Fi **:**Fidelidad Inalámbrica

WIMAX **:**Interoperabilidad Mundial para Acceso en Microondas

WLAN **:**Red de Área Local Inalámbrica

WMAN **:**Redes de Área Metropolitana Inalámbricas

WPA **:**Acceso Protegido Wi-Fi

WWAN **:**Red de Área Amplia Inalámbrica

ÍNDICE DE FIGURAS

Pag

ÍNDICE DE TABLAS

ÍNDICE DE PLANOS

INTRODUCCIÓN

El estándar IEEE 802.11 para LANs inalámbricas fue publicado en 1999. Estos productos basados en un estándar de interoperabilidad son certificados por la Alianza de Compatibilidad Ethernet Inalámbrica (Wireless Ethernet Compatibility Alliance, WECA) con el logo Wi-Fi™. Las Redes Inalámbricas basadas en el estándar de la IEEE 802.11 o Wi-Fi han sido un completo éxito, y ahora se están enfocando en conseguir una mayor cobertura. Mientras Wi-Fi ha ido borrando virtualmente la competencia en el área local, el mercado de área metropolitana se encuentra en desarrollo.

WIMAX, siglas de Interoperabilidad Mundial para Acceso en Microondas (Worldwide Interoperability for Microwave Access), es definido en el estándar IEEE 802.16, y ha sido promovido por el WIMAX Forum. El Forum se encarga de desarrollar pruebas de ajuste de interoperabilidad para asegurar soluciones a los vendedores resultando en productos de bajo costo, basados en un estándar abierto.

Debido al incremento en el reconocimiento de WIMAX en el mercado, es ahora regularmente comparado con Wi-Fi. Mientras los dos comparten ciertamente algunas características técnicas fundamentales, se están acercando al espacio inalámbrico de dos perspectivas diferentes. Además, los diferentes acercamientos en sus diseños harán poco probable que estas dos tecnologías compitan excepto en algún caso en particular.

El propósito de esta Tesis es proveer una comparación técnica de las tecnologías Wi-Fi y WIMAX, resaltando sus similitudes y diferencias

fundamentales e identificando una aplicación específica para cada tecnología y los servicios que éstas ofrecen.

CAPITULO 1

1 EVOLUCION DE LAS REDES INALAMBRICAS

La popularización de las redes de área local inalámbricas y su posible interconexión ha dado pie a que potencialmente se puedan crear redes inalámbricas, incluso móviles, de gran ancho de banda en amplias zonas urbanas dando lugar a redes metropolitanas.

1.1 Redes de área local Inalámbricas (WLAN)

Aunque la tecnología se conoce como redes de área local inalámbrica (LAN inalámbricas), en realidad se trata de tecnología de radio. Por tanto, no obstante que la historia de Wi-Fi u 802.11 sólo existe a partir de mediados de la década de los ochenta, en realidad esta tecnología comenzó aproximadamente 100 años atrás.

1.1.1 Fundamentos de las LAN Inalámbricas

Del mismo modo en que la tecnología de radiodifusión es el fundamento de la LAN inalámbrica, los primeros

trabajos en electromagnética, a su vez, representan los fundamentos de la radio.

Desde el tiempo de la creación de los sencillos, pero inteligentes dispositivos que se construyeron en laboratorios, han proliferado distintos tipos de tecnologías inalámbricas en todos los continentes, que se consideran como herramientas muy importantes en las empresas en su intento de obtener eficiencia y, además, son elementos importantes para la seguridad y la comodidad personal.

1.1.2 Las primeras LAN inalámbricas

En 1985, gracias a los cambios en las regularizaciones de la Parte 15 de la FCC, que permitieron el uso de radios a través del espectro extendido en las aplicaciones comerciales, se abrió la puerta para comercializar la tecnología. Poco después de un año de que se efectuaran los cambios en la regularización de la FCC, se creó en Toronto una compañía llamada Telesystems SLW, para explotar este desarrollo.

En 1988 fue introducido al mercado el primer sistema comercial basado en la tecnología conocida como Secuencia directa en el espectro extendido (Direct Sequence Spread Spectrum, DSSS). Además de incorporar DSSS, estos sistemas no operaban en una banda licenciada, sino que trabajaban sobre una banda sin licencia establecida recientemente por la FCC alrededor de los 902 y 928MHz. Debido a que esta banda estaba ubicada cerca de la banda licenciada para los

teléfonos celulares analógicos que se usan en Norteamérica, proporcionó a los fabricantes la ventaja de construir sus dispositivos libres de licencia con componentes existentes para nuevos propósitos y que originalmente estaban destinados para el uso de teléfonos celulares. Con DSSS fue posible la convivencia con otros usuarios sin licencia, lo que permitió a los usuarios resolver los problemas de interferencia por sí solos.

Los primeros productos de Telesystems fueron diseñados como reemplazos al cableado, ya sea para conectar múltiples computadoras de escritorio con una estación central base de manera muy parecida en la que funcionaría una red Ethernet, o para conectar las redes en edificios separados de modo semejante al que funciona un puente.

Al reconocer las ventajas de escalabilidad y consistencia geográfica de la operación del especto extendido libre de licencia, Telxon comenzó a ofrecer los radios sin licencia de Telesystems en sus terminales de adquisición de datos, como una alternativa para los radios de banda angosta con licencia que entonces eran proveídos principalmente por Motorola.

En 1999 Telxon agrupó su equipo de radios en la división Aironet Wireless Communications, que fue adquirida meses más tarde por la gigante en la industria de las redes, Cisco Systems.

No obstante que la operación de la banda de 900MHz se proporcionó para una infraestructura común a través de Estados Unidos, Canadá y Australia, estaba limitada en el sentido que no estaba asignada para la operación sin licencia en otras partes del mundo. Para llegar a los mercados ubicados fuera de estas áreas, los fabricantes comenzaron a producir radios que operaban en la parte de 2.4GHz del espectro de frecuencia que estaba disponible para la operación libre de licencia a lo largo de la mayor parte de Europa y Japón –además de Estados Unidos, Canadá y Australia-.

1.1.3 Primer estándar LAN inalámbrico

Al notar el beneficio mutuo de definir estándares de la industria para las LAN inalámbricas, en 1991 diversos competidores como Telxon, NCR, Proxim Technology y Symbol Technologies, emitieron al principio una Solicitud de autorización del proyecto (Project Authorization Request, PAR) a la IEEE, a fin de establecer un estándar interoperable para las LAN inalámbricas.

Hacia 1993, los fundamentos para un estándar estaban establecidos, y en junio de 1997, el estándar 802.11 de la IEEE, que tenía más de seis años en el proceso de creación, fue ratificado. Este primer estándar 802.11 proporcionaba velocidades de datos de 1 y 2 megabits por segundo (Mbps), así como la transmisión a través de las tecnologías de secuencia directa y de salto de frecuencia sobre una banda de 2.4GHz.

El primer estándar 802.11 que fue ratificado en 1999 y ofrece una velocidad de datos de 11 Mbps, aproximadamente la misma velocidad que el estándar Ethernet.

1.2 Redes de área metropolitana Inalámbrica (WMAN)

Una red de área metropolitana es la suma de muchas redes de área local interconectadas.

1.2.1 Aparición de la primera WMAN

La iniciativa de el 802.16 (WMAN) fue establecida en 1998 para crear un estándar para soporte de una red inalámbrica de banda ancha con conexión fija orientada punto-multipunto sobre una gran área de cobertura.

Las aplicaciones principales para el 802.16 (WMAN) incluye acceso inalámbrico de banda ancha a Internet y telefonía en Internet usando Voz sobre IP (VoIP), soluciones para empresas, pequeños negocios y casas. Estos servicios pueden ser accesados simultáneamente y se les asigna prioridades de calidad de servicio.

1.2.2 Primer estándar MAN Inalámbrico

El estándar 802.16 (WMAN) especifica el uso de las estaciones bases inalámbricas que son conectadas a redes públicas y estaciones de subscriptores las cuales proveen acceso local para empresa, negocios o casas. Las estaciones bases sirven a las estaciones de subscriptores.

Para facilitar la iniciativa de la banda ancha inalámbrica el comité 802.16 (WMAN) ha decidido trabajar sobre varios frentes estableciendo estándares para ambas bandas con y sin licencia.

Las bandas con licencia son soluciones destinadas a las empresas, mientras que las bandas sin licencia son soluciones para pequeños negocios y casas.

La MAC del 802.16 esta basada en la MAC IEEE 802.11. Fue ideada para soportar altas tasas de datos y altas frecuencias de operación.

Soporta servicios TCP/IP, ATM, entre otros, pero no creaciones de redes ad-hoc que no necesariamente van a través de la infraestructura.

Los problemas de seguridad y privacidad son diseccionados dentro de las especificaciones del 802.16 (WMAN) usando estándares existentes.

1.3 Redes de Área Amplia Inalámbricas (WWAN)

WWAN es el proceso de enlazar diferentes redes de trabajo sobre una amplia área geográfica que permita conectividad y el compartir archivos de gran tamaño.

Mientras que las computadoras están conectadas a una red de trabajo tradicional utilizando cable como medio de transmisión tales como sistemas telefónicos, las redes inalámbricas amplias se conectan vía radio, satélite y tecnología de teléfono móvil.

Las redes inalámbricas pueden ser instaladas con ambos terminales en posición fija o móvil. La topología de la red puede ser tipo anillo, y el último concepto es la combinación de tecnologías.

Un enlace inalámbrico fijo usa una antena fija utilizando partes específicas del espectro de radio para transmitir o recibir datos. Para las redes tipo anillo, los enlaces requieren "línea de vista" del equipo. Sin embargo, con redes combinadas o acopladas este aspecto no es tan crítico.

La distancia de cobertura puede verse afectada por la elección de la antena. Es posible optimizar la antena en "barrido" para cubrir un área más amplia, o en "distancia" para cubrir un rango mucho más largo.

Los enlaces inalámbricos móviles aplican a sistemas donde el receptor o los equipos terminales no están en una posición fija. Las dos claves que las soluciones móviles utilizan son sistemas satelitales y tecnología de teléfono móvil.

1.3.1 Aparición de la primera WWAN

Las redes de área amplia comerciales (WWAN) fueron introducidas hace “solo” 20 años atrás. Desde su reciente introducción (por una mejora en la tecnología), el paradigma WWAN ha revolucionado la industria de las telecomunicaciones.

1.3.2 Primer estándar WAN Inalámbrico

Desde febrero 3 del 2003, el Acceso Inalámbrico Banda Ancha Móvil (Mobile Broadband Wireless Access, MBWA), para computadoras y otros equipos están teniendo avances a pasos agigantados.

El Instituto de Ingenieros Electrónicos Eléctricos (IEEE) desarrolló un estándar para crear una interfaz aire que entregue porcentajes de disponibilidad a los usuarios móviles que viajan a velocidades tan grandes como 250Km/h.

El estándar IEEE 802.20, “Estándar de interfase Aire para Acceso Inalámbrico de Banda Ancha Móvil”, intentará alcanzar tasas de transmisión de datos en tiempo real en redes inalámbricas de área metropolitanas a una experiencia de banda ancha de 1 Mbps o más, con un radio de acción de hasta 15Km o más. El IEEE 802.20 se llamará MBWA en bandas con licencia bajo los 3.5GHz.

CAPITULO 2

2 WI-FI y WIMAX

2.1 Bandas de Frecuencia

2.1.1 Bandas de Frecuencia Wi-Fi

A pesar de que 802.11a y 802.11g comparten medios comunes de transmisión y modulación, en esencia, las similitudes terminan allí.

802.11a está definido para operar en distintas bandas dentro de la porción de 5GHz del espectro de frecuencia de radio. Mientras que 802.11g opera en exactamente la misma banda de 2.4GHz que usa 802.11b. Estas bandas distintas proporcionan beneficios muy diferentes para cada una de las tecnologías y también dan como resultado distintos inconvenientes y dificultades en la implementación.

Cuando la industria LAN inalámbrica comenzó la transmisión desde 900MHz hasta 2.4GHz a mediados de los noventa, muchas personas no valoraron las dificultades asociadas. Sin importar que los beneficios de la operación en 2.4GHz en relación con 900MHz fueran bien señalados, las peculiaridades de 2.4GHz tienden a no estar bien definidas para los fabricantes. Por supuesto lo mismo se aplica a la transmisión de la operación de 2.4 a 5GHz. El entendimiento de estos aspectos es importante para lograr una estrategia adecuada para migrar a 5GHz.

2.1.1.1 La Banda de 2.4GHz

Debido a que 802.11g opera en la banda de 2.4GHz, todos los aspectos de la física y principalmente, todas las regularizaciones internacionales que se aplican a 802.11b también se aplican a 802.11g.

Los factores conocidos que se aplican sugieren que el rango de 802.11g es más grande que el de 802.11a. Debido a que se transmite en la banda de 2.4GHz, 802.11g puede aprovechar la forma de onda relativamente larga y, gracias a esto, la puede llevar mas lejos que la forma de onda de 5GHz de 802.11a, considerando que los demás aspectos permanecen iguales. Sin embargo, no todas las demás cosas permanecen sin cambios. A pesar de que varían alrededor del mundo, las regulaciones de 2.4GHz normalmente permiten una potencia de transmisión más

grande que la que se permite para las bandas de 5GHz que usa 802.11a.

Otro contratiempo clave que aparece en 802.11g es que debido a que opera en la misma banda de 2.4GHz que usa 802.11b, 802.11g está sujeto a la capacidad y problemas de interferencia de 802.11b.

La banda de 2.4GHz solo permite el uso de tres canales, a diferencia de los ocho canales de la banda de 5GHz que está disponible en muchos países. La banda de 2.4GHz está saturada (y se está saturando más cada día).

2.1.1.2 La Banda de 5GHz

Al analizar los beneficios y desventajas asociados con la operación en la porción de 5GHz de espectro de frecuencia vemos que no es una cuestión de las leyes físicas sino de las leyes de las agencias gubernamentales reguladoras. La forma de onda de 5GHz proporciona algunas ventajas y desventajas en comparación con la forma de onda de la banda de 2.4GHz.

La onda relativamente más corta de 5GHz proporciona una desventaja importante en 802.11a comparado con 802.11b y es que existe una relación inversamente proporcional entre la longitud de onda y el rango. Esta consideración no se debe suponer como lineal (a pesar que la onda de 5GHz tiene aproximadamente la mitad

de la longitud de la onda de 2.4GHz, no se debe de asumir que solo esto podrá reducir el rango a la mitad), aún así, la relación es absoluta y significativa. Además la onda más corta de 5GHz tienden a ser capturadas con un grado más alto que la onda de 2.4GHz por los materiales de construcción comunes como por ejemplo: el concreto y la mampostería. La onda de 5GHz es más propensa a crear la propagación en múltiples trayectorias de lo que es una onda más larga de 2.4GHz.

802.11a opera en las bandas sin licencia exactamente de la misma manera que 802.11b. Es decir no existen restricciones en los tipos de dispositivos que operan en estas bandas.

Los dispositivos 802.11a asignan 200MHz a ocho canales, cada uno de ellos de 25MHz de ancho, lo cual es distinto de los tres canales de 22MHz de amplitud que no se traslapan y se usan en 802.11b y 802.11g.
Las ventajas que se presentan son la reutilización y la capacidad de los canales.

2.1.2 Bandas de Frecuencia WIMAX

Donde todas las implementaciones de Wi-Fi utilizan bandas de frecuencia sin licencia, WIMAX puede operar en ambos espectros licenciados o no. Dentro del rango de 2-11GHz del 802.16a, cuatro bandas son particularmente atractivas.

2.1.2.1 Con licencia 2.5GHz MMDS

En los Estados Unidos, la FCC tiene asignados 200MHz de espectro de radio con licencia entre los 2.5-2.7GHz para el Servicio de Distribución Multipunto Multicanal (Multichannel Multipoint Distribution Service, MMDS).

2.1.2.2 Con licencia 3.5GHz

La asignación de bandas para el uso en esta tecnología es básicamente la misma que fuera asignada para MMDS, en las bandas de 3.4 a 3.7GHz.

2.1.2.3 Sin licencia 3.5GHz

En los Estados Unidos, la FCC ha recientemente abierto un espectro de 50MHz adicional sin licencia en la banda 3.65-3.70GHz para servicios de localización fija inalámbrica.

2.1.2.4 Sin licencia 5GHz U-NII

En los Estados Unidos, 555MHz de frecuencia sin licencia han sido asignados en las bandas 5.150-5.350GHz y 5.470-5.825GHz. Este espectro es llamado la banda de Infraestructura de Información Nacional Sin Licencia (Unlicensed National Information Infrastructure, U-NII), la misma banda usada por las LANs inalámbricas 802.11a. La asignación fue incrementada de 300MHz a 555MHz por una orden de la FCC en Noviembre del 2003.

2.1.3 Plan Nacional de Frecuencias en Ecuador

El Consejo Nacional de Telecomunicaciones (CONATEL) considerando:

- Que el artículo 247 de la Constitución Política de la República, así como también el artículo 47 del Reglamento General a la Ley Especial de Telecomunicaciones reformada, disponen que el Espectro Radioeléctrico es un recurso natural limitado perteneciente al dominio público del Estado; en consecuencia es inalienable e imprescriptible;

- Que de conformidad con lo señalado en el artículo innumerado primero del artículo 10 de la Ley Especial de Telecomunicaciones reformada, el Consejo Nacional de Telecomunicaciones es el ente de administración y regulación de las telecomunicaciones en el país;

- Que el Reglamento de Radiocomunicaciones de la UIT la Nota 5.150, establece que las bandas 902 - 928 MHz, 2400 - 2500 MHz y 5725 - 5875 MHz están asignadas para aplicaciones industriales, científicas y médicas (ICM);

- Que como parte de las Resolución 229 de la Conferencia Mundial de Radiocomunicaciones 2003 (CMR-03), celebrada en Ginebra, se

estableció la utilización de las bandas 5150-5250 MHz, 5250-5350 MHz y 5470-5725 MHz para el servicio móvil para la implementación de Sistemas de Acceso Inalámbrico (WAS), incluidas las redes radioeléctricas de área local (RLAN);

- Que la implementación y operación de Sistemas de Modulación Digital de Banda Ancha, permiten utilizar una baja densidad espectral de potencia, que minimiza la posibilidad de interferencia;

- Que los sistemas de modulación digital de banda ancha pueden coexistir con sistemas de banda angosta, lo que hace posible aumentar la eficiencia de utilización del Espectro Radioeléctrico;

- Que es necesario que la administración ecuatoriana se asegure que los sistemas que emplean técnicas de modulación digital de banda ancha, como es el caso de Sistemas de Acceso Inalámbrico (WAS), incluidas las Redes Radioeléctricas de Area Local (RLAN), cumplan con las técnicas de reducción de la interferencia requeridas, de acuerdo al tipo de equipos y la observancia de normas;

- Que los avances tecnológicos y los nuevos servicios de telecomunicaciones, hacen necesario designar dentro del territorio nacional bandas de

frecuencias radioeléctricas, para operar sistemas de telecomunicaciones sin causar interferencia perjudicial a un sistema que esté operando a título primario;

- Que se hace necesaria la regulación para la operación e implementación de sistemas que emplean Modulación Digital de Banda Ancha; y,

En ejercicio de las atribuciones legales que le confiere el artículo 10, artículo innumerado tercero, y demás normas pertinentes de la Ley Especial de Telecomunicaciones reformada, y en concordancia con lo dispuesto en el artículo 41 del Reglamento General a la Ley Especial de Telecomunicaciones reformada resuelve:

Según el artículo 6 del Registro Oficial Nº- 143 del Consejo Nacional de Telecomunicaciones CONATEL-2005 dice:
Se aprobará la operación de sistemas de radiocomunicaciones que utilicen técnicas de modulación digital de banda ancha en las siguientes bandas de frecuencias como muestra la tabla 1:

BANDA (MHz)	ASIGNACION
902 – 928	ICM
2400 – 2438.5	ICM
5150 – 5250	INI
5250 – 5350	INI
5470 – 5725	INI
5725 – 5850	ICM, INI

Tabla 2.1: Bandas de Frecuencias

El CONATEL aprobará y establecerá las características técnicas de operación de sistemas de Modulación Digital de Banda Ancha en bandas distintas a las indicadas en la presente norma, previo estudio sustentado y emitido por la SNT.

2.2 Protocolo de Acceso al Medio

Existen dos mecanismos de control de acceso en RSI, los basados en protocolos de arbitraje y los basados en protocolos de contención. Los primeros establecen un controlador de grupo, capaz de coordinar los periodos de envío entre nodos. Los protocolos de contención, asumen un medio libre pero en el que pueden aparecer interferencias debido a colisiones entre envíos de nodos distintos. Existen distintas técnicas para llegar a implementar estas dos visiones distintas de entender el acceso al medio.

Los **protocolos de arbitraje**, cuentan con dos aproximaciones: Acceso Múltiple por División de Frecuencia (Frecuency Division Multiple Access, FDMA) y Acceso Múltiple por División de Tiempo (Time Division Multiple Access, TDMA).

Los **protocolos de contención** no cuentan con un coordinador de grupo, así que cualquier nodo puede disponer del medio para su envío de datos. Este enfoque conlleva ciertos problemas, como la posibilidad de que dos nodos transmitan al mismo tiempo, lo que conllevaría a interferencias en la señal, que pueden corromper el paquete original. Para evitar este problema, se cuanta con tres técnicas de control de acceso: CSMA, CSMA/CD y CSMA/CA.

La tecnología Wi-Fi utiliza el protocolo de contención con la técnica de control de acceso al medio CSMA/CA. La tecnología WIMAX utiliza el protocolo de arbitraje TDM/TDMA. Se procederá a detallar ambos protocolos.

2.2.1 Protocolo de Contención

2.2.1.1 Acceso Múltiple con Detección de Portadora Evitando Colisiones (CSMA/CA)

CSMA/CA cuenta con retardo aleatorio de transmisión de paquetes para el uso eficiente del canal inalámbrico compartido entre múltiples nodos en la red; esta clase de protocolo MAC es uno de los más populares de las redes inalámbricas y cuyo fin es brindar servicios de WLAN.

Hablar de “evitar” colisiones es, tal vez, demasiado pretencioso. Lo que en realidad hace CSMA/CA es reducir la probabilidad de colisión entre estaciones que comparten un medio inalámbrico común, al evitar que todas las estaciones intenten transmitir en el instante en que probablemente habrá una colisión: inmediatamente después de que el medio se vuelve ocioso.

El funcionamiento es el siguiente: cuando una estación quiere transmitir, escucha el medio, si está ocupado, espera durante un tiempo prefijado denominado Distribución del Espacio entre Tramas (Distributed Inter Frame Space, DIFS), si durante todo el tiempo el medio está libre, la estación puede transmitir.

Al igual que otros protocolos de su especie, para disminuir el número de colisiones cuando se espera por el canal desocupado, se utilizan tiempos de espera variables, de distribución exponencial, a este método se

le conoce como *reserva exponencial (*exponential backoff).

En la figura 2.1, se muestra los tiempos de espera que una estación tendrá que respetar a la hora de transmitir.

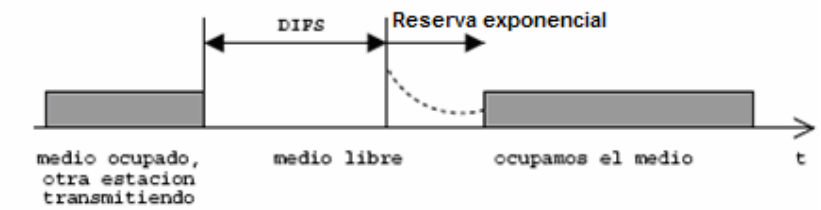


Figura 2.1: Tiempos de espera para una transmisión, escenario simple

Cada trama enviada es confirmada mediante ACKs. El tiempo de espera que una estación receptora tiene que cumplir para mandar el ACK es mucho más corto que el DIFS, de forma que se asegura que dos estaciones terminan su diálogo antes de que otra estación intervenga el medio. A este tiempo de espera para mensajes del mismo diálogo se le denomina Espacio Corto entre Tramas (Short IFS, SIFS).

En la figura 2.2, se muestra un diálogo entre dos estaciones (STA1 y STA2) y una tercera (STA3) que pretende transmitir.

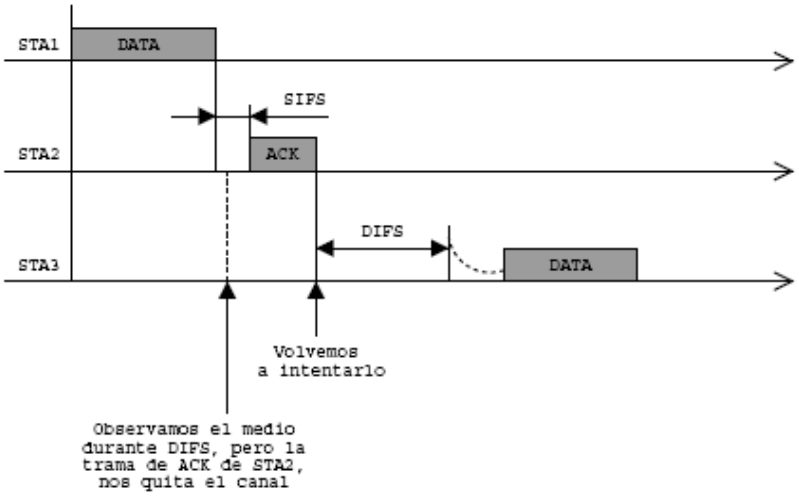


Figura 2.2: Tiempos de espera para una transmisión, un caso mas complejo

Sin embargo el sistema antes descrito tiene un problema: estamos suponiendo que una estación es capaz de saber si el medio está ocupado o no, simplemente escuchando. Esto, en redes inalámbricas centralizadas es imposible, ya que una estación no tiene por que estar en el radio de cobertura de otra STA. A esta situación se la denomina problema de los nodos ocultos.

En la figura 2.3, se muestra un posible ejemplo de esta situación, STA1 no puede detectar si STA2 está transmitiendo o no, por lo tanto, el mecanismo de CSMA/CA degenera en un simple ALOHA, mucho menos eficiente.

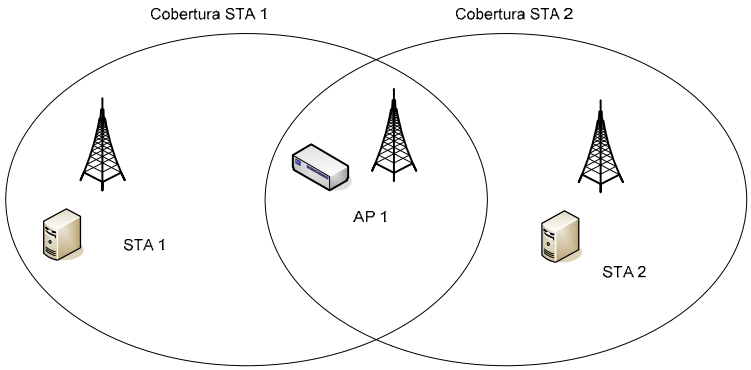


Figura 2.3: Problema de nodos ocultos

Para evitar esto se complementa el CSMA/CA con un sistema con Sensor de Portadora Virtual (Virtual Carrier Sense, VCS).

El sistema de VCS consiste en, antes de enviar los datos, calcular el tiempo total que estará el canal ocupado por esta transacción y enviarlo al receptor en una trama corta, denominada Solicitud para Enviar (Request to Sent, RTS). El receptor de un RTS lo duplica y difunde la señal Permiso para Enviar (Clear to Sent, CTS), como se muestra en la figura 2.4.

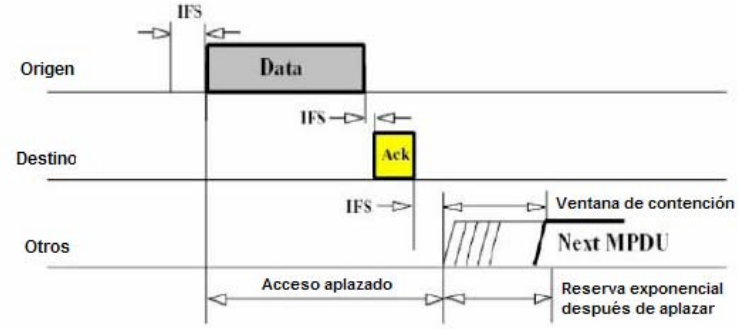


Figura 2.4: Mecanismo CSMA/CA y control RTS/CTS

De esta manera todos los nodos de la BSS susceptibles de interferir con la comunicación, están al tanto de la duración de la misma. Cuando un nodo recibe un CTS, almacena la información de cuanto va a estar el canal ocupado en un Vector de Asignación de Red (Network Allocation Vector, NAV). Mientras el NAV le indique que no debe transmitir, permanecerá callado, incluso si aparentemente, para él, el canal está libre.

De esta manera la posibilidad de colisión por un nodo oculto se ve disminuida enormemente, pues ahora solo pueden colisionar los RTS/CTS, que son tramas de duración muy corta.

En la figura 2.5, se muestra un ejemplo de un intercambio de RTS/CTS entre dos estaciones y como una tercera, que permanece oculta de la primera, reserva un NAV para la transacción.

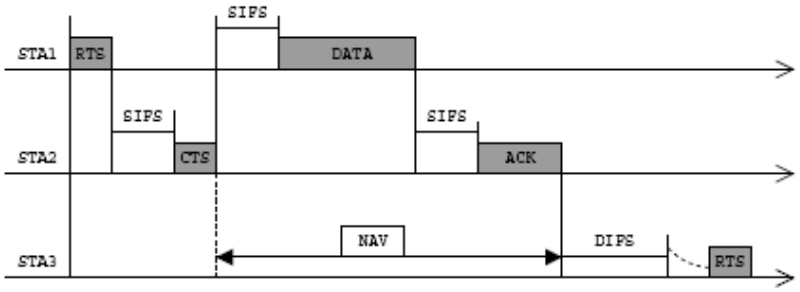


Figura 2.5: Intercambio de RTS/CTS

2.2.2 Protocolos de Arbitraje

2.2.2.1 Acceso Múltiple por División de Tiempo (TDM/TDMA)

TDMA es una tecnología de transmisión digital que permite a un número de usuarios acceder sin interferencia a un canal de radio-frecuencia para colocar en una porción de tiempo único a cada usuario dentro del canal. El esquema de transmisión digital TDMA multiplexa tres señales sobre un único canal.

Todas las técnicas de acceso múltiples dependen de la adopción de tecnología digital.

La tecnología digital es ahora el estándar del sistema de telefonía pública donde todas las llamadas análogas son convertidas a forma digital para transmitir sobre la red de transporte principal (backbone).

TDMA es básicamente el FDMA analógico con una componente de tiempo compartido construida dentro del sistema.

TDMA depende del hecho de que la señal de audio ha sido digitalizada, esto es, dividida en un número de paquetes con una longitud en tiempo de milisegundos. Este ubica un canal de frecuencia solo por un corto tiempo y entonces se mueve a otro canal. El ejemplo digital desde un solo transmisor ocupa diferentes porciones de tiempo en diferentes bandas al mismo tiempo como la muestra la figura 2.6.

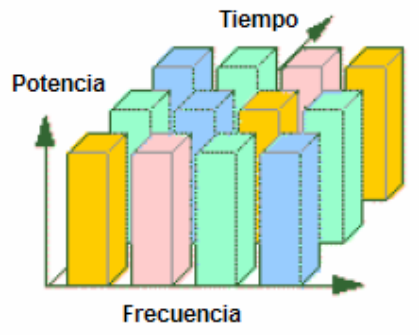


Figura 2.6: TDMA

La técnica de acceso usada en TDMA tiene tres usuarios compartiendo una frecuencia de portadora de 30 KHz. TDMA es también la técnica de acceso usada en el estándar digital Europeo, GSM, el estándar digital Japonés, y los celulares digitales personales (PDC).

