



Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Ingeniería Civil Electrónica

ESTUDIO DE FACTIBILIDAD DE LA PUESTA EN MARCHA DE SERVICIOS DE VoIP SOBRE ENLACES INALAMBRICOS DE LARGA DISTANCIA EN IPv6

Tesis para optar al título de:
Ingeniero Electrónico

Profesor Patrocinante:
Sr. José Mardones Fernández
Ingeniero Electrónico
Licenciado en Ciencias de la Ingeniería

MANUEL ALEJANDRO JARAMILLO ZURITA
RODOLFO ALEXIS MIRALLES HERMOSILLA
VALDIVIA — CHILE
2009

COMISIÓN DE TITULACIÓN

Sr. José Mardones Fernández

Profesor Patrocinante

Sr. Christian Lazo Ramírez

Profesor Informante

Sr. Pedro Rey Clericus

Profesor Informante

Fecha del Examen de Titulación: _____

*A mis amados padres,
Ramiro Miralles y Verónica Hermosilla,
pilares en mi formación de vida.*

Rodolfo Miralles Hermosilla

AGRADECIMIENTOS

Es importante destacar el apoyo y participación de ciertas personas que contribuyeron en el éxito de este trabajo, como lo son principalmente nuestros profesores:

Sr. José Mardones, Profesor Patrocinante, que siempre nos entregó una palabra de ánimo cuando las cosas no marchaban bien, quien confió siempre en nuestro trabajo y tuvo la paciencia de; gestionar los tramites requeridos para la obtención de equipos, materiales, espacios de trabajos y aguantar las presiones de nuestra parte en dichas tareas. Además sumar a esto su constante preocupación por los avances obtenidos en este largo proceso, pese a las imposibilidades profesionales y académicas que lo convocaban.

Sr. Christian Lazo, Profesor Informante, fue quien nos abrió un camino de posibilidades, al ser él quien nos ofreciera el equipamiento necesario para desarrollar nuestro anhelado enlace WiMAX, siempre dispuesto a colaborar tanto en el aspecto teórico como en la facilitación de nuevos equipos requeridos.

Sr. Pedro Rey, Profesor Informante, colaborador constante en un proceso de formación universitaria y trabajo final de titulación. Dispuesto a entregar la ayuda necesaria en todo momento, y contribuir en gestiones administrativas que permitieron acelerar ciertos procesos como lo fue la obtención de equipos necesarios en nuestro trabajo final.

Manuel Jaramillo desea agradecer de forma personal a:

Agradezco primeramente a Dios, por haberme acompañado y guiado a lo largo de esta carrera, por haber sido mi escudo y fortaleza en momentos de debilidad, y por haberme escuchado cada vez que lo he necesitado.

Doy gracias a mis Padres, Manuel y Vivian los cuales siempre me han apoyado durante toda la vida y sobre todo en mi formación universitaria. Por entenderme y tenerme paciencia, habría sido difícil lograr esta meta sin su apoyo incondicional.

A mis dos hermanos Andres y Luis, que siempre me brindaron su ayuda cuando lo necesitaba, por los momentos agradables que me hicieron pasar durante mi etapa estudiantil y el afecto diario que ellos me entregaron.

A mi Amor, Yanina, toda mi gratitud por haberme ayudado seguir adelante, por acompañarme en los buenos y malos momentos, por estar ahí siempre entregándome el amor y comprensión cada día, gracias por compartir esta meta conmigo.

A todos mis amigos y compañeros que compartieron conmigo durante mis años de estudio, por cada uno de los abrazos y palabras de aliento que pude recibir. Por cada momento vivido con Uds. Tardes y noches de estudio, salidas después de clases, o el simple hecho de haber compartido una misma sala de clases con Uds.

Rodolfo Miralles desea agradecer de forma personal a:

Dios, por poner a personas maravillosas en mi camino a lo largo de mi vida como lo son:

Ramiro y Verónica, mis padres, los seres mas importantes en mi vida, que siempre han creído en mi persona y han estado para darme calor, afecto, mucho amor y aliento en momentos que lo he necesitado a través de mi formación estudiantil y de vida.

Mis hermanas Jeniffer y Bárbara, mis guaguas de siempre, cada día de sus vidas me han apoyado y entregado el amor que he necesitado para salir de momentos complicados, muchas veces a su manera, pero como mencioné, de una u otra forma con mucho amor.

Mi “Gustin”, mi sobrino querido, pilar fundamental en este proceso final de titulación, que con una sonrisa de despedida en las mañanas y otra de regreso por la tarde, fue capaz de cambiar mi mundo en 360°, haciendo que cualquier problema se desvaneciera instantáneamente.

Mi Kathyta, mi “Mamol”, mi polola y amiga, mi compañera de cada día, que siempre estuvo alentándome en este periodo de fin de carrera, recordándome que debemos afrontar la vida mirando siempre adelante, con más optimismo y a nunca perder las esperanzas.

Finalmente a mis amigos y amigas de siempre, que me dieron la palabra justa, el abrazo necesario, en el momento preciso, que estuvieron para compartir un momento, una caminata al centro desde la U, una caipirinha, unos choripanes, tardes y noches de estudios, un encuentro en el “ene-ene”, una mesa de pool o un simple cigarro o tasa de café, a todos mis socios, tañes, partners, pelines, colegas, muchas gracias.

ÍNDICE GENERAL

CAPÍTULO I “PROTOCOLO INTERNET VERSION 6”	1
1.1 Antecedentes.....	1
1.1.1 Transición IPv4 a IPv6	3
1.2 Motivos de IPv6	3
1.3 Cabecera IPv6.....	4
1.4 Direccionamiento IPv6	8
1.4.1 Definición de direcciones IPv6.....	8
1.4.2 Notación de direcciones IPv6	9
1.5 Autoconfiguración en IPv6.....	10
1.6 Interoperabilidad entre IPv4 e IPv6.....	11
1.6.1 Técnicas de doble pila (Dual Stack Transition Mechanism, DSTM)	12
1.6.2 Tunneling	15
1.6.3 Mecanismos de traducción.....	17
 CAPÍTULO II “WIMAX (Worldwide Interoperability for Microwave Access)”	 18
2.1 Antecedentes.....	18
2.1.1 Generalidades WiMAX	19
2.2 Propagación NLOS versus LOS	21
2.3 Soluciones de la tecnología NLOS	23
2.3.1 Tecnología OFDM	23
2.3.2 Sub-canalización	24
2.3.3 Antenas para aplicaciones inalámbricas fijas	25
2.3.4 Diversidad en la transmisión y en la recepción	26
2.3.5 Modulación Adaptativa.....	26
2.3.6 Técnicas de corrección de errores.....	27
2.3.7 Control de Potencia.....	27
2.4 Rango de cobertura de WiMAX.....	27
2.5 Topologías para redes WiMAX.....	29
2.6 Uso del espectro	31

2.7 Propagación en WiMAX	31
2.7.1 Modelado de propagación.....	31
2.8 Capas del estándar IEEE 802.16/WiMAX	33
2.8.1 Capa Física (Physical Layer)	34
2.8.1.1 Tamaño del canal.....	34
2.8.1.2 OFDM	34
2.8.1.3 Tamaño de Trama y Símbolo	39
2.8.1.4 Preámbulos	39
2.8.1.5 Unidad de asignación mínima. (MAU) <i>Minimum Allocation Unit</i>	41
2.8.1.6 Diversidad	41
2.8.2 Control de acceso al medio (MAC)	42
2.8.2.1 Cabecera MAC	43
2.8.2.2 Petición de ancho de banda	45
2.8.2.3 Subcapa de convergencia CS	46
2.8.2.4 MAC Common Part Sublayer (MAC CPS)	47
2.8.2.5 Subcapa de seguridad	48
2.8.2.6 Conexiones y flujo de servicio	49
2.8.2.7 Identificadores de conexión <i>Connection Identifiers (CIDs)</i>	49
2.8.2.8 Flujos de servicio <i>Service Flows</i>	50
 CAPÍTULO III “ESTADO DEL ARTE DE LA VOIP”	51
3.1 Antecedentes.....	51
3.1.1 Historia de la red telefónica tradicional	51
3.1.2 Funcionamiento de la red de telefonía tradicional	54
3.2 Generalidades	55
3.2.1 ¿Qué es la VoIP?.....	55
3.2.2 ¿Cómo funciona VoIP?.....	56
3.2.3 Elementos de una red de VoIP	56
3.3 Protocolos de Señalización.....	57
3.3.1 Protocolo H.323	58
3.3.1.1 Descripción del estándar H.323.....	58

3.3.1.2 Componentes de un sistema H.323	59
3.3.1.2.1 Terminal	60
3.3.1.2.2 Gateway	60
3.3.1.2.3 Gatekeeper	61
3.3.1.2.4 MCU Multipoint Control Units	62
3.3.1.3 Establecimiento y control de llamada.....	63
3.3.1.3.1 Inicio de llamadas con H.225.0	63
3.3.1.3.2 Media control H.245	64
3.3.1.3.3 Establecimiento de una llamada con H.225 y H.245.....	65
3.3.2 Protocolo SIP	66
3.3.2.1 Componentes SIP	67
3.3.2.2 Protocolos especificados por SIP	68
3.3.2.2.1 SDP (Session Description Protocol).....	68
3.4 Protocolos de Transporte	70
3.4.1 RTP/RTCP <i>Transmisión de datos durante la llamada</i>	70
3.5 Codecs	72
3.5.1 Waveform codecs	73
3.5.1.1 G.711	73
3.5.1.2 G.722	73
3.5.2 Codificadores mediante vocoders	74
3.5.2.1 G.723.1	75
3.5.2.2 G.728	75
3.5.2.3 G.729	75
3.6 Aspectos importantes de VoIP	76
3.6.1 Seguridad	76
3.6.2 QoS en redes IP	77
3.6.2.1 Retardo	78
3.6.2.1.1 Fuentes de retardo.....	78
3.6.2.2 Jitter	80
3.6.2.3 Eco	81
3.6.2.4 Pérdida de paquetes	82

CAPÍTULO IV “EQUIPOS UTILIZADOS

Y PROPUESTA E IMPLEMENTACIÓN DE ENLACE WIMAX”	84
4.1 Antecedentes.....	84
4.2 Estación Base (BS)	84
4.2.1 Interfaz física	85
4.2.1.1 Interfaz SDA-4S	85
4.2.1.2 Interfaz BSR	86
4.2.2 Interfaz aire	87
4.3 Estaciones Suscriptoras (SS)	88
4.3.1 Interfaz física	89
4.3.2 Interfaz aire	89
4.4 Enlace WiMAX propuesto	91

CAPÍTULO V “CONFIGURACION DE SERVIDOR WIMAX

Y EQUIPOS ABONADOS”	92
5.1 Antecedentes.....	92
5.2 Configuración de la estación base (BS).....	92
5.2.1 Web Page de la estación base (BS).....	92
5.2.2 Configuraciones avanzadas de la BS	93
5.2.2.1 Configuración de enlace de subida.....	93
5.2.2.2 Configuración de enlace de bajada.....	94
5.3 Configuración de los equipos suscriptores CPE.....	95
5.4 Configuración Servidor Netspan	97
5.4.1 Antecedentes	97
5.4.2 Detección de estación base	97
5.4.3 Detección de estaciones suscriptoras (CPE)	99
5.4.4 Configuración de comunicación	99
5.4.4.1 Clase de servicio.....	100
5.4.4.2 Perfil de Estación Suscriptora	101

CAPÍTULO VI “CONECTIVIDAD WIMAX IPV6”	102
6.1 Antecedentes.....	102
6.2 Configuración IPv4 en equipos terminales.....	102
6.3 Conectividad IPv4 (Ping)	104
6.4 Tunnelización IPv6 en IPv4	105
6.4.1 Descripción y configuración del túnel	106
6.4.2 Conectividad IPv6 (Ping).....	107
 CAPÍTULO VII “COMUNICACION VOIP EN IPV6”	 109
7.1 Antecedentes.....	109
7.1.1 Softphone utilizado	109
7.2 Configuración del Softphone.....	109
7.2.1 Configuración PC1	110
7.2.2 Configuración PC2	111
7.3 Pruebas de llamadas	112
7.3.1 Llamadas en IPv4.....	112
7.3.1.1 Llamada de PC1 a PC2.....	113
7.3.1.2 Llamada de PC2 a PC1.....	113
7.3.2 Llamada en IPv6	114
7.3.2.1 Llamada de PC1 a PC2.....	114
7.3.2.2 Llamada de PC2 a PC1.....	114
7.4 Monitoreo por Ethereal.....	115
7.4.1 Monitoreo VoIPv4	115
7.4.2 Monitoreo VoIPv6	118
 CAPÍTULO VIII “PRUEBAS ADICIONALES Y RESULTADOS”	 120
8.1 Antecedentes.....	120
8.2 Comparación de VoIP IPv6 en WiMAX con Ethernet y WiFi	120
8.2.1 Prueba VoIP en Ethernet.....	122
8.2.2 Prueba VoIP en WiFi.....	123
8.3 Prueba de larga distancia WiMAX.....	124

8.3.1 Prueba desde Casino de Miraflores a Puente Cruces (1.34 Km.)	125
8.3.2 Prueba desde Casino de Miraflores a Alto del Cruces (2.6 Km.)	128
8.3.3 Resultados técnicos del enlace.....	130
8.3.4 Balance de potencias.....	132
8.3.4.1 Balance de potencia Uplink.....	133
8.3.4.2 Balance de potencia Downlink.....	136

ÍNDICE DE FIGURAS

Figura 1.1	La cabecera IPv4.....	4
Figura 1.2	Campos modificados y que desaparecen.....	4
Figura 1.3	La cabecera IPv6.....	6
Figura 1.4	Extensiones en IPv6.....	7
Figura 1.5	Arquitectura de capa IP dual y sus tipos de comunicación.....	13
Figura 1.6	Arquitectura de pila dual y sus tipos de comunicación.....	13
Figura 1.7	Perspectivas de una red dual stack.....	14
Figura 1.8	Encapsulación de un paquete IPv6 en un paquete IPv4.....	15
Figura 1.9	Arquitectura de protocolo para tunneling IPv6.....	15
Figura 1.10	Vista lógica de la técnica de tunneling.....	16
Figura 1.11	Configuraciones de tunneling	16
Figura 2.1	Zona Fresnel LOS	21
Figura 2.2	Propagación NLOS	22
Figura 2.3	Localización CPE en NLOS.....	22
Figura 2.4	Portadora única y OFDM.....	24
Figura 2.5	Efecto de sub-canalización.....	25
Figura 2.6	Radios relativos de la célula para la modulación adaptativa.....	26
Figura 2.7	Radio de celda para funcionalidad completa vs. estándar.....	29
Figura 2.8	Topología PMP	30
Figura 2.9	Topología Malla. La BS ya no es el centro, como en el clásico Modo PMP.	30
Figura 2.10	Modelo OSI. En WiMAX/802.16, solo las dos primeras capas son definidas	33
Figura 2.11	Capas del estándar 802.16.....	33
Figura 2.12	Capas del estándar 802.16.....	43
Figura 2.13	Formato MAC PDU	44
Figura 2.14	Formato cabecera genérica MAC (GMH).....	45
Figura 3.1	Conexión directa entre teléfonos remotos.....	51
Figura 3.2	Conexión teléfonos remotos a centralita.....	52

Figura 3.3	Elementos de una red de VoIP	57
Figura 3.4	Pila de protocolo H.323	59
Figura 3.5	Entorno H.323.....	59
Figura 3.6	Funciones del gatekeeper	61
Figura 3.7	Trama H.225.0	63
Figura 3.8	Llamada con H.225 y H.245	65
Figura 3.9	Intercambio de mensajes en SIP	69
Figura 3.10	Trama RTP	71
Figura 3.11	Trama RTCP	72
Figura 3.12	Capas tradicionales de seguridad de la información	76
Figura 3.13	Retardo en códec G729A	79
Figura 3.14	Retardos de códecs.....	80
Figura 4.1	MicroMAX-SOC Base Station Radio (BSR).....	85
Figura 4.2	SDA-4S	85
Figura 4.3	Conexión BSR a SDA-4S	86
Figura 4.4	EasyST	88
Figura 4.5	Arquitectura EasyST	89
Figura 4.6	Arquitectura enlace WiMAX.....	91
Figura 5.1	Acceso a BS vía Web Page	92
Figura 5.2	Host Name e IP de estación base	93
Figura 5.3	Ajuste de frecuencia Uplink del canal	93
Figura 5.4	Configuración Rx (canal Uplink).....	94
Figura 5.5	Ajuste de salida Tx, frecuencia Downlink y bs-id	94
Figura 5.6	Configuración Tx (canal Downlink)	95
Figura 5.7	Configuración IP de CPE EasyST.....	95
Figura 5.8	Ajuste de canal de CPE	96
Figura 5.9	Ingreso de bs-id en CPE	96
Figura 5.10	Parámetros de señal de CPE.....	96
Figura 5.11	Descubrimiento de estación base	98

Figura 5.12	Estación base descubierta.....	98
Figura 5.13	Administrador de estación base	99
Figura 5.14	Equipos CPE registrados.....	99
Figura 5.15	Editor de Clase de Servicio	100
Figura 5.16	Configuración de Flujos de Servicios	100
Figura 5.17	Perfil de configuración de estaciones suscriptoras.....	101
Figura 6.1	Propiedades Conexión área local para IPv4.....	103
Figura 6.2	Configuración IP equipos terminales	104
Figura 6.3	Ping desde 192.168.1.5 a 192.168.1.6	105
Figura 6.4	Ping desde 192.168.1.6 a 192.168.1.5	105
Figura 6.5	Ping desde 2001:10:10::1 a 2001:10:10::2.....	108
Figura 6.6	Ping desde 2001:10:10::2 a 2001:10:10::1.....	108
Figura 7.1	Apariencia de Eyebeam.....	110
Figura 7.2	Propiedades de cuenta SIP	110
Figura 7.3	Configuración de puertos	111
Figura 7.4	Modo Peer to Peer.....	111
Figura 7.5	Propiedades de cuenta SIP PC1	112
Figura 7.6	Softphone listo para usar PC1	112
Figura 7.7	Propiedades de cuenta SIP PC2	112
Figura 7.8	Softphone listo para usar PC2	112
Figura 7.9	Llamada entrante en PC2	113
Figura 7.10	Llamada contestada en PC2	113
Figura 7.11	Llamada entrante en PC1	113
Figura 7.12	Llamada contestada en PC1	113
Figura 7.13	Llamada entrante en PC2	114
Figura 7.14	Llamada contestada en PC2	114
Figura 7.15	Llamada entrante en PC1	114
Figura 7.16	Llamada contestada en PC1	114
Figura 7.17	Paquetes IPv4 monitoreados de PC1 a PC2 (inicio de llamada).....	115

Figura 7.18	Paquetes IPv4 monitoreados de PC1 a PC2 (fin de llamada)	116
Figura 7.19	Diagrama de flujo VoIPv4 entre PC1 y PC2	116
Figura 7.20	Paquetes IPv4 monitoreados de PC2 a PC1 (inicio de llamada).....	117
Figura 7.21	Paquetes IPv4 monitoreados de PC2 a PC1 (fin de llamada)	117
Figura 7.22	Diagrama de flujo VoIPv4 entre PC2 y PC1	118
Figura 7.23	Diagrama de flujo VoIPv6 entre PC1 y PC2	118
Figura 7.24	Paquetes IPv6 monitoreados de PC1 a PC2 (inicio y fin de llamada)	119
Figura 7.25	Paquetes IPv6 monitoreados de PC2 a PC1 (inicio y fin de llamada)	119
Figura 7.26	Diagrama de flujo VoIPv6 entre PC2 y PC1	119
Figura 8.1	Direcciones IPv6 de PC1	121
Figura 8.2	Conexión VoIP Ethernet IPv6 nativo.....	122
Figura 8.3	Conexión VoIP WiFi IPv6 nativo (100 mts. Aprox.)	122
Figura 8.4	Ping por Ethernet desde PC1 a PC2.....	122
Figura 8.5	Captura de paquetes en llamada Ethernet desde PC1 a PC2.....	123
Figura 8.6	Ping por WiFi desde PC1 a PC2	123
Figura 8.7	Captura de paquetes en llamada WiFi desde PC1 a PC2	124
Figura 8.8	Distancia entre Casino Miraflores al Puente Cruces.....	127
Figura 8.9	Distancia entre Casino Miraflores a Altos del Cruces	129
Figura 8.10	CPE PC1 (NLOS)	130
Figura 8.11	CPE PC2 (NLOS)	131
Figura 8.12	Absorción atmosférica de las ondas electromagnéticas	135
Figura 8.13	Diagrama balance potencias Uplink.....	135
Figura 8.14	Diagrama balance potencias Downlink.....	137
Figura A1.1	Monitoreo de paquetes SNMP entre servidor Netspan y BS	143
Figura A2.1	Opción modo Ad-Hoc	144
Figura A2.2	Nombre y seguridad de Red	145
Figura A2.3	Red Ad-Hoc detectada	145

Figura A3.1	Panel de antena.....	146
Figura A3.2	Vista frontal de antena.....	146

ÍNDICE DE FOTOGRAFÍAS

Fotografía 8.1	BS instalada, vista 1.....	125
Fotografía 8.2	BS instalada, vista 2.....	125
Fotografía 8.3	Orientación de la antena.....	126
Fotografía 8.4	Prueba 1 en terreno, vista 1.....	128
Fotografía 8.5	Prueba 1 en terreno, vista 2.....	128
Fotografía 8.6	Prueba 2 en terreno	128
Fotografía 8.7	Prueba 3 en terreno	130

ÍNDICE DE TABLAS

Tabla 1.1	Ejemplo de direcciones IPv6.....	9
Tabla 2.1	Características de WiMAX.....	20
Tabla 2.2	Ejemplo Estación Base de características completa vs. características estándar	28
Tabla 2.3	Tamaños de bloque y las velocidades de código usadas para diferentes modulaciones y velocidad de código.....	39
Tabla 3.1	Puntos débiles y ataques que afectan a cada una de las capas.....	77
Tabla 4.1	Frecuencias de operación y métodos duplex BSR	87
Tabla 4.2	Modulaciones y FEC	87
Tabla 4.3	Potencia máxima de transmisión BSR	87
Tabla 4.4	Niveles de sensibilidad y CINR en BSR.....	88
Tabla 4.5	Frecuencias de operación y métodos duplex EasyST.....	90
Tabla 4.6	Modulaciones y FEC EasyST.....	90
Tabla 4.7	Potencia Tx EasyST según modulación	90
Tabla 4.8	Niveles de sensibilidad y C/I + n en EasyST	91
Tabla 6.1	Identificadores IPv4 para los dispositivos en la red	102
Tabla 6.2	Resumen direcciones IPv4 e IPv6 equipos finales	108
Tabla 7.1	Direcciones IP de cada PC	112
Tabla 7.2	Direcciones IPv6 de ambos PC	114
Tabla 8.1	IPv6 de ambos portátiles	121
Tabla 8.2	Parámetros de señal para diferentes condiciones de propagación.....	132
Tabla A3.1	Características de la antena.....	146

RESUMEN

El presente trabajo de titulación, comprende el estudio de la posible implantación de servicios de voz sobre IP, en enlaces inalámbricos de larga distancia a través del protocolo IPv6, sucesor del protocolo universalmente usado IPv4. Partiendo de esta premisa, nace la primera necesidad, encontrar una solución de tipo inalámbrica que abarque grandes distancias, fue así como aparece el estándar IEEE 802.16, WiMAX, la base en que se desarrollo este trabajo.

El objetivo es contar con los fundamentos teóricos que nos permitan configurar de forma correcta equipos WiMAX, para así poder establecer una llamada de voz sobre IP entre dos computadores configurados en IPv6, de esta manera fue que se inició el proceso con el estudio de los protocolos involucrados, como lo son IPv6, WiMAX y VoIP, bases para realizar nuestro enlace.

La necesidad de trabajar con equipamiento de gran envergadura, alejados de nuestro alcance, nos llevo a buscar más de una alternativa de distribuidores de equipos y servicios WiMAX, presentándose finalmente la posibilidad de trabajar con una estación base (BS) y estaciones suscriptores (SS) pertenecientes a la empresa Telefónica del Sur, distribuidos por la empresa Airspan. Fue así como arrancó el proceso práctico, con la configuración de dichos equipos, manejados en conjunto por el software Netspan distribuido por la misma empresa, donde se definieron parámetros de frecuencias, canales, QoS, modulaciones y potencias requeridas para establecer comunicación.

Posteriormente se realizaron las configuraciones necesarias en los equipos finales, asignación de direcciones IP según protocolo IPv6, instalación y configuraciones del softphone para establecer comunicación por voz, la cual se comprobó en primera instancia dentro del laboratorio de comunicaciones modernas del instituto de electricidad y electrónica, y posteriormente en una prueba de larga distancia comprendiendo 2,6 Km. desde el Casino de Miraflores de la UACH, hasta el condominio Alto del Cruces, obteniendo resultados satisfactorios, dando viabilidad al estudio planteado en un comienzo y dejando abierta la posibilidad de estudios o trabajos posteriores en estas tecnologías.

ABSTRACT

This job title includes the study of the possible deployment of voice over IP, wireless links in long-distance via the IPv6 protocol, the successor to the IPv4 protocol used universally. On this premise, births the need, to find a solution that encompasses Wireless long distances, and that was how the standard appears IEEE 802.16, WiMAX , the base on which this work developed.

The aim is to provide the theoretical foundations that allow us to set up correctly WiMAX equipment, in order to establish a voice call over IP between two computers configured in IPv6, this way the process was initiated with the study of protocols involved, such as IPv6, VoIP and WiMAX, bases for our link.

The need to work with major equipment, out of our reach, led us to search more than one alternate distributor of WiMAX equipment and services, when finally the possibility presented to work with a base station (BS) and subscriber stations (SS) belonging to the company Telefónica del Sur, distributed by the Airspan enterprise. That was how the practical process started with the configuration of such equipment, operated jointly by the Netspan software distributed by the same company, which defines parameters of frequency channels, QoS, modulation and power required to establish communication.

Subsequently the necessary configurations where made on the final of IP addresses under IPv6 protocol, installation and configuration of the softphone to establish voice communication, which was tested primarily in the laboratory of the institute of modern communications and power electronics, and later on a long distance test of 2.6 kms from UACH's Miraflores Casino to the Altas cruces condos , obtaining satisfactory results, giving the feasibility to the study proposed at the beginning and leaving open the possibility of study or further work on these technologies.

INTRODUCCIÓN

La comunicación es un elemento indispensable para el hombre dada a su condición eminentemente social, la cual se manifiesta desde los inicios de éste. Con el transcurso del tiempo, los avances tecnológicos en redes de comunicaciones son uno de los que han obtenido un mayor avance, desde la creación del telégrafo, hasta la comunicación de voz sobre IP en la actualidad.

Nos encontramos en una búsqueda constante por mejorar esta comunicación, tratando de hallar los métodos que permitan cada día optimizar los sistemas de audio y sean capaces de brindar mayores prestaciones a los usuarios finales. Para lograr estos objetivos, se debe llevar de la mano la optimización de las arquitecturas usadas comúnmente, desplazando de poco las conexiones en base a hilos de cobre, por infraestructuras mas reducidas, de tipo inalámbrica con mayores áreas de cobertura. De esta manera, se hace indispensable la integración de estándares que hagan posible dicha comunicación de voz de forma inalámbrica de gran cobertura.

Es así como en nuestro caso, se fija el objetivo de lograr una comunicación de VoIP de larga distancia en IPv6 de forma inalámbrica. De acuerdo a esto, que mejor candidato para lograrlo que el estándar 802.16 WiMAX, capaz de ofrecer todos los requisitos necesarios para lograr dicha meta, posibilitando independencia de protocolos, QoS, configuración de frecuencias, de canales, de modulaciones, etc.

La solución a estas necesidades se aprecia a lo largo de este trabajo, en el cual se describirá teóricamente los estándares y protocolos utilizados, mostrando el procedimiento necesario para poder realizar la comunicación ya mencionada, como las configuraciones de softwares y hardwares, el conocimiento de las características técnicas de los equipos y los resultados obtenidos en la conectividad IPv6, y posterior prueba de llamadas de VoIP realizadas bajo el mismo protocolo, utilizando WiMAX como medio físico de transmisión.

CAPÍTULO I

PROTOCOLO INTERNET VERSION 6

1.1 Antecedentes

Dentro de las redes de comunicaciones actuales, podemos diferenciar entre las redes por conmutación de circuitos, donde la comunicación entre emisor y receptor se establece por medio de un circuito dedicado durante el tiempo en que se desarrolle ésta, y las redes de datos, basadas en la conmutación de paquetes.

Cuando se envían datos por conmutación de paquetes, los datos que se van a transmitir se dividen en paquetes de datos (esto se denomina segmentación) y se envían por separado a través de la red. Los nodos de la red pueden determinar libremente la ruta de cada paquete de manera individual, según su tabla de enrutamiento. Los paquetes que se envían de esta manera pueden tomar diferentes rutas y se vuelven a reensamblar una vez que llegan al nodo receptor. En este caso, los paquetes pueden llegar en un orden distinto del que fueron enviados y se pueden perder. Por esta razón, ciertos mecanismos se arman en paquetes para que se puedan reorganizar de ser necesario o volver a enviar si los paquetes se pierden.

Éste es el método de transferencia utilizado en Internet, el cual sigue un conjunto de protocolos y estándares para llevar a cabo dicha comunicación. Dentro de los mas esenciales, está la familia de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable, también conocido del mejor esfuerzo (best effort), es decir, no ofrece calidad de servicio o QoS. IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) llamado número IP, que actúa a modo de número de teléfono único como por ejemplo 80.123.234.111 dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar al reconectar; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Por otra parte, en la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de Internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe: libre de errores, sin pérdidas y con seguridad.

1.1.1 Transición IPv4 a IPv6

La actual generación de protocolo IP es IPv4, donde las direcciones constan de cuatro octetos. Para facilitar la conversación humana, el protocolo de direcciones IP están representados en forma de números separados por puntos, por ejemplo: 166.74.110.83, donde el número decimal es una abreviatura y corresponde a el código binario descrito por el byte en cuestión (número toma un valor entre el rango 0-255).

El protocolo Internet versión 6 (IPv6) o también conocido como IPng (IP Next Generation, en español, protocolo de Internet de la próxima generación) es un nuevo conjunto de protocolos estándar para la capa de red de Internet. IPv6 está diseñado para resolver numerosos problemas que presenta la versión actual, relacionados con la reducción de direcciones, la seguridad, la configuración automática y la extensibilidad, entre otras. IPv6 expande las capacidades de Internet para habilitar nuevos tipos de aplicaciones, entre las que se incluyen las aplicaciones móviles y de punto a punto.

Este nuevo conjunto de protocolos debe satisfacer los siguientes requisitos básicos:

- Enrutamiento a gran escala y direcciones con baja sobrecarga.
- Configuración automática para varias situaciones de conexión.
- Confidencialidad y autenticación integrada.

1.2 Motivos de IPv6

El protocolo IPv6 responde razonablemente a los objetivos fijados. Conserva las mejores funciones de IPv4, mientras que elimina o minimiza las peores y agrega nuevas cuando es necesario.

La principal innovación de IPv6 es el uso de direcciones más extensas que con IPv4, codificadas con 16 bytes, resolviendo el problema de brindar un conjunto limitado de direcciones de Internet. Llevado a números, podemos apreciar que IPv4 puede admitir $2^{32}=4,29 \cdot 10^9$ direcciones mientras

que IPv6 $2^{128}=3,4\cdot10^{38}$ direcciones. Además se ha desarrollado una simplificación de los encabezados de los datagramas. El encabezado del datagrama IPv6 básico contiene sólo 8 campos (a diferencia de los 12 de IPv4). Este cambio permite que los routers procesen datagramas de manera más rápida y mejore la velocidad en general. Por otra parte, IPv6 brinda más seguridad. La autenticación y confidencialidad constituyen las funciones de seguridad más importantes del protocolo IPv6. Finalmente, se ha prestado más atención que antes a los tipos de servicios. Si bien el campo Type of services (Tipo de servicios) en el datagrama IPv4 se utiliza pocas veces, el esperado aumento del tráfico multimedia en el futuro demanda que se le otorgue mayor importancia.

1.3 Cabecera IPv6

Para explicar las diferencias entre un datagrama IPv6 y un IPv4, se muestra en la Figura 1.1 la cabecera de un paquete IPv4, en la que por medio de su color de fondo como se ve en la Figura 1.2, se indican los campos que desaparecen y los que son modificados en IPv6.

bits:	4	8	16	20	32
Versión	Cabecera	TOS	Longitud Total		
Identificación			Indicador	Desplazamiento de Fragmentación	
TTL		Protocolo	Checksum		
Dirección Fuente de 32 bits					
Dirección Destino de 32 bits					
Opciones					

Figura 1.1 La cabecera IPv4

Campo Modificado
Campo que Desaparece

Figura 1.2 Campos modificados y que desaparecen

Como vemos la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones que dependen de cada caso.

El motivo fundamental por el cual los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera. Otros mecanismos de encapsulado ya realizan esta función como IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc. El caso del campo de “Desplazamiento de Fragmentación”, es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total “inutilidad” de este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

- **Longitud total: longitud de carga útil (payload length)** que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
- **Protocolo: siguiente cabecera (next header)**, dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
- **Tiempo de vida: límite de saltos (Hop Limit)**. Tiene una longitud de 8 bits (1 byte), equivalente al campo TTL de IPv4, donde el máximo número de saltos especificables es 255.
- **Dirección Fuente:** tiene una longitud de 128 bits (16 Bytes) para especificar la IPv6 del nodo fuente.
- **Dirección Destino:** tiene una longitud de 128 bits (16 Bytes) para especificar la IPv6 del nodo destino.

Los nuevos campos son:

- **Clase de Tráfico (Traffic Class)**, también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- **Etiqueta de Flujo (Flow Label)**, para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el formato como indica la Figura 1.3.

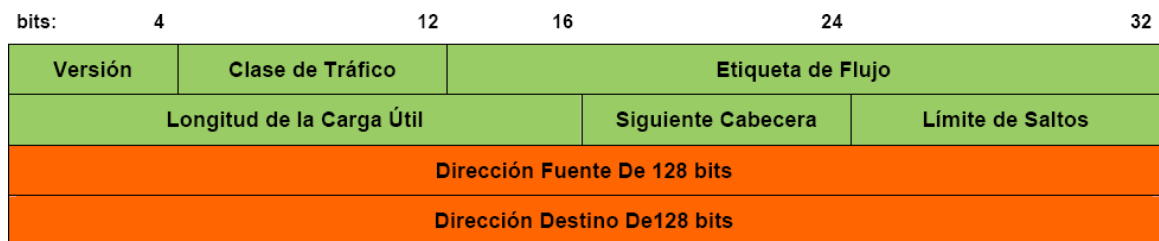


Figura 1.3 La cabecera IPv6

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.

La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes. Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en encaminadores y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin ayuda, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo “siguiente cabecera”, indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destinos finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso “salto a salto” (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, deben de ser procesadas en el orden riguroso en que aparecen en el paquete.