2.2.3 Protocolo de Acceso al Medio utilizado en cada sistema

Protocolo de Acceso al medio		CSMA	CSMA/CD	CSMA/CA	TDMA
WIFI	802.11b	●	●	●	
	802.11a	●	●	●	
	802.11g	●	●	●	
WIMAX	802.16				●
	802.16a				●
	802.16d				●
	802.16e				●

Tabla 2.2: Protocolos de acceso de cada sistema

2.3 Ancho de Banda

2.3.1 Tipos de Modulación

2.3.1.1 Introducción

Las técnicas descritas incluyen la Modulación de Fase de Cuadratura (Quadrature Phase Shift Keying, QPSK) y la Modulación de Amplitud en Cuadratura (Quadrature Amplitude Modulation, QAM) y cómo pueden estas técnicas utilizarse para aumentar la capacidad y velocidad de una red inalámbrica.

Éstas técnicas de modulación son la base de las comunicaciones para los sistemas como cable módems, módems DSL, CDMA, 3G, Wi-Fi (IEEE 802.11) y WIMAX (IEEE 802.16).

Ondas Portadoras

Las Ondas de Radio son Ondas Electromagnéticas que se mueven a la velocidad de la luz en la forma de una onda sinusoidal y pueden ser usadas para portar un mensaje a cierta distancia. Ellas pueden tener diferentes frecuencias la cual describe que tan rápido se mueven hacia arriba y abajo lo cual se mide en ciclos por segundo o Hertz. Las Ondas Portadoras con diferentes frecuencias tienen diferentes propiedades. Por ejemplo, las ondas de luz son visibles al ojo humano pero no pueden viajar a través de las paredes. Las ondas de radio (en especial aquellas a frecuencia

muy baja) pueden penetrar paredes y edificios como también refractarse alrededor de las esquinas.

Modulación

La modulación es el proceso por el cual una onda portadora es capaz de portar el mensaje o señal digital (series de unos y ceros). Hay tres métodos básicos para esto: amplitud, frecuencia y fase. Ordenes más altos de modulación permiten codificar más bits por símbolo o por periodo (tiempo).

2.3.1.2 Modulación por Desplazamiento de Amplitud (ASK)

La modulación por desplazamiento de Amplitud (Amplitude Shift Keying, ASK) comprende el incremento de la amplitud de la onda (potencia) de acuerdo con la señal digital (en otras palabras, bajo = 0, alto = 1) y es usado en transmisiones de radio AM.

2.3.1.3 Modulación por Desplazamiento de Frecuencia (FSK)

La modulación por desplazamiento de frecuencia (Frequency Shift Keying, FSK) cambia la frecuencia de acuerdo con la señal digital. Los sistemas que usan esta modulación (señal abierta de transmisión de radio FM) tienden a ser más resistentes al ruido debido a que éste usualmente cambia la amplitud de la señal. En la figura 2.7, diferentes bits son representados por diferentes frecuencias las cuales pueden ser detectadas por el receptor.

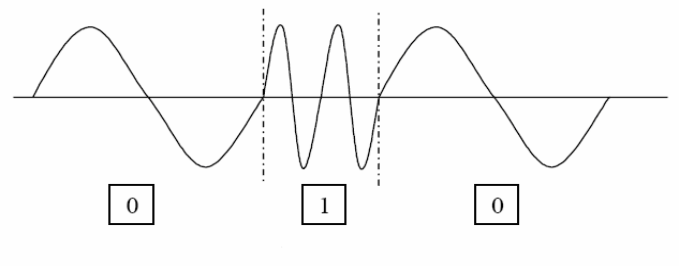


Figura 2.7: Modulación por Desplazamiento de Frecuencia

2.3.1.4 Modulación por Desplazamiento de Fase (PSK)

La modulación por Desplazamiento de Fase (Phase Shift Keying, PSK) cambia la fase de la portadora de acuerdo con el mensaje digital.

2.3.1.4.1 Modulación por Desplazamiento de Fase Binario (BPSK)

Para la modulación por Desplazamiento de Fase Binaria (Binary Phase Shift Keying, BPSK), cada símbolo puede indicar dos diferentes estados o un bit por símbolo (en otras palabras, 0 = 0, 180 = 1). En la figura 2.8, la segunda onda es cambiada en la mitad de un periodo o 180 grados. El receptor puede que reconozca éste cambio indicando un uno o un cero digital.

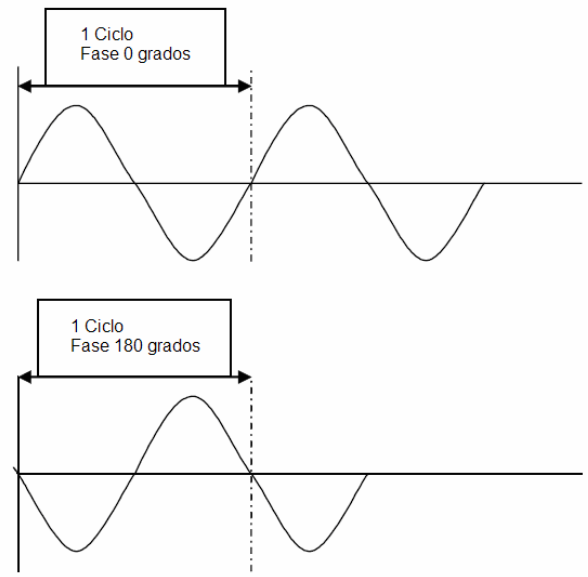


Figura 2.8: Modulación por desplazamiento de fase binario

2.3.1.4.2 Modulación por Desplazamiento de Fase en Cuadratura (QPSK)

La modulación por Desplazamiento de Fase en Cuadratura (Quadrature Phase Shift Keying, QPSK) adiciona dos fases más: 90 y 270 grados. Ahora dos símbolos por bit pueden ser transmitidos. Cada fase de un símbolo es comparada en relación al previo símbolo; así, si no hay cambio de fase (0 grados), los bits “00” son representados. Si hay un cambio de fase de 180 grados, los bits “11”, y así se representan las demás combinaciones como se muestra en la tabla 2.3.

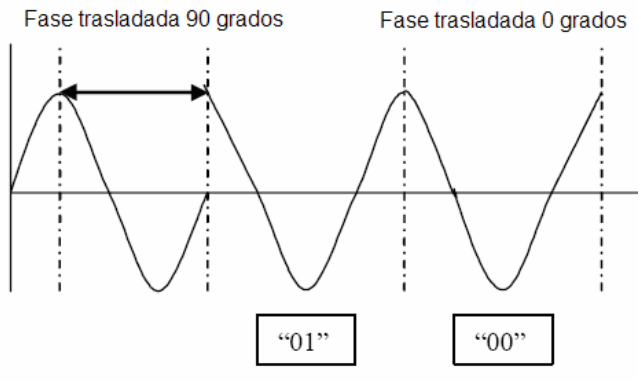


Figura 2.9: Modulación por desplazamiento de fase en cuadratura

Símbolo	Cambio de Fase
00	0 grados
01	90 grados
10	180 grados
11	270 grados

Tabla 2.3: QPSK

2.3.1.5 Modulación de Amplitud de Cuadratura (QAM)

ASK y PSK pueden ser combinados para crear QAM donde tanto la fase y la amplitud pueden ser cambiadas. El receptor entonces recibe esta señal modulada, detecta los cambios y demodula la señal y la regresa a su estado original. En la figura 2.10 se muestra 16-QAM, cada símbolo puede ahora ser representado por cuatro bits en lugar de los dos bits por símbolo en QPSK. Cada punto indica una amplitud

única y la fase de la onda (por ejemplo, el punto (1,1) indica 90 grados de fase y una amplitud de 1).

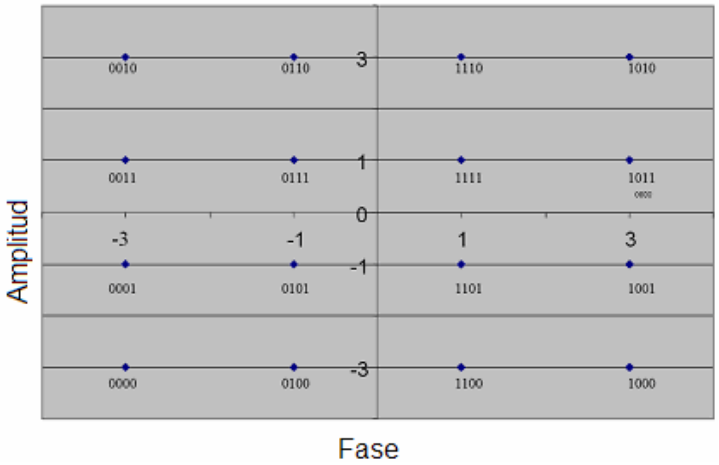


Figura 2.10: Modulación por Amplitud de Cuadratura 16-QAM

2.3.1.6 Modulación Adaptativa

Diferentes órdenes de modulación permiten enviar más bits por símbolo y con esto se consiguen tasas de transmisiones más altas o mejor eficiencia espectral. Sin embargo, se tiene que notar que cuando se usa una técnica de modulación tal como 64-QAM, mejores relaciones señal-a-ruido (SNRs) son necesarias para superar cualquier interferencia y mantener una cierta tasa de error de bit (BER).

El uso de modulación adaptativa permite a un sistema inalámbrico escoger el más alto orden de modulación dependiendo de las condiciones del canal. En la figura 2.11, se puede ver un estimado general de las

condiciones del canal necesarias para las diferentes técnicas de modulación. A medida que se incrementa el rango, se disminuye a una modulación inferior (en otras palabras, BPSK), pero si se está cerca se puede utilizar un orden de modulación alto como QAM para incrementar la velocidad de transmisión. Además, la modulación adaptativa permite al sistema superar el desvanecimiento y otras interferencias.

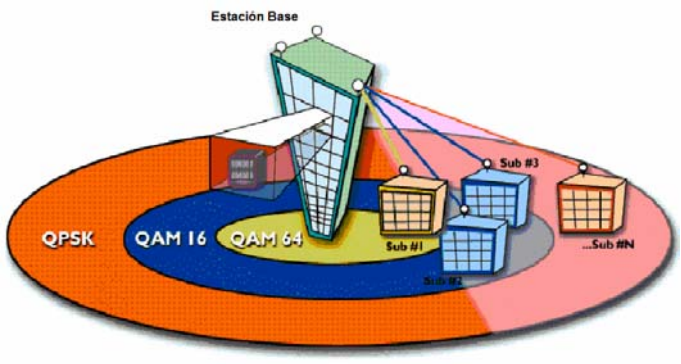


Figura 2.11: Modulación Adaptativa

2.3.2 Modulación utilizada en cada sistema

TIPO DE MODULACIÓN		ASK	FSK	CCK	PSK		QAM			ADAPTATIVA
					BPSK	QPSK	16	64	256	
WIFI	802.11b			●	●	●				●
	802.11a				●	●	●	●		
	802.11g			●	●	●	●	●		●
WIMAX	802.16					●	●	●		●
	802.16a				●	●	●	●	●	●
	802.16d				●	●	●	●	●	●
	802.16e				●	●	●	●	●	●

Tabla 2.4: Modulación de cada sistema

2.3.3 Eficiencia

La eficiencia del ancho de banda es medido por el número de bits por segundo que pueden ser transportados en un ciclo de radio frecuencia (baudios) (bps/Hertz). La tasa de transmisión es determinada multiplicando la eficiencia del ancho de banda por el ancho de banda del canal de radio que la señal ocupará. Lo fundamental a recordar es que mientras más eficientemente el transmisor codifique la señal, será más susceptible al ruido e interferencia.

Por ejemplo, a la tasa de datos soportada en un canal de 25MHz (1 a 11 Mbps), el 802.11b entrega una eficiencia de ancho de banda entre 0.04 y 0.44 bps/Hertz. La tasa de transmisión de 6 a 54Mbps soportada por el 802.11a/g de un canal de 20MHz produce una eficiencia de ancho de banda entre 0.24 y 2.7 bps/Hertz. En WIMAX, la combinación de modulación y esquemas de codificación producen una eficiencia de ancho de banda mayor a 5 bits/Hertz. Esto entregará una tasa de transmisión de 100 Mbps en un canal de radio de 20MHz. La eficiencia del ancho de banda disminuirá a medida que los rangos de transmisión incrementen, así un máximo de 3.5 bits/Hertz o 70Mbps en un canal de 20MHz será más realista.

2.4 Duplexación

Duplexación se refiere al proceso de creación de canales bi-direccionales de transmisión de datos para los enlaces de subida y bajada. La Duplexación en el Dominio del Tiempo (Time Division Duplexing, TDD) y la Duplexación en el Dominio de la Frecuencia (Frequency Division Duplexing, FDD) son ambos utilizados por los estándares 802.11 y 802.16. Soluciones con licencia usan FDD mientras las soluciones exentas de licencia utilizan TDD.

2.4.1 Duplexación en el Dominio de la Frecuencia

FDD requiere un par de canales separados para minimizar interferencia, uno para transmisión y otro para recepción. La gran mayoría de las bandas FDD son asignadas para voz, porque la arquitectura bi-direccional de FDD permite manejar la voz con el menor retardo posible. FDD, sin embargo, suma componentes adicionales al sistema y por lo tanto incrementa el costo.

FDD es usado en redes inalámbricas de tercera generación (3G), las cuales operan a una frecuencia conocida y son designadas para aplicaciones de voz. La mayoría de los esquemas de codificación usados en las redes 3G tienen limitaciones para la velocidad de transmisión de datos. A medida que el tráfico de la red se incrementa o decrementa, el área geográfica cubierta por el transmisor puede disminuir o aumentar, un fenómeno llamado “respiración de celda, (cell breathing)”. También, cuando un usuario comparte un canal y deja de transmitir, la tasa de transmisión es reducida proporcionalmente al número de usuarios para minimizar la interferencia,

resultando en un nivel de potencia de transmisión bajo. Variaciones en rango y nivel de potencia de transmisión pueden ser aceptables para aplicaciones de voz, pero son un desafío para redes de datos.

2.4.2 Duplexación en el Dominio del Tiempo

TDD es una técnica de duplexación donde la misma banda de frecuencia es usada por ambas, la estación base y las estaciones móviles (enlaces de subida y bajada), pero en diferentes divisiones de tiempo.

2.4.3 Duplexación utilizada en cada sistema

DUPLEXACIÓN		FDD	TDD
WIFI	802.11b		•
	802.11a		•
	802.11g		•
WIMAX	802.16	•	•
	802.16a	•	•
	802.16d	•	•
	802.16e	•	•

Tabla 2.5: Duplexación

2.5 Técnicas de Transmisión

2.5.1 Espectro Extendido por Secuencia Directa (DSSS)

Es una técnica compleja, la cual esparce la potencia de la señal a través de un gran ancho de banda, dispersando la portadora en lugar de moverla rápidamente a través del canal como lo hace FHSS. Esto se hace para modular directamente la portadora con una alta velocidad de código de secuencia, el cual tiene las características de ruido seudo-aleatorio (PN).

Mientras mas rápido la portadora es modulada, mayor ancho de banda se utiliza.

La secuencia esparcida es producida por modulación de la trama de datos con un código esparcido PN, resultando así en una señal la cual tiene un ancho de banda tan amplio como la información del ancho de banda solo. Por ejemplo, en el 802.11 con 1 y 2 Mbps utilizando DSSS, cada bit de dato es lógicamente combinado con un código de 11 bits Barker. Por que la tasa de bit de la secuencia esparcida es tan alta como la tasa de datos, se da que el ancho de banda es efectivamente esparcido sobre un área tan larga como pudiera otro estar ocupando si la portadora fuera modulada solo por la trama de datos. El resultado es que la potencia de la señal es esparcida sobre una banda muy amplia y se muestra a otros usuarios como un ruido de baja potencia.

2.5.2 Espectro Extendido por Salto de Frecuencia (FHSS)

Fue originalmente desarrollado como un medio para ocultar una transmisión a oyentes indeseados. Este es ahora utilizado para otro propósito que es la reducción de interferencia. La frecuencia de saltos trabaja para transmitir la señal portadora por un período de tiempo corto sobre una banda angosta, entonces salta a otra y así sucesivamente. En un período de tiempo, la potencia promedio de la señal es esparcida así sobre una banda de frecuencias muy ancha.

La frecuencia salta y aparece aleatoriamente a alguien que no conoce un patrón de salto pre-dispuesto, lo que hace imposible sintonizar y escuchar a una transmisión por que la señal portadora nunca permanece lo suficiente en una frecuencia para que el oyente pudiera localizar ésta y resincronizar el receptor a la nueva frecuencia. En la actualidad al emplear FHSS en LANs y PANs inalámbricas no se ofrece seguridad debido a que el patrón de salto es ya conocido. Esto hace sin embargo que se reduzca la interferencia desde y hacia otros dispositivos.

2.5.3 Multiplexación por División Ortogonal de Frecuencia (OFDM)

La Multiplexación por División Ortogonal de Frecuencia es una técnica de transmisión de multi-portadoras que ha sido recientemente reconocida como un excelente método para comunicaciones inalámbricas de datos a alta

velocidad bi-direccional. OFDM comprime efectivamente las múltiples portadoras moduladas juntándolas estrechamente, reduciendo el ancho de banda requerido pero mantiene la señal ortogonal modulada sin interferencia de unas con otras.

Actualmente la tecnología es usada en sistemas tales como: la Línea de Subscriptor Digital Asimétrico (Asymmetric Digital Subscriber Line, ASDL), así como también en sistemas inalámbricos tales como IEEE 802.11 a/g (Wi-Fi) e IEEE 802.16 (WIMAX).

Está basado en FDM, la cual es una tecnología que usa múltiples frecuencias para transmitir simultáneamente múltiples señales en paralelo. Cada señal tiene su propio rango de frecuencia (sub-portadora) la cual es entonces modulada por los datos. Cada sub-portadora es separada por una banda de guarda (guard band) para asegurar que ellas no se superpongan. Estas sub-portadoras son entonces moduladas en el receptor usando filtros para separar las bandas como muestra la figura 2.12.

Figura 2.12: FDM con nueve subportadoras usando filtros

OFDM es similar a FDM pero con mucha más eficiencia espectral porque el espaciamiento de los sub-canales es menor (hasta que ellos estén realmente traslapados). Esto es hecho para encontrar frecuencias que sean ortogonales lo cual significa que éstas sean perpendiculares en un sentido matemático, permitiendo al espectro de cada sub-canal traslapar otro sin interferir con éste. En la figura 2.13, se muestra como el ancho de banda requerido es reducido en gran proporción por que las bandas de guarda son removidas y se permite que las señales se traslapen.

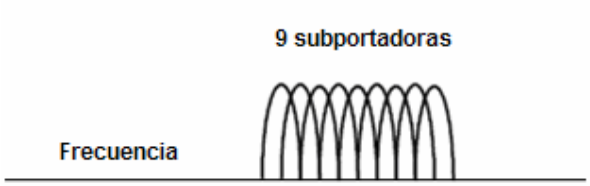


Figura 2.13: OFDM con nueve sub-portadoras

A fin de demodular la señal, es necesaria una Transformada Discreta de Fourier (DFT). Los circuitos integrados (CI) de la Transformada Rápida de Fourier (FFT) están comercialmente disponibles, haciendo esto una operación relativamente fácil.

2.5.4 Multiplexación por División Ortogonal de Frecuencia Codificada (COFDM)

Cuando la OFDM se emplea junto con codificación de canal para detección y corrección de errores, se designa como COFDM.

2.5.5 Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA)

Básicamente lo que hace OFDMA es asignar diferentes portadoras a diferentes usuarios. Un esquema simple de OFDMA consiste en particionar el conjunto de N portadoras en M subconjuntos de N/M portadoras cada una y asignar un grupo de diferentes portadoras a diferentes usuarios. De esta manera, los recursos pueden ser repartidos a N/M usuarios diferentes en el mismo tiempo.

Una de las mayores limitaciones sobre los canales de enlace de subida en los sistemas inalámbricos es la potencia de transmisión disponible. Comparado a TDMA, la técnica OFDMA incrementa el rango de la celda sobre los flujos de subida, por que esta transmite la potencia disponible en una pequeña fracción del ancho de banda del canal. Asumiendo que la atenuación de la señal es proporcional al cuadrado de la distancia, un sistema OFDMA con M = 8 incrementará la cobertura de la celda en el enlace de subida en 18dB. La extensión del rango de la celda puede también ser alcanzada en el enlace de bajada para repartir potencia tanto a las portadoras asignadas a usuarios distantes como a portadoras

asignadas a usuarios que están cercanos a la estación base.

2.5.6 Técnica de transmisión utilizada en cada sistema

TECNICAS DE TRANSMISIÓN		DSSS	FHSS	OFDM	COFDM	OFDMA
WIFI	802.11b	●				
	802.11a			●		
	802.11g	●		●		
WIMAX	802.16					
	802.16a			●	●	●
	802.16d			●		●
	802.16e			●		

Tabla 2.6: Técnica de transmisión

2.6 Velocidad de Transmisión

2.6.1 Tasa de Transmisión y Tasa Efectiva de Transmisión

La Tasa de Transmisión (Data Rate) es la cantidad de datos digitales que es transmitida desde un lugar a otro en un tiempo dado, usualmente en segundos.

En telecomunicaciones, la Tasa de Transmisión es usualmente medida en bits por segundo. Por ejemplo, una conexión típica de baja velocidad a Internet puede ser de 33.6 kilobits por segundo (Kbps). En una red de área local Ethernet, la Tasa de Transmisión puede ser tan rápida como 10 megabits por segundo.

En tecnología de información, la Tasa Efectiva de Transmisión (Data Throughput) es la tasa a la cual una computadora o red envía o recibe datos. Esto es una buena medida de la capacidad del canal de un enlace de comunicaciones, y en conexiones a Internet son usualmente tasadas en términos de cuanta cantidad de bits pasan por segundo (bit/s).

2.6.2 Capacidad de transmisión de cada sistema

VELOCIDAD DE TRANSMISIÓN		Mbps
WIFI	802.11b	11
	802.11a	54
	802.11g	54
WIMAX	802.16	32 a 134
	802.16a	≤ 70 o 100
	802.16d	hasta 75
	802.16e	hasta 15

Tabla 2.7: Capacidad de transmisión

2.7 Corrección de Errores en la Recepción (FEC)

Cuando se utiliza una modulación de señal más eficiente en un ancho de banda, la probabilidad de encontrar errores aumentará. Para compensar eso, los sistemas de radio digital típicamente incluyen alguna forma de FEC. La idea detrás de FEC es incluir bits redundantes en la transmisión que permitirán al receptor detectar y corregir un cierto porcentaje de los errores encontrados. Entonces mientras el código FEC aumenta la tasa de transmisión, el impacto total es una mejoría en el funcionamiento. El enlace de radio original Wi-Fi 802.11b no incluye FEC, pero un código convolucional FEC fue incorporado en el 802.11a y g. WIMAX utiliza el código convolucional y un sistema FEC Reed-Solomon.

En los sistemas de comunicación actual es común usar un código convolucional de Reed-Solomon (R-S) por concatenación serial (SCRSCC). En la decodificación, el código convolucional es primero decodificado a una palabra código de probabilidad máxima y esta es usada como entrada para el decodificador R-S.

2.7.1 Código Convolucional

Los códigos convolucionales son buenos para corregir errores aleatorios. Junto con el Código Reed-Solomon en una combinación efectiva corrigen la gran parte de los errores causados por el canal inalámbrico hostil.

El codificador Convolucional es de tasa ½ y 7 de longitud comprimida. El bloque generador se muestra en la figura 2.14.

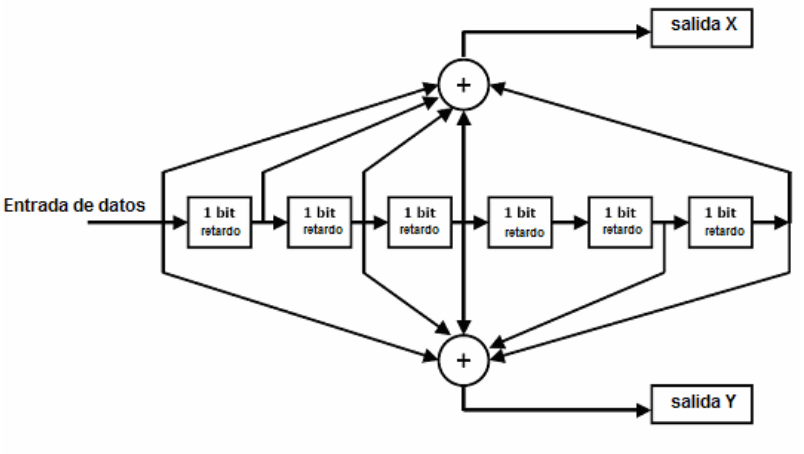


Figura 2.14: Codificador Convolucional tasa ½

Un decodificador Viterbi es utilizado al final de la recepción para decodificar datos y corregir errores.

2.7.2 Código Convolucional de Reed-Solomon

La corrección de error Reed-Solomon es un esquema de código, el cual trabaja primero construyendo un polinomio de los símbolos de datos a ser transmitidos y luego envía un diagrama sobre-muestreado del polinomio en lugar de los símbolos originales en sí. Debido a la redundancia de información contenida en los datos sobre-muestreados, es posible reconstruir el polinomio original y así los símbolos de datos incluso en la fase de transmisión de errores, elevan un cierto grado de error.

2.7.3 Algoritmo de Viterbi

El algoritmo de Viterbi permite la corrección de errores. A cada paso de decodificación son posibles solo 2 caminos de los 4 existentes. Cada camino en el **diagrama de árbol** que se puede efectuar acumula un número de errores creciente con excepción del camino correcto que tiene el mínimo número de errores y por ello la máxima probabilidad de ocurrencia.

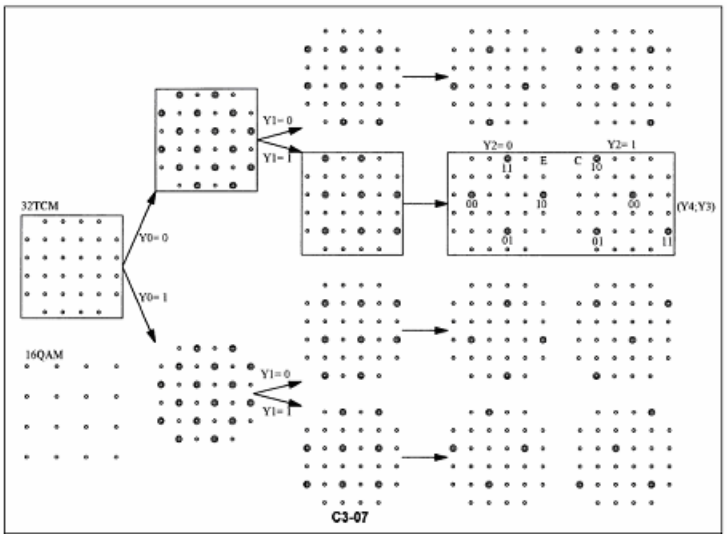


Figura 2.15: Corrección de errores mediante algoritmo de Viterbi

2.8 Rango de Cobertura

2.8.1 Línea de Vista Directa (LOS)

En un enlace LOS, una señal viaja sobre un camino directo y libre desde el transmisor al receptor. Un enlace LOS requiere que mas de la primera zona Fresnel este libre de alguna obstrucción, si este criterio no es cumplido hay una reducción significante de la potencia de la señal. El espacio libre de Fresnel requerido depende de la frecuencia de operación y la distancia localizada entre el transmisor y el receptor.

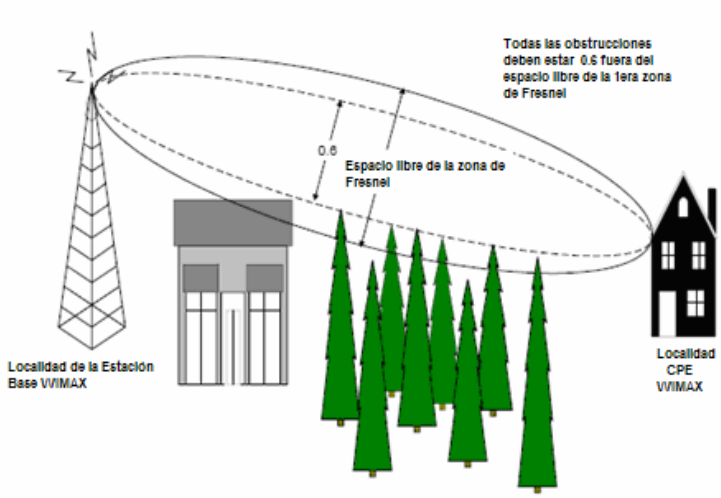


Figura 2.16: Línea de vista directa

2.8.2 Sin Línea de Vista Directa (NLOS)

En un enlace NLOS, una señal alcanza el receptor a través de reflexiones, dispersión y difracciones. Las señales que llegan al receptor consisten de las

componentes del camino directo, los múltiples caminos reflectados, la energía esparcida y los caminos de propagación difractados. Estas señales tienen diferentes retardos de propagación, atenuación, polarización y relativa estabilidad del camino directo.

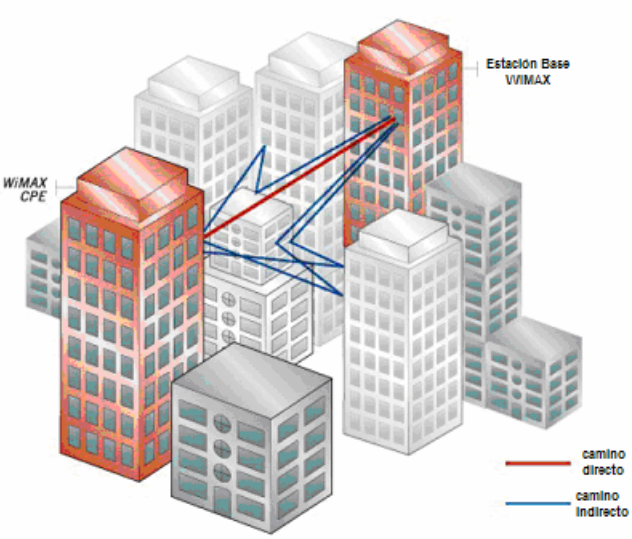


Figura 2.17: Propagación sin línea de vista

2.8.3 Rango de cobertura de cada sistema

RANGO DE COBERTURA		LOS	NLOS
WIFI	802.11b	100 mts	
	802.11a	100 mts	
	802.11g	125 mts	
WIMAX	802.16	1.61 a 4.83 Km	
	802.16a		4.83 a 8.05 Km
	802.16d	max 48.3 Km	4.83 a 8.05 Km
	802.16e		Móvil hasta 5 Kmts

Tabla 2.8: Rango de Cobertura

2.9 Calidad de Servicio (QoS)

La calidad de servicio hace referencia a la capacidad de una red para proveer el mejor servicio para seleccionar el tráfico de red, también es definido como la medida del rendimiento de un sistema de transmisión que refleja la calidad de transmisión y la disponibilidad de los servicios, el cual es un elemento crucial de QoS.

Las tecnologías de QoS proveen la construcción elemental de bloques para negocios multimedia y aplicaciones de voz usadas en campus, WAN y proveedores de servicios de red. El QoS permite administrar la red para establecer un acuerdo en los niveles de servicios con los usuarios de la red.

Este habilita los recursos de la red para ser compartidos más eficientemente y facilitar el manejo de las aplicaciones críticas. Además administra el delicado tiempo multimedia y el tráfico de aplicaciones de voz para asegurar que este tráfico reciba alta prioridad, gran ancho de banda y menor retardo.

La calidad de servicio puede ser implementada exitosamente, por que la infraestructura de red es altamente disponible. La calidad de transmisión en la red es determinada por los siguientes factores: la latencia, la inestabilidad (jitter) y la pérdida de paquetes.

El QoS provee servicios de red realzados y previsibles en las siguientes formas:

- Soportando ancho de banda dedicado para usuarios y aplicaciones críticas.

- Controlando la inestabilidad y latencia (requerido para tráfico en tiempo real).
- Manejando y minimizando la congestión de la red.
- Ordenando el tráfico de red para suavizar el flujo del tráfico.
- Poniendo prioridad de tráfico en la red.