En la Figura 1.4 podemos apreciar algunos ejemplos gráficos del uso del concepto de las “cabeceras de extensión” (definidas por el campo “siguiente cabecera”), mecanismo por el que cada cabecera es “encadenada” a la siguiente y anterior (en caso de existir):

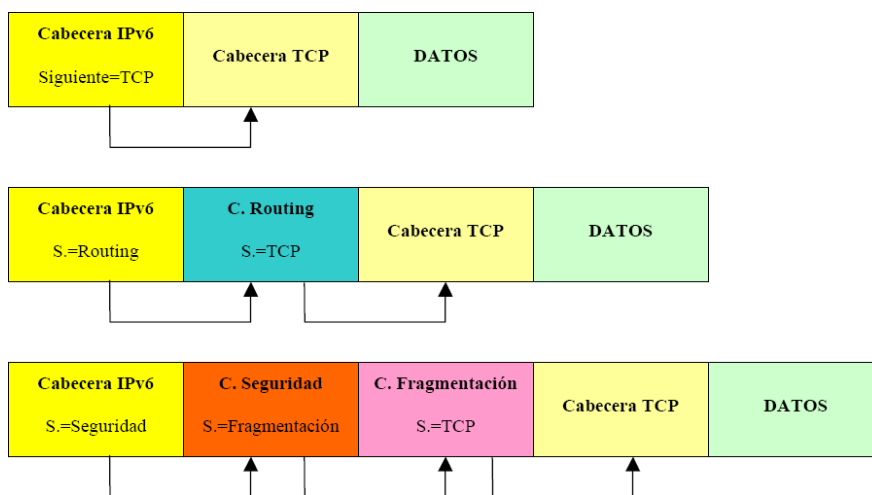


Figura 1.4 Extensiones en IPv6

El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de

cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

Dado que IPv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo de su propio mecanismo de checksum.

1.4 Direccionamiento IPv6

1.4.1 Definición de direcciones IPv6

Como hemos comentado anteriormente, las direcciones IPv6 son identificadores de 128 bits de longitud. Identifican interfaces de red (ya sea de forma individual o grupos de interfaces). A una misma interfaces de un nodo se le pueden asignar múltiples direcciones IPv6. Dichas direcciones se clasifican en tres tipos:

- **Unicast:** Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.
- **Anycast:** Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la que este más “cerca”). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera “cae”.
- **Multicast:** Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

1.4.2 Notación de direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

X : X : X : X : X : X : X : X

Donde “X” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPv6.

La Tabla 1.1 muestra algunos ejemplos de direcciones IPv6:

Formato extendido	Formato abreviado	Tipo de Dirección
1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A	(una dirección unicast)
FF01:0:0:0:0:0:0:101	FF01::101	(una dirección multicast)
0:0:0:0:0:0:0:1	::1	(la dirección loopback)
0:0:0:0:0:0:0:0	::	(dirección no especificada)

Tabla 1.1 Ejemplo de direcciones IPv6

La representación de los prefijos IPv6 tiene un formato: ***dirección IPv6/longitud del prefijo***

Donde:

- ***Dirección IPv6:*** es una dirección IPv6 en cualquiera de las notaciones válidas
- ***Longitud del prefijo:*** valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

12AB:0:0:CD30:123:4567:89AB:CDEF/60

1.5 Autoconfiguración en IPv6

La autoconfiguración es el conjunto de pasos por los cuales un Host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es "Plug & Play".

El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración "stateless" (sin intervención), no requiere ninguna configuración manual del Host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un Host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos

que identifican la subred (o subredes) asociadas con el enlace, mientras el Host genera un "identificador de interfaz", que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de un router, el Host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración "stateful" (predeterminada), el Host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada Host.

Ambos tipos de autoconfiguración (stateless y stateful), se complementan. Un Host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración "sin intervención" se emplea cuando no importa la dirección exacta que se asigna a un Host, sino tan sólo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada Host tiene una determinada dirección, asignada manualmente.

La autoconfiguración esta diseñada para Hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que "aprobar" el algoritmo de detección de direcciones duplicadas.

1.6 Interoperabilidad entre IPv4 e IPv6

Las organizaciones con redes IPv4 existentes han de enfrentarse al reto de identificar el impacto del cambio, planificar la transición y poner en práctica la migración a IPv6. Cuando hablamos de migración nos estamos refiriendo a redes únicamente IPv4 a las que se van añadiendo o solapando nodos IPv6 en el transcurso del tiempo hasta conformar una red exclusivamente IPv6,

o más comúnmente, una red IPv6 que siga soportando IPv4. A continuación trataremos de abordar las tecnologías y estrategias de migración que pueden emplearse.

- **Pila dual (dual stack):** soporte conjunto de IPv4 e IPv6 en cada dispositivo de red.
- **Tunneling:** encapsulación de un paquete IPv6 en un paquete IPv4 para ser transmitido sobre una red IPv4.
- **Traducción:** traducción de direcciones de red o puertos por medio de un dispositivo gateway o mediante un código de traducción TCP/IP en los Hosts y routers, que permitan comunicar nodos IPv6-only con nodos IPv4-only.

1.6.1 Técnicas de doble pila (Dual Stack Transition Mechanism, DSTM)

La solución de pila dual (RFC 2893), a la que a partir de ahora nos referiremos mediante su nombre original en inglés, dual stack, consiste en implementar ambas pilas de protocolos, IPv4 e IPv6, en los dispositivos que requieran acceso a las capa de red de ambas tecnologías, incluidos routers, dispositivos de usuario final o cualquier otro nodo de la infraestructura de red. Tales dispositivos serán configurados tanto con direcciones IPv4 como con direcciones IPv6 y podrán obtener estas direcciones por medio de cualquier método previsto por los respectivos protocolos y siempre que el administrador o administradores los hayan habilitado. Por ejemplo, una dirección IPv4 podría obtenerse vía DHCP mientras que la dirección IPv6 puede ser obtenida aprovechando los mecanismos de autoconfiguración del nuevo protocolo; esto es, no sería necesario que las direcciones IPv4 e IPv6 se obtengan mediante un mecanismo común como la asignación estática.

Existe una nomenclatura tipificada para referirse a los nodos en función de qué pilas de protocolos soportan. Un nodo que sólo soporte IPv4 se caracteriza como IPv4-only. De modo análogo un nodo que sólo soporte IPv6 será referido como IPv6-only. Cuando decimos que un nodo es IPv4 estamos indicando que o bien es IPv4-only o bien es un nodo dual IPv6/IPv4 compatible con IPv4. Por otra parte, cuando hablamos de un nodo IPv6 apuntamos a un nodo que o bien es IPv6-only o se trata de una nodo dual IPv6/IPv4 compatible con IPv6.

Aunque el enfoque sea dual stack, éste puede variar en función de qué partes de la pila de protocolos son compartidas y cuáles son independientes para cada versión de IP. Lo ideal sería que sólo la capa de red estuviese duplicada y que las demás capas fuesen compartidas (arquitectura de capa IP dual; véase Figura 1.5), sin embargo existen arquitecturas que dualizan la capa de red y la de transporte (arquitectura de pila dual generalizada; véase Figura 1.6), por lo que en algunos casos los administradores han de aplicar configuración redundante para cada pila. En la mitad derecha de las Figuras 1.5 y 1.6 la flecha azul intermedia corresponde a paquetes IPv6 encapsulados en una cabecera IPv4, técnica denominada tunneling que veremos posteriormente. En términos generales, la aproximación dual stack no requiere necesariamente la creación de túneles, mientras que para crear túneles es imprescindible una aproximación dual stack. Aunque lo normal es que un nodo IPv6/IPv4 implemente ambas tecnologías.

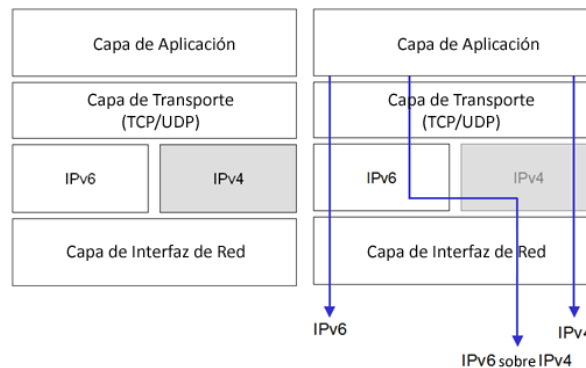


Figura 1.5 Arquitectura de capa IP dual y sus tipos de comunicación

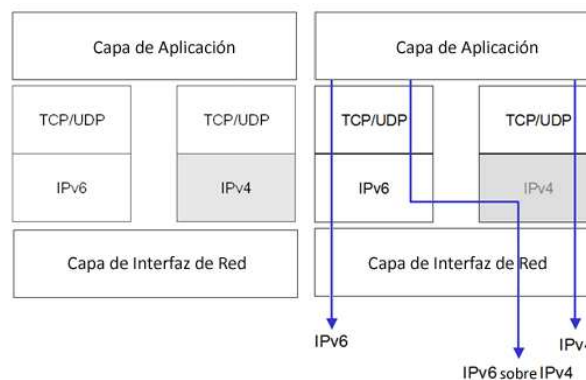


Figura 1.6 Arquitectura de pila dual y sus tipos de comunicación

Otros diseños pueden incluso extender la dualidad hasta la capa de Host a red, mediante dos interfaces de red diferentes, una para IPv6 y otra para IPv4. Aunque esta solución es contraria en gran medida a los beneficios de un modelo estructurado en capas, puede resultar deseable especialmente en servidores de red con múltiples aplicaciones o servicios, cuando muchos de ellos soportan sólo una u otra versión pero no ambas. La implantación más frecuente de dispositivos con dual stack compartiendo una interfaz de red común supone que tanto IPv4 como IPv6 operan sobre el mismo enlace físico. De hecho, Ethernet y otras tecnologías de capa de enlace soportan ambos tipos de carga de datos. Se requiere además que los routers que soportan estos enlaces también sean de tipo dual stack. La Figura 1.7 muestra este enfoque. El diagrama puede extenderse más allá de una LAN física a una red multipunto donde los routers soporten, como ya dijimos, tanto IPv4 como IPv6 y encaminen los paquetes IPv4 entre hosts nativos IPv4 y los paquetes IPv6 entre los Hosts compatibles con IPv6.

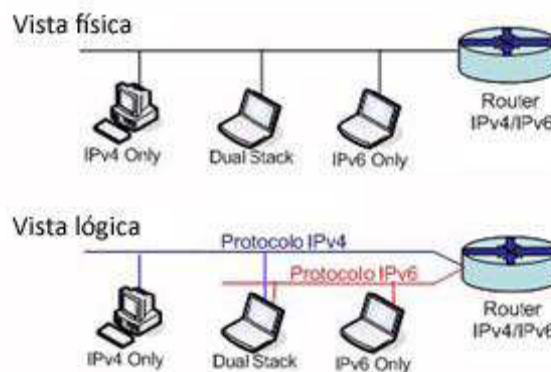


Figura 1.7 Perspectivas de una red dual stack

La desventaja de la técnica de dual stack es que es necesaria una actualización completa del software de red para poder ejecutar las dos versiones del protocolo. Esto se traduce en que hay que mantener la configuración y todas las tablas (como por ejemplo, las tablas de enrutamiento) dualizadas. Desde el punto de vista del administrador de red, significará tener comandos separados para las mismas funciones dependiendo del protocolo (por ejemplo, ping.exe para IPv4 y ping6.exe para IPv6 en un Host con sistema operativo de Microsoft, con distintos parámetros para cada comando) y resulta evidente que requerirá mayor capacidad de cómputo y de memoria para conseguir el mismo rendimiento que en redes con un solo protocolo.

1.6.2 Tunneling

El tunneling consiste en usar la infraestructura de transporte IPv4 existente para encapsular paquetes IPv6, es decir, utiliza la infraestructura IPv4 para proporcionar conectividad IPv6 básica. Esta encapsulación de paquetes IPv6 en paquetes IPv4 (rellenando el campo ID de tipo de protocolo con el valor 41) se ilustra en la Figura 1.8.

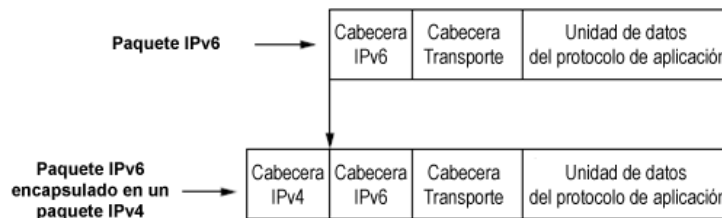


Figura 1.8 Encapsulación de un paquete IPv6 en un paquete IPv4

La técnica de tunneling funciona tal y como ilustra las Figura 1.9 y 1.10, los puntos de salida de las redes enlazadas encapsulan paquetes IPv6, para los destinos IPv6 especificados, a través de las interfaces IPv4. Los paquetes fluyen normalmente por el sistema de ruteo IPv4 y son desencapsulados en el otro extremo del túnel, siendo el paquete IPv6 enviado al Host correcto mediante el sistema de ruteo IPv6. Se han definido distintos métodos para determinar el punto final del túnel. El RFC 2893 distingue entre configuraciones estáticas en los sistemas de encapsulación/desencapsulación y técnicas de tunneling automáticas dependientes de formas especiales de direccionamiento IPv6.

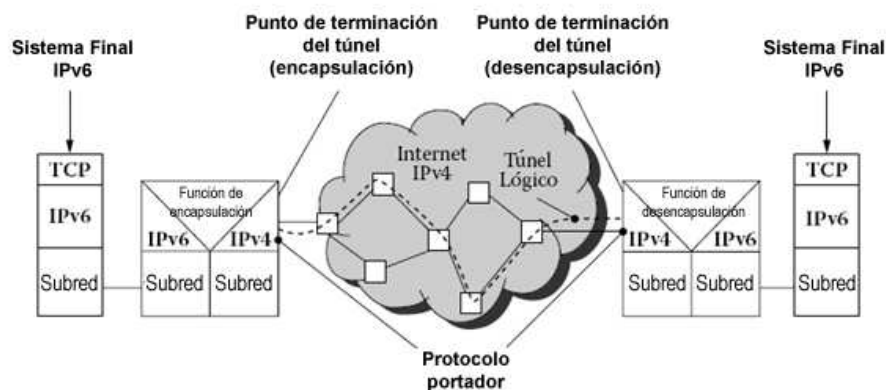


Figura 1.9 Arquitectura de protocolo para tunneling IPv6

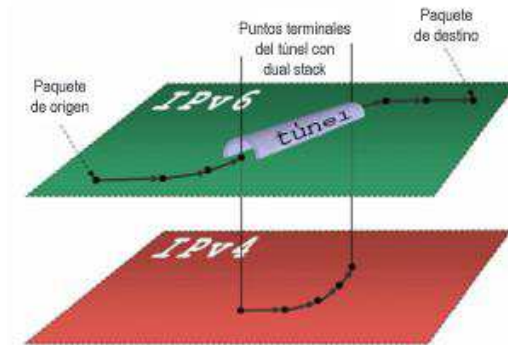


Figura 1.10 Vista lógica de la técnica de tunneling

Para el tunneling de IPv6 sobre IPv4 la MTU IPv6 (Maximum Transmission Unit) es típicamente inferior en 20 octetos con respecto a la MTU IPv4. Sin embargo, si la MTU IPv4 no se almacena para cada túnel, habrá casos en que el paquete IPv4 tenga que ser fragmentado en algún router IPv4 intermedio. En este caso, los paquetes IPv6 encapsulados en IPv4 deben enviarse con el flag *Don't Fragment* puesto a 0 en la cabecera IPv4.

El RFC 2893 define las siguientes configuraciones de tunneling con tráfico IPv6 entre nodos IPv6/IPv4 sobre una infraestructura IPv4 visualizándolas en la Figura 1.11.

- Router a Router
- Host a Router o Router a Host
- Host a Host.

Router-to-router Interconexión de islas IPv6 a través de redes IPv4	
Host-to-Router Útil para conectar sistemas IPv6 aislados (i.e. sin routers IPv6 locales)	
Host-to-Host Sistemas IPv6 aislados	
Router-to-Host Sistema destino sin router IPv6 local	

Figura 1.11 Configuraciones de tunneling

Hay que advertir que IPv6 sobre IPv4 sólo describe la encapsulación de paquetes IPv6 en la cabecera IPv4 de manera que los nodos IPv6 resulten alcanzables mediante la infraestructura IPv4 existente. A diferencia de lo que ocurre con el protocolo PPTP (Point-to-Point Tunneling Protocol) y el protocolo L2TP (Layer Two Tunneling Protocol), no se producen intercambios de mensajes para configurar el túnel, ni para mantenimiento o terminación del mismo. El tunneling IPv6 sobre IPv4 tampoco proporciona entrega segura para los paquetes IPv6 encapsulados.

1.6.3 Mecanismos de traducción

Los mecanismos de traducción se basan en traducir los encabezados de los paquetes de una versión de IP a la otra y viceversa, es decir, se ha de usar en la comunicación entre Host IPv6-only y Host IPv4-only. Sin embargo, los mecanismos de traducción han tenido menos éxito y no son los más aconsejados por los organismos impulsores de IPv6.

Dentro de estos mecanismos podemos identificar:

- SIIT (Stateless Internet Protocol/Internet Control Messaging Protocol Translation).
- BIS (Bump In the Stack).
- BIA (Bump In the API).
- NAT-PT (Network Address Translation – Protocol Translation).
- TRT (Transport Relay Translator).

CAPÍTULO II

WIMAX (Worldwide Interoperability for Microwave Access)

2.1 Antecedentes

Durante los últimos años se han creado expectativas y realidades entorno al acceso de banda ancha de última milla. El cableado representa altos costos de instalación que no siempre justifican su tendido hasta áreas rurales o geográficamente inaccesibles. Llevar servicios ADSL a estas áreas no es económicamente efectivo para los operadores de telefonía. El operador de cable tradicional aún se encuentra en el proceso de transición hacia el transporte de datos. La tecnología celular, presente (UMTS), sólo permite tasas de velocidad limitadas.