El QoS se consigue ya sea elevando la prioridad de un flujo o limitando la prioridad de otro flujo. Cuenta con herramientas de manejo de congestión, con lo cual se intenta aumentar la prioridad de un flujo encolado y mantener colas de diversas maneras. La herramienta de mantenimiento de colas que es utilizada para evitar la congestión, aumenta la prioridad de hacer decaer a flujos de baja-prioridad antes que los flujos de alta-prioridad. Al vigilar y configurar se proporciona prioridad a un flujo limitando el rendimiento de procesamiento de otros flujos.

El protocolo 802.16 puede soportar múltiples tipos de servicios de comunicaciones (datos, voz y video) con diferentes requerimientos de QoS. El QoS señala mecanismos y funciones definidos en la capa MAC para controlar la transmisión de datos entre la BS y la SS. Hay 4 tipos de servicios en la capa MAC que caracterizan a los parámetros QoS similares a los de las WLANs, estos son: latencia, inestabilidad, velocidad efectiva, la tasa de tráfico mínima reservada y la tasa de tráfico máxima sostenida.

2.9.1 Pérdida de paquetes

Como el nombre lo sugiere, la *pérdida de paquetes* es simplemente la cantidad de paquetes que se pierden durante la transmisión y normalmente se expresa como un porcentaje de todos los paquetes. La pérdida de paquete (un paquete "extraviado") será reconocida por la estación receptora, lo cual implica la necesidad de un reenvío. Cuando se trata de datos, esto no es un gran problema. Con los datos de voz, hay muy poco tiempo para volver a enviar un paquete de forma que se pueda reinsertar en la secuencia adecuada, justo en el punto correcto de la conversación.

Los distintos tipos de tráfico de red determinan un nivel aceptable de pérdida de paquetes. La pérdida de un paquete cuando se transmiten datos a través de una parte libre de licencia del espectro de frecuencia de radio es mucho más posible que cuando se transmite a través de un cable de cobre. El control de la pérdida de paquetes y la QoS relacionada en una red inalámbrica es más complejo que en una red cableada.

2.9.2 Retraso o Latencia de los paquetes

El *retraso* es la medida de la duración de tiempo que se necesita para que un paquete vaya de una estación de la red a la siguiente. Esta cantidad de tiempo, que también se conoce como *latencia*, tiene un mínimo absoluto que es una función de los protocolos de red. La cuantificación más importante, la cual es la más difícil de controlar, es la latencia que provoca la congestión en la red.

2.9.3 Variación en el retraso o Inestabilidad

El flujo de voz y video difiere de la transmisión de datos normales en el sentido de que el receptor debe generar el flujo original desde un búfer de reproducción, en donde el tamaño del búfer de reproducción requerido está determinado por la medida del retraso. Por lo tanto, la *variación en el retraso*, la cantidad de variación entre cada retraso de paquete, tiene un impacto en la calidad percibida en la transmisión. La inestabilidad puede ser el resultado de una red congestionada, en especial una que está saturada con tráfico "urgente" como el de video y otros tipos de datos.

2.9.4 Efecto en Aplicaciones

La pérdida de paquetes en la tecnología 802.11 permite una cantidad relativamente alta de paquetes extraviados, con más de 1% de todo lo que se envía. Las redes de "alta disponibilidad" como, por ejemplo, las que manejan el procesamiento basado en transacciones como el del tráfico de un lugar a otro que se establece entre un lector del código de barras y un sistema de inventarios, no debe perder más del 1% de los paquetes. El tráfico de voz, obviamente, tiene los requerimientos más estrictos para la pérdida de paquetes; la cantidad de paquetes perdidos cuando se controla el tráfico de voz debe aproximarse a cero. Para los paquetes de voz, la latencia no debe ser mayor a 150ms (el 15% de un segundo), que es un periodo bastante corto, en especial cuando una estación debe esperar continuamente para enviar datos debido a la

cantidad alta de tráfico en la red. Para el tráfico de voz, la inestabilidad (jitter) debe mantenerse en menos de 30ms.

Para el caso de WIMAX, este ofrece una baja latencia a través del tramo inalámbrico. La mayoría de los equipos WIMAX tienen una latencia menor a 10ms desde la estación base a la CPE y viceversa. En el caso de voz sobre IP si la latencia excede los 150ms la calidad de la conversación empezará a degradarse. De ser mayor a 200ms muchos usuarios pueden percibir una conversación incompresible.

En los enlaces WIMAX, la mayor parte de la latencia no se presenta en el enlace inalámbrico entre la estación base y el subscriptor, si no en la parte alámbrica de la conexión entre el subscritor y el resto de la red.

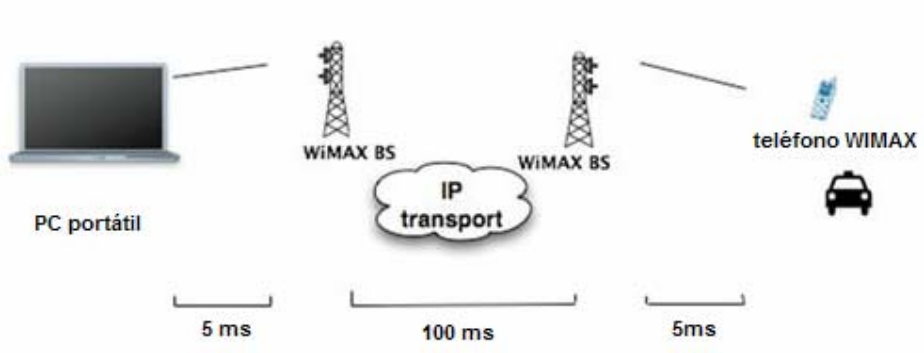


Figura 2.18: Latencia en los sistemas WIMAX

2.10 Seguridad

La seguridad es importante para las comunicaciones de datos inalámbricas debido al hecho de que uno no puede controlar el acceso a la infraestructura física usada en los medios inalámbricos ya que su medio de transmisión es el aire.

Ninguna red, ya sea alámbrica o inalámbrica, puede ser completamente segura al 100%. La seguridad puede ser revisada solamente en niveles relativos, donde cada nivel discreto provee más protección que el último pero viene con un costo relacionado en operadores, equipos y velocidad efectiva (throughput). El propietario de la red debe determinar lo que ellos están tratando de proteger, y cuanto ellos están dispuestos a gastar en términos de equipos y mano de obra adicional para la protección.

Una red inalámbrica presenta dos diferentes áreas relacionadas aún con sus propios problemas de seguridad: la señal inalámbrica actual y la red IP.

La seguridad para la porción de la señal inalámbrica involucra técnicas de encriptación para enmascarar la información que se está enviando a través de un enlace inalámbrico y prevenir la conexión sin autorización a este enlace.

La red IP usada en los sistemas alámbricos e inalámbricos es virtualmente idéntica. Los mismos protocolos de seguridad que son usados al comprar con tarjetas de crédito en Internet pueden y deberían ser aplicadas a las redes inalámbricas. Los protocolos de seguridad tales como el filtrado de MAC ID, la Capa para Conexiones Seguras (Secure Sockets Layer, SSL), autenticación

Radius, Redes Privadas Virtuales (VPN) y 802.1x están disponibles para ser usadas sobre una red inalámbrica. Estos protocolos de seguridad direccionan la autenticación de equipos sobre las redes antes de permitir el tráfico de datos que procede a lo largo de la red.

2.10.1 Seguridad Wi-Fi

La seguridad en las redes inalámbricas ha sido un obstáculo para el rápido crecimiento de estas. Algunas compañías han vacilado en comprometerse a una red inalámbrica.

El Acceso Protegido Wi-Fi (WiFi Protected Access, WPA), desarrollado en Mayo del 2003 por la Alianza Wi-Fi en conjunto con el Instituto de Electricidad e Ingenieros Electrónicos (IEEE), mejoraron la seguridad versus el estándar anterior. Así incrementó dramáticamente la protección disponible para LANs inalámbricas, el Acceso Protegido Wi-Fi (WPA) habilitó a las empresas a avanzar y a comenzar a disfrutar de una realzada productividad, conveniencia y ahorro de costos en redes móviles inalámbricas. Y, desde que WPA es un subconjunto de la próxima generación en la especificación 802.11i, ésta ofrece fáciles e inmediatas soluciones basadas en estándares para la seguridad de las WLAN. También, WPA es compatible con las tecnologías pasadas y futuras además está diseñada para ser desplegada como un software mejorado tanto para puntos de accesos como para clientes.

2.10.1.1 Objetivos de la Seguridad

El objetivo común del despliegue inalámbrico es una red que provea todos los beneficios de las tradicionales LANs alámbricas, incluyendo una conectividad continua y confiable entre un cliente y la red corporativa. La palabra clave aquí es *confiable*. Así como en la contraparte alámbrica, las redes inalámbricas dependen de una cadena de confianza que protejan la red y sus recursos, los cuales son:

- La Autenticación verifica la fuente u origen de los datos que viajan a través de la red.
- La Autorización asegura que el usuario tenga permitido acceder solamente a los servicios autorizados.
- La Protección confidencial de los datos contra la intercepción desautorizada.
- La Integridad asegura que los datos no sean modificados por un individuo desautorizado.

Careciendo de alguno de estos cuatro elementos de la cadena, las compañías exponen sus recursos al riesgo. Los piratas de red (hackers) pueden explotar la conocida vulnerabilidad de la seguridad en el estándar original 802.11 y abrir la brecha de la confiabilidad y la integridad de la red.

2.10.1.2 Mecanismos de Seguridad antes de 802.11g

El estándar original 802.11 para las LAN inalámbricas incorpora tres mecanismos primarios de seguridad: El Identificador de Conjunto de Servicios (Service Set Identifier SSID), el filtrado direccionado de Control de Acceso al Medio (Media Access Control, MAC) y la Privacidad Equivalente al Cableado (Wired Encriptation Privacy, WEP). Sin embargo, cada una de estas ha demostrado que tiene vulnerabilidades.

2.10.1.2.1 Identificador de Conjunto de Servicio (SSID)

Este segmenta la LAN inalámbrica en múltiples redes, cada una de las cuales tiene su propio identificador. Por ejemplo, cada departamento de una compañía puede tener su propia red. Para acceder a una de las múltiples redes dentro de la LAN inalámbrica, el cliente y el equipo de punto de acceso necesitan ser configurados con el SSID apropiado. Sin embargo, si las compañías siguen la práctica común de usar los SSIDs por omisión y contraseña, los identificadores SSID pueden ser expuestos a un intruso.

2.10.1.2.2 Filtrado de Direcciones MAC

Este incrementa la seguridad ya que requiere que cada punto de acceso inalámbrico sea configurado con las direcciones MAC de los equipos de los clientes autorizados. Solamente los equipos de los clientes en la lista de direcciones MAC pueden conectarse a través de este punto de acceso. Las

flaquezas de esta propuesta es que un atacante puede interceptar la dirección MAC por “rastreo” o fisgoneando la red para interceptar paquetes, y entonces configura una tarjeta inalámbrica atacante sobre un equipo del cliente con la dirección MAC para ganar acceso a la red. Encriptando los datos enviados entre el cliente inalámbrico y el punto de acceso se puede ayudar a proteger en contra de estos rastreadores, pero una efectiva protección requiere fuertes algoritmos de encriptación. En la figura 2.19 se puede apreciar esta característica en un Punto de Acceso Inalámbrico.

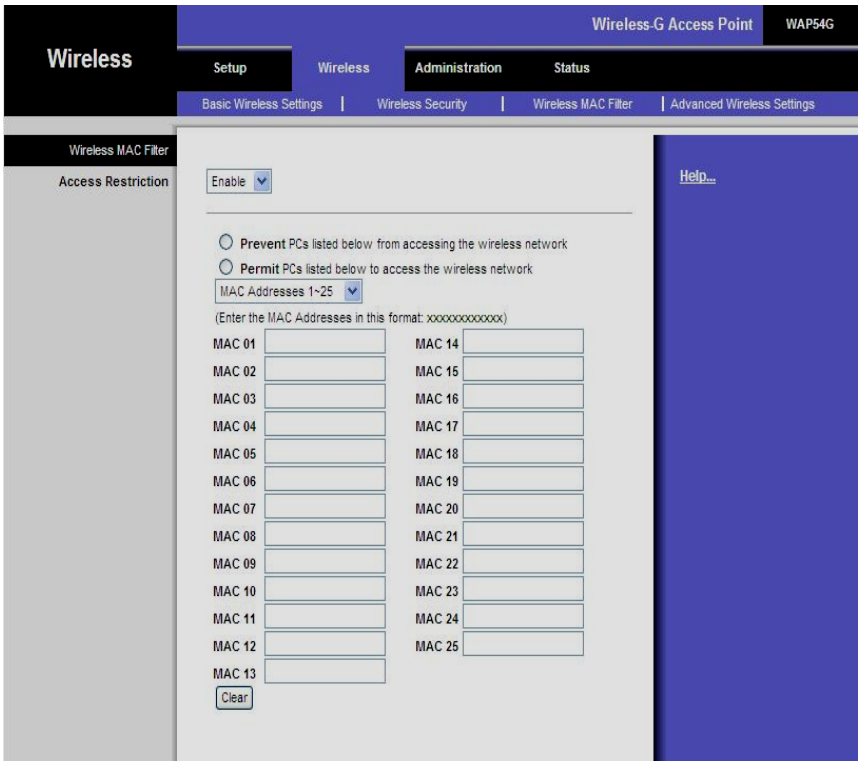


Figura 2.19: Filtrado de direcciones MAC

2.10.1.2.3 Privacidad Equivalente al Cableado (WEP)

Este fue diseñado para proveer encriptación y autenticación como parte del estándar 802.11. La encriptación inicial usa una clave (una secuencia de números ingresados por el usuario). En la figura 2.20 se puede apreciar esta característica en un Punto de Acceso Inalámbrico.

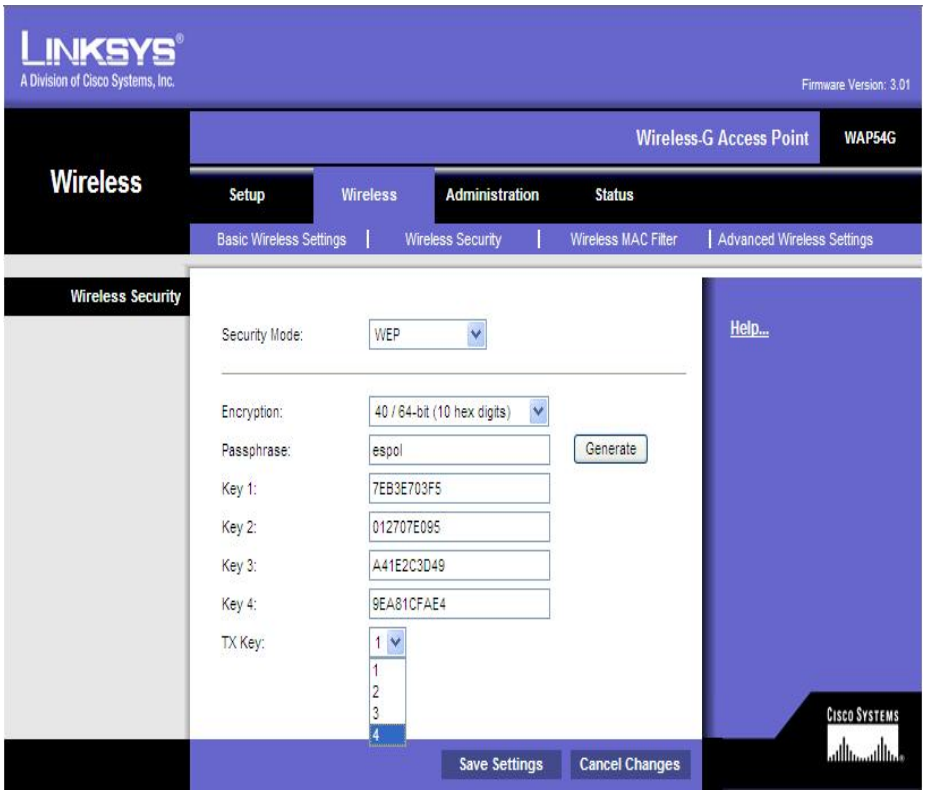


Figura 2.20: WEP

Con WEP, los clientes inalámbricos y los puntos de accesos son manualmente configurados con la misma clave de 40 bits. Las claves WEP son estáticas así como también relativamente cortas y manualmente distribuidas. La falta de una administración de clave automática contribuye a tener claves con una trama de vida infinita. Adicionalmente, el método de encriptación revela parte de la trama de la clave en la inicialización del vector y así es defectuosa.

Estas flaquezas juntas hacen que las redes inalámbricas estén sujetas a brechas atacantes confidencialmente pasivas, en las cuales un intruso puede leer datos sobre la red y activar estas brechas donde ellos insertan tráfico sobre la red y compromete la integridad de los datos. Adicionalmente, las herramientas disponibles están diseñadas para habilitar a los intrusos a olfatear las transmisiones de la red y recuperar las claves de encriptación WEP. El WEP también carece de la habilidad para identificar la fuente de cada paquete.

Sumándose a las flaquezas inherentes de la especificación original 802.11, las empresas que evitan el despliegue de las WLANs pueden encontrar su seguridad de red comprometida por el renombre de computar inalámbricamente. Los empleados quienes desean las conexiones inalámbricas pueden instalar puntos de accesos LANs inalámbricos que

puedan exponer los recursos corporativos al ataque. Ahora, las soluciones están disponibles, estas permiten la seguridad del despliegue de las LANs inalámbricas, estas soluciones incluyen:

1. Desplegar una solución de una Red Virtual Privada (VPN) probada con WEP.
2. Combinar funcionalmente el estándar WEP con el IEEE 802.1X con y sin una VPN.
3. Desplegar el nuevo Acceso Protegido Wi-Fi para acceder a redes remotas públicas dentro de una empresa usando VPN.

2.10.1.2.4 Acceso Protegido Wi-Fi (WPA)

El Acceso Protegido Wi-Fi (Wi-Fi Protect Access, WPA) direcciona todas las vulnerabilidades conocidas en WEP para asegurar la autenticidad de los datos en las redes LANs inalámbricas y proteger contra cualquier ataque. Fue diseñada para minimizar el impacto sobre el desempeño de las redes y también puede ser usada como una actualización de software en más de 650 productos Wi-Fi certificados en el mercado de hoy.

WPA usa el Protocolo de Integridad de clave temporal (Temporal Key Integrity Protocol ,TKIP) para la encriptación y emplea autenticación 802.1X con un tipo del estándar del Protocolo de Autenticación Extensible (Extensible Autentication Protocol, EAP) disponibles hoy.

En la figura 2.21 se puede apreciar esta característica en un Punto de Acceso Inalámbrico.

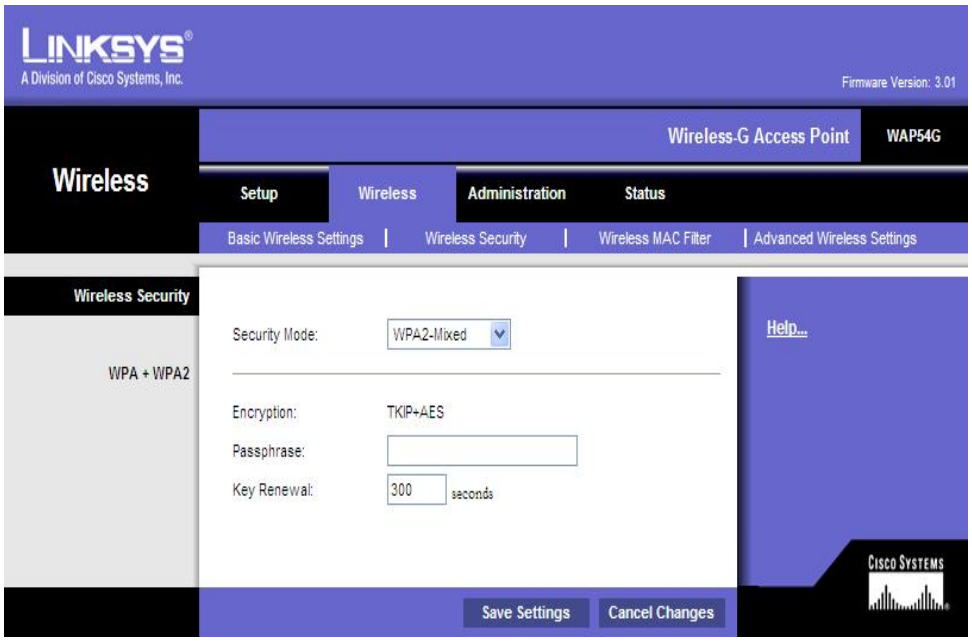


Figura 2.21: WPA

2.10.1.2.4.1 Mecanismo de seguridad de WPA

WPA usa un gran esquema de encriptación realzado y TKIP. Junto con la autenticación 802.1X/EAP, TKIP emplea una clave jerárquica que realza la protección. Éste adiciona también un Chequeo de Integridad de Mensaje (Message Integrity Check, MIC), algunas veces llamado “Michael”, para proteger contra paquetes intrusos.

2.10.1.2.4.2 Encriptación

TKIP incrementa el tamaño de la clave de 40 a 128 bits y reemplaza la simple clave estática de WEP con claves que son dinámicamente generadas y distribuidas por el servidor de autenticación. TKIP usa una clave jerárquica y una metodología de administración de clave que remueve lo predecible de las claves.

Luego, el servidor de autenticación acepta las credenciales de usuarios, usando 802.1X para producir una clave única principal llamada clave “pair-wise” o clave de doble palabra, para que la sesión se inicie. TKIP distribuye esta clave a los clientes y al AP estableciendo una clave jerárquica y un sistema de administración, usando así la clave de doble palabra para generar dinámicamente una clave única de encriptación de datos para encriptar cada paquete de datos que se está comunicando inalámbricamente durante ésta sesión del usuario.

La clave jerárquica de TKIP cambia la simple clave estática de WEP por más de 500 trillones de claves posibles que pueden ser usadas sobre un paquete de datos enviado.

Por la gran expansión del tamaño de las claves, el número de claves usadas y la creación de un mecanismo de chequeo integral, TKIP aumenta la

complejidad y dificultad la decodificación de los datos sobre una red Wi-Fi. Así mismo, incrementa el poder y la complejidad de la encriptación inalámbrica, haciendo esto resulta más difícil y hasta imposible que un intruso acceda a la red Wi-Fi.

TKIP fue diseñado para ser desplegado con equipos Wi-Fi certificados ya existentes y también es incluido en el estándar WPA2.

2.10.1.2.4.3 Autenticación

WPA usa autenticación 802.1X con uno de los Protocolos de Autenticación Extensibles (EAP) disponibles hoy. 802.1X es un puerto basado en un método de control de acceso a las redes tanto alámbricas como inalámbricas. Esta fue adoptada como un estándar por la IEEE en Agosto del 2001.

EAP maneja la presentación de las credenciales de usuarios, en forma de certificados únicos digitales estos son: los nombres de usuario (username), la clave (password), las tarjetas inteligentes, los IDs de seguridad, o cualquier otra credencial de identidad que el administrador haya usado. WPA permite flexibilidad tanto en el tipo de credencial que sea usado y en la selección de un tipo de EAP.

Con EAP, 802.1X establece una estructura en la cual la estación de trabajo del cliente se autentica mutuamente con el servidor de autenticación. Esta mutua autenticación previene que usuarios se conecten accidentalmente o desautoricen a los APs sobre la red Wi-Fi y también asegura que los usuarios que accedan a la red sean quienes deban estar allí. Cuando un usuario solicita el acceso a la red, el cliente envía la credencial del usuario al servidor de autenticación a través del AP. Si el servidor acepta la credencial del usuario, la clave principal TKIP se envía al cliente y al AP.

2.10.1.3 802.11i (WPA2)

En enero de 2001, el grupo de trabajo i fue creado en IEEE para mejorar la seguridad en la autenticación y la encriptación de datos. En junio de 2004, la edición final del estándar 802.11i fue adoptada y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. Este estándar introdujo varios cambios fundamentales como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura fuerte y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. La nueva arquitectura para las redes inalámbricas se llama Red de Seguridad Robusta (Robust Security Network, RSN) y utiliza autenticación 802.1X.

Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica.

El establecimiento de un contexto seguro de comunicación consta de cuatro fases:

- Acuerdo sobre la política de seguridad
- Autenticación 802.1X
- Derivación y distribución de las claves
- Confidencialidad e integridad de los datos RSNA

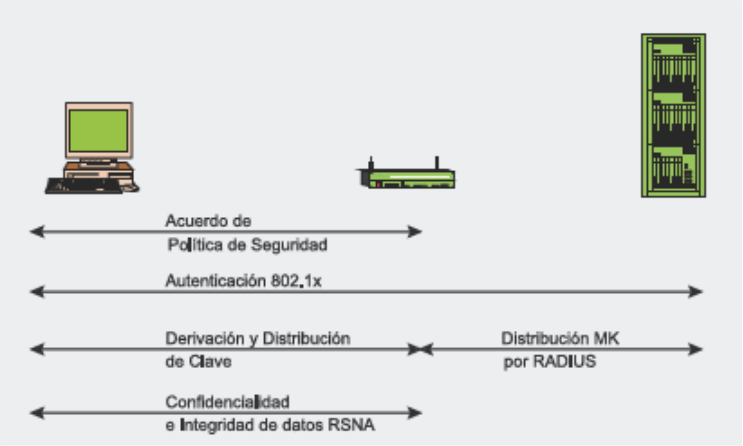


Figura 2.22: Fases del establecimiento de seguridad

2.10.2 Seguridad WIMAX

La subcapa de privacidad IEEE 802.16 proporciona al usuario privacidad para encriptar el enlace entre la Estación Base (BS) y la Estación de Usuario (SS), y éste proporciona protección contra el robo de servicio por servicio de encriptación que fluye dentro de la red. La subcapa de privacidad emplea un protocolo autenticado de administración de clave cliente/servidor que es capaz de soportar el Estándar de Encriptación Avanzada (AES). En este protocolo la Estación Base (BS), actúa como servidor, controlando la distribución de clave a la Estación de Usuario (SS), la cual actúa como cliente.

La subcapa de privacidad emplea a los componentes de los protocolos para llevar a cabo toda la seguridad relacionadas con las tareas. El primero es un protocolo de encapsulamiento, el cual es usado para la encriptación de paquetes de datos a través de la red. Éste protocolo define las reglas asociadas con el uso de conjuntos criptográficos para encriptar la información útil en el MAC PDU. Estos conjuntos criptográficos son los algoritmos de encriptación y autenticación.

La segunda componente de la subcapa de privacidad es el Protocolo de Administración de Clave Privada (Protocol Key Managment, PKM). Este es usado para proporcionar distribución segura de claves entre la Estación Base y las Estaciones de Usuario. Este protocolo es además usado por la BS y la SS para mantener la sincronización de la

asignación de claves de los datos entre ellos, y por la BS para controlar el acceso a los servicios de red.

2.10.2.1 Arquitectura de Seguridad

La entrada a la red de una Estación Subscriptora envuelve los siguientes pasos:

- Alguna SS intentando unirse a la red suele buscar en sus alrededores una señal conveniente para el enlace de bajada de la BS, ésta señal será usada para establecer los parámetros del canal.
- Usando ésta señal, la SS establece un Canal de Administración Primario (Primary Management Channel, PMC) con la BS. Éste canal suele ayudar en la negociación de la capacidad, autorización y administración de clave.
- Una vez que la negociación preliminar sea completada, el protocolo PKM entra en juego y autoriza la SS a la BS.
- La BS en respuesta al mensaje registra a la SS.
- Una vez que la SS esta registrada, la BS envía una respuesta en la cual ésta asigna una conexión ID para una conexión de administración secundaria.
- Finalmente la SS y la BS crean una conexión de transporte.

La arquitectura de seguridad de 802.16 es dividido en dos categorías:

- El Protocolo de Encapsulación para encriptar los paquetes de datos. Éste define y pone una serie de criptogramas y reglas para aplicar estos algoritmos a los paquetes.
- El Protocolo de Administración de Clave para asegurar la distribución de la asignación de clave de los datos desde la BS a la SS.

2.10.2.2 Asociación de Seguridad

Esta es una relación entre el transmisor y el receptor que provee parámetros de seguridad para el tráfico. El protocolo define la Autorización de la SA, conteniendo: el perfil del certificado X.509 de la SS, los 160 bits de Clave de Autorización (Authorization Key, AK), tiempo de vida del AK, el algoritmo de generación de clave de encriptación (key encriptation key, KEK) usada por la BS para encriptar las Claves de Encriptación de Tráfico (Traffic Encryption Keys, TEK). Similarmente hay: una asociación de seguridad de datos, su almacenamiento a la base de datos SAID (único identificador por cada SA), los detalles de los cripto-algoritmos del soporte de la SS, dos TEKs, el tiempo de vida de los TEKs, los 64 bits IV por cada TEK.

2.10.2.3 Certificado X.509

Estos certificados son usados para identificar la comunicación de las partes. El perfil del certificado que es definido en el estándar consiste de la siguiente información:

- El formato de versión del certificado

- El número de serial del certificado
- El nombre del emisor del certificado
- Validación del certificado
- Contenedor del Certificado de Identidad (Certificate holders identity) (dirección MAC de la SS)
- Contenedor del Certificado de Clave Pública del certificado (Certificate holders public key)

El estándar define un Certificado de Manufactura y un Certificado de la SS. La BS usa la clave pública del Certificado de Manufactura para verificar la autenticidad del Certificado de la SS. El modelo asume que la SS almacena la clave privada en un almacenamiento sellado.

2.10.2.4 Privacidad y Mantenimiento de Clave

Autorización de la SS: La Estación Base autoriza primero a una SS intentando unirse a la red. El proceso de autorización envuelve un intercambio de tres mensajes entre la BS y la SS. En el primer mensaje la SS envía su Información de Autorización (Authorization Information, AI), en la cual la BS autoriza a la SS. Una vez aceptada la autorización, la SS envía una solicitud de autenticación (Areq). Una vez que la SS esta autenticada, la BS envía a ésta una clave de autorización (Authorization Key, AK) la cual es encriptada con la clave pública de la SS.

Después de alcanzar la autorización inicial, la SS necesita solicitar periódicamente la reautorización para

obtener un nuevo AK. La SS emplea una máquina de estado para alcanzar esto.

Intercambio del TEK: Después de obtener un AK desde la BS, la SS inicia una máquina de estado para obtener el tráfico encriptando claves desde la BS. Ésta maquina de estado TEK es responsable de manejar la asignación de claves del material asociado con cada SAID. La secuencia de los mensajes intercambiados durante éste período es como se presenta en la figura 2.23.

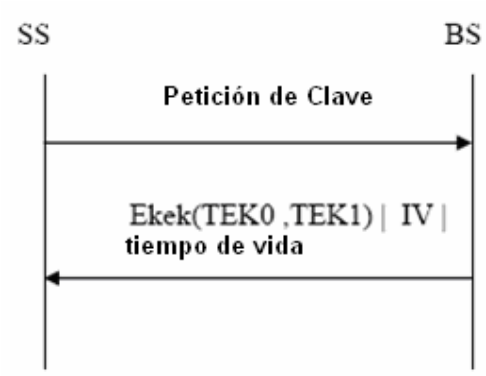


Figura 2.23: Secuencia de intercambio de mensajes

El primer mensaje mostrado en la figura 2.23 es opcional, este mensaje es enviado desde la BS solamente cuando este quiere reasignar claves a una SA de datos o crear una nueva SA. Hay una máquina de estado, la cual gobierna la operación del intercambio del TEK. La máquina de estado de autorización dispara esta máquina de estado una vez que el AK es recibido.

2.10.2.5 Tratamiento de la Clave

AK: La BS es responsable de mantener toda la información con clave para todas las SAs. Cuando la BS recibe una repuesta de autorización ésta inicializa dos claves de Autorización. Esta clave activada es enviada a la SS. Una vez que el tiempo de vida de la clave esta cerca de expirar la SS hace una solicitud de reautorización. Respondiendo a ésta, la BS activa la segunda clave y la envía como respuesta al mensaje de reautorización recibido desde la SS. Como ésta activa la segunda clave, ésta inicia una tercera clave, la cual es mantenida en espera de una próxima operación. Desde aquí, la BS estará siempre preparada para enviar un AK a la SS. La BS asocia un número de secuencia en orden creciente para cada AK y evitar ataques.