Estas y otras limitaciones tecnológicas y topográficas, asociadas a la rápida adopción del acceso a Internet, han motivado el desarrollo de un estándar inalámbrico llamado WiMax (Worldwide Interoperability for Microwave Access) que llegue a un mayor número de usuarios y propicie la introducción de nuevos y mejores servicios de telecomunicaciones.

WiMAX es un concepto parecido a WiFi, pero cualitativamente diferente como veremos por sus características, no sólo por conseguir mayores coberturas y tasa binaria de transmisión. WiFi, comprendida en la familia de estándares 802.11, fue diseñada para ambientes inalámbricos internos como una alternativa al cableado estructurado de redes y con capacidad sin línea de vista (NLOS, por sus siglas en inglés) de muy pocos metros.

2.1.1 Generalidades WiMAX

En Abril de 2003, el IEEE aprobó el estándar 802.16a, el cual cubre bandas de frecuencias entre 2 GHz y 11 GHz. Este estándar es una extensión del estándar IEEE 802.16 para 10-66 GHz publicado en Abril de 2002. Este subrango de frecuencias en 11 GHz permite el desempeño de enlaces sin línea de vista, haciendo al IEEE802.16a la tecnología apropiada para aplicaciones de última milla donde los obstáculos como árboles y edificios están siempre presentes y en donde las estaciones bases pueden necesitar ser montadas sin discreciones en los techos de viviendas o edificios en vez de en torres o montañas.

La configuración más común 802.16a consiste en una estación base montada en un edificio o torre que comunica en configuración punto-multipunto a abonados ubicados en oficinas u hogares. El 802.16a posee un rango de hasta 48 Km. con celdas típicas de 6.5 a 9.5 Km.

Con datos compartidos de hasta 75 Mbps, un “sector” simple de una estación base 802.16a, donde un sector es definido como un par simple de radios transmisor/receptor en la estación base, provee suficiente tasa binaria de transmisión para soportar simultáneamente 60 puntos de negocio con conectividad nivel T1 y cientos de hogares con conectividad nivel DSL, usando canales de 20 MHz. de ancho de banda.

Para soportar un modelo de negocio rentable, los operadores y proveedores de servicio necesitan sostener una mezcla de abonados de alto nivel de ingresos y un alto volumen de abonados residenciales. El 802.16a ayuda a satisfacer este requerimiento mediante el soporte de niveles de servicio diferenciados, los cuales pueden incluir servicios de nivel T1 garantizados para negocios, o servicios DSL ‘best effort’ para usuarios residenciales.

La especificación 802.16 también incluye funciones de seguridad robustas y la Calidad de Servicio (QoS) necesaria para soportar servicios que requieren baja latencia como video y voz.

El servicio de voz 802.16 puede ser el tradicional TDM o voz sobre IP (VoIP).

La Tabla 2.1 resume las principales características de esta tecnología inalámbrica:

Características	Descripción
Sin Línea de Vista (NLOS)	No necesita línea de visión entre la antena y el equipo del suscriptor
Modulación OFDM (Orthogonal Frequency Division Multiplexing)	Permite la transmisión simultánea de múltiples señales a través de cable o aire en diversas frecuencias; usa espaciamiento ortogonal de las frecuencias para prevenir interferencias.
Antenas inteligentes	Soporta mecanismos de mejora de eficacia espectral en redes inalámbricas y diversidad de antenas
Topología punto-multipunto y de malla (mesh)	Soporta dos topologías de red, servicio de distribución multipunto y la malla para comunicación entre suscriptores.
Calidad de Servicio (QoS)	Califica la operación NLOS sin que la señal se distorsione severamente por la existencia de edificios, por las condiciones climáticas ni el movimiento vehicular.
FDM (Frequency Division Multiplexing) y TDM (Time Division Multiplexing)	Tipos de multiplexaje que soporta para propiciar la interoperabilidad con sistemas celulares (FDM) e inalámbricos (TDM).
Seguridad	Incluye medidas de privacidad y criptografía inherentes en el protocolo. El estándar 802.16 agrega autenticación de instrumentos con certificados x.509 usando DES en modo CBC (<i>CipherBlockChaining</i>).
Bandas bajo licencia	Opera en banda licenciada en 2.4 GHz y 3.5 GHz para transmisiones externas en largas distancias
Bandas libres (sin licencia)	Opera en banda libre en 5.8, 8 y 10.5 GHz (con variaciones según espectro libre de cada país)
Canalización	De 5 y 10 MHz
Codificación	Adaptiva
Modulación	Adaptiva
Ecualización	Adaptiva
Potencia de Transmisión	Controla la potencia de transmisión
Acceso al Medio	Mediante TDMA dinámico
Corrección de errores	ARQ (retransmisión inalámbrica)
Tamaño del paquete	Ajuste dinámico del tamaño del paquete
Aprovisionamiento	Aprovisionamiento dinámico de usuarios mediante DHCP y TFTP
Tasa de transmisión	Hasta 75 Mbps
Espectro de frecuencia	• IEEE 802.16a entre 2-11 GHz (LOS) para comunicación entre antenas • IEEE 802.16b entre 5-6 GHz con QoS • IEEE 802.16c entre 10-66 GHz • IEEE 802.16e entre 2-6 GHz (NLOS) para distribución a suscriptores, móvil.
Alcance	• 20 Km sin Línea de Vista • 4- 6 Km en áreas de alta densidad
Aplicaciones	Voz, video y datos

Tabla 2.1 Características de WiMAX

2.2 Propagación NLOS versus LOS

El canal de radio de un sistema de comunicación inalámbrico se describe a menudo como LOS o NLOS. En un enlace LOS, una señal viaja a través de un camino directo y sin obstáculos desde el transmisor al receptor. Un enlace LOS exige que la mayor parte de la primera zona de Fresnel esté libre de cualquier obstrucción, véase la Figura 2.1, si éste criterio no se cumple entonces hay una reducción significativa en la fuerza de la señal. La separación de Fresnel requerida depende de la frecuencia de funcionamiento y la distancia entre el transmisor y la localización del receptor.

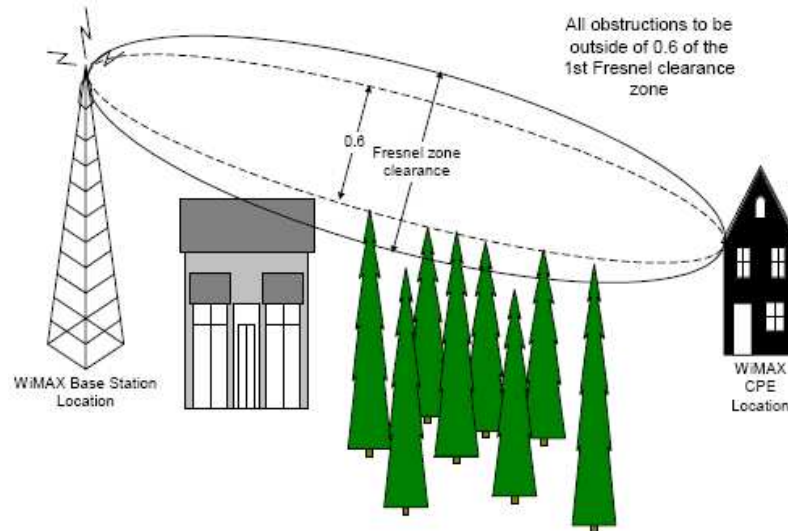


Figura 2.1 Zona Fresnel LOS

En un enlace NLOS como se observa en la Figura 2.2, una señal llega al receptor por medio de reflexiones, dispersiones, y difracciones. Las señales que llegan el receptor consisten en componentes de trayectoria directa, múltiples trayectorias reflejadas, energía dispersa, y trayectorias de propagación difractada. Estas señales tienen diferentes retardos, atenuación, polarización, y relativa estabilidad para trayectorias directas.

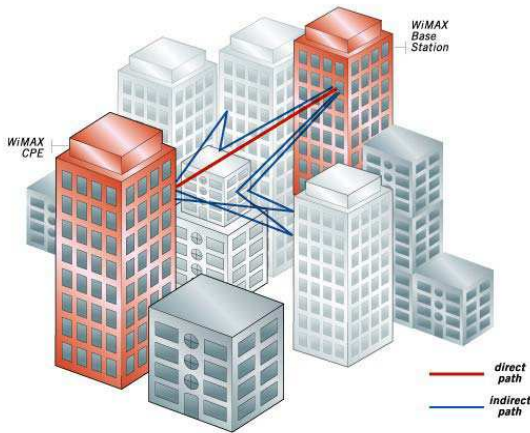


Figura 2.2 Propagación NLOS

Hay varias ventajas que hacen a los despliegues NLOS deseables. Los requisitos de planificación y las restricciones de la altura de la antena a menudo no permiten que la antena sea colocada para LOS. Para gran escala los despliegues celulares contiguos, donde la frecuencia de reutilización es fundamental, la reducción de la antena es ventajosa para reducir la interferencia co-canal entre sitios de célula adyacente. Esto fuerza a menudo a las estaciones base para funcionar en condiciones NLOS. Los sistemas LOS no pueden reducir alturas de la antena porque afectaría la trayectoria de la visión directa requerida del CPE a la estación base. La tecnología NLOS también reduce costos de instalación, permitiendo el uso de CPE de aleros bajos que facilitan la problemática de hallar localizaciones adecuadas para el montaje del CPE con línea a vista como podemos ver en la Figura 2.3.

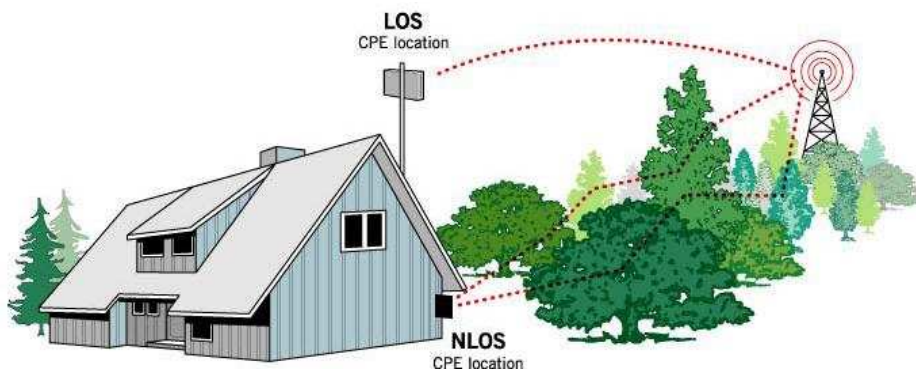


Figura 2.3 Localización CPE en NLOS

La tecnología NLOS y las características mejoradas en WiMAX permiten utilizar en el interior el equipo local de cliente (CPE). Esto tiene dos desafíos principales; en primer lugar superar las pérdidas de penetración en el edificio y en segundo lugar, las distancias razonables de cobertura con la potencia más baja de transmisión y la ganancia de la antena que se asocian generalmente al CPEs de interior. WiMAX hace esto posible, y la cobertura NLOS puede mejorarse aún más por la movilización de algunas de capacidades opcionales de WiMAX.

2.3 Soluciones de la tecnología NLOS

La tecnología WiMAX, resuelve o mitiga los problemas derivados de condiciones NLOS mediante el uso de:

- Tecnología OFDM.
- Sub-canalización.
- Antenas direccionales.
- Diversidad en la transmisión y en la recepción.
- Modulación adaptable.
- Técnicas de corrección de errores.
- Control de potencia.

2.3.1 Tecnología OFDM

La tecnología OFDM proporciona operadores con medios eficientes para superar los desafíos de propagación NLOS. La forma de onda de OFDM WiMAX ofrece la ventaja de poder funcionar con Spread Delay muy grandes en ambientes NLOS.

En virtud del tiempo del Símbolo OFDM y el uso de un prefijo cíclico, la forma de onda OFDM elimina los problemas de Interferencia Inter-Símbolo (ISI) y las complejidades de ecualización adaptativa. Debido a que la forma de onda OFDM se compone de múltiples portadoras ortogonales de banda estrecha, el desvanecimiento selectivo es localizado en un subconjunto de

portadores que sean relativamente fáciles de ecualizar. Un ejemplo se demuestra en la Figura 2.4 como una comparación entre una señal de OFDM y una señal de portadora única, con la información que es enviada paralelamente para OFDM y en serie para el solo portador.

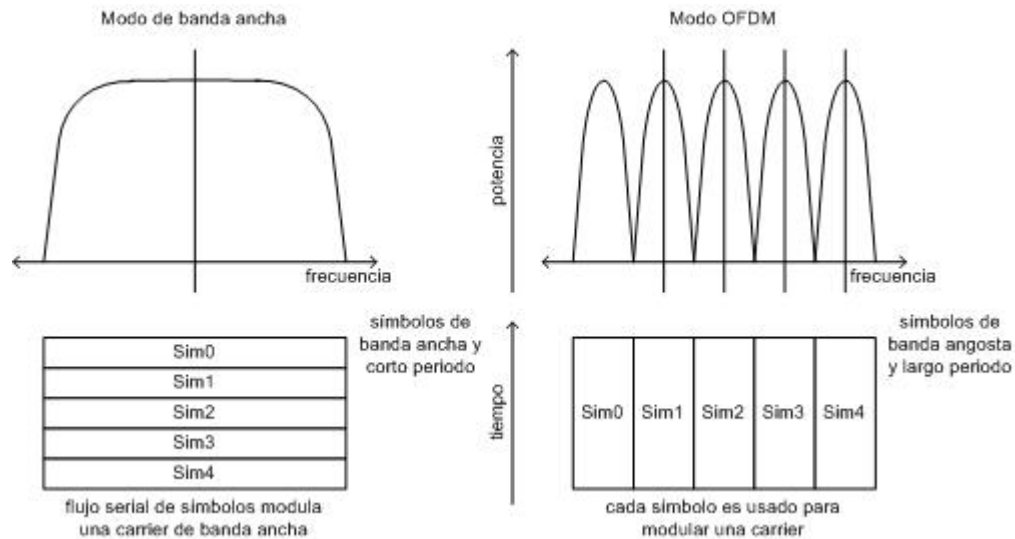


Figura 2.4 Portadora única y OFDM

2.3.2 Sub-canalización

La sub-canalización en el enlace ascendente es opcional en WiMAX. Sin la sub-canalización, las restricciones regulatorias y la necesidad para un costo efectivo de los CPEs, típicamente causa que el enlace sea asimétrico, este provoca que el rango de sistema esté limitado en el enlace ascendente. La sub-canalización habilita que el enlace sea balanceado de tal forma que la ganancia del sistema es similar en ambos enlaces (ascendente y descendente). La sub-canalización concentra la transmisión de potencia en unas pocas portadoras OFDM, esta es la forma de incrementar la ganancia del sistema que puede ser usada para extender el alcance del sistema, superar las pérdidas de penetración, o reducir el consumo de potencia del CPE como se aprecia en la Figura 2.5. El uso de la sub-canalización es más importante en OFDM permitiendo un uso más flexible de los recursos que pueden soportar movilidad o portabilidad.

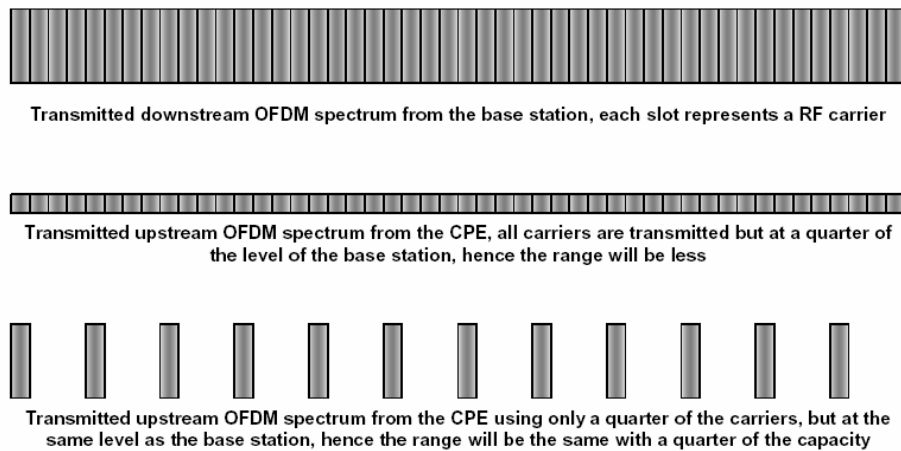


Figura 2.5 Efecto de sub-canalización

2.3.3 Antenas para aplicaciones inalámbricas fijas

Las antenas direccionales incrementan el margen de fading mediante la adición de mayor ganancia. Esto incrementa la disponibilidad del enlace, demostrado en comparaciones del factor K para antenas omnidireccionales v/s direccionales. La dispersión de retardo es reducida en antenas direccionales en las estaciones base y equipos de abonados. El patrón de antena suprime cualquier señal multi-trayecto que arriba en los lóbulos laterales. La efectividad de estos métodos fue probada y demostrada en despliegues exitosos, en los cuales el servicio operaba bajo un fading NLOS significativo.

Los sistemas de antenas adaptativa (AAS) son una parte opcional del estándar 802.16. Estas tienen la propiedad de dirigir su foco a una particular dirección o direcciones. Esto significa que durante la transmisión, la señal puede ser limitada a la dirección requerida del receptor, como un reflector. Recíprocamente durante la recepción, el ASS puede ser hecho para enfocar solamente en la dirección desde la cual viene la señal deseada. También poseen la propiedad de supresión de interferencia co-canal de otras localidades. Los sistemas de antena adaptativa son consideradas para un desarrollo futuro que podrá, eventualmente, mejorar el re-uso del espectro y la capacidad de la red WiMAX.

2.3.4 Diversidad en la transmisión y en la recepción

Los esquemas de diversidad se utilizan para obtener una ventaja del multi-path (Multi-trayectoria) y las reflexiones de la señal que ocurren en condiciones de NLOS. La diversidad es una característica opcional en WiMAX. Los algoritmos de diversidad ofrecidos por WiMAX, tanto en transmisión como en recepción incrementan la disponibilidad del sistema. La opción de transmisión en diversidad en WiMAX utiliza la codificación en espacios de tiempo para proporcionar una fuente de transmisión independiente, esto reduce el fading y combate la interferencia. Para la diversidad en recepción, varias técnicas se combinan para mejorar la disponibilidad del sistema.

2.3.5 Modulación Adaptativa

La modulación adaptativa permite al sistema WiMAX, ajustar el esquema de la modulación de la señal dependiendo de la relación señal ruido (SNR) del enlace de radio como se observa en la Figura 2.6. Cuando el enlace de radio es de alta calidad, el esquema más alto de modulación se utiliza, dando al sistema más capacidad. Durante el desvanecimiento de la señal, el sistema WiMAX puede cambiar de puesto a un esquema más bajo de modulación para mantener la estabilidad de la calidad y el enlace de la conexión. Esta característica permite al sistema superar los desvanecimientos selectivos en el tiempo.

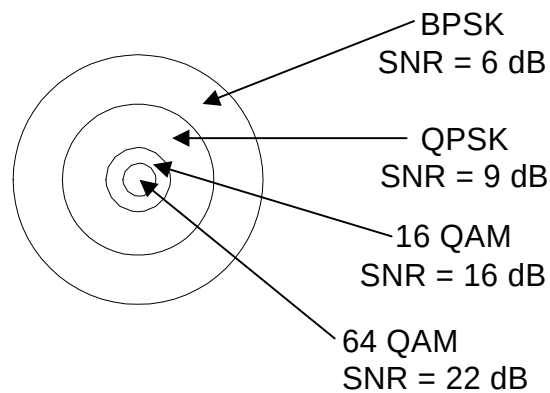


Figura 2.6 Radios relativos de la célula para la modulación adaptativa

2.3.6 Técnicas de corrección de errores

Las técnicas de la corrección de errores se han incorporado en WiMAX para reducir los requerimientos de la relación señal a ruido. El FEC (Forward Error Correction) permite su corrección en el receptor sin retransmisión de la información original. Se utiliza en sistemas sin retorno o sistemas en tiempo real donde no se puede esperar a la retransmisión para mostrar los datos. Estas técnicas de corrección ayudan a recuperar tramas erróneas que pueden haber sido perdidas por desvanecimientos selectivos de frecuencia o ráfagas de errores. El ARQ (Automatic repeat request) es usado para corregir errores que no pueden ser corregidos por el FEC. Esto mejora significativamente la BER para similares niveles umbrales.

2.3.7 Control de Potencia

Los algoritmos de control de potencia se utilizan para mejorar el funcionamiento total del sistema. Estos son implementados por la estación base, la cual manda información sobre el control de potencia a cada CPE para que regule su nivel de potencia de transmisión, de forma que el nivel recibido en la estación base sea un nivel predeterminado. En ambientes con cambios dinámicos por desvanecimiento este nivel predeterminado significa que el CPE sólo puede transmitir suficiente potencia para cumplir este requisito. Lo opuesto sería que el CPE transmitiese el nivel basándose en las condiciones peores. El control de potencia reduce sobre todo el consumo de potencia del CPE y la potencial interferencia con otras estaciones base co-localizadas. Para LOS la potencia transmitida por el CPE es aproximadamente proporcional a la distancia a la estación base. Para NLOS esto depende altamente del nivel de obstrucción existente.

2.4 Rango de cobertura de WiMAX

En esta sección se describen dos tipos de estación base y sus capacidades:

- *Una estación base estándar con:*
 - Implementación básica de WiMAX.

- o Potencia RF de salida estándar para una estación base de bajo costo.
- *Una estación base por completo ofrecida con:*
 - o Potencia de salida RF mayor que la estación base estándar.
 - o Tx/Rx de variedad combinada con codificación de espacio-tiempo y recepción de MRC.
 - o Sub- canalización.
 - o ARQ.

Ambas estaciones bases pueden ser compatibles con WiMAX, Sin embargo el rendimiento que puede lograrse por cada uno de ellos es muy diferente. La Tabla 2.2 muestra la cantidad de diferenciación entre los dos tipos diferentes, para una configuración del sistema de referencia. Es importante entender que hay un número de opciones dentro de WiMAX que dan los operadores y proveedores la capacidad de construir redes que mejor se adapten a su aplicación y negocio. El máximo rendimiento en el enlace ascendente (Tabla 2.2) asume que un solo sub-canal es utilizado para extender el borde de la célula lo más lejos posible.

		Frecuencia: 3.5 GHz		Completa		Estándar	
		Ancho de Banda: 3.5MHz					
		60° por sector.		Desde	Hasta	Desde	Hasta
Radio de célula (Km)	LOS			30	50	10	16
	NLOS			4	9	1	2
	Instalación de CPE interior			1	2	0.3	0.5
Máxima tasa de transferencia por sector (Mbps)	Downlink			11.3	8	11.3	8
	Uplink			11.3	8	11.3	8
Máxima tasa de transferencia por CPE al margen de la célula (Mbps)	Downlink			11.3	2.8	11.3	2.8
	Uplink			0.7	0.1	11.3	2.8
				75			
Máximo número de suscriptores.				Más.		Menos.	

Tabla 2.2 Ejemplo Estación Base de características completa vs. características estándar

Acorde a lo mostrado el rendimiento alcanzable con el equipo de abonado de interior autoinstalable de funcionalidad completa tiene un incremento de las implicaciones LOS y NLOS de los dos diferentes tipos de estaciones base como se ve en la Figura 2.7.

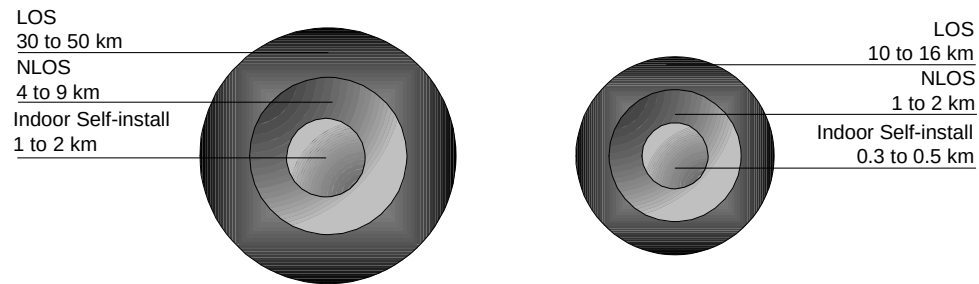


Figura 2.7 Radio de celda para funcionalidad completa vs. estándar

2.5 Topologías para redes WiMAX

El estándar IEEE 802.16 define dos posibles topologías de red:

- Topología PMP (Punto-a-multipunto).
- Topología Malla o Modo Malla.

La principal diferencia entre los dos modos es la siguiente: en el modo PMP como muestra la Figura 2.8, el tráfico se llevará a cabo sólo entre una BS y sus CPEs, mientras que en el modo Malla el tráfico puede ser encaminado a través de otros CPEs hasta BS e incluso puede sólo ocurrir entre CPEs. PMP es una topología centralizada donde la BS es el centro del sistema mientras en la topología Malla no.

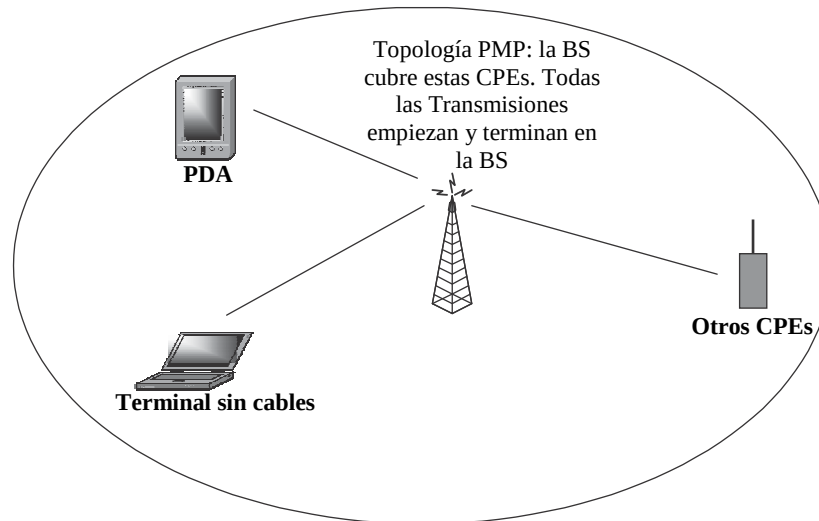


Figura 2.8 Topología PMP

Los elementos en la topología Malla son llamados nodos, por ejemplo, un CPE es un nodo tal como se aprecia en la Figura 2.9. En la topología malla, cada estación puede crear su propia comunicación con cualquier otra estación en la red y entonces no se restringe comunicarse solo con las BS. Por lo tanto, una de las principales ventaja del modo malla es que el alcance de una BS puede ser mucho mayor, dependiendo del número de saltos, hasta las más distantes CPE. Por otro lado también el modo malla es muy común en una red Ad Hoc (sin infraestructura fija).

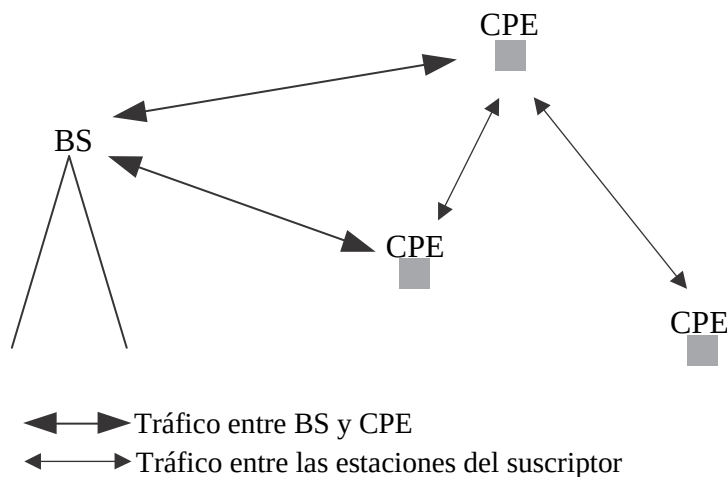


Figura 2.9 Topología Malla. La BS ya no es el centro, como en el clásico Modo PMP

Cuando es autorizada una red de malla, un candidato CPE recibe un nodo de 16-bit Nodo ID (identificador) a petición de un CPE identificado como BS en la malla. El Nodo ID es la base del nodo de identificación. El Nodo ID es transferido en la subheader de malla de una trama MAC genérica tanto unicast como broadcast.

2.6 Uso del espectro

El estándar 802.16 considera la banda de frecuencia 2-66 GHz. Esta banda se divide en dos porciones:

- El primer rango está entre 2 y 11 GHz y está destinado a transmisiones de NLOS. Esto era previamente el estándar 802.16a. Esta es la única gama actualmente incluida en WiMAX para este rango son consideradas por el momento las bandas: 2.5 GHz, 3,5 GHz y 5,7 GHz.
- La segunda gama está entre 11 y 66 GHz y está destinadas para las transmisiones LOS. Este no se utiliza en WiMAX

2.7 Propagación en WiMAX

Los ambientes de propagación no están ciertamente especificados para WiMAX, pero los niveles de rendimiento en diferentes ambientes deben ser cuantificados. Las características de propagación dependen de la banda de operación y se repasan en esta sección.

2.7.1 Modelado de propagación

Las diferentes bandas del espectro tienen características de propagación muy distintas y requieren diferentes modelos de predicción.

Un cúmulo de modelos empíricos fueron ampliamente aceptado para las comunicaciones celulares; su éxito se debe principalmente a su simplicidad y a su predicción bastante buena para el modelado de primer orden. El acercamiento más simple para estimar la relación de poder entre el transmisor y el receptor en función de la distancia de separación d , relación que se refiere a la pérdida en el camino. Un argumento físico como la fórmula de Friis para él la potencia de la transmisión esta descrito en la ecuación 1.

$$\text{Eq. 1) } \frac{P_r}{P_t} = \frac{G_t G_r \lambda^2}{(4\pi d)^2}$$

Donde P_t y P_r es la potencia transmitida y recibida, G_t y G_r la ganancia transmisora y receptora, λ la longitud de onda de la señal, y d la distancia de separación. Esta ecuación muestra una dependencia de espacio libre de $1/d^2$.

El exponente $n=2$ se refiere a la pérdida de trayectoria. Si la pérdida de trayectoria se mide en decibelio ($P_L = 10 \times \log (P_t/P_r)$), esta varía logarítmicamente con la distancia de separación como se muestra en la ecuación 2.

$$\text{Eq. 2) } P_{LO}(dB) = P_L + 10n \times \log\left(\frac{d}{d_o}\right)$$

Donde la intersección P_{LO} es la pérdida de trayectoria a una distancia de referencia arbitraria d_o .

La ecuación anterior Friis conduce a:

$$\text{Eq. 3) } P_L(dB) = 32.44 + 20 \times \log\left(\frac{f}{f_o}\right) + 20 \times \log\left(\frac{d}{d_o}\right)$$

Donde $f_o = 1\text{MHz}$ y $d_o = 1 \text{ km}$.

2.8 Capas del estándar IEEE 802.16/WiMAX

El estándar de Red IEEE 802.16 utiliza el modelo OSI. Este modelo es de uso frecuente para describir diversos aspectos de una tecnología de Red. Las capas que involucran WiMAX son las dos más bajas: Capa física (PHY) o Capa 1, y Capa de Enlace de Datos o Capa 2. IEEE 802 a la vez fractura la Capa 2 en dos Sub-Capas llamadas: Control de enlace lógico (LLC) y Control de acceso al medio (MAC) como se observa en la Figura 2.10.

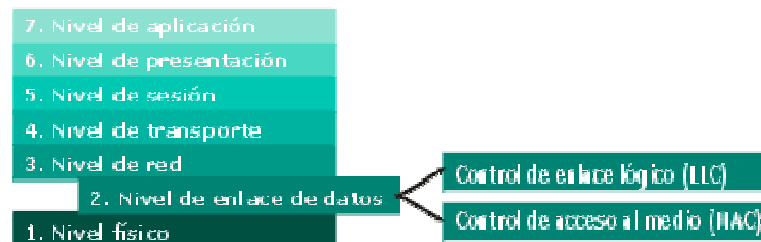


Figura 2.10 Modelo OSI. En WiMAX/802.16, solo las dos primeras capas son definidas

La arquitectura de las capas definida en WiMAX/802.16 se muestra en la Figura 2.11. El estándar 802.16 define solamente las dos capas más bajas, la capa física y la capa del MAC, que es la parte principal de la capa de transmisión de datos. La capa LLC que es usada por 802.2 no es usada en 802.16. A sí mismo la capa MAC se divide en 3 sub-capas: La CS (sub-capa de convergencia), el CPS (sub-capa de la parte común) y la sub-capa de seguridad.

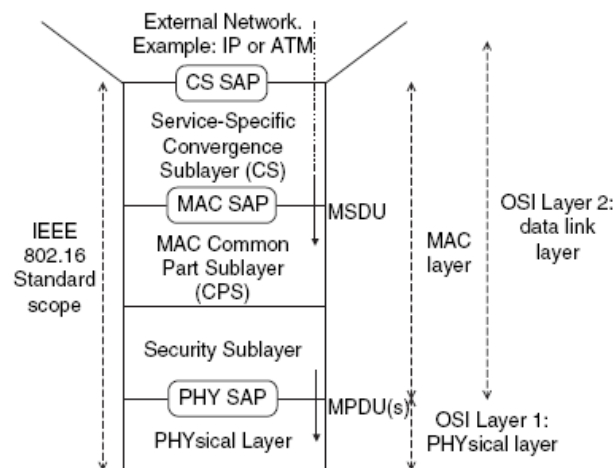


Figura 2.11 Capas del estándar 802.16

2.8.1 Capa Física (Physical Layer)

El protocolo WiMAX añade procesos para el tráfico de usuario, partiendo con la capa física, que transmite MAC PDUs a la capa física pasando hacia el enlace aéreo. En esta sección se presentan los procesos efectuados en la capa PHY incluyendo elementos obligatorios y opcionales. Varios factores incluyendo la modulación adaptativa y tasa de código serán discutidos. La capa física (PHY) toma MAC PDUs en la entrada PHY SAP y lo arregla para el transporte sobre la ruta aérea.

2.8.1.1 Tamaño del canal

Una comprensión básica de la capacidad de un sistema WiMAX comienza con saber cual es su espectro de radio disponible. El espectro de radio disponible en última instancia, limita el tamaño del ancho de banda en frecuencia de los canales. El tamaño del canal, fija la capacidad del canal, canal de doble tamaño implica doble capacidad (no obstante la gama en general disminuirá). Los rangos de ancho de banda del canal van ("por debajo de 11 GHz") para OFDM/OFDMA en canales de tamaño (de 1.25 a 20 MHz).

Muchos de los grandes operadores tienen una fuerte motivación, ya sea competitiva o reglamentaria, para operar en bandas del espectro con licencia. De las bandas disponibles en el mercado mundial regulado está la licencia del espectro 3.5 GHz ITU FDD. Por esta razón, la mayoría de los equipos WiMAX han sido certificados para su uso en la banda de 3,5 GHz. El perfil disponible del tamaños del canal son múltiplos de 1,75 MHz (1,75, 3,5, 7 MHz). El tamaño del canal es impulsado según el operador y la regulación del país.