TEK: El diagrama de interacción de mantenimiento del TEK es similar al del AK. La BS genera dos TEKs inicialmente por cada SA. Subsecuentemente, este se mantiene generando nuevas claves como las antiguas expiradas. La BS utiliza la mas antigua de las dos claves activadas para encriptar el canal del enlace de bajada considerando que éste usa cualquiera de las claves para desencriptar el tráfico del enlace de subida dependiendo de cual clave esté usando la SS. La BS cambiará su clave siempre que la clave existente expire. La responsabilidad de actualizar las claves es dejada a la SS. La máquina de estado del TEK disparará la solicitud para una nueva clave siempre que

la clave existente esté cerca de expirar. La SS usará la más actual de las dos claves disponibles con esto se encripta el tráfico de subida del enlace, considerando que éste puede usar cualquiera de las claves para desencriptar el tráfico de bajada del enlace dependiendo de que clave esta siendo usada por la BS.

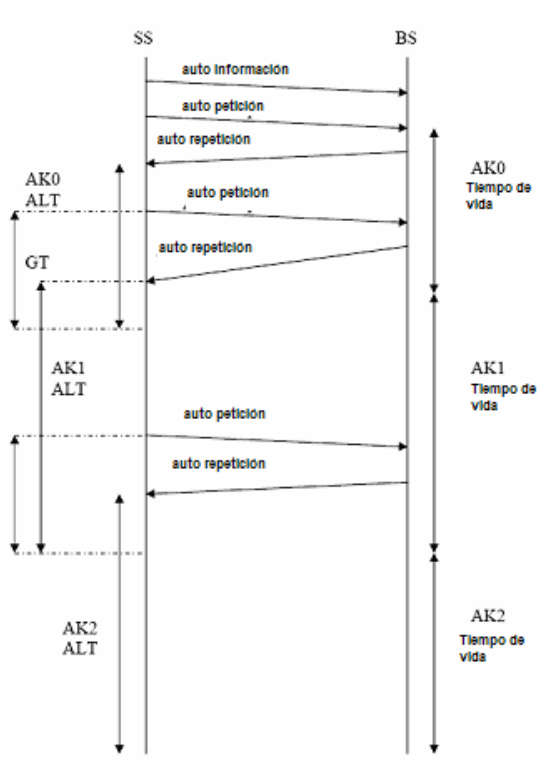


Figura 2.24: Uso del AK

2.10.2.6 Criptografía

Todos los datos útiles son encriptados con DES en modo (Cipher Block Chaining, CBC). El Vector de Inicialización (Initialisation Vector, IV) del CBC es calculado como el IV en el mensaje TEK.

El TEK es encriptado usando KEK en 3DES. Los HMACs en el mensaje son también derivados desde la AK.

CAPITULO 3

3 APLICACIONES Y SERVICIOS

3.1 Red Wi-Fi

3.1.1 Pacifictel

3.1.1.1 Descripción de la Infraestructura

La infraestructura se encuentra ubicada a 2° 9’ 43’’ S y 79° 53’ 51’’O (en la Avenida Francisco de Orellana en el antiguo edificio del Banco del Progreso) y utiliza desde el cuarto al sexto piso de éste. El área total de cada piso es de 36.34 x 36.34 m^2. Ver en anexo de planos.

Consta en su interior de paredes falsas y de concreto y paredes exteriores de concreto y vidrio. El piso es de losa con recubrimiento de marmetón.

Cada piso cuenta con un cuarto de equipos y el principal esta ubicado en el quinto piso.

3.1.1.2 Descripción de la red

Pacifictel cuenta con una topología de red estrella. Los APs se encuentran conectados a un conmutador (switch) propio de cada piso y estos a su vez están conectados a un switch principal ubicado en el 5to piso, donde llega el proveedor a través de fibra óptica.

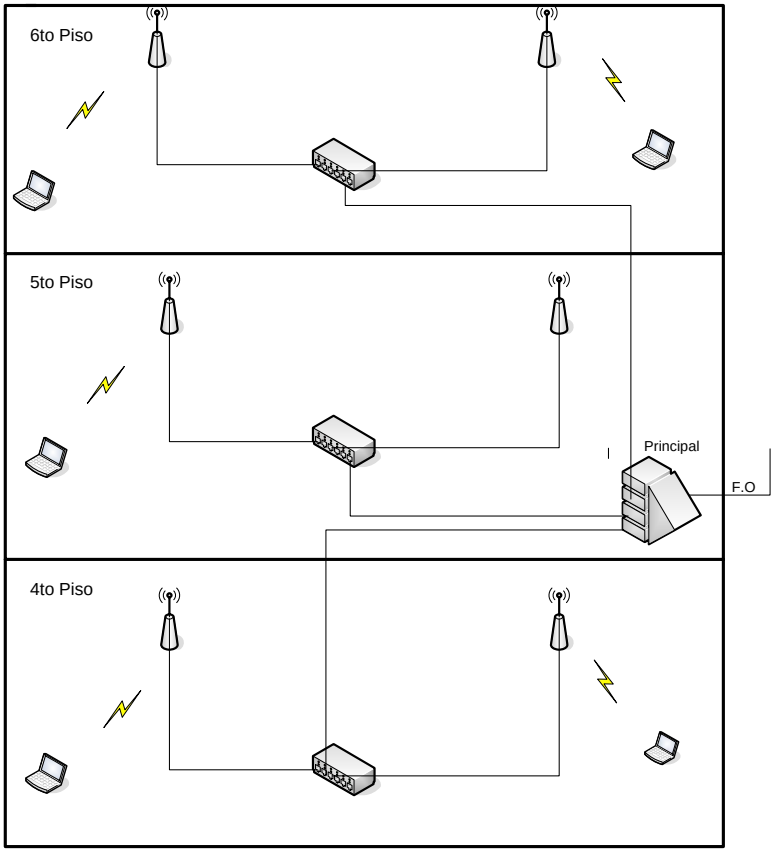


Figura 3.1: Topología de la red Pacifictel

Con los APs inalámbricos colocados estratégicamente se da cobertura a todas las PCs ubicadas en cada departamento de los diferentes pisos como se puede observar en los planos ubicados en el Anexo de planos.

Los equipos utilizados en esta red operan en la banda de frecuencia de 2.4MHz Half Duplex.

Los servicios de esta red están limitados a los que el proveedor les brinde, siendo hasta el momento utilizada para transmisión de datos.

3.1.1.3 Parámetros y mediciones

Los parámetros tomados en consideración fueron:

- Nivel de señal
- Nivel de ruido
- Relación señal a ruido

Con esto se obtuvo el lugar óptimo para cada AP. Una vez ubicados estos se realizaron pruebas de alcance de señal en diferentes puntos de la zona cubierta por cada AP, estos datos se muestran en las tablas de la 3.1 a 3.12 y en el Anexo de planos.

CUARTO PISO:

Prueba 1

AP 402

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 54	- 96	40
B	- 60	- 96	40
C	- 60	- 97	34
D	- 45	- 97	34
E	- 50	- 95	43
F	- 45	- 95	43
G	- 63	- 97	35
H	- 58	- 96	40
I	- 60	- 100	35
J	- 50	- 98	47
K	- 65	- 96	34
L	- 45	- 96	40
M	- 45	- 96	30
N	- 50	- 96	33
O	- 50	- 96	22
P	- 54	- 96	20
Q	- 58	- 98	30

Tabla 3.1: Mediciones prueba 1 cuarto piso

Prueba 2

AP 404

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dBm]
A	- 75	- 96	20
B	- 50	- 95	43
C	- 45	- 97	34
D	- 55	- 96	40
E	- 45	- 95	43
F	- 45	- 97	34
G	- 50	- 98	47
H	- 55	- 97	45
I	-45	- 97	56

Tabla 3.2: Mediciones prueba 2 cuarto piso

Prueba 3

AP 408

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 60	- 96	35
B	- 54	- 96	40
C	- 45	- 95	43
D	- 45	- 97	56
E	- 54	- 96	40
F	- 60	- 97	43

Tabla 3.3: Mediciones prueba 3 cuarto piso

Prueba 4

AP 410

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 60	- 97	43
B	- 60	- 100	39
C	- 45	- 100	39
D	- 60	- 100	39
E	- 58	- 98	38
F	- 45	- 97	56
G	- 57	- 99	43
H	- 62	- 96	30
I	- 62	- 96	35

Tabla 3.4: Mediciones prueba 4 cuarto piso

QUINTO PISO

Prueba 1

AP 501

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 53	- 98	43
B	- 45	- 98	46
C	- 59	- 95	34

Tabla 3.5: Mediciones prueba 1 quinto piso

Prueba 2

AP 503

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 50	- 96	34
B	- 63	- 96	38
C	- 45	- 96	49
D	- 58	- 96	36

Tabla 3.6: Mediciones prueba 2 quinto piso

Prueba 3

AP 509

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 58	- 96	36
B	- 68	- 96	26

Tabla 3.7: Mediciones prueba 3 quinto piso

Prueba 4

AP 505

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 60	- 96	38
B	- 55	- 98	42
C	- 45	- 98	55

Tabla 3.8: Mediciones prueba 4 quinto piso

SEXTO PISO

Prueba 1

AP 602

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 62	- 96	32
B	- 57	- 96	40
C	- 50	- 97	52
D	- 60	- 94	30

Tabla 3.9: Mediciones prueba 1 sexto piso

Prueba 2

AP 604

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 50	- 96	43
B	- 45	- 96	50
C	- 45	- 97	55
D	- 45	- 96	45
E	- 55	- 94	41
F	- 57	- 96	39
G	- 53	- 97	40

Tabla 3.10: Mediciones prueba 2 sexto piso

Prueba 3

AP 610

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 53	- 97	40
B	- 45	- 97	51
C	- 60	- 96	37

Tabla 3.11: Mediciones prueba 3 sexto piso

Prueba 4

AP 608

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 55	- 97	37
B	- 45	- 97	52

Tabla 3.12: Mediciones prueba 4 sexto piso

Prueba 5

AP 606

Lugar de medición	Nivel de Señal [dBm]	Nivel de Ruido [dBm]	Señal/Ruido [dB]
A	- 60	- 96	39

Tabla 3.13: Mediciones prueba 4 sexto piso

Luego se procedió al análisis de frecuencias para evitar interferencia entre ellos y con otros APs ajenos a la red.

3.2 Red WIMAX

3.2.1 Setel

3.2.1.1 Descripción de la Infraestructura

La red WIMAX de SETEL, cuenta con dos nodos uno ubicado a 2° 7’ 5’’ S y 79° 56’ 39’’ O (Km. 10 ½ Vía a Daule, pinturas Hempel) conocido como nodo Norte y el otro a 2° 11’ 27’’ S y 79° 53’ 16’’ O (Velez entre Pedro Moncayo y 6 de Marzo, Edificio Forum) que se lo denomina nodo Centro.

En el nodo Norte las antenas se encuentran instaladas en la cúspide de una torre de 40 metros en una zona de baja altitud y libre de obstáculos como se ilustra en la figura 3.2.

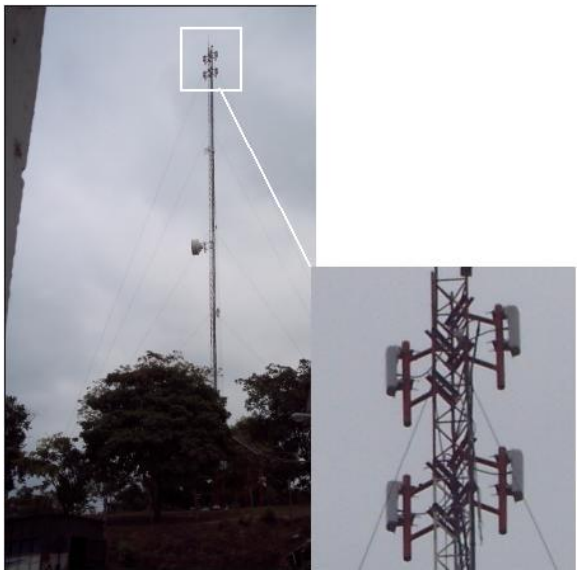


Figura 3.2: Nodo Norte Hempel

En el nodo centro las antenas se encuentran instaladas en uno de los edificios mas altos de la urbe, sobre una torre de 15 metros de altura, como se ilustra en la figura 3.3.

Figura 3.3: Nodo Centro Forum

3.2.1.2 Descripción de la Red

La red WIMAX es una red multipunto como se muestra en la figura 3.4, en la cual cada estación base es independiente de la otra, es decir no cuanta con una topología definida. La red de Setel llega a los nodos mediante fibra óptica. Se utiliza un convertidor de fibra óptica a 10/100 base T para conectar las radio bases WIMAX a esta red, debido a que los equipos utilizan cable UTP cat 5.

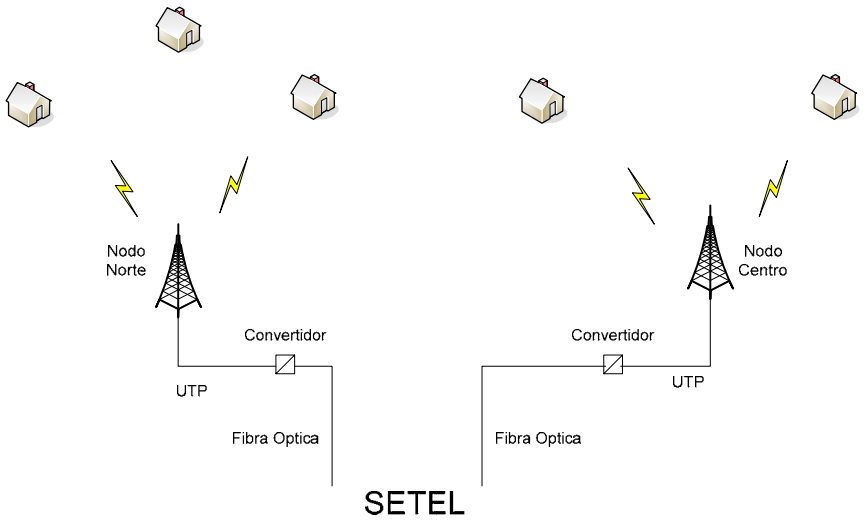


Figura 3.4: Red WIMAX

El nodo Norte cuenta con dos radio bases, una de las cuales da cobertura hasta el kilómetro 17 ½ de la vía a Daule (hasta el centro de rehabilitación del Litoral) y la otra hasta el kilómetro 4 ½ de la vía a Daule. Como se mencionó anteriormente, este nodo no cuenta con la altura suficiente para dar cobertura a la zona noreste de la cuidad y Durán.

El nodo Centro brinda una extensa cobertura abarcando los sectores centro, sureste y suroeste de la cuidad hasta el Puerto Marítimo.

Los equipos utilizados en esta red operan en la banda de frecuencia de 3.5GHz Full Duplex.

Los servicios que SETEL ofrece son hasta el momento telefonía IP e Internet de banda ancha. La preferencia de los usuarios en el sector norte ha sido hacia la telefonía IP, en el sector centro y sur de la cuidad hacia el Internet de banda ancha.

3.2.1.3 Parámetros y mediciones

Los parámetros tomados en consideración para la instalación de las estaciones de usuarios fueron:

- Relación señal a ruido
- Intensidad de la señal recibida

Con los resultados de estos parámetros se determina la posibilidad del enlace, debido a que hay sectores de la ciudad que aún no están cubiertos.

A continuación se presentan algunas pruebas realizadas en diferentes sectores de la urbe. En la tabla 3.13 se muestran clientes enlazados al nodo centro y en la tabla 3.14 a clientes enlazados al nodo norte.

Punto	SNR [dB]	RSS [dBm]	Modulación	Pot. de Tx [dBm]
2° 11’ 41’’S 79° 54’ 10’’O Ayacucho 2912a y G. Lara	32,2	- 65,2	64 QAM 3/4	10
2° 17’ 12’’S 79° 53’ 33’’O Puerto Marítimo	28,8	- 75,9	64 QAM ¾	19
2° 14’ 32’’S 79° 55’ 30’’O Trinipuerto	31	- 72,8	64 QAM ¾	18,5
2° 11’ 56’’S 79° 53’ 2’’O Chile 1102 y Av Olmedo	31,4	- 63	64 QAM ¾	10,5
2° 16’ 21’’S 79° 52’ 43’’O Guasmo Sur Coop. Unión Bananeros	29,9	- 80,3	64 QAM ¾	19
2° 13’ 57’’S 79° 54’ 12’’O Cdla Huancavilca Mz C4	32,1	- 71	64 QAM 3/4	14
2° 12’ 5’’S 79° 54’ 57’’O Portete y Milagro	29,5	- 71,3	64 QAM 3/4	15,5
2° 12’ 45’’S 79° 53’ 8’’O Fitsur	20.5	- 76,7	16 QAM1/2	24

Tabla 3.14: Parámetros de enlace nodo centro

Punto	SNR [dB]	RSS [dBm]	Modulación	Pot. de Tx [dBm]
2° 7' 36''S 79° 55' 52''O Napo Montacargas	30,6	- 67,9	64 QAM ¾	16
2° 5' 1'' S 79° 55' 43''O Cosedone	32,9	- 73,5	64 QAM ¾	16
2° 9' 8''S 79° 55' 54''O Intaco	28,8	- 79,5	64 QAM ¾	19
2° 9' 12''S 79° 55' 50''O Santa Priscilla	31,5	- 66,1	64 QAM ¾	19
2° 7' 47''S 79° 55' 55''O Fehierro	32,2	- 60	64 QAM ¾	7
2° 6' 26''S 79° 56' 0''O Plásticos	32,5	- 47,1	64 QAM ¾	6,5
2° 2' 50''S 79° 56' 51''O Km 17,5	17,4	- 83,3	QPSK 1/2	21

Tabla 3.15: Parámetros de enlace nodo norte

3.3 Servicios que soportan ambas tecnologías

Los estándares 802.11 y 802.16 han sido desarrollados para dirigir un amplio rango de servicios. Estos servicios se los puede clasificar en aquellos que necesiten ejecutarse en tiempo real entre los cuales tenemos:

- Juegos Interactivos
- Voz sobre IP, Video Conferencia
- Medios de Comunicación continuos

Y aquellos que no se ejecutan en tiempo real, como lo son:

- Tecnología de Información
- Descarga de Contenido Multimedia

Estos servicios requieren un ancho de banda determinado para su funcionamiento, los cuales se detallan en la tabla 3.15

Clase	Tiempo Real?	Tipo de Aplicación	Ancho de Banda
Juegos Interactivos	Si	Juegos Interactivos	50 – 85 Kbps
VoIP, Video Conferencia	Si	VoIP	4 – 64 Kbps
		Video Teléfono	32 – 384 Kbps
Medios de Comunicación Continuos	Si	Música/Discurso	5 – 128 Kbps
		Video Clips	20 – 384 Kbps
		Películas Continuas	> 2 Mbps
Tecnología de Información	No	Mensajes Instantáneos	< 250 bytes por mensaje
		Publicaciones Web	> 500 Kbps
		Correo (con archivos adjuntos)	> 500 Kbps
Descarga de Contenido Multimedia	No	Gran cantidad de Datos, Descarga de Películas	> 1 Mbps
		Punto a Punto	> 500 Kbps

Tabla 3.16: Servicios que soportan ambas tecnologías

CAPITULO 4

4 ANALISIS COMPARATIVO

4.1 Parámetros y especificaciones que pueden ser comparadas

4.1.1 Aspectos teóricos de Wi-Fi versus aspectos teóricos de WIMAX

- **Bandas de Frecuencia**

El estándar de redes LAN inalámbricas 802.11 describe únicamente cuatro interfaces de radio enlaces que operan en las bandas de radio sin licencia de 2.4GHz o 5GHz, a diferencia del estándar 802.16 que incluye un rango mucho mayor de frecuencias, de 10 a 66GHz y de 2 a 11GHz. Una ventaja de WIMAX es que en las bandas de frecuencia mas bajas puede soportar NLOS, eliminando la necesidad de alinear el equipo del usuario con la estación base y además incorpora una característica de Selección Dinámica de Frecuencia, donde el equipo

automáticamente busca un canal libre, siendo un gran beneficio en las bandas sin licencia, esta característica no está presente en la tecnología Wi-Fi.

- **Protocolo de Acceso al medio**

Wi-Fi utiliza un protocolo de acceso al medio llamado CSMA/CA, las WLAN usan configuraciones de medios compartidos half duplex donde todas las estaciones transmiten y reciben sobre un mismo canal de radio. El problema fundamental que éste crea en un sistema de radio es que una estación no puede “escuchar” mientras está transmitiendo, lo que hace imposible detectar una colisión. A diferencia en las redes WIMAX, el acceso al canal de entrada será controlado por la estación base. Los usuarios que deseen transmitir, primero envían una petición a un canal de acceso basado en contención. Los permisos exclusivos para usar el canal de entrada es designado por la estación base utilizando un sistema de permisos para enviar. Como sólo una estación tiene permiso para enviar en un tiempo determinado, no habrá colisiones en el tráfico entrante.

- **Modulación**

Ambas tecnologías, Wi-Fi y WIMAX hacen uso de la modulación adaptativa. Es decir, el transmisor automáticamente cambiará a una técnica de modulación mas robusta aunque menos eficiente en condiciones adversas, siendo así, en este aspecto, ambas gozan de los mismos beneficios.

- **Duplexación**

Todas las redes Wi-Fi son sistemas TDD basados en contención, donde todos los AP y las estaciones móviles compiten por el uso del mismo canal. Debido a la operación de medios compartidos se necesitan tiempos de guarda lo cual reduce a menos del 50% la velocidad de transmisión y el uso es menos eficiente para tecnologías de voz. Sin embargo, los sistemas WIMAX pueden ser configurados para utilizar FDD o TDD. Al usar FDD no se requieren tiempos de guarda con lo cual no se ve afectada la velocidad de transmisión y puede ser usada para tecnologías de voz y video pero tiene un costo monetario asociado para su implementación.

- **Técnicas de Transmisión**

En la especificación original del estándar 802.11, se incluyó una opción para el uso de FHSS, pero ésta con el transcurso del tiempo fue desechada, en la actualidad ambas tecnologías gozan de los beneficios que otorga el uso de OFDM, entre los cuales tenemos: el aprovechamiento del ancho de banda, la resistencia a interferencias y al desvanecimiento de la señal, lo que conlleva a un mayor alcance.

- **Velocidad de Transmisión**

En teoría la mayor velocidad de transmisión que alcanza la tecnología Wi-Fi es de 54Mbps pero se ve superada por la tecnología WIMAX que en teoría alcanza 134Mbps.

- **Rango de Cobertura**

Se cuentan con enlaces LOS y NLOS. Los enlaces Wi-Fi son en su totalidad LOS por lo tanto su mayor alcance (en teoría 125m) es menor en comparación con los enlaces WIMAX que pueden ser no solo LOS (max. 48 Km) sino también NLOS (max 8 Km) y por lo tanto brinda una mayor cobertura.

Los sistemas 802.16 tienen una mayor ganancia total del sistema, consiguiendo mayor penetración a través de obstáculos a distancias mayores, un mejor nivel de reflexión multitrayecto y dispersión del retardo gracias a la implementación de una FFT de 256 en vez de la FFT de 64 de los sistemas 802.11.

Esta es la característica y diferencia más importante al comparar teóricamente ambas tecnologías.

- **Seguridad**

Otra gran diferencia entre Wi-Fi y WIMAX es la privacidad o la habilidad de proteger a las transmisiones de los espías de red. La seguridad ha sido una de las mayores deficiencias en Wi-Fi, aunque mejores sistemas de encriptación están disponibles ahora. En Wi-Fi, la encriptación es opcional y tres técnicas diferentes han sido definidas: WEP, WPA y WPA2. En cambio, dado que WIMAX fue diseñado para aplicaciones de redes públicas, virtualmente todas las transmisiones WIMAX son encriptadas, como resultado no se han presentado los

problemas de seguridad que existieron en las primeras versiones de Wi-Fi.

4.1.2 Resultados prácticos de red Wi-Fi versus resultados prácticos de red WIMAX

Los parámetros que pudieron ser comparados en la práctica y a los cuales se tuvo acceso dado a los equipos utilizados fueron: bandas de frecuencia, modulación, duplexación, técnicas de transmisión, seguridad, velocidad de transmisión y rango de cobertura.

- **Bandas de Frecuencia**

  En la red WIMAX no se presentaron problemas de interferencia, debido a que la banda de frecuencia de 3.5GHz en la que están operando los equipos no se encuentra saturada. A diferencia que al levantar la red Wi-Fi se presentó mucha interferencia debido a que la banda de 2.4GHz se encuentra saturada. En la zona céntrica de Guayaquil éste problema se incrementa considerablemente debido a la gran cantidad de equipos que operan en esta banda y a la cercanía de éstos.

- **Modulación**

  En los equipos WIMAX se pudo visualizar la característica de adaptabilidad en la modulación y se comprobó que cuando la distancia del enlace

aumenta, automáticamente se asigna una modulación más robusta pero menos eficiente lo cual produjo un nivel de señal mas bajo. En los equipos Wi-Fi utilizados aunque en teoría gozan de esta característica, en la práctica no pudo ser comprobada.

- **Duplexación**

  Al examinar los resultados obtenidos en las pruebas prácticas se comprobó que se cumple lo anteriormente analizado en la teoría para ambas tecnologías.

- **Técnicas de Transmisión**

  Luego de analizar los resultados se comprobó que las señales WIMAX son más resistentes a interferencias que las señales Wi-Fi debido al uso de OFDM con 256 subportadoras a diferencia de Wi-Fi que utiliza OFDM con 64 subportadoras.

- **Seguridad**

  La red WIMAX analizada utiliza la encriptación como método de seguridad pero en la práctica no se pudo comprobar la efectividad de ésta, debido a que por ahora es la única red WIMAX operando en la cuidad.

  A pesar de que Wi-Fi tiene una gran variedad de técnicas para seguridad éstas fueron relativamente

poco efectivas para proteger la red, ya que se comprobó el intento de acceso ilegal a la red.

- **Velocidad de Transmisión y Rango de Cobertura**

  A continuación se tabulan las velocidades de transmisión efectivas (throughput) y el rango de cobertura en las pruebas realizadas en la red Wi-Fi de Pacifictel con los equipos LINKSYS de Cisco, en la cuales se envió un paquete de datos de 100 Kbytes. Para la ubicación de éstos consultar el anexo.

AP 402

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	8.98	12.383	12.74
- 50	14.45	20.20	17.7
- 54	12.88	22.47	14.39
- 58	13.93	19.9	16.665
- 60	16.83	22.22	11.33
- 63	16.71	18.605	22.1
- 65	7.33	10.18	18.18

Tabla 4.1: Mediciones del AP 402

AP 404

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	4.32	20.62	18.18
- 50	7.93	27.585	17.465
- 55	12.11	21.98	25.48
- 75	17.07	21.98	19.61

Tabla 4.2: Mediciones del AP 404

AP 408

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	5.09	21.39	18.1
- 54	7.33	25	22.73
- 60	12.6	23.53	13.56

Tabla 4.3: Mediciones del AP 408

AP 410

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	4.33	27.585	27.585
- 57	8.71	22.22	17.095
- 58	5.25	20.305	15.935
- 60	11.61	13.745	6.04
- 62	9.47	19.325	18.87

Tabla 4.4: Mediciones del AP 410

AP 501

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	6.28	19.225	15.685
- 53	10.19	20.835	19.705
-59	10.5	25.48	25.48

Tabla 4.5: Mediciones del AP 501

AP 503

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	8.96	21.055	19.9
- 50	5.87	26.49	22.345
- 58	7.21	20.41	16.88
- 63	9.9	19.51	18.87

Tabla 4.6: Mediciones del AP 503

AP 505

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	5.75	22.345	20.41
- 55	11.67	18.35	18.35
- 60	12.12	21.74	18.02

Tabla 4.7: Mediciones del AP 505

AP 509

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 58	3.09	20.1	14.495
- 68	9.09	20.2	15.875

Tabla 4.8: Mediciones del AP 509

AP 602

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 50	6.82	22.855	16.735
- 57	7.97	21.39	15.325
- 60	11.79	21.98	16.665
- 62	15.15	22.22	19.35

Tabla 4.9: Mediciones del AP 602

AP 604

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	5.32	18.435	17.855
- 50	3.2	22.47	16.13
- 53	5.54	20.62	15.625
- 55	6.31	26.845	16.88
- 57	10.24	15.685	15.325

Tabla 4.10: Mediciones del AP 604

AP 606

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 60	6.68	24.095	17.935

Tabla 4.11: Mediciones del AP 606

AP 608

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	10.08	19.9	16.735
- 55	9.48	21.39	19.14

Tabla 4.12: Mediciones del AP 608

AP 610

Nivel de Señal [dBm]	Distancia al AP [mts]	Velocidad bajada [Mbps]	Velocidad subida [Mbps]
- 45	8.58	20.725	23.67
- 53	7.59	22.22	17.17
- 60	10.38	22.6	18.69

Tabla 4.13: Mediciones del AP 610

Seguidamente se tabulan las velocidades de transmisión efectivas (throughput) y el rango de cobertura de las pruebas realizadas en la red WIMAX de Setel con los equipos AIRSPAN de Asmax, para el efecto se envió un paquete de datos de 1518 bytes. Para la ubicación de éstos consultar el anexo planos.

Nodo Norte (Hempel)

Lugar de Medición	Nivel de la señal [dBm]	Distancia del Enlace [Km]	Velocidad de bajada [Mbps]	Velocidad de subida [Mbps]
2° 7' 36''S 79° 55' 52''O Napo Montacargas	- 67,9	0,78	8.13	6.39
2° 5' 1'' S 79° 55' 43''O Cosedone	- 73,5	2,04	7.68	6.02
2° 9' 8''S 79° 55' 54''O Intaco	- 79,5	1,9	7.90	6.21
2° 9' 12''S 79° 55' 50''O Santa Priscilla	- 66,1	1,9	7.78	6.11
2° 7' 47''S 79° 55' 55''O Fehierro	- 60	1,2	7.98	6.27
2° 6' 26''S 79° 56' 0''O Plásticos	- 47,1	0,66	8.21	6.45
2° 2' 50''S 79° 56' 51''O Km 17 ½	- 83,3	4,8	1.68	1.32

Tabla 4.14: Mediciones en la Base Nodo Norte

Nodo Centro (Forum)

Lugar de Medición	Nivel de la señal [dBm]	Distancia del Enlace [Km]]	Velocidad de bajada [Mbps]	Velocidad de subida [Mbps]
2° 11’ 41’’S 79° 54’ 10’’O Ayacucho 2912a y G. Lara	- 65,2	1,020	8.12	6.38
2° 17’ 12’’S 79° 53’ 33’’O Puerto Marítimo	- 75,9	6,240	7.63	5.99
2° 14’ 32’’S 79° 55’ 30’’O Trinipuerto	- 72,8	4,2	7.77	6.10
2° 11’ 56’’S 79° 53’ 2’’O Chile 1102 y Av Olmedo	- 63	0,66	8.19	6.42
2° 16’ 21’’S 79° 52’ 43’’O Guasmo Sur Coop Unión Bananeros	- 80,3	5,160	7.71	6.06
2° 13’ 57’’S 79° 54’ 12’’O Cdla Huancavilca Mz C4	- 71	3	7.83	6.14
2° 12’ 5’’S 79° 54’ 57’’O Portete y Milagro	- 71,3	1,98	7.93	6.22
2° 12’ 45’’S 79° 53’ 8’’O Fitsur	- 76,7	1,44	3.59	2.82

Tabla 4.15: Mediciones en la Base Nodo Centro

Analizando las tablas de Wi-Fi anteriormente mostradas se ha deducido que el porcentaje en el cual la velocidad se ve disminuida es del 22% en el enlace de bajada y 33% en el enlace de subida, en cambio para la red WIMAX analizada, se presenta una disminución del 14% en el enlace de bajada y subida, lo cual demuestra que dentro de sus capacidades de velocidad la tecnología WIMAX es mas eficiente y supera a la tecnología Wi-Fi.

Con respecto al rango de cobertura de estas tecnologías se puede concluir que Wi-Fi se aproxima al alcance teórico en un ambiente libre de obstáculos pero al presentarse éstos, el nivel de la señal decae de manera drástica. En las pruebas realizadas se comprobó que estas señales difícilmente atraviesan paredes de concreto lo cual implicó un aumento en la cantidad de equipos utilizados para cubrir determinadas áreas.

Similarmente, el rango de cobertura de la red WIMAX alcanzó aproximadamente los valores esperados, aunque debido a la topografía de la cuidad y a la ubicación de uno de sus nodos no se alcanzó a cubrir en su totalidad las zonas esperadas.

4.2 Otros aspectos

4.2.1 Wi-Fi Roaming

En el 2004 la IEEE inició el desarrollo de un estándar de roaming para Wi-Fi, lo cual significa que los operadores de redes inalámbricas permitan que sus clientes accedan a otras redes, pero hasta la fecha la especificación no ha sido desarrollada. Entre tanto, los proveedores de equipos para WLAN como Cisco, Aruba, Airespace han desarrollado sus protocolos propietarios. Al igual que los productos de Wi-Fi mesh.

En el Ecuador ésta característica difícilmente podrá ser implementada a corto plazo ya que no se cuenta con la infraestructura para poder desarrollarla debido a que el mercado muestra preferencia hacia la telefonía celular.

4.2.2 WIMAX Móvil

El WIMAX móvil está basado en el estándar IEEE 802.16e-2005 e iniciará sus operaciones en las bandas de frecuencia de 2.3GHz, 2.5GHz, 3.3GHz, 3.4 - 3.8GH. Para el uso en bandas adicionales dependerá de la demanda del mercado y de nuevas asignaciones del espectro.

El WIMAX Forum planeó iniciar la certificación de los equipos para WIMAX móvil a mediados de este año, con la expectativa de que el primer producto certificado salga al mercado a finales de este año o en el primer trimestre del 2007. Todos los productos WIMAX móviles soportarán

mecanismos de ahorro de potencia. Mas funcionalidades móviles avanzadas serán gradualmente adicionadas para soportar alta velocidad, roaming y tecnologías de múltiple antenas, tales como MIMO y estar disponibles en equipos a mediados del 2007.

El atractivo de WIMAX móvil va mas a allá de la movilidad, este ofrece una verdadera conexión de banda ancha que soporta el uso de múltiples escenarios, incluyendo el acceso fijo, portable y móvil utilizando la misma infraestructura de red.

En el Ecuador, las redes WIMAX se encuentran actualmente en desarrollo, pero la versatilidad del estándar promete que la característica de movilidad pueda ser probablemente implementada a corto plazo.

Debido a que la VoIP con equipos fijos tuvo una gran demanda en el mercado industrial y residencial, se espera que la característica móvil sea igualmente aceptada ya que entraría a competir con las compañías de telefonía celular.

CAPITULO 5

5 OTRA TECNOLOGÍA

El objetivo de este capítulo es presentar otra alternativa inalámbrica presente en el mercado, ésta no está basada en los estándares IEEE 802.11 ni IEEE 802.16 analizados en los capítulos anteriores, pero presenta algunas características similares con estas tecnologías.

5.1 Tecnologías Propietarias

5.1.1 Motorola

5.1.1.1 Canopy

El sistema Canopy™, es la nueva oferta de banda ancha inalámbrica de Motorola, se basa en la tecnología que permite acceso de alta velocidad a Internet. Este sistema ha sido diseñado para proporcionar un acceso económico de datos a alta velocidad en la “última milla” para clientes residenciales y comerciales.

Con Canopy, Motorola introduce la tecnología de radio al mercado de los proveedores de servicios de Internet. En la figura 5.1 podemos ver el módulo Canopy.

Figura 5.1: Módulo Canopy

Esta solución inalámbrica de Internet funciona en el espectro de Infraestructura de Información Nacional Sin Licencia (U-NII) de 5.25 – 5.35GHz y 5.725 – 5.825GHz, por lo que no hay necesidad de adquirir espectro o licencia para sitios. Y a su vez esta tecnología elimina la necesidad de utilizar la red telefónica o de cable existente.

Los módulos Canopy de 2,4 y 5GHz permiten que los proveedores de servicios desplieguen redes de acceso de banda ancha fiables y de gran calidad. Los operadores de redes podrán:

- Extender la cobertura de la red de banda ancha para satisfacer la demanda de los abonados, ya

que nuevos abonados pueden añadirse a la red rápidamente.

- Establecer enlaces E1/T1

El sistema ofrece los siguientes beneficios:

- **Tolerancia a interferencias**, ya que tiene un índice de portadora a interferencia de < 3dBm en radios de 10Mbps y 8dBm en radios de 20Mbps, lo cual garantiza fiabilidad cuando hay otros transmisores en el área.

- **Escalabilidad,** cuenta con una sincronización GPS que permite a los operadores de redes volver a usar frecuencias y añadir capacidad sin que se vea afectada la calidad del servicio a los clientes existentes.

- **Seguridad,** usa una técnica de sincronización y modulación de señal lo cual mejora las capas de encriptación múltiple y la autenticación para evitar el acceso a usuarios no autorizados. Los módulos cuentan con el Estándar de Encriptación de Datos (Data Encriptation Standard, DES) de 56 bits y están disponibles con el Estándar de Encriptación Avanzada (Advantage Encriptation Standard, AES) de 128 bits.

El alcance y el caudal de transferencia de la comunicación inalámbrica depende, entre otras

condiciones, del terreno, el follaje y la energía de RF del entorno, por este motivo se recomienda realizar un sondeo físico y de radiofrecuencias en el lugar de la instalación.

La tecnología Canopy™ es un sistema fijo con alcances máximos de aproximadamente 3Km. (2 millas). Con esta tecnología se logra una experiencia semejante a la de cualquier otro dispositivo inalámbrico fijo.

5.1.1.1.1 Módulo de Punto de Acceso (AP)

El Módulo de Punto de Acceso (AP), distribuye redes o servicios de Internet en un sector de 60° a 200 subscriptores o menos (y no más de 4096 direcciones MAC, las cuales pueden ser conectadas directamente a PCs, dispositivos IP, puertas de enlaces (gateways), SMs). El AP es configurable a través de una interfase web.

Existen dos tipos de Módulo de Punto de Acceso: el Módulo Lite y el Módulo Advantage en las frecuencias antes citadas. Ofreciendo con la plataforma Advantage mejores ventajas tales como un mayor caudal de transferencia y menor latencia lo cual se resume en las tablas 5.1 y 5.2, dependiendo con cuales de estos se haya realizado el enlace.

MÓDULO	Rango de visibilidad directa (LOS) típico	Velocidad de Transmisión de datos	Actualizable para nuevas funciones	Latencia	Capacidad de Transmisión agregada
AP y SM lite de 2,4 GHz a 100 mW	2 Km (1,2 millas)	10 Mbps	No	20 ms	6,2 Mbps
AP Advantage 2,4 GHz y SM lite a 100 mW	2 Km (1,2 millas)	10 Mbps	Si	5-7 ms	7 Mbps
AP Advantage 2,4 GHz con SM Advantage a 100 mW	2 Km (1,2 millas)	20 Mbps	Si	5-7 ms	14 Mbps a 1Km, 7 Mbps a 2Km

Tabla 5.1: Comparación entre enlaces de módulos

MÓDULO	Rango de visibilidad directa (LOS) típico	Velocidad de Transmisión de datos	Actualizable para nuevas funciones	Latencia	Capacidad de Transmisión agregada
AP Canopy Lite de 5,2 y 5,7 GHz	3,2 Km (2 millas)	10 Mbps	No	20 ms	6,2 Mbps
AP Canopy Advantage de 5,2 y 5,7 GHz	3,2 Km (2 millas)	10 Mbps	Si	5-7 ms	~ 7 Mbps
AP Canopy de 5,2 y 5,7 GHz	1,6 Km (1 milla)	20 Mbps	Si	5-7 ms	~ 14 Mbps

Tabla 5.2: Comparación de los distintos módulos Canopy

Los grupos de Módulos de Punto de Acceso o “cluster” consisten de dos a seis APs que juntos distribuyen la red o el servicio de Internet a una comunidad de unos 1200 o menos subscriptores.

Cada AP transmite y recibe en un sector de 60° por esto un grupo de APs cubre 360°.

Figura 5.2: Grupo de APs o cluster

5.1.1.1.2 Módulo de Subscriptor (SM)

El Módulo de Subscriptor es un equipo local de cliente (customer premises equipment, CPE), estos equipos extienden la red o los servicios de Internet para la comunicación con un AP. El SM es configurable a través de una interfase web.

Un SM montado directamente en una estructura es mostrado en la figura 5.3:

Figura 5.3: CPE montado en estructura

Al igual que en el Módulo de Punto de Acceso el Módulo de Subscriptor cuenta con la versión Lite con un rendimiento de 512Kbps y la versión Advantage con un rendimiento de 14Mbps. La figura 5.4 muestra la comparación entre el caudal de transferencia de estas dos versiones:

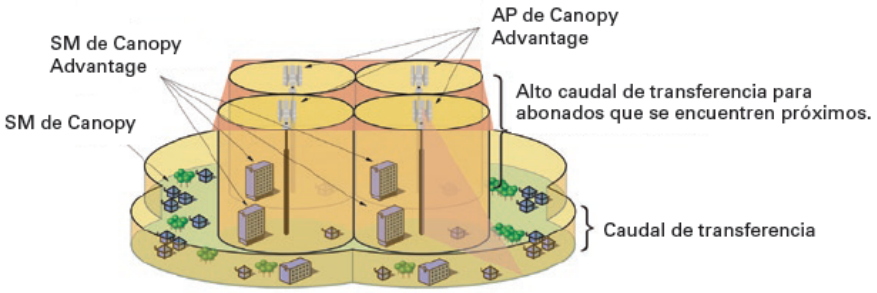


Figura 5.4: Vista del despliegue

5.1.1.1.3 Modulo para enlaces punto a punto (BH)

El Módulo de Backhaul (BH) provee conectividad punto a punto ya sea en:

- Un enlace alámbrico o RF independiente a otro BH.
- Un enlace alámbrico a través de un módulo de administración de grupo a un grupo de AP.

Estos se pueden configurar ya sea como un sincronizador principal (BHM) o un sincronizador esclavo (BHS). El BHM provee sincronismo al BHS.

En la figura 5.5 se muestra un BH montado con un reflector pasivo de disco y en las tablas 5.3 y 5.4 se describen las características teóricas de los enlaces punto a punto en las bandas de 2,4 y 5GHz respectivamente:

Figura 5.5: Backhaul con disco reflector

Enlaces Punto a Punto en la banda de 2,4GHz	10 Mbps BH	10 Mbps BH con reflector	20 Mbps BH	20 Mbps BH con reflector
Velocidad de transmisión de datos	10 Mbps	10 Mbps	20 Mbps	20 Mbps
Caudal de transferencia agregado	7,5 Mbps	7,5 Mbps	14 Mbps	14 Mbps
Rango de Visibilidad directa (LOS) típico a 100 mW Estándar Europeo	2 Km (1,2 millas)	2 Km (1,2 millas)	1 Km (0,6 millas)	1 Km (0,6 millas)
Rango de Visibilidad directa (LOS) típico a 100 mW FCCI de EEUU	8 Km (5 millas) a 2W	56 Km (35 millas) a 25, 1 W	4 Km (2,4 millas) a 2W	56 Km (35millas) a 25,1 W

Tabla 5.3: Características de enlaces punto a punto en 2,4GHz

Enlaces Punto a Punto en la banda de 5GHz	10 Mbps BH	10 Mbps BH con reflector	20 Mbps BH	20 Mbps BH con reflector
Velocidad de transmisión de datos	10 Mbps	10 Mbps	20 Mbps	20 Mbps
Caudal de transferencia agregado	7,5 Mbps	7,5 Mbps	14 Mbps	14 Mbps
Rango de Visibilidad directa (LOS) típico 5,4 + 5,2 a 1W	3,2 Km (2 millas) a 1W	16 Km (10 millas)	1,6 Km (1 millas) a 1W	8 Km (5 millas)
Rango de Visibilidad directa (LOS) típico 5,7	3,2 Km (2 millas) a 1W	56 Km (35 millas) a 63 W	1,6 Km (1 millas) a 1W	56 Km (35millas) a 63 W

Tabla 5.4: Características de enlaces punto a punto en 5GHz

5.2 Análisis del sistema y resumen de características

5.2.1 Enlaces AP – SM

5.2.1.1 Distancias en enlace AP – SM

Los APs y los Módulos de Subscriptores están disponibles en las bandas de frecuencias: 900MHz, 2.4GHz, 5.2GHz, 5.4GHz, y 5.7GHz. Debido a la restricción de las agencias reguladoras un SM de 5.2GHz no puede ser usado con un reflector en los Estados Unidos o Canadá. Un SM de 2.4GHz o 5.7GHz puede ser usado con un reflector de disco pasivo Canopy. Este reflector extiende el máximo alcance del enlace.

Para un enlace AP-SM en 900MHz, el rango en condiciones típicas es de 40millas (64Km). Sin embargo, se puede usar el AP de 900MHz en un rango tan grande como 120millas (más de 190Km) para establecer enlaces a través de distancias muy largas donde la zona de Fresnel esta sin interrupción y el ambiente RF esta sin interferencias.

Para un enlace AP-SM en 2.4GHz, la máxima distancia es:

- 15millas (24Km) con un reflector en el SM
- 5millas (8Km) sin reflector

Para un enlace AP-SM en 5.2GHz, la máxima distancia es:

- 2millas (3.2Km) sin reflector

Para un enlace AP-SM en 5.4GHz, la máxima distancia es:

- 2millas (3.2Km) con o sin reflector

Para un enlace AP-SM en 5.7GHz, la máxima distancia es:

- 10millas (16Km) con reflector en el SM
- 2millas (3.2Km) sin reflector

5.2.1.2 Capacidad de Transmisión en enlace AP – SM

Los Módulos Canopy usan TDD sobre una frecuencia común que divide las tramas para el enlace de subida y bajada usado. En la figura 5.6, las tramas del enlace de subida se muestran en naranja y las de bajada en verde.

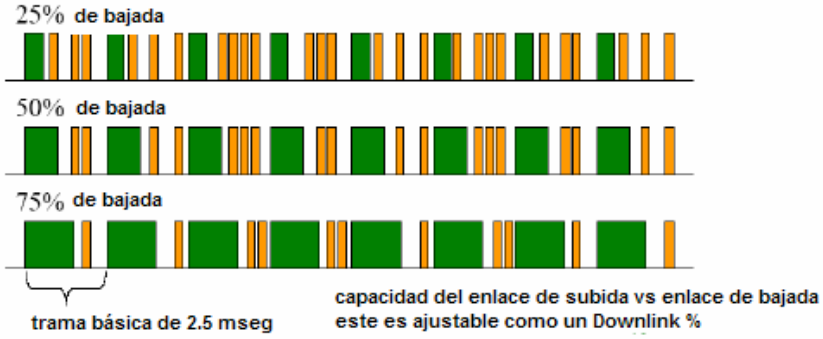


Figura 5.6: Tramas Canopy divididas con TDD

Capacidad Punto a Multipunto

Los APs Canopy se comunican con los SMs usando un protocolo punto a multipunto. Un enlace AP-SM tiene más baja velocidad de transmisión efectiva (throughput) y más alta latencia que un enlace backhaul por dos razones:

- Algunos puntos terminales están involucrados.
- El pedido de ancho de banda y el proceso de reserva consumen ancho de banda.

En el rango de la banda de frecuencia de 900MHz, la latencia en el enlace de subida y bajada es típicamente de:

- 40mseg con software basado en cronograma
- 15mseg con hardware basado en cronograma.

En todos los otros rangos de frecuencia, la latencia en los enlaces de subida y bajada típicamente son:

- 20mseg con software basado en cronograma.
- 6mseg con hardware basado en cronograma.

Como en los APs de 900MHz el rango alcanzado es mayor de 40millas (64Km), mayores lapsos de tiempo entre los ciclos de transmisión y recepción compensan el gran retardo en el aire. En cada trama, éste reduce el número de porciones de datos, el cual reduce directamente la velocidad de transmisión efectiva agregada del enlace. Sin embargo, la velocidad de

transmisión efectiva es tan predecible como en otros enlaces Canopy punto a multipunto.

La velocidad de transmisión efectiva es un factor del parámetro de **Rango Máximo** en el AP y es efectivo para todos los SMs, sin hacer caso de la distancia al AP. La velocidad de transmisión efectiva agregada que es usada por cada AP en los otros rangos de frecuencia Canopy es de 6.2Mbps con software basado en cronograma (7Mbps con hardware basado en cronograma), sin importar el porcentaje del enlace de bajada. Esta velocidad de transmisión efectiva incluye todos los datos del enlace de bajada a todos los SMs y todos lo datos del enlace de subida desde todos los SMs que estén enlazados al AP.

La velocidad de transmisión efectiva del enlace de bajada a un solo SM puede ser tan grande como 4Mbps. La velocidad de transmisión efectiva del enlace de subida a un AP puede ser aproximadamente de 2Mbps, dependiendo del radio del enlace de subida y bajada. Sin embargo, poner el radio al 50% en un enlace Canopy punto a multipunto no rinde una división uniforme del ancho de banda entre el tráfico del enlace de subida y bajada.

Esto se puede observar en los valores de la velocidad de transmisión efectiva listados en las tablas 5.5 y 5.6 que fueron tomadas en pruebas de campo a diferentes distancias:

Porcentaje del enlace de bajada	Porción de datos en bajada	Porción de datos en subida	Velocidad efectiva del enlace de bajada (MHz)	Velocidad efectiva del enlace de subida (MHz)
95	31	2	4.9	0.4
90	30	3	5.1	0.5
85	28	5	5.6	0.8
80	26	7	4.9	1.1
75	25	8	4.9	1.2
70	23	9	4.4	1.3
65	21	11	3.9	1.5
60	20	12	3.9	1.6
55	18	14	3.6	1.7
50	16	16	3.3	1.9
45	15	17	3.0	2.0
40	13	19	2.6	2.1
35	11	21	2.2	2.3
30	10	22	2.0	2.2
25	8	23	1.6	2.4
20	6	25	1.2	2.4
15	5	26	1.0	2.6
10	3	2.8	0.6	2.5
5	2	29	0.4	2.7
0	1	29	0.4	2.7

Tabla 5.5: Velocidad de transmisión efectiva de subida y bajada en enlace de 2millas punto a multipunto con software basado en cronograma.

Porcentaje del enlace de subida	Porción de datos en bajada	Porción de datos en subida
95	29	2
90	28	3
85	26	4
80	25	5
75	23	7
70	21	9
65	20	10
60	18	12
55	17	13
50	15	15
45	14	16
40	12	18
35	10	19
30	9	20
25	7	22
20	6	23
15	4	25
10	3	26
5	2	27
0	2	27

Tabla 5.6: Velocidad de transmisión efectiva de subida y bajada en enlace de 15millas punto a multipunto con software basado en cronograma.

5.2.2 Enlaces BH – BH

5.2.2.1 Distancias en enlace BH – BH

Los módulos de Backhaul están disponibles en:

- Bandas de frecuencia de 2.4, 5.2 y 5.4GHz con una tasa de transferencia de datos de 10 y 20Mbps.
- Bandas de frecuencia de 5.7GHz con una tasa de transferencia de datos de 10, 20 y 45Mbps.

Seleccione los BHs basándose en la capacidad conveniente de datos manejables, el rango del enlace conveniente y si los BHs operarán ya sea en un ambiente de red o serán colocados con un AP o grupo de APs.

Los BHs de 2.4, 5.4 y 5.7GHz pueden ser usados con un reflector sobre una o ambas terminales. Los BHs de Rango Extendido (Extended Range, ER) en 5.2GHz usan muy poca potencia de transmisión y son permitidos con reflector en los Estados Unidos y Canadá así como también en otros países. En los lugares donde estos BHs con Rango Extendido son desplegados, el uso de reflectores en ambas terminales es recomendado.

Sobre una o ambas terminales de un enlace, un disco Reflector Pasivo Canopy, extiende el rango de transmisión y recepción del BH.

Para un enlace BH de 2.4GHz, la máxima distancia es:

- 35millas (56Km) con reflector en ambas terminales.
- 15millas (24Km) con reflector en una terminal a 10Mbps de modulación.
- 5millas (8Km) con reflector en una terminal a 20Mbps de modulación.
- 5millas (8Km) sin reflector a 10Mbps de modulación.
- 3millas (4.8Km) sin reflector a 20Mbps de modulación.

Para un enlace BH de 5.2GHz, la máxima distancia es:

- 10millas (16Km) con reflector en ambas terminales a 10Mbps de modulación, excepto cuando el reflector no está permitido.
- 5millas (8Km) con reflector en ambas terminales a 20Mbps de modulación.
- 2millas (3.2Km) con reflector en una terminal a 10Mbps de modulación.
- 1milla (1.6Km) con reflector en una terminal a 20Mbps de modulación.

Para un enlace BH en 5.4 o 5.7GHz, la máxima distancia es:

- 35millas (56Km) con reflector en ambas terminales.
- 10millas (16Km) con reflector en una terminal a 10Mbps de modulación.

- 5millas (8Km) con reflector en una terminal a 20Mbps de modulación.
- 2millas (3.2Km) sin reflector a 10Mbps de modulación.
- 1 milla (1.6Km) sin reflector a 20 Mbps de modulación.

5.2.2.2 Capacidad de Transmisión en enlace BH – BH

Capacidad Punto a Punto

Los BHs Canopy se comunican entre si usando un protocolo punto a punto. Este protocolo usa una trama de 2.5mseg. Un enlace BHs tiene una alta velocidad de transmisión efectiva y baja latencia (típicamente 5mseg, 2.5mseg en cada dirección) por dos razones:

- Solamente dos puntos terminales están involucrados
- No involucra solicitud de ancho de banda ni proceso de reserva

Para los BHs de 10Mbps, la velocidad de transmisión efectiva agregada sobre el canal es de 7Mbps. Para los BHs de 20MHz es de 14Mbps. Si un BH es puesto a un radio de enlace de bajada del 50%, entonces el ancho de banda en cada dirección es la mitad del total del ancho de banda del enlace de BH.

5.3 Consideraciones Prácticas

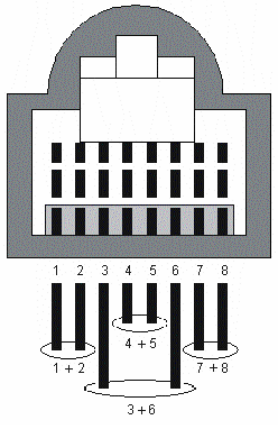
A continuación se presentan los enlaces punto a multipunto y punto a punto realizados en la cuidad de Guayaquil:

- **Enlace punto a multipunto**

  La base (AP) del enlace se encuentra ubicada a 2° 11’ 20’’ S y 79° 53’ 16’’ O, (Edificio Induato ubicado en las calles Av. Quito y Av. Nueve de Octubre), sobre una torre de 12mts, siendo la altura del edificio de 88mts.

  El equipo se encuentra instalado sin reflector en la parte mas alta de la torre apuntando hacia el este de la cuidad de Guayaquil, cubriendo aproximadamente desde los 2° 11’ 45’’ S y 79° 52’ 55’’ O (calle Sucre) hasta los 2° 11’ 16’’ S y 79° 52’ 43’’ O (calle Tomás Martínez).

  El tipo de cable que se debe utilizar es cable UTP blindado categoría 5, el cual debe tener correctamente colocados los conectores RJ45 siguiendo el código de colores como se ilustra en la figura 5.7.



Color del Cable	Pin
Azul	1
Blanco / Azul	2
Naranja	3
Blanco / Naranja	6
Café	4
Blanco / Café	5
Verde	7
Blanco / Verde	8

Figura 5.7: Código de colores

Los parámetros importantes para el correcto enlace entre los radios Canopy son: el Indicador de la Intensidad de la Señal de Recepción (Received Signal Strength Indicador, RSSI) y la Inestabilidad (Jitter).

El RSSI es una identificación del nivel de potencia que recibe la antena. Normalmente mientras mas alto sea el nivel del indicador RSSI más potente será la señal. En términos generales, se considera aceptable un nivel igual o superior a 700.

El jitter es una medida de la variabilidad en la posición temporal (la variación entre el momento de llegada real y el previsto). Se considera aceptable un nivel uniforme igual o superior a 9. La escala del jitter bordea entre 5 y 15, donde cinco es el valor ideal como se muestra en la figura 5.8.

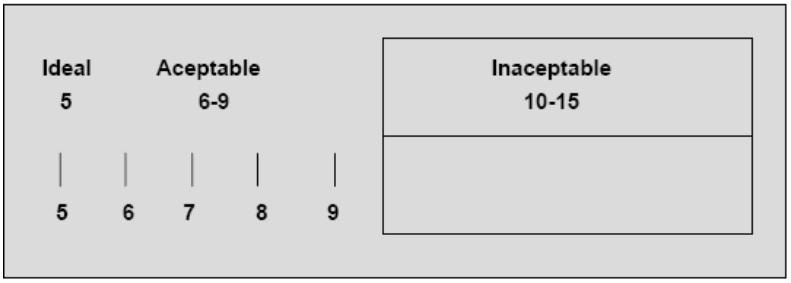


Figura 5.8: Rangos de la variación de la pérdida de paquetes

El primer módulo de subscriptor se encuentra ubicado a 2° 11' 16'' S y 79° 52' 43'' O (en las calles Manuel de Luzárraga 201 y Panamá), el equipo se instaló con reflector a una altura aproximada de 18mts, y una distancia de 1.1Km de la base.

En este enlace el valor del RSSI conseguido fue de 1306, y un jitter de 2, como se ilustra en la figura 5.9.

CANOPY
Motorola Wireless Internet Platform

Device Information	
Device type	5.7GHz - Multipoint - Subscriber Modem - 0a-00-3e-f0-eb-a0
Software Version	CANOPY 7.3.6 Oct 24 2005 12:06:56 SM-DES
Software Boot Version	CANOPYBOOT 3.0
FPGA Version	051104 (DES)
Uptime	4d, 23:42:01
System Time	12:07:41 10/23/2006
Ethernet Interface	100Base-TX Full Duplex
Subscriber Modem Stats	
Session Status	REGISTERED
Registered AP	0a-00-3e-f0-cb-a8
RSSI	1306 (-65 dBm)
Jitter	2
Air Delay	79 (approximately 0.73 miles (3871 feet))
Site Information	
Site Name	Maint
Site Contact	No Site Contact

Figura 5.9: RSSI y Jitter primer modulo de subscriptor

Con este enlace se está entregando Internet de banda ancha con el único fin de navegación web, repartido entre varios usuarios.

El segundo módulo suscriptor se encuentra ubicado a 2° 11’ 45’’ S y 79° 52’ 55’’ O (en las calles Pedro Carbo entre Sucre y 10 de Agosto), el equipo se instaló con reflector a una altura aproximada de 14mts, y una distancia de 1.09Km de la base.

En este enlace el valor del RSSI conseguido fue de 1481, y un Jitter de 2 como se ilustra en la figura 5.10.

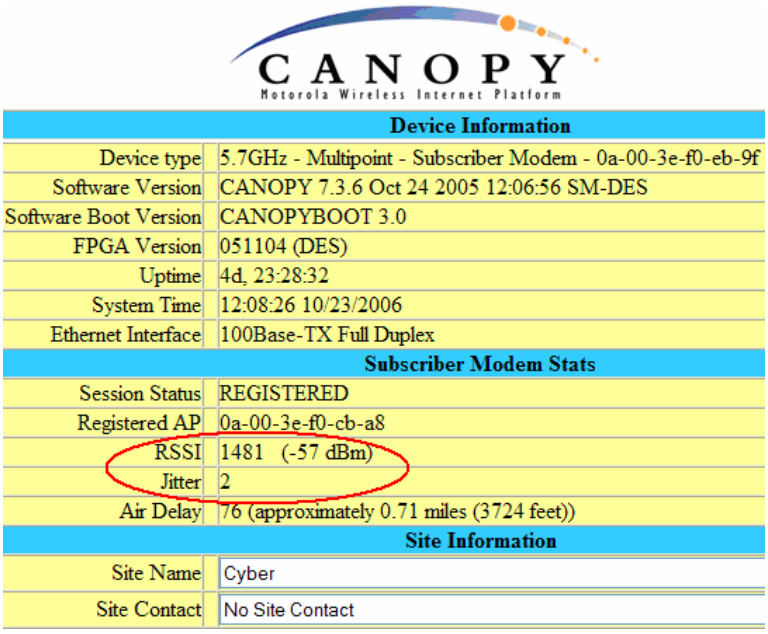


Figura 5.10: RSSI y Jitter segundo módulo de subscriptor

En el Anexo Plano 19 se ilustra el enlace antes descrito.

Con este enlace se está entregando Internet de banda ancha para ser utilizado tanto en navegación web, llamadas telefónicas (VoIP), video conferencias y juegos en línea.

La velocidad promedio efectiva conseguida en el enlace de subida fue de 772,7Kbps y en el enlace de bajada fue 1867,4Kbps.

- **Enlace punto a punto**

  El Módulo Master del enlace se encuentra ubicado a 2° 11’ 30’’ S y 79° 52’ 48’’ O (en las calles Nueve de Octubre entre Panamá y el Malecón Simón Bolívar, Edificio La Previsora), el equipo se instaló sin reflector a una altura de 134mts sobre una torre de 4mts como se muestra en la figura 5.11.

Figura 5.11: Módulo Master

El Módulo Esclavo se encuentra ubicado a 2° 11’ 20’’ S y 79° 53’ 20’’ O (Edificio Induato), sobre una torre de 12mts, siendo

la altura del edificio de 88mts. El equipo esta instalado con reflector a 1.50mts sobre la base de la torre, como se muestra en la figura 5.12, teniendo una distancia de 1.1Km del Módulo Master.

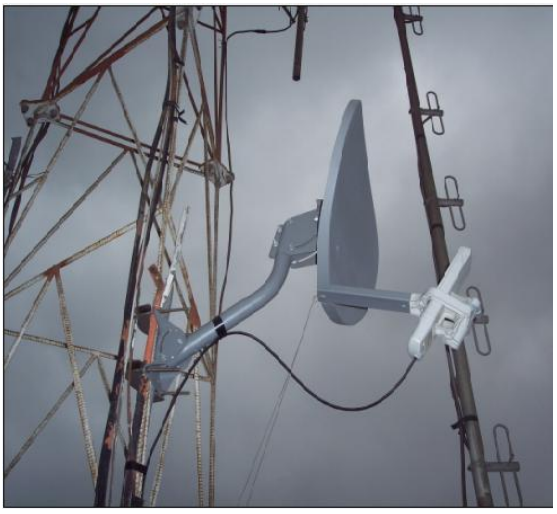
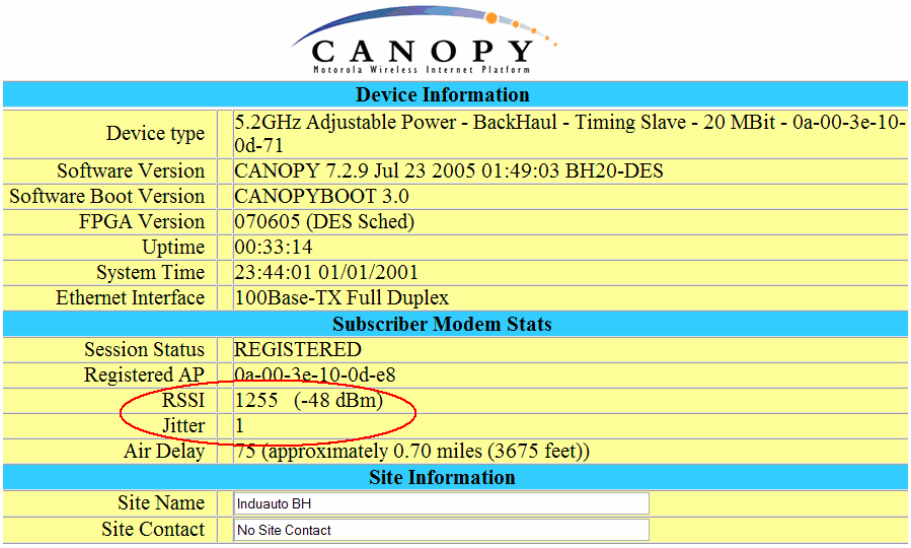


Figura 5.12: Módulo Esclavo

En el Anexo Plano 20 se ilustra el enlace antes mencionado.