2.8.1.2 OFDM

En OFDM, el espectro ocupado se divide en muchos canales de banda estrecha discretos conocido como "sub-portadoras" ("tonos"). Cada portadora de datos es modulada sobre un símbolo de tiempo que es inversamente proporcional a la frecuencia portadora espaciada de modo que las sub-portadoras tienen el mínimo de interferencia entre ellas.

En este sentido, las sub-portadoras son "ortogonales" o independientes el uno del otro. La capacidad de cada sub-portadora depende del orden de la modulación, que puede ser BPSK (1 bit por sub-portadora), QPSK (2 bit por sub-portadora), 16QAM (4 bit por sub-portadora), o 64QAM (6 bits bit por sub-portadora) en el caso de OFDM PHY. En general, más energía se requiere para una modulación de orden superior, a fin de lograr la misma gama de rendimiento.

En el OFDM PHY hay 256 sub-portadoras que abarcan el espectro de muestreo y se define como:

$$\text{Eq. 4)} F_s = \text{FLOOR}\left(n \times BW / 8000\right) \times 8000$$

Donde **n** es el factor de muestreo, una constante dependiente del tamaño del canal y BW es el ancho de banda por canal en Hz. El número de sub-portadoras corresponde al tamaño de la FFT/IFFT usado para recibir y transmitir los símbolos OFDM. Para reducir la complejidad de los algoritmos de procesamiento digital es conveniente utilizar tamaños FFT que son potencias de 2. Para canales en la banda de 3,5 GHz los canales son múltiplos de 1,75 MHz y $n = 8 / 7$. Para un canal de ancho de 3,5 MHz de espectro de muestreo es 4.0 MHz. Las 256 sub-portadoras se distribuyen por igual en todo el espectro de muestreo que implica una distancia de:

$$\text{Eq. 5)} \Delta f = F_s / 256$$

Por ejemplo $\Delta f = F_s / 256 = 15,625$ Hz por un canal de **3.5 MHz**

Con el fin de proporcionar un mayor margen de interferencia co-canal y la facilidad de restricciones de filtrado de radio, no todas las sub-portadoras están con energía. Hay 28 menores y 27 superiores sub-portadoras "guardia" además de la sub-portadora DC, que nunca están energizadas. De un total de 256 sub-portadoras se utilizan sólo 200 lo que deja un espectro total ocupado $\Delta f \cdot 200 = 3,125$ MHz para un canal de 3,5 MHz. Este ejemplo implica un canal básico, ocupando un ancho de banda con eficiencia del 89% ($3.125/3.5 = 89\%$), pero el número varía para otros anchos de banda y factores de muestreo en el canal. Este es el primer ejemplo que

hemos encontrado de lo que puede ser considerado como canal sobrecargado que disminuye la capacidad del canal, en este caso se requiere del diseño para mejorar la calidad de canales cuando el espectro adyacente está ocupado.

No todas las 200 sub-portadoras ocupadas se utilizan para llevar tráfico de datos. Hay ocho sub-portadoras piloto que son dedicadas para fines de estimación del canal, dejando 192 sub-portadoras de datos para el usuario y gestión del tráfico. Con el fin de calcular la capacidad del canal es útil para entender cuantos bits de datos pueden ser llevados por la sub-portadora.

La capacidad de la sub-portadora, antes de tomar la sobrecarga añadida por bits de corrección de errores redundante, viene dada por la modulación de orden: 6 bits/sub-portadora para 64QAM, 4 bits/sub-portadora para 16 QAM, y así sucesivamente. Por ejemplo, un canal capaz de soportar la modulación 64QAM podría enviar seis bits para cada portadora de dato por símbolo.

Como hemos señalado, la ortogonalidad de las sub-portadoras se logra mediante el mantenimiento de una relación inversa entre el espaciamiento de la sub-portadora y el tiempo del símbolo. Por lo tanto, el tiempo de símbolo útil es simplemente la inversa del espaciamiento de la sub-portadora:

$$\text{Eq. 6)} T_b = 1/\Delta f$$

Por ejemplo, un canal de 3,5 MHz tiene un tiempo útil de símbolo de $1 / 15625 = 64 \mu\text{s}$. Sin embargo, para canales de multi-camino, debemos tener en cuenta de los errores de sincronización y del retardo de propagación. En OFDM, esto se logra repitiendo una fracción de la última porción de símbolo de tiempo útil y añadiendo en el comienzo del símbolo un tiempo símbolo resultante de:

$$\text{Eq.7)} T_s = T_b + G \times T_b$$

Donde G es la fracción:

$$\text{Eq. 8)} \quad G = \frac{1}{2m}, \quad m = \{2, 3, 4, 5\}$$

La fracción repetida del símbolo se llama “prefijo cíclico”. Un prefijo cíclico incrementado implica una sobrecarga crecientes (la capacidad disminuida desde el prefijo cíclico no lleva nueva información), sin embargo, proporciona una mayor inmunidad a la ISI (Interferencia Inter-Símbolo) de multi-trayectoria y errores de sincronización.

Para un canal de 3,5 MHz el tiempo de símbolo útil es de 64 μ s y el mínimo tiempo total de símbolo es $T = 64 \mu s + 64/32 \mu s = 66 \mu s$. La capacidad del canal por símbolos es:

$$\text{Eq. 9)} \quad C_{raw} = 192 \times \frac{k}{T_s}$$

Donde K es el bit por símbolo de la modulación utilizada.

Asumiendo modulación 64QAM (6 bits por símbolo): 192 de sub-portadoras x 6 bits/sub-portadora / 66 μ s = 17.45 Mbps

Pero en la práctica en cualquier sistema inalámbrico podemos esperar a tener errores ocasionales presentados por la transmisión imperfecta, el enlace aéreo, o la detección imperfecta. La solución es enviar bits redundantes con la información de bits en cada símbolo para la ayuda de detección y corrección de errores, técnica conocida como Forward Error Correction (FEC). En el OFDM PHY FEC se realiza utilizando una combinación de código externo Reed-Solomon combinado con un código interno convolucional. Adición de bits redundante añade sobrecarga y reduce la capacidad del canal. La meta del diseño es balancear la sobrecarga añadida contra la mejora en el rendimiento del enlace y la relación tasa de error residual.

Observe que las tasas de modulación se han diseñado de manera que un bloque de código FEC sólo encaja en un símbolo cuando 192 sub-portadoras son utilizadas. Por ejemplo, para 64QAM, $144 \text{ bytes} = 1152 \text{ bits} / 6 \text{ bits} / \text{símbolo} = 192 \text{ sub-portadoras}$. La capacidad útil del canal por el símbolo es el siguiente:

$$\text{Eq. 10) } C = C_{raw} \times OCR,$$

Donde OCR es la tasa de codificación total que figura en la Tabla 2.3. Por ejemplo, para un canal de 3,5 MHz la capacidad útil del canal por símbolo asumiendo la mayor tasa de modulación y codificación es la siguiente: $C = 17.45 \text{ Mbps} \times 3/4 = 13.1 \text{ Mbps}$.

$$\text{Eq. 11) } C = 17,45 \text{ Mbps} \times \frac{3}{4} = 13,1 \text{ Mbps}$$

Es útil resumir la discusión de la capacidad del canal en términos de la eficiencia espectral. La eficiencia espectral es expresada en unidades de bits por segundo por Hz y se obtiene dividiendo la capacidad del canal por la anchura del canal:

$$\text{Eq. 12) } E = C / BW$$

Podemos ver que nuestro canal de 3,5 MHz tiene una eficiencia espectral (hasta ahora) de $13,1 \text{ Mbps} / 3,5 = 3,74 \text{ MHz bps/Hz}$. La eficiencia espectral es una figura útil y merecedora de tener en cuenta, porque permite calcular rápidamente la capacidad de otros tamaños de canal que apoya WiMAX.

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate	RS code	CC code rate
BPSK	12	24	1/2	(12,12,0)	1/2
QPSK	24	48	1/2	(32,24,4)	2/3
QPSK	36	48	3/4	(40,36,2)	5/6
16-QAM	48	96	1/2	(64,48,8)	2/3
16-QAM	72	96	3/4	(80,72,4)	5/6
64-QAM	96	144	2/3	(108,96,6)	3/4
64-QAM	108	144	3/4	(120,108,6)	5/6

Tabla 2.3 Tamaños de bloque y las velocidades de código usadas para diferentes modulaciones y velocidad de código

2.8.1.3 Tamaño de Trama y Símbolo

En la especificación OFDM PHY los tamaños de la trama permitida son las siguientes: $T_f = (2, 5, 4, 5, 8, 10, 12.5, 20 \text{ ms})$. Para un canal de 3,5 MHz con un ancho de 1/8 de prefijo cíclico, el símbolo es de 72 μs de longitud. Asumiendo unos 10 ms de longitud de trama, el número entero de símbolos por cada trama es el siguiente:

$$\text{Eq. 13) } N = \text{FLOOR}\left(\frac{T_f}{T_s}\right)$$

Donde T_f es la longitud de trama. En este caso, $N = \text{FLOOR}(10\text{ms}/72\mu\text{s}) = 138$ símbolos. La diferencia al final de la trama es, por lo tanto, $T_f - (138 \times T_s) = 64 \mu\text{s}$, equivalente aproximadamente al 0,6% de reducción de la capacidad del canal sostenible.

2.8.1.4 Preámbulos

- **Sincronización**

Los receptores necesitan un modo de sincronización para el comienzo de la trama TDMA y el símbolo de tiempo.

En el enlace descendente (downlink) la sincronización es proporcionada por un patrón de preámbulo fijo de bits que es transmitido al principio de cada trama.

Puesto que el preámbulo no transmite ningún dato real su presencia reduce la capacidad del canal. El preámbulo de downlink tiene dos símbolos OFDM por cada trama. Por lo tanto, la sobrecarga se incrementa en un $2/N$, donde N es el número de símbolos por trama. Esto afecta obviamente las longitudes más cortas puesto que N es más pequeño. Por ejemplo, el canal de 3,5 MHz con un $1/8$ de prefijo cíclico y una trama de 10 ms, la sobrecarga del preámbulo de downlink asciende a $2/138 = 1,4\%$.

Por otra parte el enlace ascendente (uplink) se reparte entre un grupo de estaciones de abonado y la estación base receptora del mismo modo para sincronizar las necesidades de cada suscriptor a la estación emisora cuando comienzan a transmitir una ráfaga de datos que consta de uno o más símbolos consecutivos en una trama. Esto exige a cada estación de abonado anteponer un preámbulo al comienzo de cada ráfaga.

Los preámbulos ocupan un símbolo en el comienzo de cada ráfaga. La sobrecarga que este presenta es variable en función del tamaño de la ráfaga en términos del número de símbolos.

- **Alcance**

En un sistema WiMAX que consiste en una estación base que se comunica con una colección de estaciones de suscriptor en diferentes rangos, necesitamos un método que compense el retardo del tránsito variable sobre la ruta aérea (Airlink) de modo que la estación base pueda coordinar el uso selectivo del enlace ascendente (uplink) y evite recibir los símbolos que se traslapan en el tiempo. Esto es logrado midiendo la distancia (retardo) entre cada estación de suscriptor y su estación base. El objetivo es hacer que cada estación de suscriptor aparezca para ser colocada con la estación base en términos de alineación de la transmisión.

Una vez que una estación de suscriptor se ha unido a una red, necesita periódicamente actualizar los valores de alcance (proceso de “alcance” periódico)

2.8.1.5 Unidad de asignación mínima. (MAU) *Minimum Allocation Unit*

Una de las fortalezas de la tecnología OFDM es su capacidad de enviar cantidades muy pequeñas de información utilizando únicamente una sola sub-portadora de datos para un símbolo de tiempo. Por ejemplo, utilizando la modulación de orden más alto (64QAM), una sola sub-portadora de datos podría utilizarse para enviar tan sólo 6 bits a la vez.

El uso del canal está por lo tanto, por lo menos en principio, altamente - *granular*. En términos de capacidad del canal esta granulosidad ayuda a reducir la cantidad de ancho de banda perdida en el envío de los paquetes sobre el canal.

Sin embargo, existen restricciones sobre la forma en que la OFDM PHY 802,16 organiza las sub-portadoras de datos en unidades mínimas de asignación “Minimum Allocation Units” (MAU). La MAU es la mas pequeña y es de dos dimensiones cuánticas de frecuencia y tiempo que pueden ser asignados para el envío de información a través del canal. En el OFDM PHY la capacidad útil (Bytes) de MAU es variable y depende de la modulación y de la codificación elegida según la siguiente ecuación:

$$\text{Eq. 14) } \text{SIZEOF}(\text{MAU}) = \text{FLOOR}\left(N_c \times N_{cs} \times \frac{OCR}{16}\right)$$

N_c = Tamaño de bloque codificado en bytes (véase la Tabla 2.3), y N_{cs} = número asignado de sub-canales (1 .. 16) para el enlace ascendente o 16 para enlace descendente.

2.8.1.6 Diversidad

El aumento de la resistencia al desvanecimiento del canal se puede lograr mediante la combinación de las señales de múltiples canales de camino independiente. El método, denominado de Multiple-In Multiple-Out (MIMO) de estimación de canal, combina las señales de M transmisores (M-In) y de N receptores (N-Out) con el objetivo de mejorar tanto la resistencia al desvanecimiento, aumentar la eficiencia espectral combinada del canal, o alguna

combinación de ambos. MIMO es muy eficaz, pero con la desventaja de un aumento de los costos de hardware y la complejidad procesamiento de señales.

- **Space-Time Coding (STC)**

La codificación del espacio-tiempo (STC) es una forma de diversidad de transmisión downlink, y es una capacidad opcional de PHY que puede añadir un margen de enlace de 15 dB de atenuación (fading) en entornos NLOS. Este beneficio se proporciona a través de una cadena adicional de transmitir a la estación base y la lógica de decodificación en la estación del suscriptor. Técnicamente STC es un caso especial de MIMO: Multiple-In Single-Out (MISO). Puesto que hay normalmente muchas más estaciones de suscriptor que estaciones base STC es una manera particularmente rentable de agregar diversidad de enlace descendente sin requerir el hardware costoso adicional de la estación del suscriptor. La estación base genera dos flujos de código diferente para las dos cadenas de transmisión de manera que la estación del suscriptor pueda utilizar un algoritmo de decodificación relativamente simple al combinar las dos señales.

La capa PHY, añade la aplicación STC que agrega ciertas sobrecargas requiriendo un preámbulo adicional en cada trama de OFDM. Ráfagas de datos sobre el enlace descendente se enviarán sobre las dos cadenas de transmisión que debe ser precedida por un preámbulo de símbolo (*one-symbol preamble*). El único requisito adicional es que el número total de símbolos debe ser un múltiplo de dos, desde el receptor se procesa en pares según el algoritmo de Alamouti. Sólo un grupo STC de símbolos está permitido por trama y una vez que comienza la estación base debe transmitir desde ambas antenas hasta terminar la trama. El aumento de la sobrecarga es por lo tanto, un símbolo en cada trama.

2.8.2 Control de acceso al medio (MAC)

La interfaz de WiMAX para el tráfico de usuario es la capa Media Access Control, que transmite MAC SDUs en los pares de MAC sobre la capa PHY. En esta sección se presentan los procesos efectuados en la capa MAC incluyendo elementos obligatorios y opcionales.

2.8.2.1 Cabecera MAC

Refiriéndose a la Figura 2.12, la capa MAC 802.16 consta de tres partes: la Sub-capas de convergencia (CS), la Sub-capas de parte común (CPS), y la sub-capas de Seguridad (SS). La capa MAC acepta la capa superior PDUs y los coloca en la carga útil (payload) de uno o más MAC PDUs antes de enviarlos a la capa PHY para el transporte durante el enlace. En la dirección opuesta, la capa MAC recibe MAC PDUs de la capa PHY y reconstruye la PDU original de la capa superior antes de pasarlas por encima de la pila de transporte sobre interfaces externas. Los datos de carga útil (payload) pueden fluir dentro o fuera de la capa MAC, ya sea a través de interfaces de tráfico de usuario, o plano de gestión.

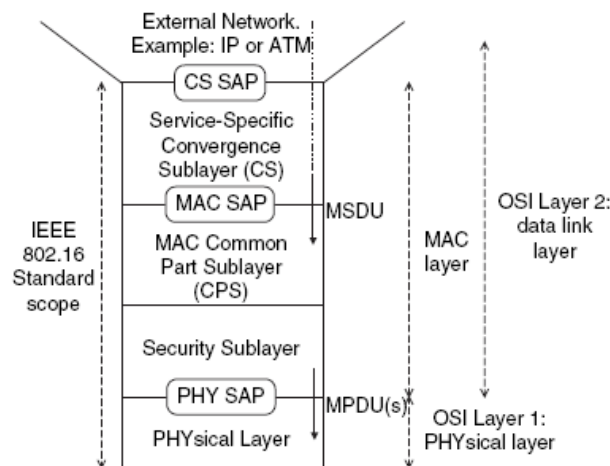


Figura 2.12 Capas del estándar 802.16

La estructura de la PDU MAC se muestra en la Figura 2.13. La cabecera MAC se puede encontrar en dos modos: la genérica cabecera MAC (GMH) “Generic MAC Header”, o cabecera de petición de ancho de banda de (BRH) “Bandwidth Request Header”. Ambos GMH y BRH son de longitud fija y 6 Bytes de longitud. La estructura de GMH se muestra en la siguiente figura reproducida a partir del estándar. Observe que el campo de longitud (LEN) “length” es de 11 bits y por lo tanto puede especificar la PDU del MAC incluyendo la cabecera hasta 2047 Bytes. El campo identificador de conexión (CID) “Connection Identifier” identifica la conexión virtual y flujo de servicio de la PDU del MAC.