En este enlace el valor del RSSI conseguido fue de 1255, y un Jitter de 1, como se ilustra en la figura 5.13.



CANOPY
Motorola Wireless Internet Platform

Device Information	
Device type	5.2GHz Adjustable Power - BackHaul - Timing Slave - 20 MBit - 0a-00-3e-10-0d-71
Software Version	CANOPY 7.2.9 Jul 23 2005 01:49:03 BH20-DES
Software Boot Version	CANOPYBOOT 3.0
FPGA Version	070605 (DES Sched)
Uptime	00:33:14
System Time	23:44:01 01/01/2001
Ethernet Interface	100Base-TX Full Duplex
Subscriber Modem Stats	
Session Status	REGISTERED
Registered AP	0a-00-3e-10-0d-e8
RSSI	1255 (-48 dBm)
Jitter	1
Air Delay	75 (approximately 0.70 miles (3675 feet))
Site Information	
Site Name	Induauto BH
Site Contact	No Site Contact

Figura 5.13: RSSI y Jitter Módulo Esclavo

Con este enlace se esta transportando la señal que llega al edificio La Previsora proveniente de la telefónica Movistar al Edificio Induato para sea desde allí repartida a los usuarios.

CONCLUSIONES Y RECOMENDACIONES

Al término de esta Tesis se ha podido concluir:

- Al analizar el rango del espectro de frecuencia sin licencia de 2.4GHz en la cuidad de Guayaquil, se determinó que éste está próximo a saturarse, por lo que el futuro de la tecnología Wi-Fi en esta banda se verá amenazado, a diferencia de la tecnología WIMAX que utiliza la banda de 3.5GHz que se encuentra menos inundada y además opera en bandas de frecuencia con licencia asegurando el uso exclusivo de un rango del espectro, beneficiándose de lo que todo esto conlleva.

- Se comprueba que gracias a la modulación adaptativa, los enlaces WIMAX con una modulación menos eficiente no presentaron una disminución significativa en el nivel de la señal, por lo cual se pudieron instalar puntos más lejanos superando el rango de cobertura esperado.

- La señal Wi-Fi proveniente de un AP, comienza a degradarse cuando trabajan más de 20 personas de forma concurrente; por el contrario, WIMAX permite que una misma estación tenga cientos de personas trabajando en la red.

- En Wi-Fi el envío de datos a velocidades menores requiere menos tiempo, pero pueden tolerar más interferencia o menor calidad de la señal, mientras que el envío de datos equivalentes a velocidades mayores toleró menos degradación de la señal y por lo tanto operó con distancias menores. Con las pruebas realizadas se comprobó que para tener una cobertura de aproximadamente 210mts se necesita tener una velocidad de 1Mbps y conforme se aumenta la velocidad de transmisión la cobertura disminuye así para 11Mbps y 54Mbps se alcanza aproximadamente 60 y 35mts respectivamente. La velocidad en las pruebas realizadas en los enlaces WIMAX se mantuvo estable aun con la presencia de variación en la distancia de la antena de subscriptor a la base.

- Cabe resaltar que los costos de inversión en una red Wi-Fi son relativamente menores en comparación con la adquisición de equipos WIMAX, se espera que con la estandarización del 802.16 los costos de los equipos se vean reducidos considerablemente.

- Analizando el futuro de las redes inalámbricas se ha podido concluir que WIMAX no competirá con Wi-Fi sino que ambas son tecnologías complementarias, la primera alimentará los denominados hotspots o puntos de accesos al público en general de Wi-Fi, mientras ésta última permitirá el acceso del usuario a las aplicaciones de internet.

Al término de esta Tesis se puede recomendar:

- Basándose en la variedad de los ambientes y los requerimientos del usuario, es imprescindible realizar una inspección del lugar como primer paso en el planeamiento del diseño y de la implementación de las redes inalámbricas.

- Como se concluyó anteriormente la distancia entre los APs pueden causar variaciones de la velocidad de transmisión para los usuarios dependiendo de la distancia al AP. La recomendación es limitar la velocidad de datos al AP a velocidades de datos más altas de 11 o 54Mbps.

- Para ambientes donde se presenta cantidades altas de interferencia se recomienda el uso de equipos con antenas de mayor ganancia.

- Luego de analizar la infraestructura de la red WIMAX de Setel implementada en la ciudad de Guayaquil se recomienda instalar un nodo que cubra el sector noreste que presenta importantes cliente potenciales.

- Además se debe considerar el crecimiento de la ciudad.

ANEXO

PLANOS

APÉNDICE A

ESPECIFICACIONES TÉCNICAS DEL PUNTO DE ACCESO LINKSYS DE CISCO

Modelo:	WAP54G
Estándar:	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Puertos/Botones:	1 puerto 10/100 Auto-Cruce sobre (MDI/MDI-X), 1 puerto de encendido Botones de reseteo y SES
Tipo de cableado:	RJ-45
Leds:	De encendido, actividad y enlace
Potencia de Tx:	802.11g: 13.5 +/- 2dBm 802.11b: 13.5 +/- 2dBm
Seguridad:	WPA, Encriptación WEP, Filtrado MAC
Bits de clave WEP:	64/128-bit
Dimensiones:	7.32'' x 1.89'' x 6.65''
Peso del equipo:	16.23 oz. (0.46 Kg)
Alimentación:	Externa, 12V DC
Certificaciones:	FCC
Temp. de operación:	De 0°C a 40°C

FÓRMULAS

- Potencia recibida a una distancia referencial de 1 metro

$$Po = PtGtGr\left[\frac{\lambda}{4\pi}\right]^2$$

Donde:
Pt = Potencia del Transmisor
Gt = Ganancia de la antena del Transmisor
Gr = Ganancia de la antena del Receptor
λ = Longitud de onda

- Pérdida de trayectoria de 1 metro de distancia

$$Lo = 10\log(Pt) - 10\log(Po)$$

- Pérdida de trayectoria total

$$Lp = Lo + 20\log(d) + \sum mw$$

Donde:
d = distancia en metros
m = número de obstáculos
w = pérdida debido al material en dB

APÉNDICE B

CÁLCULO DE PÉRDIDA DE TRAYECTORIA (PATH LOSS) PARA RED WIFI

CUARTO PISO

							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
402	A	22,38	1	0,0022	40,05	11,48	6	1	10	0	1	0	67,2	-53,7	-54
	B	22,38	1	0,0022	40,05	7,14	6	2	10	0	1	0	69,1	-55,6	-60
	C	22,38	1	0,0022	40,05	5,04	6	1	10	1	1	0	70,1	-56,6	-60
	D	22,38	1	0,0022	40,05	5,88	6	0	10	0	1	0	55,4	-41,9	-45
	E	22,38	1	0,0022	40,05	9,48	6	0	10	1	1	0	69,6	-56,1	-50
	F	22,38	1	0,0022	40,05	8,46	6	0	10	0	1	0	58,6	-45,1	-45
	G	22,38	1	0,0022	40,05	14,39	6	2	10	1	1	0	85,2	-71,7	-63
	H	22,38	1	0,0022	40,05	10,47	6	0	20	1	1	0	80,4	-66,9	-58
	I	22,38	1	0,0022	40,05	13,78	6	1	10	0	1	0	68,8	-55,3	-60
	J	22,38	1	0,0022	40,05	4,82	6	1	10	0	1	0	59,7	-46,2	-50
	K	22,38	1	0,0022	40,05	6,64	6	2	10	0	1	0	68,5	-55,0	-65
	L	22,38	1	0,0022	40,05	7,34	6	0	10	0	1	0	57,4	-43,9	-45
	M	22,38	1	0,0022	40,05	3,84	6	0	10	0	1	0	51,7	-38,2	-45
	N	22,38	1	0,0022	40,05	8,3	6	1	10	0	1	0	64,4	-50,9	-50
	O	22,38	1	0,0022	40,05	9,52	6	1	10	0	1	0	65,6	-52,1	-50
	P	22,38	1	0,0022	40,05	11,34	6	1	10	0	1	0	67,1	-53,6	-54
	Q	22,38	1	0,0022	40,05	8,48	6	2	10	0	1	0	70,6	-57,1	-58

							Pared de Oficina		Pilar		Puerta de Madera				
AP	**PRUEBA**	**Pt [mW]**	**Gt dBi] y Gr[dBi]**	**Po [mW]**	**Lo [dB]**	**d [mts]**	**w [dB]**	**m**	**w [dB]**	**m**	**w [dB]**	**m**	**Lp [dB]**	**Nivel Esperado**	**Nivel Obtenido de Pruebas**
404	A	22,38	1	0,0022	40,05	16,06	6	3	10	0	1	0	82,2	-68,7	-75
	B	22,38	1	0,0022	40,05	8,07	6	0	10	0	1	0	58,2	-44,7	-50
	C	22,38	1	0,0022	40,05	3,67	6	0	10	0	1	0	51,3	-37,8	-45
	D	22,38	1	0,0022	40,05	9,41	6	1	10	0	1	0	65,5	-52,0	-55
	E	22,38	1	0,0022	40,05	6	6	0	10	0	1	0	55,6	-42,1	-45
	F	22,38	1	0,0022	40,05	4,57	6	0	10	0	1	0	53,2	-39,7	-45
	G	22,38	1	0,0022	40,05	7,21	6	1	10	1	1	0	73,2	-59,7	-50
	H	22,38	1	0,0022	40,05	9,33	6	1	10	0	1	0	65,4	-51,9	-55
	I	22,38	1	0,0022	40,05	3,14	6	0	10	0	1	0	50,0	-36,5	-45

							Pared de Oficina		Pilar		Puerta de Madera				
AP	**PRUEBA**	**Pt [mW]**	**Gt[dBi] y Gr[dBi]**	**Po [mW]**	**Lo [dB]**	**d [mts]**	**w [dB]**	**m**	**w [dB]**	**m**	**w [dB]**	**m**	**Lp [dB]**	**Nivel Esperado**	**Nivel Obtenido de Pruebas**
408	A	22,38	1	0,0022	40,05	11,55	6	3	10	0	1	0	79,3	-65,8	-60
	B	22,38	1	0,0022	40,05	7,29	6	1	10	1	1	0	73,3	-59,8	-54
	C	22,38	1	0,0022	40,05	5,02	6	0	10	0	1	0	54,1	-40,6	-45
	D	22,38	1	0,0022	40,05	4,95	6	0	10	0	1	0	53,9	-40,4	-45
	E	22,38	1	0,0022	40,05	5,32	6	1	10	0	1	0	60,6	-47,1	-54
	F	22,38	1	0,0022	40,05	13,49	6	2	10	0	1	0	74,6	-61,1	-60

							Pared de Oficina		Pilar		Puerta de Madera				
AP	**PRUEBA**	**Pt [mW]**	**Gt[dBi] y Gr[dBi]**	**Po [mW]**	**Lo [dB]**	**d [mts]**	**w [dB]**	**m**	**w [dB]**	**m**	**w [dB]**	**m**	**Lp [dB]**	**Nivel Esperado**	**Nivel Obtenido de Pruebas**
410	A	22,38	1	0,0022	40,05	9,79	6	2	10	0	1	0	71,9	-58,4	-60
	B	22,38	1	0,0022	40,05	7,49	6	0	10	1	1	0	67,5	-54,0	-60
	C	22,38	1	0,0022	40,05	3,76	6	0	10	0	1	0	51,5	-38,0	-45
	D	22,38	1	0,0022	40,05	10,16	6	1	10	1	1	0	76,2	-62,7	-60
	E	22,38	1	0,0022	40,05	6,12	6	1	10	0	1	0	61,8	-48,3	-58
	F	22,38	1	0,0022	40,05	5,57	6	0	10	0	1	1	56,0	-42,5	-45
	G	22,38	1	0,0022	40,05	5,95	6	0	10	0	1	0	55,5	-42,0	-57
	H	22,38	1	0,0022	40,05	12,12	6	2	10	0	1	0	73,7	-60,2	-62
	I	22,38	1	0,0022	40,05	10,6	6	0	20	1	1	0	80,6	-67,1	-62

QUINTO PISO

							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
501	A	22,38	1	0,0022	40,05	5,71	6	1	10	0	1	0	61,2	-47,7	-53
	B	22,38	1	0,0022	40,05	6,08	6	0	10	0	1	0	55,7	-42,2	-45
	C	22,38	1	0,0022	40,05	12,02	6	1	10	0	1	0	67,6	-54,1	-59

							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
503	A	22,38	1	0,0022	40,05	5,78	6	1	10	0	1	0	61,3	-47,8	-50
	B	22,38	1	0,0022	40,05	8,94	6	0	10	1	1	0	69,1	-55,6	-63
	C	22,38	1	0,0022	40,05	7,97	6	0	10	0	1	0	58,1	-44,6	-45
	D	22,38	1	0,0022	40,05	5,72	6	0	10	0	1	0	55,2	-41,7	-58

							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
509	A	22,38	1	0,0022	40,05	4,1	6	0	20	2	1	0	92,3	-78,8	-58
	B	22,38	1	0,0022	40,05	14,69	6	1	10	2	10	1	99,4	-85,9	-68

							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
505	A	22,38	1	0,0022	40,05	12,52	6	2	20	1	1	0	94,0	-80,5	-60
	B	22,38	1	0,0022	40,05	10,55	6	1	10	0	1	0	66,5	-53,0	-55
	C	22,38	1	0,0022	40,05	5,8	6	0	10	0	1	0	55,3	-41,8	-45

SEXTO PISO

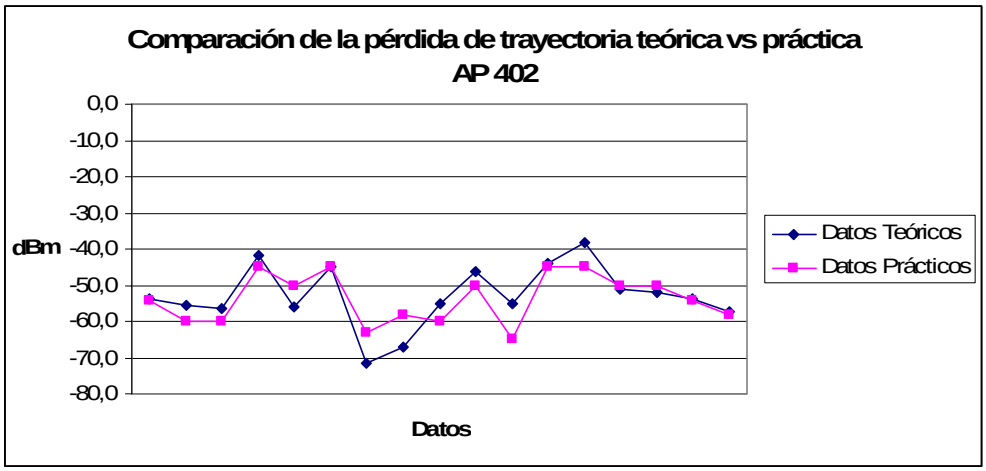
							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
602	A	22,38	1	0,0022	40,05	14,47	6	1	10	0	1	1	70,3	-56,8	-62
	B	22,38	1	0,0022	40,05	8,03	6	1	10	0	1	0	64,1	-50,6	-57
	C	22,38	1	0,0022	40,05	7,1	6	1	10	0	1	0	63,1	-49,6	-50
	D	22,38	1	0,0022	40,05	12,34	6	1	10	0	1	0	67,9	-54,4	-60

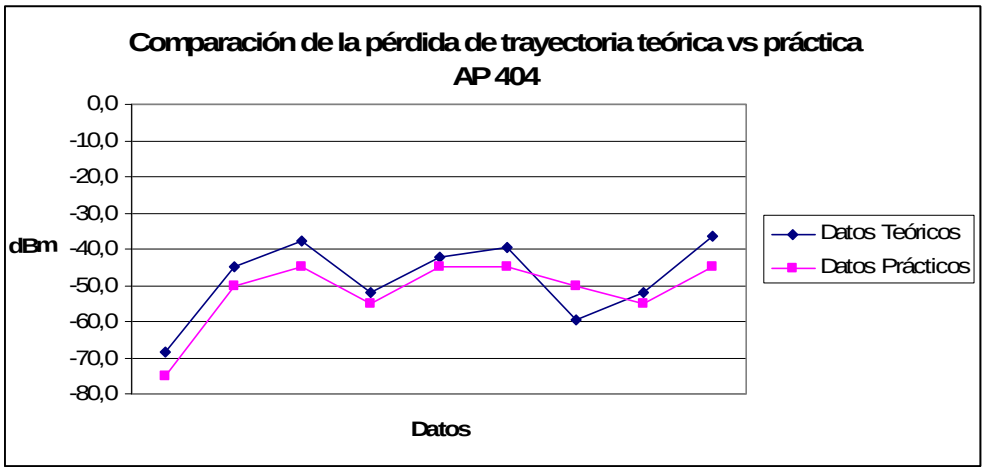
							Pared de Oficina		Pilar		Puerta de Madera				
AP	PRUEBA	Pt [mW]	Gt dBi] y Gr[dBi]	Po [mW]	Lo [dB]	d [mts]	w [dB]	m	w [dB]	m	w [dB]	m	Lp [dB]	Nivel Esperado	Nivel Obtenido de Pruebas
604	A	22,38	1	0,0022	40,05	2,55	6	0	10	1	1	0	58,2	-44,7	-50
	B	22,38	1	0,0022	40,05	3,46	6	0	10	0	1	0	50,8	-37,3	-45
	C	22,38	1	0,0022	40,05	5,18	6	0	10	0	1	0	54,3	-40,8	-45
	D	22,38	1	0,0022	40,05	7,1	6	1	10	0	1	0	63,1	-49,6	-45
	E	22,38	1	0,0022	40,05	6,97	6	0	10	1	1	0	66,9	-53,4	-55
	F	22,38	1	0,0022	40,05	10,61	6	1	10	1	1	0	76,6	-63,1	-57
	G	22,38	1	0,0022	40,05	5,49	6	1	10	0	1	0	60,8	-47,3	-53

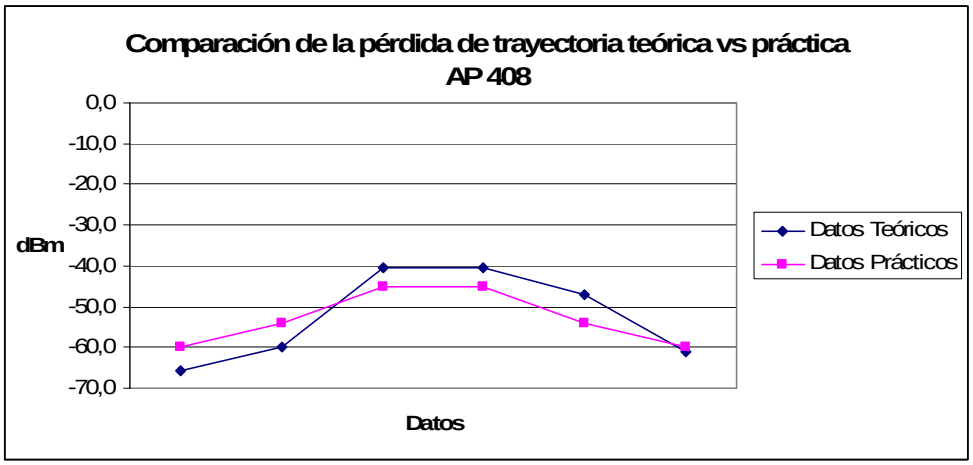
							Pared de Oficina		Pilar		Puerta de Madera				
AP	**PRUEBA**	**Pt [mW]**	**Gt[dBi] y Gr[dBi]**	**Po [mW]**	**Lo [dB]**	**d [mts]**	**w [dB]**	**m**	**w [dB]**	**m**	**w [dB]**	**m**	**Lp [dB]**	**Nivel Esperado**	**Nivel Obtenido de Pruebas**
610	A	22,38	1	0,0022	40,046	8,49	6	2	10	0	1	0	70,62	-57,1	-53
	B	22,38	1	0,0022	40,046	8,2	6	3	10	0	1	0	76,32	-62,8	-45
	C	22,38	1	0,0022	40,046	10,14	6	3	10	0	1	1	79,17	-65,7	-60

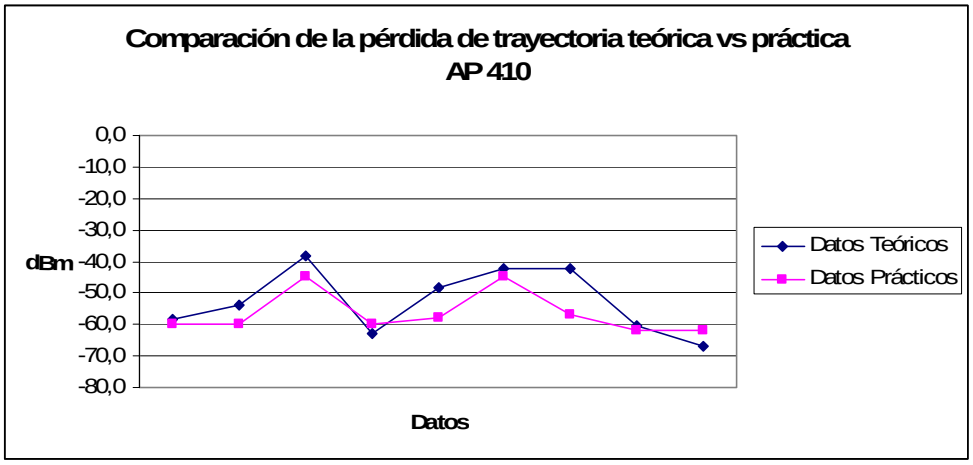
							Pared de Oficina		Pilar		Puerta de Madera				
AP	**PRUEBA**	**Pt [mW]**	**Gt[dBi] y Gr[dBi]**	**Po [mW]**	**Lo [dB]**	**d [mts]**	**w [dB]**	**m**	**w [dB]**	**m**	**w [dB]**	**m**	**Lp [dB]**	**Nivel Esperado**	**Nivel Obtenido de Pruebas**
608	A	22,38	1	0,0022	40,046	8,13	6	1	10	0	1	0	64,25	-50,7	-55
	B	22,38	1	0,0022	40,046	10,96	6	0	10	0	1	0	60,84	-47,3	-45

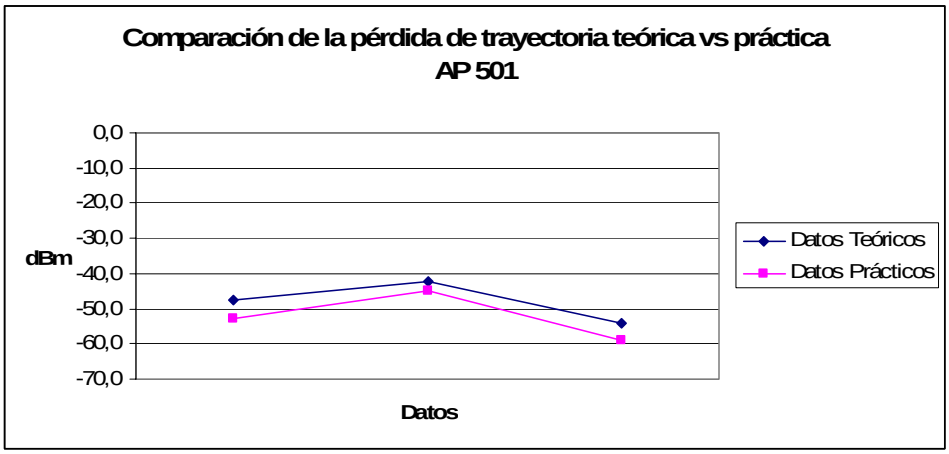
							Pared de Oficina		Pilar		Puerta de Madera				
AP	**PRUEBA**	**Pt [mW]**	**Gt dBi] y Gr[dBi]**	**Po [mW]**	**Lo [dB]**	**d [mts]**	**w [dB]**	**m**	**w [dB]**	**m**	**w [dB]**	**m**	**Lp [dB]**	**Nivel Esperado**	**Nivel Obtenido de Pruebas**
606	A	22,38	1	0,0022	40,046	7,06	6	1	10	0	1	0	63,02	-49,5	-60

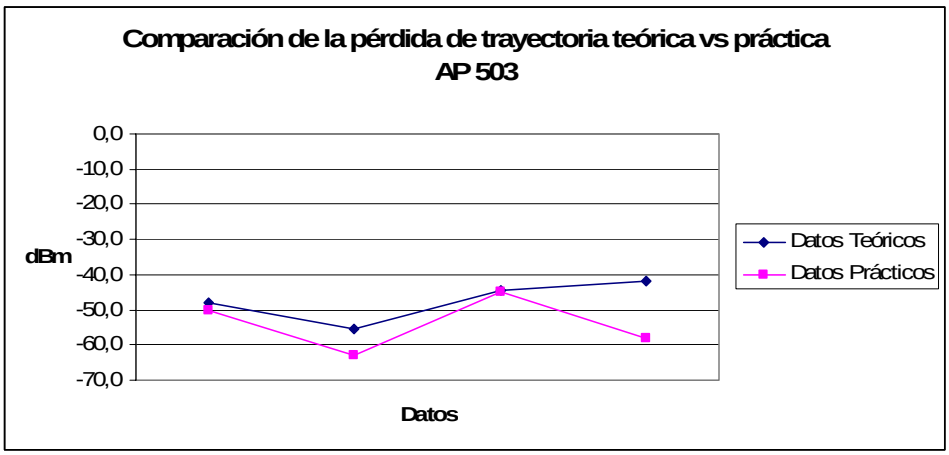

Comparación de la pérdida de trayectoria teórica vs práctica
AP 402
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
-80,0
dBm
Datos
Datos Teóricos
Datos Prácticos

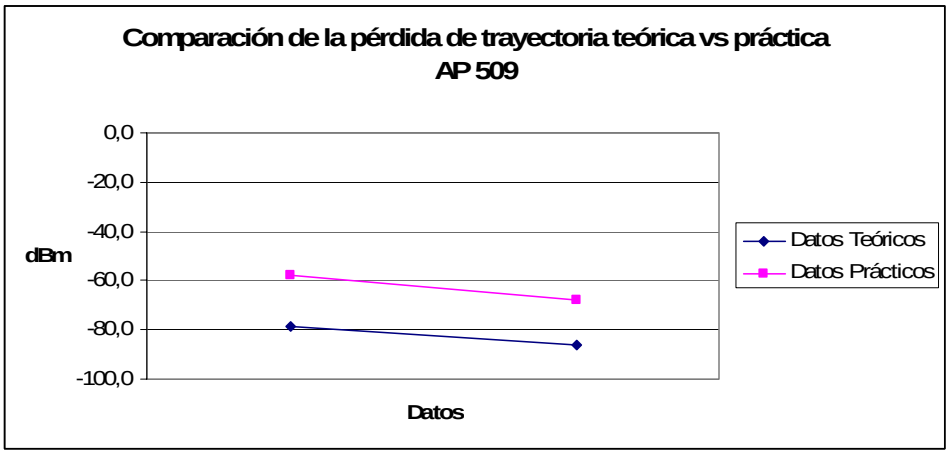

Comparación de la pérdida de trayectoria teórica vs práctica
AP 404
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
-80,0
dBm
Datos
Datos Teóricos
Datos Prácticos

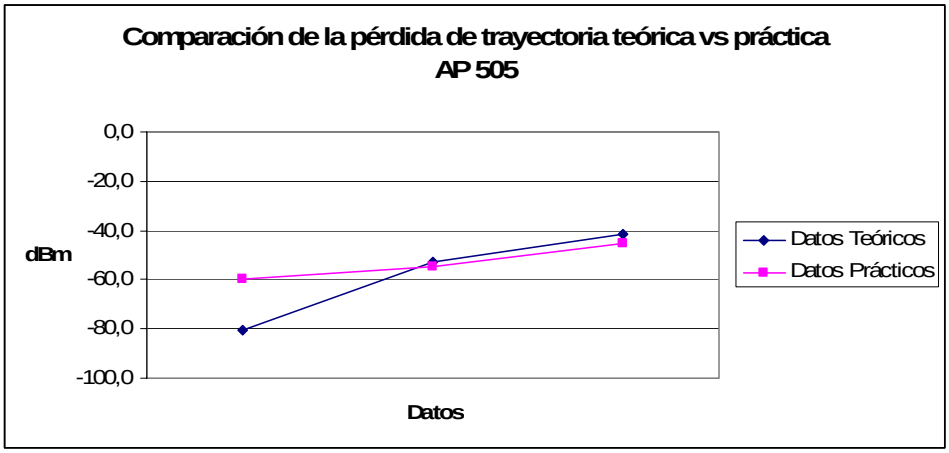

Comparación de la pérdida de trayectoria teórica vs práctica
AP 408
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos

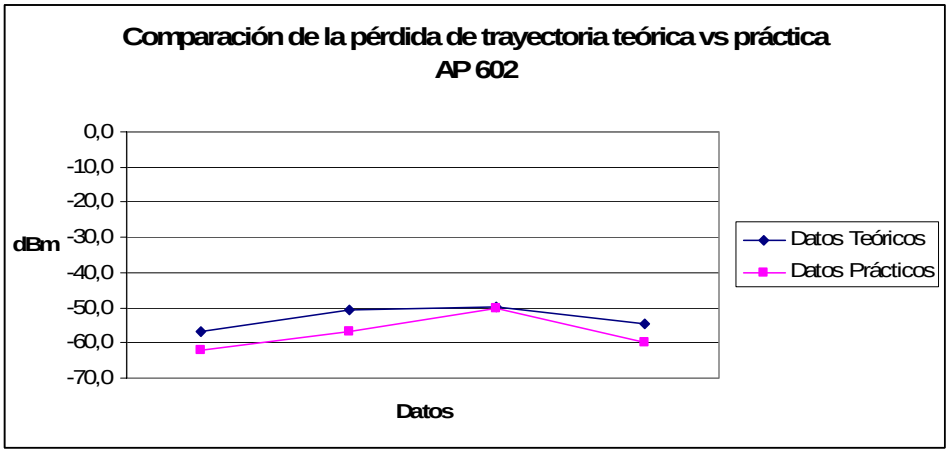

Comparación de la pérdida de trayectoria teórica vs práctica
AP 410
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
-80,0
dBm
Datos
Datos Teóricos
Datos Prácticos

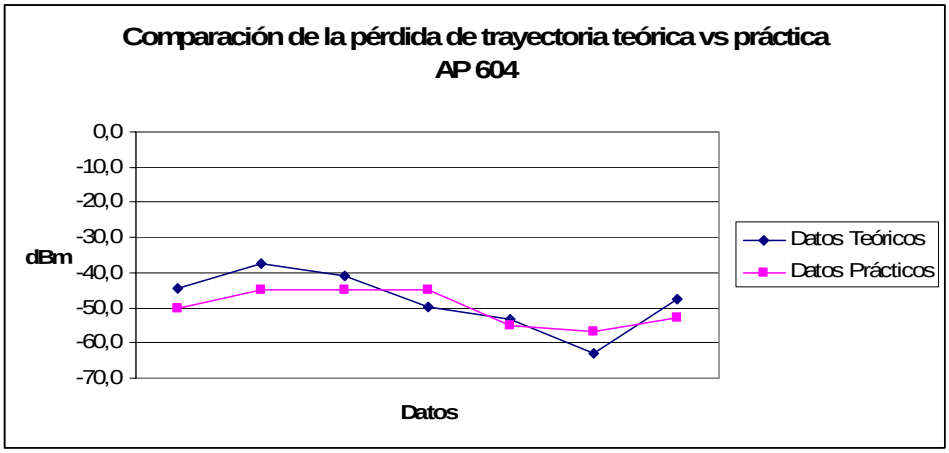

Comparación de la pérdida de trayectoria teórica vs práctica
AP 501
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos

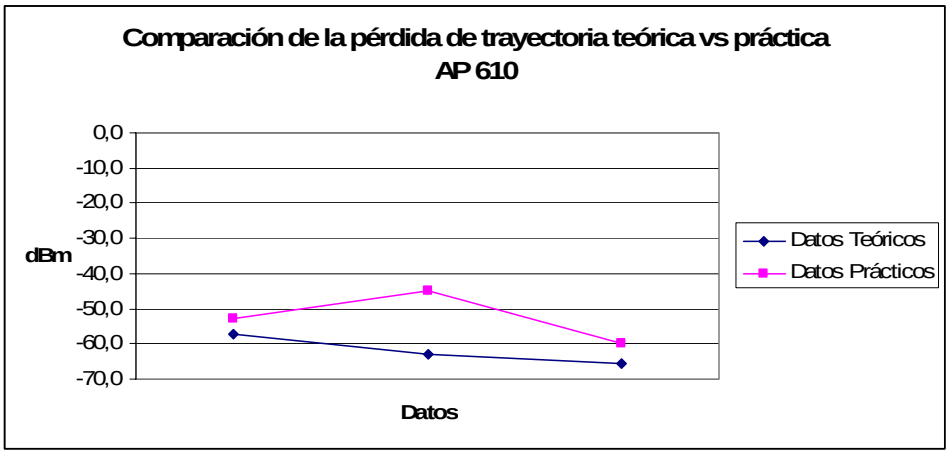

Comparación de la pérdida de trayectoria teórica vs práctica
AP 503
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos

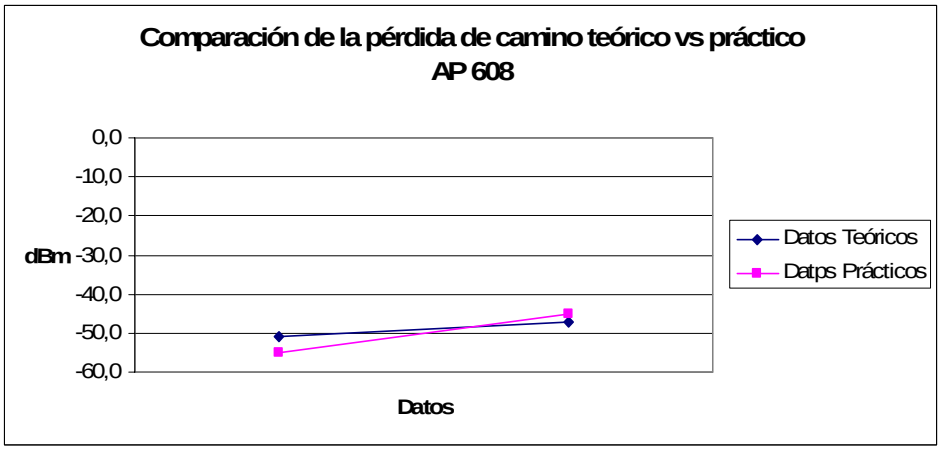

Comparación de la pérdida de trayectoria teórica vs práctica
AP 509
0,0
-20,0
-40,0
-60,0
-80,0
-100,0
dBm
Datos
Datos Teóricos
Datos Prácticos

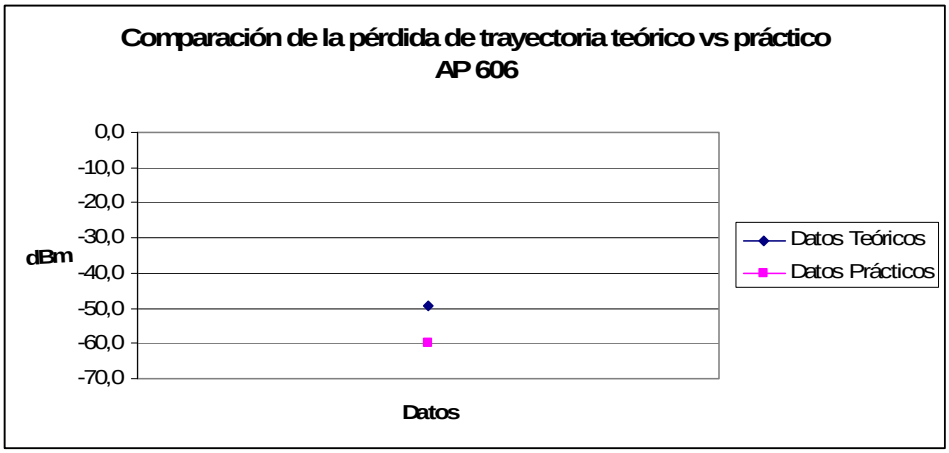

Comparación de la pérdida de trayectoria teórica vs práctica
AP 505
0,0
-20,0
-40,0
-60,0
-80,0
-100,0
dBm
Datos
Datos Teóricos
Datos Prácticos


Comparación de la pérdida de trayectoria teórica vs práctica
AP 602
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos


Comparación de la pérdida de trayectoria teórica vs práctica
AP 604
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos


Comparación de la pérdida de trayectoria teórica vs práctica
AP 610
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos


Comparación de la pérdida de camino teórico vs práctico
AP 608
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
dBm
Datos
Datos Teóricos
Datps Prácticos


Comparación de la pérdida de trayectoria teórico vs práctico
AP 606
0,0
-10,0
-20,0
-30,0
-40,0
-50,0
-60,0
-70,0
dBm
Datos
Datos Teóricos
Datos Prácticos

APÉNDICE D

ARQUITECTURA, CAPA FÍSICA Y CAPA MAC DEL ESTÁNDAR 802.16

ARQUITECTURAS DEL DESPLIEGUE

Una típica red de WIMAX está constituida por una estación base central (Base Station, BS) que se comunica con una o más estaciones de subscriptor (Suscriber Stations, SS). Esta comunicación puede desarrollarse en diferentes arquitecturas de redes descritas a continuación:

- Punto a Punto (Point-to-Point, PTP): Es una conexión entre dos nodos, en este caso una BS y una SS. Los enlaces PTP tienen la ventaja de ser mucho más extensos que los enlaces PMP.

- Punto a Multipunto (Point-to-multipoint, PMP): Es una conexión entre una BS y múltiples nodos de SS. Generalmente necesita el uso de antenas sectorizadas u omnidireccionales para crear un área de cobertura con más de una SS. Esta arquitectura soporta comunicación multicasting.

- Punto a Punto Consecutivo (Point-to-consecutive point, PTCM): Implica la creación de lazos cerrados a través de múltiples conexiones PTP.

- Malla (Mesh): El subestándar IEEE 802.16a, donde cada nodo está habilitado para dirigir o rutear datos adaptativamente a su destino. Las arquitecturas Malla se organizan y restablecen automáticamente.

LA CAPA FÍSICA (PHYSICAL LAYER, PHY)

Los estándares IEEE 802.16 e IEEE 802.16a especifican cada uno una interfase de aire distinta debido a los diferentes rangos de frecuencia, pero ambos utilizan el mismo protocolo MAC. Esta habilidad de aplicar una MAC a diferentes interfaces PHY tiene mucho potencial para aplicaciones comerciales y militares. La estandarización de dos interfaces de aire por separado hace posible para las operadoras tomar ventaja de los beneficios de ambos rangos de frecuencia dependiendo de la situación. Para propósitos militares, puede ser posible adaptar el estándar IEEE 802.16 para emplear una PHY que sea apropiada para sus operaciones.

- **Sistemas de 10-66GHz**

  Las altas frecuencias de las señales de microonda en el rango de 10-66GHz son asignadas al estándar IEEE 802.16. Este estándar sólo soporta la operación LOS y tiene un rango de cobertura muy corto, de sólo unos kilómetros, cuando se lo compara con un sistema de frecuencia más bajas. Este rango es capaz de soportar tasas de datos mayores a 120Mbps. La principal ventaja de este rango de frecuencia sobre los demás es su gran disponibilidad de ancho de banda. A diferencia de los rangos más bajos donde las bandas de frecuencia son comúnmente de un ancho menor a 100MHz, la mayoría de las bandas de frecuencia sobre los 20GHz pueden proveer cientos de megahertz de ancho de banda. Además, los canales dentro de estas bandas son típicamente de un ancho de 25 o 28MHz.

  El estándar IEEE 802.16 utiliza una modulación de portadora simple (WirelessMAN-SC) usando ya sea QPSK, 16-QAM o 64 QAM. La

comunicación en el enlace de bajada, lo cual típicamente involucra a una BS con múltiples SSs, se realiza utilizando TDM. El enlace de subida usa las técnicas de TDMA y DAMA (Demand Assigned Multiple Access) combinadas. El canal del enlace de subida es dividido en varias ranuras de tiempo y la asignación de dichas ranuras es controlada dinámicamente por la MAC de la BS y basándose en las necesidades del sistema.

El estándar IEEE 802.16 permite ambas duplexaciones, en tiempo (TDD) y en frecuencia (FDD). En TDD, tanto el enlace de subida como el de bajada toman turnos para transmitir en un canal compartido, mientras que en FDD se asignan canales separados para cada uno. El estándar también soporta FDD half duplex, donde el enlace de subida y bajada comparten el mismo canal como sucede en TDD.

Otra única característica del estándar IEEE 802.16 de alta frecuencia es el uso de un perfil de paquete configurable (adaptive burst profiling). Éste hace posible para el equipo de radio hacer ajustes a la modulación y a los esquemas de codificación que están siendo utilizados, en respuesta a los cambios de las condiciones ambientales y el resultado de la calidad de la señal. Los sistemas que utilizan un perfil de paquete configurable estarán constantemente monitoreando la calidad de la señal y haciendo ajustes trama por trama, cambiando entre el más eficiente y menos robusto QAM al menos eficiente pero más robusto QPSK, según la necesidad.

- **Sistemas de 2-11GHz**

  El estándar IEEE 802.16a está dirigido a las señales de microonda de baja frecuencia en el rango de 2-11GHz. Las señales en este rango de frecuencia tienen muchas ventajas sobre las señales de frecuencias más altas, como lo son la habilidad de atravesar paredes, funcionamiento NLOS, mayores rangos de cobertura que en las señales de mayor frecuencia (mas de 30 millas utilizando antenas altamente direccionales), poseen un soporte para una modulación más compleja, y una alta robustez y eficiencia espectral. De hecho, muchas de las más ventajosas capacidades de la PHY del IEEE 802.16 se encuentran en este rango de frecuencia.

  El estándar IEEE 802.16a utiliza OFDM con una transformada de 256-puntos.

  El estándar IEEE 802.16a también utiliza TDM y TDMA para programar las transmisiones de los enlaces de subida y bajada. Además, utiliza TDD y FDD de la misma forma que en los sistemas IEEE 802.16.

- **Control de Errores**

  El estándar IEEE 802.16 utiliza dos métodos para control de errores en la PHY: Corrección de Errores en la Recepción (Forward Error Correction, FEC) y Petición de Retransmisión Automática (Automatic Retransmission Request, ARQ).

a. FEC

FEC es utilizado en ambas interfases de aire. El IEEE 802.16 normalmente utiliza Reed-Solomon GF (256) FEC, pero tiene la opción de utilizar un código más robusto, el Block Turbo, para ya sea incrementar el rango de cobertura de la BS o incrementar la velocidad efectiva de transmisión.

b. ARQ

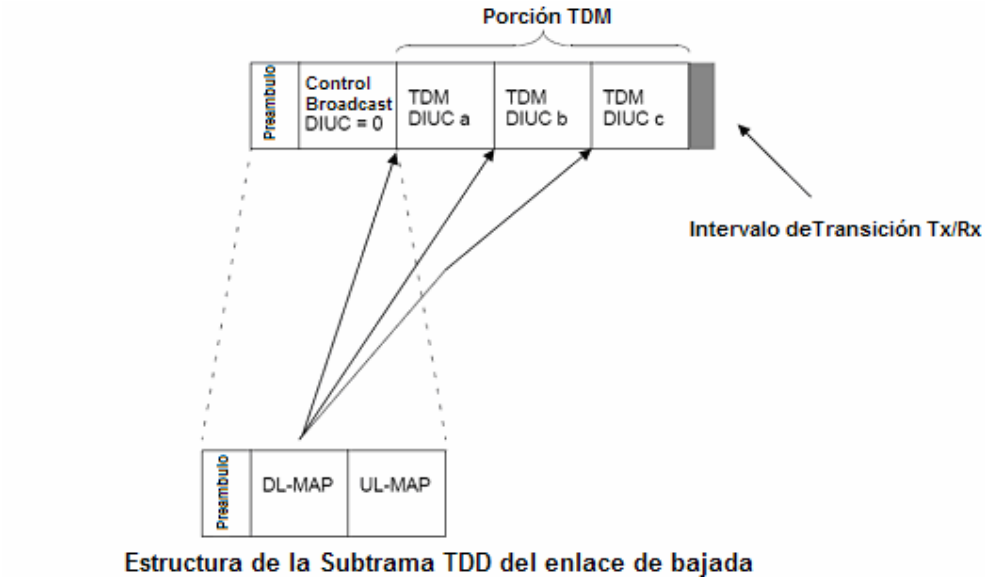
ARQ es una característica de la PHY que es usada para encargarse de los errores ocurridos debido a las anomalías en la programación. ARQ implica la retransmisión de bits individuales de datos que pueden haberse perdido en la transmisión original. La eficiencia de la retransmisión individual de bits hace posible corregir los errores antes que el dato sea enviado a una capa superior para su proceso. ARQ es una característica del estándar IEEE 802.16a únicamente, no está especificado en el estándar IEEE 802.16.

- **Tramado**

  La PHY del IEEE 802.16 utiliza tramas de 0.5, 1 o 2 milisegundos de duración. Cada trama es dividida en ranuras físicas de longitud 4-QAM. Las ranuras físicas son utilizadas para asignación de ancho de banda y transiciones de PHY. En los sistemas TDD, cada trama es dividida entre porciones de subtrama del enlace de subida y bajada. Para cada trama, la subtrama del enlace de bajada es transmitida primero, seguida por un espacio de transmisión/recepción que da al equipo un tiempo para hacer el cambio entre transmisión y recepción, lo cual es entonces seguido por la subtrama del enlace de subida.

También hay un breve espacio de tiempo entre las tramas. En los sistemas FDD, la transmisión y recepción se realiza simultáneamente sobre canales separados.

a. Subtrama del Enlace de Bajada



Estructura de la Subtrama TDD del enlace de bajada

Como se muestra en la figura, cada subtrama del enlace de bajada comienza con un preámbulo seguido por una sección de la trama de control que contiene un mensaje de mapeo del enlace de bajada (Dounlink map, DL-MAP) y un mensaje de mapeo del enlace de subida (Uplink map, UP-MAP).

El preámbulo inicial de la trama es una secuencia de 32-símbolos generada por la repetición de una secuencia de 16-símbolos.

La sección de la trama de control es utilizada para pasar información de control por los canales para todas las SSs, y estos datos no son encriptados.

Esta información incluye: sincronización de PHY, un mensaje que describe el estado del canal del enlace de bajada (Downlink Channel Descriptor, DCD), un identificado de la BS programable de 48-bit, y el número de elementos de datos que siguen. El identificador del DCD y la BS identifica el canal y la BS, respectivamente, y son útiles en situaciones donde una SS se encuentra en el borde de múltiples sectores o celdas IEEE 802.16. El mensaje DL-MAP debe estar organizado como se muestra en la tabla.

Sintaxis	Tamaño	Notas
DL-MAP_Message_Format() {		
Management Message Type = 2	8 bits	
PHY Synchronization Field	Variable	Ver especificaciones apropiadas de PHY
DCD Count	8 bits	
Base Station ID	48 bits	
Number of DL-MAP Elements *n*	16 bits	
Begin PHY Specific Section {		Ver sección aplicable a PHY
for (*i* = 1; *i* <= *n*; *i*++) {		Para cada elemento DL-MAP de 1 a n
DL_MAP_Information_Element()	Variable	Ver correspondiente especificación de PHY
if !(byte boundary) {		
Padding Nibble	4 bits	Bits redundantes para cada límite de byte
}		
}		
}		
}		

El formato del mensaje DL-MAP

El UL-MAP es utilizado para comunicar las asignaciones de acceso al canal del enlace de subida para las SSs. La información

que provee el UL-MAP incluye: Identificador de canal del enlace de subida, un mensaje que describe el estado del canal del enlace de subida (Uplink Channel Descriptor, UCD), información de un número de elementos a ser enmascarados, tiempo de inicio de asignación y elementos de información enmascarados. El UCD es utilizado para proveer a las SSs con información considerando el perfil de paquete requerido por el enlace de subida. El mensaje de los elementos de información enmascarados identifica la SS y esta información se aplica utilizando un identificador de conexión (Connection Identifier, CID). Este mensaje también provee un código de uso del intervalo del enlace de subida (Uplink Interval Usage Code, UIUC) y compensaciones que serán utilizadas por la SS al transmitir en el enlace de subida. El UIUC es utilizado para especificar el perfil de paquete a ser utilizado por la SS en el enlace de subida. El mensaje UL-MAP debe ser organizado como se muestra en la tabla.

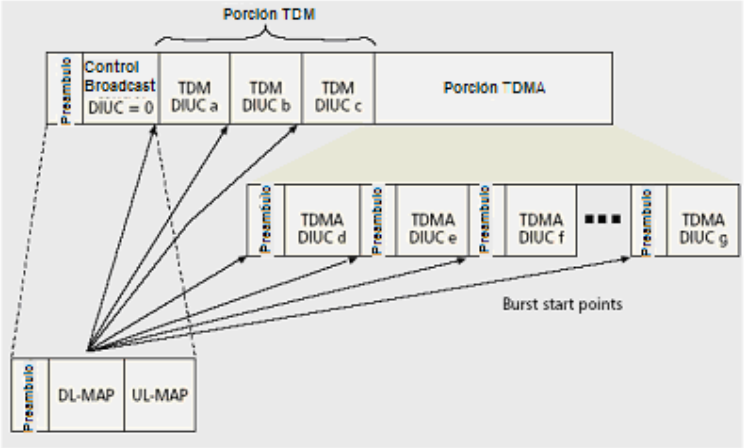
La sección de la trama de control es típicamente seguida por una porción de TDM donde el dato del enlace de bajada es transmitido a cada SS. Estas secciones de TDM son utilizadas para transmitir datos o mensajes de control para una SS específica. Cada una de estas transmisiones es portada de acuerdo al perfil de paquete negociado entre la BS y la SS y la información es transmitida en orden decreciente de resistencia.

Sintaxis	Tamaño	Notas
UL-MAP_Message_Format() {		
Management Message Type = 3	8 bits	
Uplink Channel ID	8 bits	
UCD Count	8 bits	
Number of UL-MAP Elements *n*	16 bits	
Allocation Start Time	32 bits	
Begin PHY Specific Section {		Ver sección aplicable a PHY[1].
for (*i* = 1; *i* <= *n*; *i*++) {		Por cada elemento UL-MAP de 1 a n
UL_MAP_Information_Element()	Variable	Ver especificación correspondiente a PHY
}		
}		
}		

Formato del mensaje UL-MAP

La SS destino es especificada en la cabecera de la MAC de cada transmisión de datos, no en la porción de DL-MAP del mensaje de la trama de control. Esto es necesario en SSs full duplex para escuchar todas las subtramas del enlace de bajada en orden de filtrar sus datos.

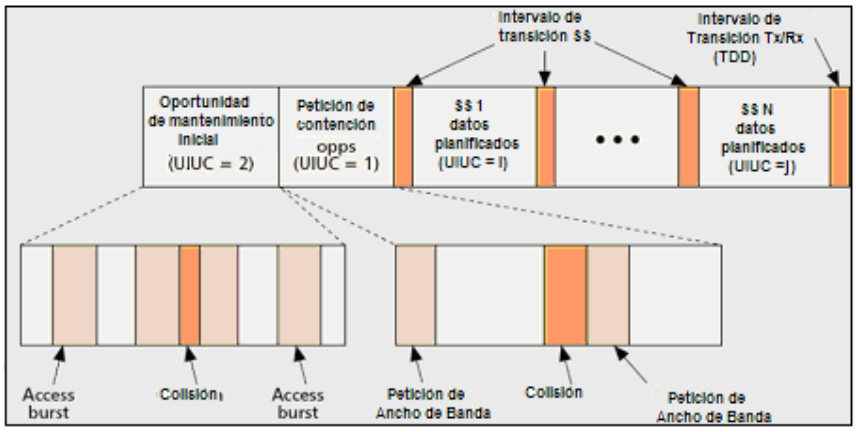
En los sistemas FDD con capacidad para half duplex, la porción de TDM de la subtrama del enlace de bajada puede ser seguido por una porción de TDMA designada para permitir sistemas half duplex para recobrar la sincronización con la BS. En este caso, un preámbulo separado puede preceder cada ranura TDMA como se muestra en la figura. Los parámetros del perfil de paquetes y la presencia de una porción de TDMA podrían variar en cada trama como lo dicte la demanda de ancho de banda y servicio.



Estructura de subtrama del enlace de bajada

b. Subtrama del Enlace de Subida

La subtrama del enlace de subida es utilizada por las SSs para transmitir información a la BS. Una estructura típica de una subtrama de enlace de subida se muestra en la figura.



Estructura de la subtrama del enlace de subida

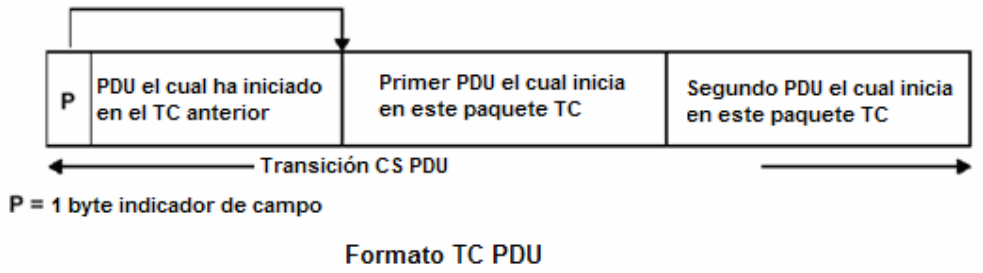
Existen por lo menos tres posibles clases de paquetes que podrían esta presentes en cada subtrama de enlace de subida:

- Contención basada en mantenimiento inicial o en oportunidades de acceso iniciales.
- Contención basada en oportunidades definidas por intervalos de requerimientos como respuesta a un sondeo para multicast o broadcast.
- No contención basada en intervalos planificados distribuidos para especificar las SSs en UL-MAP de ancho de banda otorgado desde la BS.

Cualquiera de estas tres clases de paquetes pueden estar presentes en cualquier trama, en cualquier orden y en cualquier cantidad por trama como es dictado por la planificación de la BS en un mensaje UL-MAP.

- **Subcapa de Convergencia de Transmisión (Transmission Convergence Sublayer, TC)**

La subcapa TC existe entre la PHY y la MAC. La subcapa TC toma unidades de datos de protocolo (Protocol Data Unit, PDU) MAC de longitudes variables y los organiza dentro de bloques fijos FEC antes de la transmisión. Un byte-1 es adicionado al inicio el TC PDU para indicar el primer byte de la siguiente MAC PDU dentro de la TC PDU. En el caso de perdida de datos en las transmisiones, este puntero permite la resincronización entre la SS y la BS. El formato del TC PDU se muestra en la figura.



P = 1 byte indicador de campo

Formato TC PDU

CAPA DE CONTROL DE ACCESO AL MEDIO (MAC)

La MAC del IEEE 802.16 es el mecanismo responsable para compartir eficiente del medio disponible. La MAC del IEEE 802.16 es superior a la PHY, es un protocolo independiente, con la capacidad de soportar servicios TDM de voz y datos, conectividad IP, o empaquetar aplicaciones como VoIP. Es también capaz de soportar tráfico continuo o intermitente (bursty) y asegurar que QoS sea consistente con el tipo de tráfico que esta siendo transmitido. Además, la MAC del IEEE 802.16 es capaz de soportar servicios como el Modo Asincrónico de transferencia (Asynchronous Transfer Mode, ATM) y Tasa Garantizada de Trama (Guaranty Frame Rate, GFR).

A través de una variedad de métodos, la MAC es capaz de proveer servicios diferenciados a usuarios en el mismo medio. Más importante, la MAC es capaz de garantizar un nivel de servicio específico y requerir QoS para cada conexión.

- **Orientación de la Conexión**

  Una conexión es una máscara (mapping) unidireccional entre la MAC de la BS y la SS con el propósito de transportar los servicios de una corriente de tráfico. El IEEE 802.16 es un protocolo orientado a conexión, donde todos los servicios son dirigidos a una conexión. Esto es cierto incluso en los servicios intrínsecamente sin conexión. Mientras cada SS tiene una dirección MAC única de 48-bits, este número no es utilizado para referenciar las múltiples conexiones asociadas a cada SS. En cambio, las conexiones son referenciadas utilizando un CID de 16-bits. Los CIDs son utilizados para todas las interacciones con la BS para incluir requerimientos de ancho de

banda, control de QoS en las conexiones, y enrutamiento de datos para la apropiada subcapa.

Cuando una SS es incluida en una red, la BS le asignará tres conexiones de mantenimiento en cada dirección. Cada conexión es utilizada para la transmisión de mensajes de diferentes longitudes y prioridades. Las tres conexiones de mantenimiento y el tipo de mensaje que ellos transmiten son como los siguientes:

- La conexión básica – corto, mensajes de tiempo crítico de la MAC y control del radio enlace.
- La conexión de mantenimiento primario – largo, mensajes con mayor tolerancia al retardo (ej. Mensajes de autenticación o montaje de la conexión)
- La conexión de mantenimiento secundaria – mensajes basados en estándares tales como mensajes DHCP, TFTP y SNMP.

Existen varios tipos de conexión para soportar las varias funciones MAC del IEEE 802.16. Un segundo grupo de conexiones, conocidas como conexiones de transporte, son establecidas de acuerdo con los servicios que están siendo soportados y la QoS requerida y los parámetros del tráfico. Estas conexiones no hay que confundirlas con conexiones de capa 4 o capa de transporte existente en el modelo OSI. Las conexiones de transporte son típicamente asignadas en pares. Otras conexiones pueden se establecidas para contención basada en acceso inicial, transmisiones broadcast, transmisiones multicast, etc.

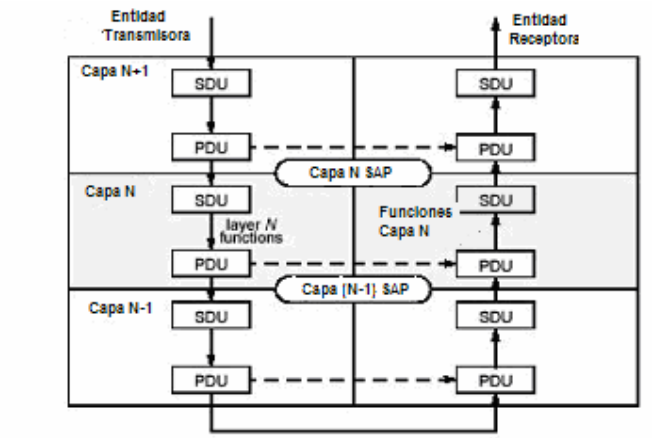
- **La MAC PDU**

a. Descripción de la PDU

La definición de una MAC PDU es como sigue:

La MAC PDU es una unidad de datos intercambiable entre las capas MAC de la BS y sus SSs. Una MAC PDU consiste de una cabecera de longitud fija, una información útil (payload) de longitud variable, y un Chequeo de Redundancia Cíclica (Cyclic Redundancy Check, CRC) opcional.

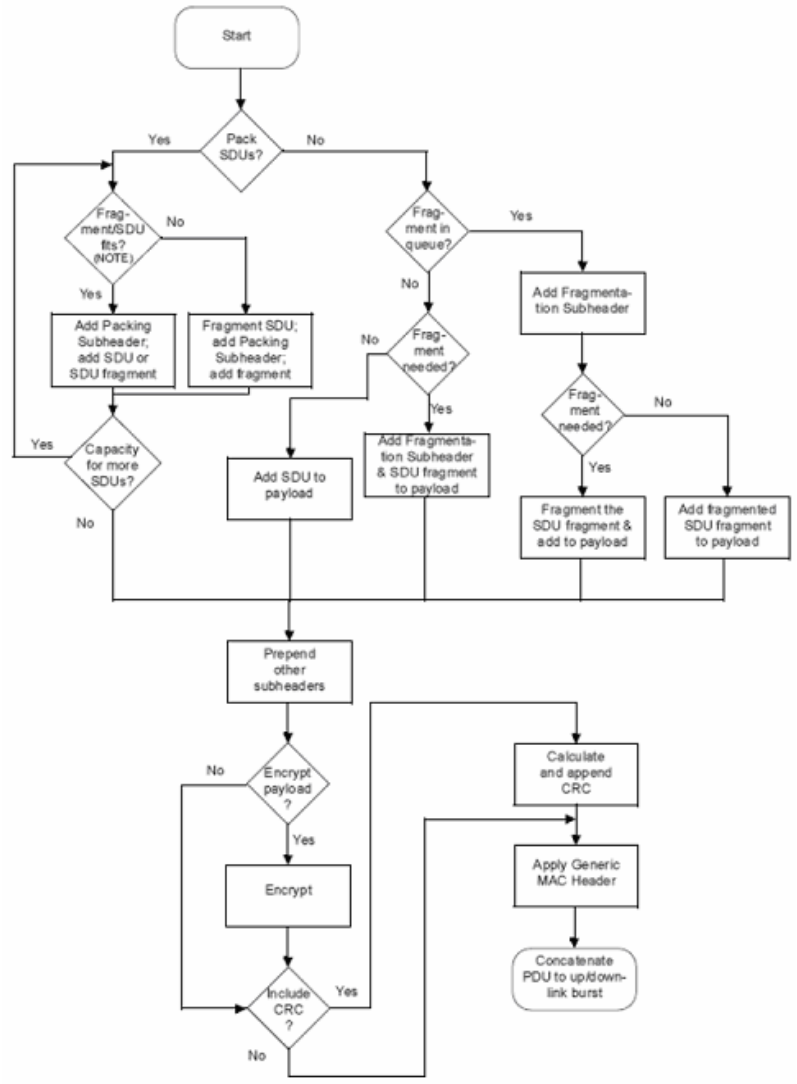
Más específicamente, los PDUs son intercambiados entre un par de identidades en la misma capa de protocolo, de capas superiores a inferiores en la dirección de bajada y de capas inferiores a superiores en la dirección de subida. Este intercambio de PDUs se muestra en la figura. En la dirección de bajada, cada capa encapsula el PDU de la capa superior dentro de un formato MAC SDU antes de pasarlo a la siguiente capa.



PDU y SDU en una Pila de Protocolo

b. Construcción de la MAC PDU

Antes de transmitir, la MAC puede tomar ventaja de varios métodos de construcción de la MAC PDU para maximizar la eficiencia de la transmisión. El proceso de construcción de la MAC PDU es mostrado en la figura.