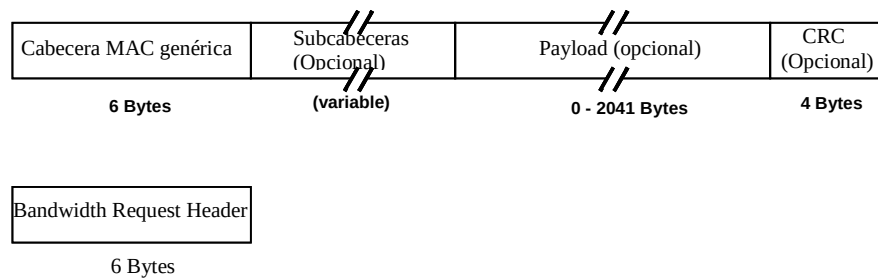


Figura 2.13 Formato MAC PDU

El GMH puede, opcionalmente, tener una o más sub-cabeceras adjuntos de la siguiente manera:

- Sub-cabecera de fragmentación (2 Bytes, opcionalmente, 1 Bytes)
- Empaquetamiento (3 Bytes, opcionalmente, 2 Bytes)
- Administrador de concesiones (2 Bytes)
- Sub-subcabecera de malla (2 Bytes)
- Fast-Feedback-Allocation (1 Bytes)
- Sub-cabecera extendida (de longitud variable).

Las sub-cabeceras pueden producirse sólo una vez por cada MAC PDU a excepción de la sub-cabecera de empaquetamiento que podrá ser insertado antes de cada MAC SDU empaquetado en la carga útil (payload).

Después del GMH y de las sub-cabeceras opcionales viene la carga útil opcional que es de longitud variable hasta $(2047 - 6) = 2041$ Bytes pero con la restricción de que toda la PDU MAC incluida la cabecera, sub-cabeceras, carga útil y la CRC debe ser inferior a 2048 bytes. Posterior al GMH, a la sub-cabecera opcional, el CRC es opcional con 4 Bytes de longitud. El BRH es de 6 Bytes de longitud.

Los MAC PDUs siempre comenzará con un GMH o un BRH y, por lo tanto, al menos 6 Bytes de longitud. Los MAC PDUs que transportan las cargas útiles (Payload) de datos comenzarán siempre con un GMH.

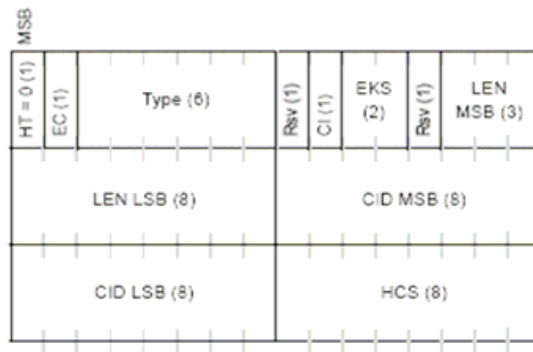


Figura 2.14 Formato cabecera genérica MAC (GMH)

Con estos antecedentes podemos entender la sobrecarga añadida por la cabecera MAC, sub-cabeceras, y la suma de comprobación (checksum) a la carga útil que es transportada. De la Figura 2.14 vemos que los MAC PDUs son variables en longitud y pueden ser tan corto como seis bytes, o como mucho como 2047 Bytes ($2^{11} - 1$). La sobrecarga para transportar la carga útil por lo tanto depende del tamaño de la carga útil. Por ejemplo, una trama Ethernet de 1514 Bytes (preámbulo y CRC removidos) tiene un mínimo de sobrecarga por MAC-PDU de $10 / (1514 + 10) = 0,7\%$ suponiendo ninguna sub-cabecera, pero incluyendo un MAC CRC. Por otra parte un único paquete corto TCP/IP ACK de 40 Bytes sobre Ethernet tendrá un mínimo de sobrecarga por MAC-PDU de $10 / (54 + 10) = 15,6\%$.

2.8.2.2 Petición de ancho de banda

El protocolo MAC 802.16 especifica varias formas en que la estación suscriptor puede informar a la estación base que ha de enviar los datos sobre el enlace ascendente. La mayor parte de estos métodos implican el enviar un BRH para el cual la estación del suscriptor debe primero obtener un canal de enlace ascendente. Dado que existe sobrecarga asociada con obtener las concesiones, así como el envío de solicitudes que están interesadas en los detalles en los mecanismos de solicitud de ancho de banda.

2.8.2.3 Subcapa de convergencia CS

La subcapa de Convergencia (especifica de servicio), más conocida como CS, se encuentra situada inmediatamente sobre la capa CPS de la MAC (véase Figura 2.12). El CS utiliza los servicios proporcionados por el MAC CPS, a través de MAC (SAP-Service Access Point). El CS realiza las siguientes funciones:

- Aceptar higher-layer PDUs de las capas más altas. En la versión actual del estándar, se proporcionan especificaciones de CS para dos tipos de capas más altas: Asynchronous Transfer Mode (ATM) CS y el Packet CS. Para el Packet CS, los protocolos pueden ser IPv4 o IPv6.
- Clasificación y asignación de MSDUs en apropiados CIDS (identificador conexión). Esta es una función básica de la Calidad de Servicio (QoS), mecanismo de gestión de 802,16 BWA.
- Procesamiento (si es necesario) PDUs high-layer basado en la clasificación.
- Una función opcional de CS es PHS (supresión de la cabecera de carga útil), el proceso de supresión de partes repetitivas de las cabeceras de carga útil en el remitente y el restablecimiento de estas cabeceras en el receptor.
- Entregando CS PDUs en apropiados MAC SAP y recibiendo CS PDUs desde pares de entidad.

Acepta los PDUs de las capas más arriba y los transmite al MAC CPS donde se aplican los clásicos procedimientos MAC, clasificando y trazando los MSDUs en apropiado CIDs (identificador de conexión) hecho por el CS son funciones básicas de los mecanismos de QoS de WiMAX/802.16. Entre otras funciones del CS es el opcional payload header supresión (PHS), el

proceso de suprimir repetitivas partes de payload headers en el remitente y restaurando los Headers en el receptor.

Dos especificaciones de CS son tomadas para describir el estándar:

La primera especificación CS es el CS ATM, Asynchronous Transfer Mode (ATM) CS, es una interface lógica que asocia diferentes servicios ATM con la MAC CPS SAP. El ATM CS acepta celdas desde la capa ATM, realiza la clasificación si son provisionados por PHS. Entonces el ATM CS entrega CS PDUs al apropiado MAC SAP.

La otra especificación disponible de CS es el paquete CS. El paquete CS es usado para el transporte de todos los protocolos “ Packet-based” tales como Internet Protocol (IP), IPv4, IPv6, Point-to-Point Protocol (PPP) y el estándar IEEE 802.3 (Ethernet).

2.8.2.4 MAC Common Part Sublayer (MAC CPS)

La subcapa common part (CPS) reside en la mitad de la capa MAC. El CPS representa el núcleo del protocolo MAC y es responsable de:

- Asignación del ancho de banda.
- Establecimiento de la conexión
- Mantener la conexión entre los dos lados.

El estándar 802.16-2004 define un conjunto de gestión y transferencia de mensajes. La gestión de mensajes se intercambian entre la CPE y la BS antes y durante del establecimiento de la conexión. Cuando la conexión se realiza, la transferencia de mensajes puede ser intercambiada para permitir la transmisión de datos.

El CPS recibe datos de varios CSs, a través MAC SAP, clasificado para particulares conexiones MAC. El QoS se tiene en cuenta para la transmisión y programación de datos a través de la capa

PHY. La CPS incluye muchos procedimientos de diferentes tipos: construcción de trama, acceso múltiple, asignación y demanda de ancho de banda, programación, la gestión de recursos de radio, gestión de QoS, etc

2.8.2.5 Subcapa de seguridad

La subcapa MAC también contiene una subcapa de Seguridad (Figura 2.12) proporcionando autenticación, Intercambio seguro de claves, encriptación y control de la integridad de todo el sistema BWA. Los dos temas principales de seguridad de una red de datos son el encriptación de datos y autenticación.

Los algoritmos que realizan estos objetivos deben evitar todos los ataques conocidos de seguridad cuyos objetivos pueden ser de denegación de servicio, robo de servicio, etc.

En el estándar 802.16, la encriptación de las conexiones entre CPE y BS se realiza con un protocolo de cifrado de datos aplicados en ambos sentidos. Este protocolo define un conjunto de soporte criptográfico, es decir, parejas de cifrado de datos y algoritmos de autenticación. Una encapsulación de protocolo se utiliza para encriptar paquetes de datos a través de la BWA. También se dan las normas para la aplicación de los algoritmos para una carga útil MAC PDU.

Un protocolo de autenticación, el protocolo de privacidad de administración de claves (PKM) se utiliza para proporcionar la distribución segura de datos desde BS a CPE. A través de este intercambio seguro de clave, debido al protocolo de gestión de claves de la CPE y la BS sincronizan datos keying. Los mecanismos básicos de privacidad son fortalecidos agregando el certificado digital basada en la autenticación CPE al protocolo administrador de claves además, las BS utilizan el protocolo de PKM para garantizar el acceso condicional a los servicios en red. 802.16e define PKMv2 que tiene el mismo marco de trabajo que PKM, con algunas adiciones por ejemplo nuevos algoritmos de encriptación, la autenticación mutua entre los CPEs y la BS, la ayuda para una entrega y un nuevo algoritmo de control de la integridad.

2.8.2.6 Conexiones y flujo de servicio

El CS proporciona cualquier transformación o trazado de datos externos de la red recibidos a través CS Service Access Point (SAP) en el MAC SDUs recibido por MAC Common Part Sublayer (CPS) a través del MAC SAP (véase la Figura 2.12). Esto incluye clasificar los (SDUs) de la red externa y asociarlas a un apropiado MAC “identificador de flujo de servicio” (SFID) e identificador de la conexión (CID). La clasificación y el trazado de la capa MAC se basa en dos conceptos fundamentales:

- **Conexión:** es una conectividad a nivel de MAC entre BS y las CPE. Es un trazado unidireccional entre un MAC BS y CPE con el propósito de transportar el tráfico del flujo de servicio. Una conexión se encuentra para un tipo de servicio (ej. la voz y el email no pueden estar en la misma conexión MAC). Una conexión es identificada por un CID (Connection Identifier), una información cifrada en 16 bit.
- **Flujo de servicio (SF):** es un servicio de transporte MAC que proporciona un transporte de paquetes unidireccionales en enlace uplink o downlink. Un flujo de servicio es identificado por un SFID (identificador del flujo del servicio) de 32 bit. El flujo de servicio define los parámetros de QoS para paquetes (PDUs) que se intercambian en la conexión.

2.8.2.7 Identificadores de conexión *Connection Identifiers (CIDs)*

En WiMAX, El identificador de conexión es una asignación unidireccional entre una estación base (BS) y una estación de suscriptor (CPE) de entidades MAC. El MAC es señalizado y el tráfico de usuario es transportado en diferentes CIDs asociados con parámetros de calidad de servicio (QoS), conocidos como flujos de servicio. El CID es de 16 bits.

Un identificador de conexión (CID) identifica una conexión donde cada MAC SDU es asignado en un servicio de comunicación dado. Un CID es de 16 bits que identifica una conexión

unidireccional entre pares equivalentes de un BS y un CPE en la capa MAC. Todo tráfico 802.16 es llevado sobre una conexión.

El uso de un CID de 16 bits permite un total de 64K conexiones dentro de cada canal downlink y uplink. Hay varios CIDs definidos en el estándar. Algunos CIDs tienen significado específico.

2.8.2.8 Flujos de servicio *Service Flows*

El flujo del servicio (SF) define la calidad del servicio (Qos) de una conexión. Este es identificado por un identificador de flujo de servicio o SFID (Service Flow Identifier) de 32 bits. Es un servicio de transporte MAC que proporciona un transporte unidireccional de paquetes uplink y downlink. Un flujo del servicio es caracterizado por un sistema de parámetros QoS. Los parámetros QoS incluyen los detalles de cómo los CPE pueden solicitar asignaciones del ancho de banda uplink y el comportamiento previsto del planificador uplink del BS.

CAPÍTULO III

ESTADO DEL ARTE DE LA VOIP

3.1 Antecedentes

Con el transcurso del tiempo, las tecnologías en redes de comunicación, específicamente la telefonía, han obtenido grandes logros, desde la creación del telégrafo hasta la actualidad, en donde producto de los avances de la informática y telecomunicaciones, es posible la transmisión de voz digitalizada en paquetes a través de la redes de datos IP, que conocemos actualmente como Voz sobre IP (VoIP).

3.1.1 Historia de la red telefónica tradicional

Cuando Graham Bell inventó el teléfono (mérito que se le reconoció mas tarde correctamente a Antonio Meucci en el 2002), éste consistía en un aparato con un altavoz y un micrófono, que era unido mediante un cable con otro aparato semejante situado a cierta distancia. A través de dicho cable se enviaba y recibía la voz de cada uno de los extremos, lo que permitió mantener conversaciones con personas situadas a distancia. En su primera etapa, cada familia que deseara tener un teléfono debía realizar la unión con los teléfonos remotos con los que deseara mantener una conversación. Si no se ponía ese cable, era imposible hablar con el otro extremo. Eso provocó la aparición de montones de cables tirados por las ciudades uniendo teléfonos particulares como se aprecia en la Figura 3.1.

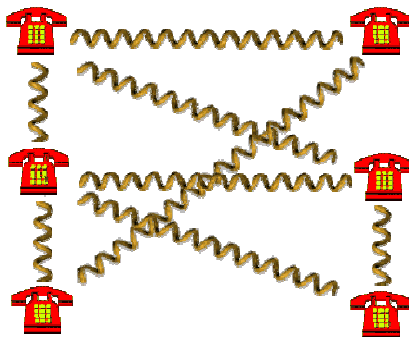


Figura 3.1 Conexión directa entre teléfonos remotos

Enseguida se vio lo inmanejable de la situación y se le puso solución. Una entidad global se encargó de gestionar los cables, de modo que cada teléfono se unió a una centralita (ver Figura 3.2). Cuando alguien deseaba realizar una llamada, en la centralita se unían los cables de ambos teléfonos, lo que permitía hablar con cualquier teléfono que estuviera conectado a la centralita, sin necesidad de conectar un cable específico con cada teléfono. Para conseguir esto, se hizo necesaria la identificación de cada teléfono mediante un número.

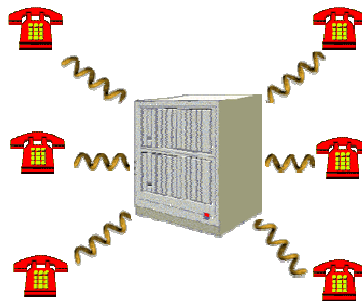


Figura 3.2 Conexión teléfonos remotos a centralita

Al principio las centralitas eran manuales. Era necesaria la existencia de un operador que realizara la unión de los cables, a través de grandes paneles con montones de conectadores. Con el tiempo, se inventó la centralita automática, que permitió eliminar la necesidad de esa persona, además de acelerar el proceso.

Posteriormente comenzaron a instalarse centralitas en distintas ciudades, que luego eran unidas entre sí. Gracias a eso, se pudieron realizar llamadas interurbanas. Para lograrlo, la centralita origen debía unir el cable del teléfono que realizaba la llamada con el cable que la unía con la centralita destino. Y ésta, a su vez, debía unir este cable con el del teléfono destino.

Durante mucho tiempo, toda la red telefónica fue analógica. La información transmitida por los cables era una transformación directa de la voz en voltaje, que era lo que se enviaba y recibía. En su camino desde el origen al destino, la señal atravesaba diversos filtros analógicos (debido a la multiplexación por división de frecuencia), repetidores y amplificadores. Todos estos dispositivos (además de los posibles problemas del cable o interferencias) provocaban la aparición de ruidos

en el sonido que no podían ser eliminados fácilmente, y que originaban una baja calidad de sonido en el otro extremo.

Con la aparición de la telefonía digital, las cosas mejoraron. Mediante el uso de conversores analógico/digital y digital/analógico, se elimina completamente el ruido en una conversación, dado que en lugar de enviar la voz convertida en voltaje, se envía esa voz digitalizada, la cual cuando llega a un punto intermedio de la red (centralita, repetidor, etc.) la señal original puede ser restaurada completamente.

Progresivamente, las redes telefónicas de los distintos países se han ido transformando en digitales, en lo que a conexión entre centralitas se refiere. La conexión entre los teléfonos y la centralita sigue siendo analógica, pero las centralitas recogen la señal y la digitalizan, por lo que no se acumula ruido en el sonido por culpa de la conexión entre centralitas. Además, el uso de señales digitales modifica el modo de multiplexar las conexiones entre ellas, que pasan de utilizar división de frecuencia, para comenzar a usar división de tiempo, eliminando la existencia de filtros analógicos.

La multiplexación por división en el tiempo se basa en la posibilidad de enviar una determinada porción de la conversación en menos tiempo del que ésta ha durado. Imaginemos que es posible enviar la voz emitida por uno de los extremos durante un segundo al otro extremo a través de un cable, utilizando únicamente medio segundo. Gracias a eso, el cable quedará libre el resto del medio segundo, que podemos utilizar para enviar otro segundo de una conversación diferente. Haciendo esto continuamente, lograremos enviar a través de un solo cable dos conversaciones simultáneamente, repartiendo el uso del teléfono entre las dos.

Esto es posible únicamente gracias a la digitalización de la voz, que permite almacenar partes de la conversación y mandarlas instantes después. Es posible dividir, por ejemplo, cada conversación en secciones de milésimas de segundo que son enviadas a través del cable en mucho menos tiempo aún, pudiendo aprovechar el mismo cable para cientos de conversaciones.