Construcción de la MAC PDU

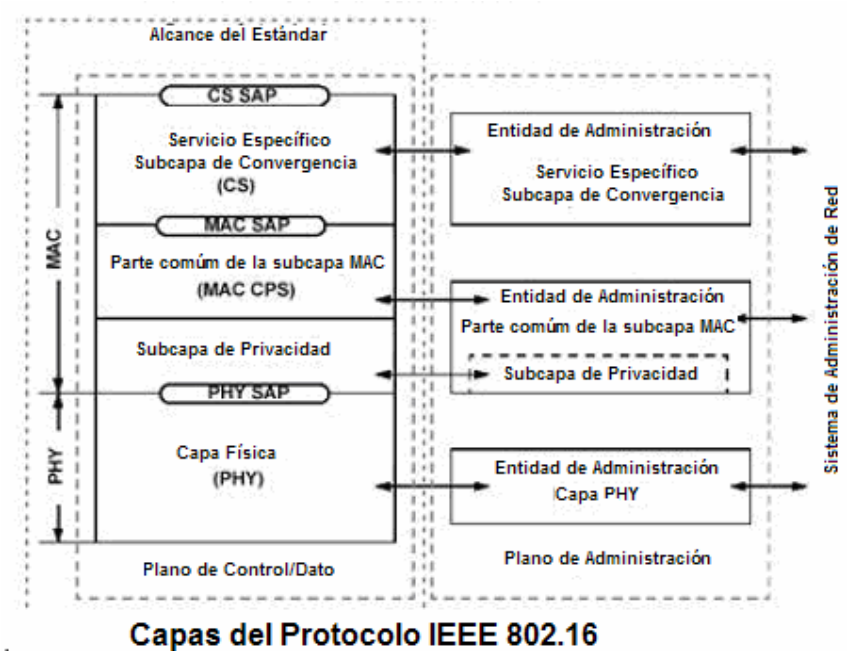
Los siguientes métodos son utilizados en la construcción de MAC PDUs:

- ❖ Concatenación. Entiende la concatenación de múltiples MAC PDUs en una transmisión. Puede realizarse tanto en el enlace de subida como en el de bajada.
- ❖ Fragmentación. Es la división de una MAC SDU en diversas MAC PDUs. Puede ser utilizado para soportar servicios donde el tamaño de la MAC SDU puede ser muy largo, tales como aplicaciones de video. La fragmentación puede realizarse también en ambos direcciones de los enlaces.
- ❖ Empaquetamiento. Es el empaquetamiento de múltiples MAC SDUs en una MAC PDU. La conexión debe estar autorizada para transportar paquetes de longitud variable para poder aprovechar esta característica. El empaquetamiento puede realizarse en cualquiera de los enlaces dependiendo de la estación de transmisión.

- **Sub-Capas**

  La MAC está constituida de tres subcapas: la subcapa de Convergencia Específica de Servicio (Service Specific Convergence Sublayer, CS), la subcapa Parte Común MAC (MAC Common Part Sublayer, MAC CPS), y la subcapa de Privacidad. Las subcapas están organizadas como se muestra en la figura, con la CS al inicio como la interfase a las capas superiores, la MAC CPS debajo de la CS, y la subcapa de Privacidad debajo de la MAC CPS. Entre cada subcapa existe un servicio de punto de acceso, es cual actúa como

una interfase entre las dos capas fronteras. Es importante notar que la CS SAP actúa como la interfase a la capa 3.



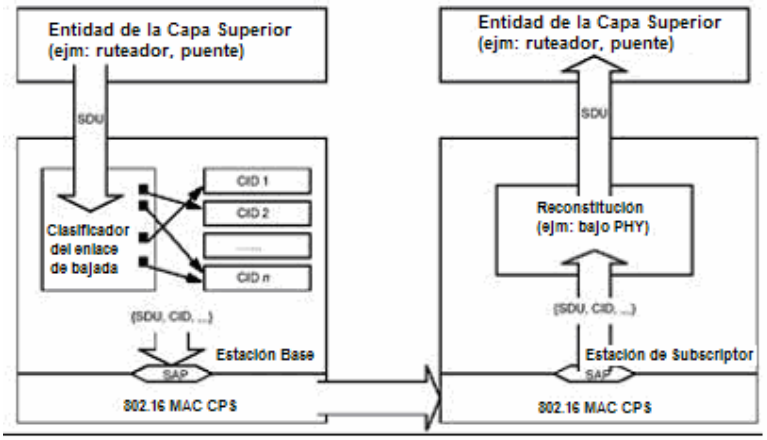
Capas del Protocolo IEEE 802.16

a. Subcapa de Convergencia

La CS es utilizada para enmascarar los servicios desde y hacia conexiones MAC. Técnicamente, la CS acepta, clasifica y procesa los PDUs recibidos desde una capa superior, entrega CS PDUs (o SDUs en el caso de una capa inferior) a la correcta MAC SAP, y recibe CS PDU de cualquier entidad.

Existen dos especificaciones para los CSs, el ATM CS, para servicios ATM y el paquete CS, para enmascarar paquetes de servicios tales como IPv4, IPv6, Ethernet, y Redes de Area Local Virtuales (Virtual Local Area Network, VLAN).

La MAC CPS provee el núcleo principal de la MAC del IEEE 802.16 para incluir: acceso al sistema, asignación de ancho de banda, establecer conexiones, y mantenimiento de conexiones. Esta capa es también responsable para la aplicación a conexiones específicas con QoS por medio de una planificación de transmisión apropiada. La figura muestra una clasificación típica y la secuencia de enmascarado entre una BS y una SS.



Clasificación y mapeo del CID

b. Subcapa de Privacidad

La subcapa de privacidad es responsable de la encriptación entre la BS y la SS. La subcapa de privacidad protege a los usuarios contra ladrones de servicio y el acceso no autorizado a la red. Esta subcapa emplea un protocolo de manejo de clave cliente/servidor y un certificado digital basado en la autenticación de la SS.

c. Supresión de la Cabecera de Información Útil

En orden para incrementar la eficiencia del intercambio de MAC SDU entre la CS y otras identidades, es posible suprimir la porción respectiva a la cabecera de información útil. En casa caso la entidad emisora suprime la cabecera y la entidad receptora reconstruye la porción suprimida de la cabecera de información útil.

- **Control del enlace de Radio**

  El controlador del enlace de radio del estándar IEEE 802.16 (Radio Link Controler, RLC) es responsable del manejo de los perfiles de paquetes configurables, control de potencia y rango. Un perfil de paquete diferente es utilizado para cada canal como determinado por el RLC, basado en “un número de factores, tales como lluvia, región y capacidad de los equipos”. Bajo condiciones de enlace favorables, el RLC empleará el perfil de paquete disponible mas eficiente disponible, y cambiará a un perfil de paquete menos eficiente cuando las condiciones del enlace sean menos favorables. El ajuste del perfil de paquete, la potencia y los parámetros de rango son controlados por la BS, la cual monitorea la calidad de la señal en el enlace de subida y maneja los requerimientos de las SSs asociadas para hacer ajustes en el enlace de bajada.

- **Ingreso a la Red e Inicialización**

  La figura muestra las etapas de un error sin inicialización de una SS ingresando a la red. Hay muchos caminos posibles de este procedimiento que se pueden presentar debido a errores durante la

inicialización. Este procedimiento de inicialización está designado para eliminar la necesidad de configuración manual para cada SS.

Cada paso en el proceso de inicialización será visto a continuación:

a. Escaneo y Sincronización del Enlace de Bajada

Las SSs están diseñadas para escanear sus listas de frecuencias por canales de enlace de bajada activos inmediatamente la instalación este lista o seguido de cualquier periodo de pérdida de señal. En el caso de pérdida de señal, la SS almacenará los parámetros operacionales de la última señal y tratará de

restablecer la conexión. Luego de adquirir un canal con una señal de enlace de bajada válida, la SS intentará sincronizar la PHY escuchando los mensajes administración DL-MAP. La SS continuará escuchando los mensajes y en el caso de pérdida de los mensajes, la SS repetirá el proceso de escaneo y la sincronización.

b. Obtención de los Parámetros de Transmisión

Una vez que los mensajes DL-MAP hayan sido detectados, la subcapa MAC escuchará los parámetros del enlace de subida y bajada. Al escuchar por los mensajes UCD provenientes de la BS, la SS es capaz de determinar un canal de enlace de subida utilizable. Los mensajes UCS son mensajes de broadcast, enviados periódicamente, proveyendo parámetros pertinentes para todos los canales de enlace de subida disponibles. La SS colectará los mensajes UCD para cada canal disponible, e intentará establecer comunicación en un canal apropiado. Si la comunicación fallara en un canal, la SS se moverá al siguiente canal apropiado hasta que se establezca una conexión o ya no existan canales, en cuyo caso iniciará el procedimiento de escaneo nuevamente.

c. Rango y Ajuste de Potencia

Como se describe en el estándar IEEE 802.16, Rango es el proceso de adquirir el correcto tiempo de compensación con lo cual las transmisiones de la SS son alineadas a un símbolo que marca el inicio de una mini ranura limitante. El tiempo de compensación es distado por la distancia de la SS a la BS y el

retardo de la propagación de la señal correspondiente. La SS comienza este procedimiento escaneando los mensajes UL-MAP por un intervalo de mantenimiento disponible. Una vez que el intervalo de mantenimiento ha sido determinado, la SS enviará un mensaje de Petición de Rango (RNG-REQ), dentro de este periodo de mantenimiento inicial basado en contención, a la BS al menor nivel de potencia. Si esta transmisión no recibe una respuesta, la SS aumentará el nivel de potencia incrementándolo como sea necesario, pero no excederá la máxima potencia de transmisión especificada. La BS responderá con un mensaje Respuesta de Rango (RNG-RSP), el cual especifica el apropiado tiempo de avance y el ajuste de potencia para la SS, así como también los manejos CIDs básicos y primarios.

d. Negociación de las Capacidades Básicas

La SS utilizará los mensajes de Petición de Capacidad Básica de la SS (SS Basic Capability Request, SBC-REQ) para reportar sus capacidades a la BS. Este mensaje provee la capacidad de la PHY de la SS, modulación soportada y esquemas de codificación, y métodos de duplexación soportados. La BS responderá entonces con un mensaje de Respuesta de Capacidad Básica de la SS (SS Basic Capability Response, SBC-RSP) para detallar cuales de las capacidades de la SS soportará. Esta respuesta será utilizada para ajustar el perfil de paquete del más eficiente perfil utilizado. Hasta este punto todas las transmisiones previas son portadas utilizando el mas robusto perfil de paquete disponible.

e. Autorización al SS para realizar el Intercambio de Clave

La autorización y el intercambio de clave será cubierto con mas detalle en la sección de seguridad.

f. Registro

De acuerdo con el estándar IEEE 802.16, el registro es el proceso por el cual la SS recibe su CID de manejo secundario y se convierte en administrable. Esto es conseguido mediante el mensaje de Petición de Registro (Registration Request, REG-REQ) enviado por la SS y el mensaje de Respuesta de Registro (Registration Response, REG-RSP) enviado por la BS.

g. Establecimiento de Conectividad IP

La SS puede incluir la versión de IP utilizada en el REG-REQ. Si no lo incluye la BS autorizará el uso de IPv4 por defecto para la conexión de manejo Secundaria. La SS y la BS utilizaran entonces el Protocolo de Configuración de Host Dinámica (Dynamic Host Configuration Protocol, DHCP) en la conexión de manejo secundario para completar la conectividad IP.

h. Establecimiento de Hora del Día

La hora del día es utilizada para marcar el tiempo de los eventos registrados en ambos, la BS y la SS. La SS utiliza nuevamente la conexión de manejo secundaria para recuperar el tiempo del

servidor. La transmisión es enviada mediante el Protocolo de Datagrama del Usuario (User Datagram Protocol, UDP). El tiempo que retorna del servidor es combinado con el tiempo de compensación de la SS en orden para determinar el tiempo local actual.

i. Transferencia de Parámetros Operacionales

La SS utilizará TFTP para transferir el archivo de configuración de la SS. El archivo de configuración contiene la fijación de la configuración de una variedad de parámetros usados en la operación de la SS.

j. Fijar Conexiones

La SS empezará a establecer conexión para flujos de servicio pre-provisionales, donde un flujo de servicio es definido como un transporte unidireccional de paquetes en ya sea el enlace de subida o de bajada. Cada flujo de servicio es asociado con un juego específico de parámetros de QoS para el servicio soportado. Estos flujos de servicio utiliza un modelo de activación de dos fases donde una flujo de servicio puede ser admitido (la BS tiene recursos reservados, pero el servicio no está activo), o activo (la BS tiene recursos reservados, pero el servicio está activo). Un tercer estado es posible para un flujo de servicios, es el estado provisional, donde la BS ha asignado un identificador de flujo de servicio, pero no tiene reservados ningún recurso para este flujo de servicio.

- **Requerimientos de Ancho de Banda y Concesiones**

  El estándar IEEE 802.16 administra la asignación de ancho de banda utilizando un protocolo de petición/concesión. En este protocolo, las SSs piden asignación de ancho de banda de la BS mediante una variedad de métodos. La BS hace asignación de ancho de banda asignando ranuras de tiempo de transmisión (mediante TDMA) únicamente a aquellas SSs que hayan enviado una petición de ancho de banda (mediante DAMA). La BS utilizará mensajes UL-MAP para relacionar las asignaciones de ancho de banda a todas las SSs en la red.

  Las SSs pueden ser divididas en dos clases basándose en como ellas manejan las concesiones de ancho de banda. La primera clase de SS acepta la concesión de ancho de banda para cada conexión, o sobre una base de conexión por concesión (grant per connection, GPC). La segunda clase de SS es capaz de aceptar las concesiones para las necesidades de ancho de banda de todas las SSs, o sobre una base de SS por concesión (grant per SS, GPSS). Estas son detalladas a continuación:

  a. GPC

  La SS GPC recibe la concesión únicamente por conexiones específicas (para incluir manejo de conexión) y como resultado más peticiones de ancho de banda por cada conexión individual como sea necesario. Además, la SS GPC debe pedir ancho de banda adicional recibir cualquier petición RLC inesperada. Por estas razones, los sistemas GPC son menos eficientes que los sistemas GPSS, pero también son simples.

b. GPSS

La SS GPSS recibe una concesión de ancho de banda, la cual se utiliza para conocer las necesidades de todas sus conexiones. Como resultado, la SS por sí misma debe manejar cuanto ancho de banda más es asignado a cada conexión. En situaciones donde una conexión pide más ancho de banda que el esperado, la SS tiene la opción de "robar" ancho de banda de otra conexión para cubrir la falta temporal de ancho de banda. La BS es también responsable de la prioridad del encolado basada en los tipos de tráfico. La SS puede entonces enviar una petición a la BS pidiendo que su concesión de ancho de banda sea incrementada para responder a sus necesidades. Las SSs GPSS son la única clase de SS disponibles en el rango de frecuencia de 10-66GHz.

La concesión de ancho de banda es provista basada en un protocolo de auto-corrección lo opuesto a un protocolo de reconocimiento. En este protocolo, si la SS no recibe una concesión de ancho de banda en respuesta a su petición de ancho de banda, la SS asumirá que la petición se perdió o no fue concedida, y simplemente enviará otra petición a la BS, sin tener que esperar por algún reconocimiento a la petición original. Este protocolo elimina la sobrecarga asociada con los mensajes de reconocimiento.

- **Requerimientos de Ancho de Banda**

  Las SSs irán incrementando las peticiones de ancho de banda a medida que nuevas peticiones de ancho de banda se presenten, y la BS irá adicionando la petición de ancho de banda al total de peticiones percibidas por la SS.

a. Periodos de Petición

Con el incremento de las peticiones, la BS no tiene conocimiento si ha concedido el total correcto de peticiones de ancho de banda a la SS, debido a que el total concedido de ancho de banda puede ser afectado por la pérdida de los paquetes de petición. Debido a esta posibilidad, las SSs pueden ir incrementando la petición de ancho de banda. Las peticiones agregadas son usadas para resetear la percepción de la BS del total de peticiones de ancho de banda de la SS. Cuando una BS recibe una petición agregada, almacenará el valor de la petición de ancho de banda como el nuevo total del requerimiento pedido por la SS.

Hay una variedad de métodos disponibles para que una SS pida asignación de ancho de banda a la BS. Las peticiones de ancho de banda pueden estar relacionadas a la BS durante periodos de petición de ancho de banda dedicados específicamente a una SS o durante un periodo de contención. El método de encuestar utilizado por la BS para informar a las SS de la venida de los periodos de petición de ancho de banda es lo que determina si el periodo de petición de ancho de banda es dedicado o un periodo de petición de contención.

b. Cabecera de Petición de Ancho de Banda

Además de los períodos de petición de ancho de banda asignados mediante encuesta, las SSs pueden pedir asignación de ancho de banda en cualquier momento enviando a la BS una MAC PDU de petición de ancho de banda con una cabecera de petición de ancho de banda y sin información útil. Este método de petición de

ancho de banda puede ser utilizado en cualquier concesión de ancho de banda para las SSs GPSS y en intervalos de petición de concesión o intervalos de concesión de datos para una conexión específica.

c. Petición Piggyback

Un método similar de petición de ancho de banda es utilizar una subcabecera de manejo de concesión para piggyback una petición adicional de ancho de banda para la misma conexión dentro de la MAC PDU.

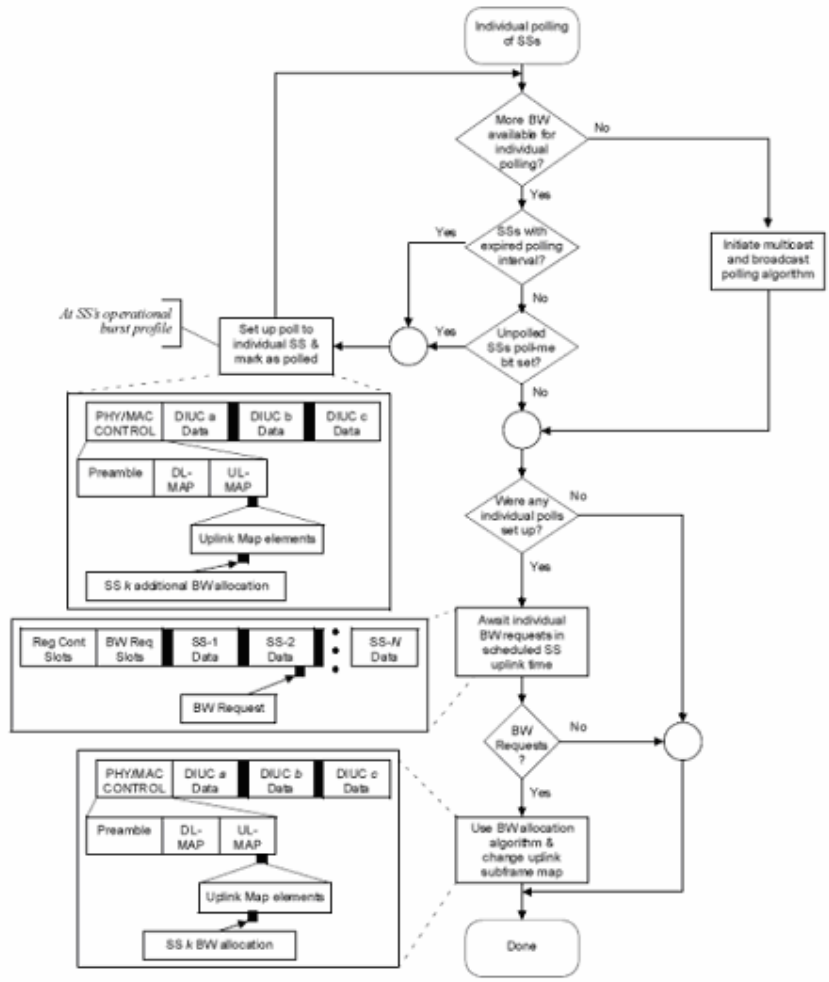
- **Sondeo (Polling)**

  El Sondeo es el proceso utilizado por la BS para asignar oportunidades de petición de ancho de banda a las SSs. Cuando la BS quiere notificar a una SS la oportunidad de petición de ancho de banda entrante, utilizará un mensaje de elemento de información (Information Element, IE) UL-MAP para hacerlo. El UL-MAP IE concesionará suficiente ancho de banda para la SS o SSs para notificar sus peticiones de ancho de banda durante el periodo de petición especificado. Las asignaciones de oportunidad de petición de ancho de banda pueden ser hechas en un unicast, multicast o broadcast. Una descripción breve de cada método de sondeo se describe a continuación:

  a. Sondeo Unicast

  En un sondeo unicast, una SS es sondeada individualmente por la BS. La SS responderá con bytes basura si la concesión de ancho

de banda no es necesaria. El proceso por el cual la BS conduce la sondeo unicast se muestra en la figura:



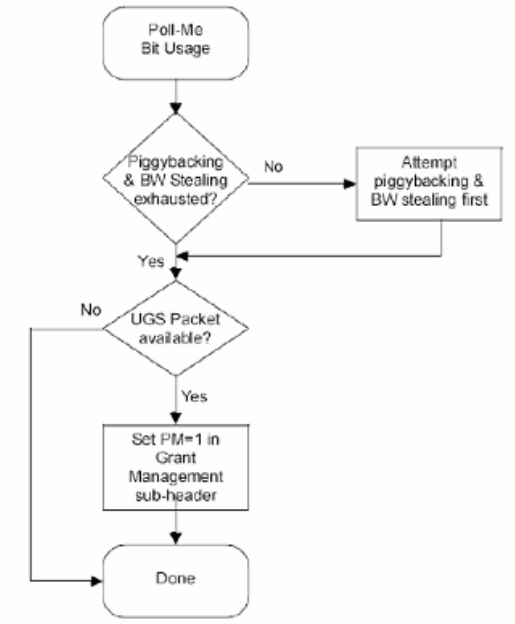
b. **Sondeo Multicast y broascast**

La BS acudirá al sondeo multicast o broadcast cuando no haya suficiente ancho de banda para los sondeos individuales de las SSs. Los sondeos multicast y broadcast también son realizados mediante mensajes UL-MAP de la misma manera que los sondeos

unicast. La BS reserva algunos CIDs para grupos de multicast y broadcas. La diferencia principal aquí es que el mensaje de sondeo es dirigido a través de un CID multicast o broadcast en lugar de un CID o SS individual.

c. Poll-Me Bit

El poll me bit es usado por las SSs utilizando el servicio de Planificación del Enlace de Subida de Concesión no Solicitada (Unsolicited Grant Service, UGS) para notificar a la BS que necesitan se polled. El poll-me bit es parte de una subcabecera de manejo de concesiones. Una vez que el poll-me bit haya sido detectado, la BS publicará un sondeo unicast a la SS que lo pidió. La figura 16 muestra el proceso para utilizar el poll-me bit.



- **Servicios de Planificación del Enlace de Subida**

  El estándar IEEE 802.16 utiliza un servicio de planificación de enlace de subida para incrementar la eficiencia de las transmisiones en el enlace de subida en cada conexión sobre el servicio provisto por la conexión. Los cuatro servicios de planificación del enlace de subida son: Servicio de Concesión no Solicitado, Servicio de Sondeo en tiempo real, Servicio de Sondeo en tiempo irreal, y Servicio del Mejor Esfuerzo. El servicio de planificación que una conexión utilizará es determinado al tiempo que la conexión es instalada. A continuación se detallan los servicios de planificación:

  a. Servicio de Concesión no Solicitado

  Este servicio es utilizado primeramente para la sincronización, los servicios en tiempo real los cuales generan unidades fijas de datos periódicamente, tales como la Tasa de Bit Constante (CBR) ATM, T1/E1 sobre ATM o VoIP sin la supresión del silencio. En este servicio, la BS provee concesiones de datos de tamaño fijo periódicamente, como se negoció durante la instalación de la conexión, sin la necesidad de que la SS envíe peticiones de ancho de banda.

  Esta concesión de ancho de banda no solicitada elimina la sobrecarga y la latencia asociada con las peticiones de ancho de banda y como resultado ayuda a reducir la variación del retardo y el retardo.

  La SS es capaz de proveer información a la BS en lo concerniente a esta del flujo de servicios empleando una bandera indicadora de error (slip) en la cabecera de manejo de concesiones. La bandera indicadora de error es utilizada par indicar una cola de reserva, lo

cual puede ser caudado por una variedad de factores para incluir pérdida de concesiones con redes externas. Una vez que la BS ha sido notificada del error (slippage), puede concesionar ancho de banda adicional en orden para eliminar la reserva.

b. Servicio de Sondeo en Tiempo Real

Este servicio está diseñado para conocer las necesidades de servicios en tiempo real necesarios para transmitir periódicamente, paquetes de datos de tamaño variable. Este servicio es propio para aplicaciones tales como flujos de video o audio, o VoIP. Una aplicación militar apropiada podría ser en los sistemas de dirección de misiles, donde un misil en vuelo podría requerir información actual de trayectoria periódicamente. El sondeo en tiempo real funciona asignando oportunidades de petición de ancho de banda dedicados periódicamente (unicast) en cada conexión. Debido a que la SS debe pedir ancho de banda explícitamente, hay mayor sobrecarga y latencia asociada con este servicio que con el servicio de concesión sin petición, sin embargo, es algo eficiente al utilizar paquetes de datos de tamaño variable.

c. Servicio de Sondeo en Tiempo no real

Este servicio trabaja similarmente al servicio de sondeo en tiempo real, con la excepción que las conexiones utilizan oportunidades de acceso basado en contención para transmitir peticiones de ancho de banda. Las oportunidades del sondeo unicast son utilizadas también para garantizar al menos una tasa de tráfico de reserva mínima, aunque estas oportunidades son menos frecuentes que aquellas halladas en el sondeo de tiempo real. El

sondeo en tiempo no real es apropiado para soportar servicios que pueden tolerar algo de variación del retardo, tales como FTP de gran banda ancha, conexiones a Internet, y ATM GFR. El sondeo en tiempo no real también utiliza los parámetros de tráfico de prioridad, contenidos en el archivo de configuración de la SS y establecidos al fijarse la conexión, para determinar cual flujo de servicio tiene prioridad en relación con los demás.

d. Servicio del Mejor Esfuerzo

No hay garantías de velocidad efectiva o retardos asociados con este servicio. Las conexiones utilizan oportunidades basadas en contención. Además la SS puede utilizar unicast u oportunidades no solicitadas de petición de ancho de banda. La disponibilidad de oportunidades unicast es asunto de la carga de la red y no está garantizada. El servicio de mejor esfuerzo es el más eficiente en ancho de banda porque no reserva ancho de banda para una estación que puede o no estar utilizándolo.

- **Calidad de Servicio**

  Hay varios parámetros asociados con la QoS del estándar IEEE 802.16. Estos parámetros son utilizados para el establecimiento de un flujo de servicio para determinar los requerimientos de QoS de un servicio soportado. A continuación algunos parámetros QoS especificados en el estándar IEEE 802.16:

  - Tipo de conjunto de parámetros QoS – especifica la aplicación propia del grupo de parámetros de QoS a un grupo provisional, admitido o activo.

- Prioridad en el tráfico – utilizado para asignar prioridad a un tráfico de flujo de servicio.
- Tasa de tráfico máximo sostenido – calculado por el byte que sigue a la cabecera MAC al final de la MAC PDU.
- Tasa de tráfico mínima reservada – especifica la tasa mínima reservada para un flujo de servicio.
- Parámetros QoS específicos para vendedores – puede ser utilizado por vendedores para codificar sus propios parámetros QoS.
- Tipo de planificación de flujo de servicio – especifica el servicio de planificación del enlace de subida siendo utilizado para el flujo de servicio.
- Política de petición/transmisión – utilizado para especificar varias reglas de planificación de servicios y políticas de restricción en una petición en el enlace de subida y transmisiones.
- Variación del retardo tolerado – especifica la máxima variación del retardo (jitter) para una conexión
- Retardo máximo – especifica el máximo retardo entre el receptor del paquete en la interfase de red y reenvío par la interfase RF.
- Longitud fija versus el indicador de longitud variable SDU – indica que los paquetes de datos pueden ser de longitud fija o variable.

- **Seguridad**

  La subcapa de privacidad del estándar IEEE 802.16 provee a los usuarios privacidad por encriptación del enlace entre la BS y la SS, y provee protección contra ladrones de servicio encriptando los flujos de servicio dentro de la red. La subcapa de privacidad emplea un protocolo de manejo de clave cliente/servidor autenticado que es capaz de soportar el Estándar de Encriptación Avanzado (Advanced Encryption Standard, AES). En este protocolo la BS, actuando como el servidor, controla la distribución de la clave a la SS, la cual actúa como el cliente.

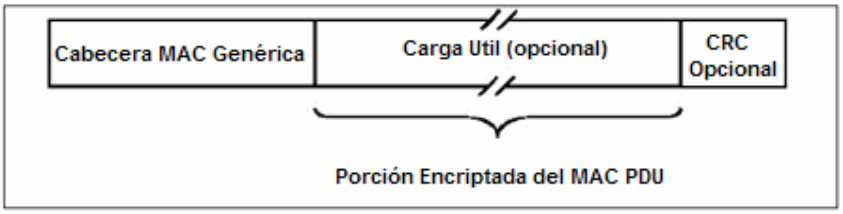
  La subcapa de privacidad emplea protocolos para portar todas las tareas relacionadas con la seguridad. El primero es un protocolo de encapsulamiento, el cual es utilizado en la encapsulación de paquetes de datos en la red.

  La segunda componente de la capa de privacidad es el protocolo de Manejo de Clave de Privacidad (Privacy Key Management Protocol, PKM). PKM es utilizado para proveer seguridad en la distribución de claves entra la BS y la SS. Este protocolo es utilizado ampliamente por la BS y la SS para mantener la sincronización de datos clave entre ellas, y por la BS para controlar el acceso a los servicios de red.

  a. Paquete de Encriptación de Datos

  Cuando la encriptación es habilitada en un sistema IEEE 802.16, no todos los paquetes e incluso todas las porciones de los paquetes serán encriptadas. En el orden de facilitar el ranging y el registro, todos los mensajes de manejo de MAC son enviados sin tráfico. Adicionalmente, los paquetes de datos encriptados contienen una carga útil encriptada con una cabecera no

encriptada. La cabecera MAC PDU no encriptada contendrá información específica de la encriptación tal como un campo de control de encriptación, un campo de secuencia de claves de encriptación y el correspondiente CID. Esta información es utilizada por la BS o la SS receptora para desencriptar la información útil de la MAC PDU. La figura muestra el formato para una MAC PDU encriptada.



Encriptación MAC PDU

b. Protocolo de Manejo de Clave

Todas las SSs de un sistema IEEE 802.16 deben contener un certificado digital X.509 publicado por el fabricante, el cual es utilizado para la autenticación de la SS y el intercambio de clave de autorización inicial. El certificado digital contendrá la clave pública de la SS para encriptar la clave de autorización, y la clave de autorización será usada para la encriptación de los datos subsecuentes y el intercambio de clave. Además de los certificados digitales, todas las SSs tienen par de claves privada/pública RSA instaladas por el fabricante, o lo algoritmos apropiados para generar estas claves automáticamente. El algoritmo de encriptación de clave-pública RSA, y algoritmos simétricos fuertes son utilizados po el protocolo PKM para facilitar el intercambio.

c. Asociaciones de Seguridad

Una Asociación de Seguridad (Security Association, SA) es definida como el grupo de información de seguridad de una BS y una o mas de sus clientes SS en orden de soportar comunicaciones seguras. Al instalar, cada SS establecerá por lo menos una SA con la BS. Con la excepción de las conexiones básica y primaria, todas las nuevas conexiones son enmascaradas a la SA.

BIBLIOGRAFIA

1. LES OWENS, TONY BAUTTS, ERIC OUELLET, CHRISTIAN BARNES, Hack Proofing Your Wireless Network, Primera Edición, Editorial Syngress Publishing
2. NEIL REID, RON SEIDE, 802.11 (Wi-Fi) Manual de Redes Inalámbricas, Primera Edición, Editorial Mc Graw Hill
3. www.IEEE.org
4. http://greco.dit.ump.es
5. www.lpi.usra.edu
6. www.intel.com
7. www.personal.us.es
8. www.personales.unican.es
9. http://bach.gast.it.uc3m.es
10. http://searchnetworking.techtarget.com
11. http://web1.nps.navy.mil
12. www.hsc.fr
13. www.sequans.com
14. http://uk.itronix-europe.com
15. www.cisco.com
16. www.3gamericas.org
17. www.hp.com

18. www.wi-fi.org
19. www.ppgia.pucpr.br
20. www.ece.utexas.edu
21. http://motorola.canopywireless.com