3.1.2 Funcionamiento de la red de telefonía tradicional

A pesar de los diversos avances, el funcionamiento básico de las redes de telefonía no ha cambiado. La realización de una llamada se compone de tres fases: realización de la conexión, conversación, finalización de la conexión.

Cuando un usuario decide realizar una llamada, descuelga el teléfono. Esto es detectado en la centralita a la que está conectado (A), lo que hace que se envíe el tono, invitando a marcar. Cuando la centralita recoge el número destino, debe conseguir realizar una conexión entre ambos extremos. Para eso, decide en función del número, con qué centralita cercana debe conectarse para que la unión entre los extremos se realice. Una vez elegida, se reserva un canal de comunicación con esa centralita (B). Ese canal sería un canal de frecuencia en las centralitas analógicas, o uno de tiempo en las digitales.

La centralita B realiza la misma operación, con una centralita C, y ésta con otra, y así sucesivamente hasta que se llega a la centralita donde está conectado el teléfono destino. Cuando esto ocurre, esta última realiza la conexión entre el canal proveniente del origen y el teléfono destino, que comenzará a sonar. Como resultado de todo el proceso, existe un canal de comunicación reservado entre el origen y el destino, que se mantendrá inmutable durante toda la llamada.

Para finalizar la llamada, el teléfono origen es colgado, lo que se detecta en la centralita A, que cierra la conexión entre el teléfono y la centralita B. Ésta se da cuenta de este hecho, y cierra la conexión entre la centralita A y la C, y así sucesivamente hasta llegar al teléfono destino. Al final, todos los canales reservados se liberan, pudiendo ser utilizados de nuevo para otras llamadas.

Lo más destacable en este proceso es la existencia del canal reservado. Éste no podrá ser utilizado por ninguna otra llamada mientras no se libere, al finalizar la llamada, incluso aunque el canal no se utilice. Si en algún momento ninguno de los extremos habla, el canal estará de todas formas

utilizado. Esto supone un claro desperdicio de recursos, en especial si nos damos cuenta de que las centralitas tienen limitado el número de canales disponibles, y su configuración.

3.2 Generalidades

3.2.1 ¿Qué es la VoIP?

La VoIP o Voz sobre el IP, es una tecnología que permite la transmisión de voz comprimida y digitalizada en paquetes a través de redes de datos, en lugar de establecer circuitos dedicados como en la telefonía tradicional, RTPC (Red Telefónica Pública Conmutada) o PSTN. La comunicación se realiza por medio del Protocolo IP (Internet Protocol), que permite aprovechar el ancho de banda y conexiones de redes cableadas e inalámbricas disponibles, ahorrando costos importantes para empresas y particulares. Sin embargo, una de las grandes desventajas de ésta tecnología es que el protocolo IP no ofrece QoS (Calidad de Servicio), por lo tanto se pueden obtener retardos en las transmisiones que podrían afectar la calidad en la recepción de la voz.

Ligado a lo que es VoIP, hay otro concepto el cual es ToIP o mejor conocido como Telefonía IP, el cual por lo general suele tratarse como sinónimo de la primera, sin embargo, hay que dejar en claro que existe cierta diferencia entre ambas. La telefonía IP hace referencia a servicios de comunicaciones (aplicaciones de voz, de fax y/o de mensajería de voz) que se transporta a través de una red IP. El componente clave de la telefonía IP son los equipos que convierten la señal de voz analógica en paquetes IP. Estos equipos pueden ser tarjetas específicas para PC, software específico o servidores-pasarela de voz. Esta red IP puede ser la red de su empresa, por ejemplo para las llamadas internas de la empresa. La telefonía IP también se puede utilizar para llamadas externas, usando por ejemplo Internet, en lugar de la red de telefonía pública conmutada (PSTN). En otras palabras, la Telefonía IP es una aplicación práctica que utiliza la tecnología de voz IP.

El Protocolo Internet en un principio se utilizó para el envío de datos, actualmente debido al creciente avance tecnológico, es posible enviar también voz digitalizada y comprimida en paquetes de datos, los cuales pueden ser enviados a través de tecnologías como Frame Relay,

ATM, Satélite, etc. Una vez que estos paquetes llegan a su destino son nuevamente reconvertidos en voz.

3.2.2 ¿Cómo funciona VoIP?

Años atrás se descubrió que mandar una señal a un destino remoto también podía hacerse de manera digital, antes de enviar la señal se debía digitalizar con un convertidor análogo-digital, transmitirla y en el extremo de destino transformarla de nuevo a formato análogo con un convertidor digital-análogo.

VoIP funciona de esa manera, digitalizando la voz en paquetes de datos, enviándola a través de la red y reconvirtiéndola a voz en el destino. Básicamente el proceso comienza con la señal análoga de voz que es digitalizada en señales PCM (Pulse Code Modulation) por medio del codificador/decodificador de voz (codec). Las muestras PCM son pasadas al algoritmo de compresión, el cual comprime la voz y la fracciona en paquetes que pueden ser transmitidos. En el extremo receptor se realizan exactamente las mismas funciones en un orden inverso.

3.2.3 Elementos de una red de VoIP

En la actualidad podemos encontrar en el mercado una serie de elementos disponibles que nos permitirían construir aplicaciones de VoIP. Algunos de estos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC / IP).
- Gatekeeper.
- Unidades de audio conferencia múltiple. (MCU Voz)
- Servicios de Directorio.

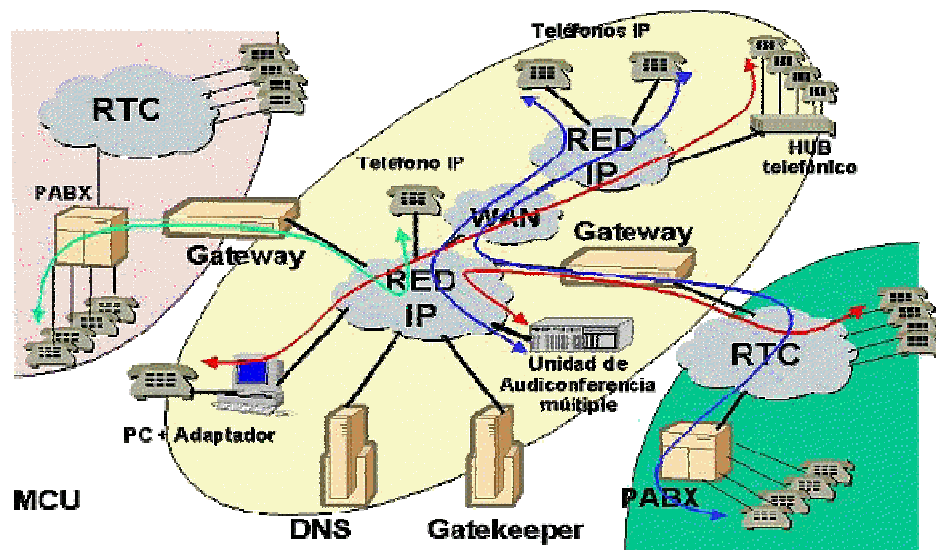


Figura 3.3 Elementos de una red de VoIP

Todos estos elementos los podemos ver en la Figura 3.3, la cual muestra una red convencional de VoIP que se conecta a la red de telefonía tradicional o RTC (red de telefonía conmutada). Unos de los elementos más importantes de la VoIP son los Gatekeeper y los Gateway, ya que la presencia de ellos dentro de la red son de gran relevancia y sus tareas a desarrollar los convierten en elementos claves en las redes de VoIP comerciales.

3.3 Protocolos de Señalización

En los últimos años, los protocolos de señalización para el servicio de transmisión de voz han experimentado una fuerte evolución, puesto que cada vez más, se están usando las redes de conmutación de paquetes para transportar tráfico de voz. Las necesidades de calidad de servicio hacen que sea necesaria una gestión de recursos que asegure la optimización de la capacidad de transporte de la voz extremo a extremo, para ello surgen los protocolos de la señalización.

Por señalización se entiende el conjunto de informaciones intercambiadas entre los dos extremos de la comunicación que permiten efectuar operaciones de:

- Supervisión (detección de condición o cambio de estado).

- Direccionamiento (negociación y establecimiento de llamada).
- Explotación (gestión y mantenimiento de la red).

Para cumplir los requerimientos de señalización existen principalmente dos protocolos: H.323 y SIP, los cuales serán descritos a continuación.

3.3.1 Protocolo H.323

3.3.1.1 Descripción del estándar H.323

H.323 es una recomendación de la Unión Internacional de Telecomunicaciones (ITU) que fija los estándares para comunicaciones multimedia sobre LANs sin calidad de servicio (QoS) garantizada. Estas redes dominan la mayoría de ordenadores de las empresas de hoy en día y funcionan no solo con redes TCP/UP, sino también IPX sobre Ethernet, Fast Ethernet y Token Ring. Por lo tanto, H.323 es un importante bloque para toda una nueva área de aplicaciones LAN para comunicaciones multimedia. La arquitectura de H.323 define todo lo necesario (componentes, protocolos, señalización, códecs, etc.) para llevar a cabo la comunicación y garantizar así la compatibilidad entre dispositivos.

Los protocolos usados en la comunicación H.323 son:

- Control de las llamadas: H.245, H.225.0
- Datos: T.120
- Audio: G.711, G.722, G.723.1, G.728, G.729.
- Vídeo: H.261, H.263.

La pila de protocolos queda estructurada como indica la Figura 3.4.

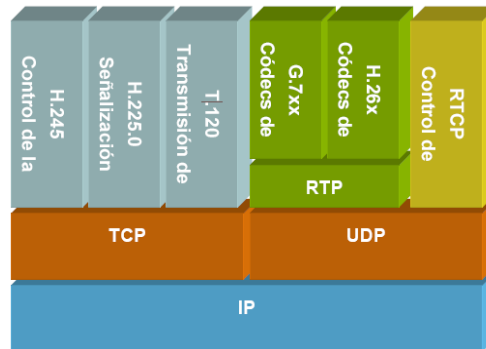


Figura 3.4 Pila de protocolo H.323

3.3.1.2 Componentes de un sistema H.323

En la Figura 3.5 observamos los componentes de H.323 que consisten en:

- Terminales.
- Gateways.
- Gatekeepers.
- Unidades de control punto multipunto.

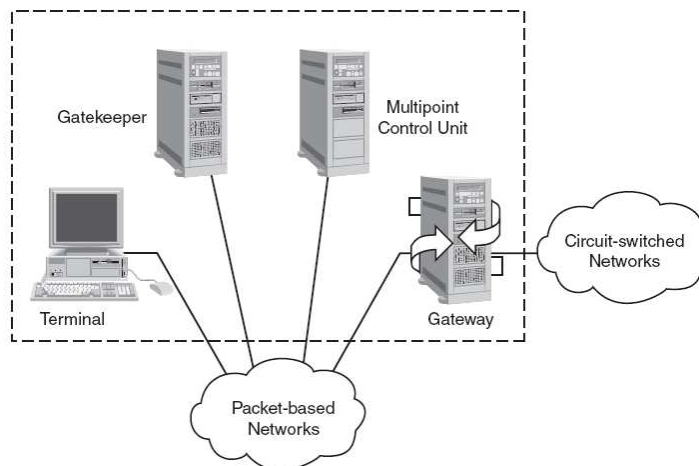


Figura 3.5 Entorno H.323

3.3.1.2.1 Terminal

Un terminal H.323 es la interfaz entre el usuario final y la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, Gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y / o datos entre los dos terminales. El terminal se comunica con el Gateway VoIP usando los protocolos H.245 para el control de llamada, Q.931 para el establecimiento de llamada, y RAS para el registro y administración con su Gatekeeper local.

3.3.1.2.2 Gateway

Un Gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o Gateways en una red conmutada. En general, el propósito del Gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. En otras palabras, nos servirá de pasarela entre el entorno de vídeo sobre IP H.323 y el entorno vídeo sobre RDSI H.320.

Los Gateways no son necesarios a menos que se requiera la interconexión con la Red de telefonía pública conmutada. Por lo tanto, los terminales H.323 pueden comunicarse directamente sobre la red de paquetes sin conectarse con un Gateway. El Gateway actúa como un terminal H.323 o MCU en la red IP y un terminal telefónico en la red de telefonía pública. Podemos considerar al Gateway como una caja que por un lado tiene una interfase LAN y por el otro dispone de una o varias de las siguientes interfaces:

- FXO. Para conexión a extensiones de centralitas o a la red telefónica básica.
- FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI (2B+D)
- PRI. Acceso primario RDSI (30B+D)
- G703/G.704. (E&M digital) Conexión específica a centralitas a 2 Mbps

3.3.1.2.3 Gatekeeper

El Gatekeeper es una entidad que se encarga del control, el enrutamiento y la seguridad de la comunicación, de manera que no se produzcan situaciones de saturación en la red. Es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de éste. En la Figura 3.6 se muestran sus funciones principales

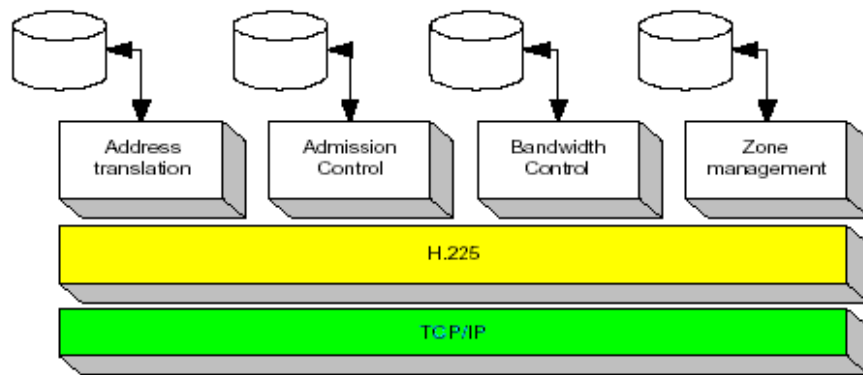


Figura 3.6 Funciones del gatekeeper

Funciones principales del Gatekeeper:

- **Traducción de direcciones:** esta función permite a cualquier terminal o Gateway, recuperar la dirección IP a partir de una dirección alias, o viceversa. Además, evita que el terminal o el Gateway tenga que hacer la traducción localmente, logrando de esta manera que no existan errores de conexión o direcciones IP desconocidas.
- **Control de admisión (RAS, Registration Admission and Status):** el Gatekeeper gestiona el control de admisión basándose en criterios como el ancho de banda disponible en la red y otros criterios.
- **Control del ancho de banda:** maneja el ancho de banda disponible en la red H.323, con el que el administrador puede limitar el número de conexiones simultáneas y así evitar problemas de congestión en la red que puedan reducir la calidad del servicio.

- **Gestión de su zona:** define qué terminales H.323 están registrados en este Gatekeeper. Cada terminal es responsable de registrarse a un Gatekeeper.
- **Conversión de números de teléfono estándar E164 a direcciones nativas H.323:** Esta funcionalidad es imprescindible cuando se pretende establecer comunicación (a través de un Gateway) con la red telefónica tradicional.

3.3.1.2.4 MCU Multipoint Control Units

El MCU es el elemento encargado de controlar las diferentes situaciones que pueden producirse a lo largo de una comunicación (conferencia) y facilitar que ésta se pueda llevar a cabo. Sus características más importantes son:

- Soporta conferencia entre 3 o más terminales.
- Realiza la distribución de comunicaciones unicast, multicast o híbridos, ahorrando ancho de banda.
- Controla el dinamismo de llamadas multimedia (*join, invite*, controles de la conferencia).
- A menudo, las funciones del MCU son llevadas a cabo por un terminal (el usuario que se conecta a una conferencia permite a los otros usuarios que se conecten con él).

Partes del MCU:

- El Multipoint Controller.
- El Multipoint Processor: es opcional. conmuta los datos de audio/video de todos los terminales H.323 bajo el control de H.245. Tiene las mismas funciones de audio/video Vocoder que las incluidas en todos los otros terminales o Gateways H.323. El MCU se puede integrar en un Gateway o Gatekeeper local.

3.3.1.3 Establecimiento y control de llamada

3.3.1.3.1 Inicio de llamadas con H.225.0

Hay dos partes en H.225.0 empezaremos con la de “Call Signaling” (señalización de llamada) para establecer las llamadas entre dos terminales. El protocolo utilizará Q.932 para iniciar y finalizar las llamadas, si bien Q.932 se diseñó inicialmente para redes RDSI, H.225.0 adopta su formato.

Las llamadas podrán realizarse directamente de terminal a terminal, o bien pasar por un gatekeeper que las enrutará. El uso del call signaling es obligatorio para el establecimiento de una llamada entre dos puntos terminales. El formato de la trama se muestra en la Figura 3.7.

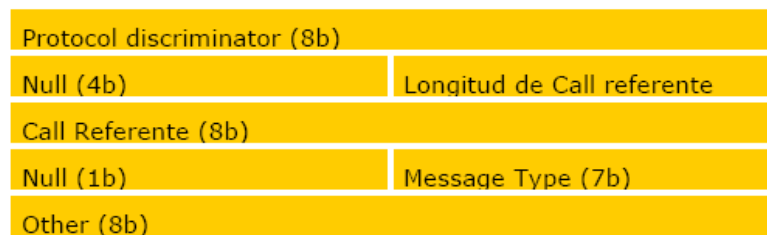


Figura 3.7 Trama H.225.0

Dado que estos mensajes son críticos para el establecimiento de la llamada, se realizarán sobre TCP, orientado a conexión, y con garantía de recepción. Los mensajes posibles serán:

- Mensajes de establecimiento:
 - o Alerta, aviso de llamada (alerting).
 - o Proseguir llamada (Call proceeding).
 - o Conectar (connect).
 - o Configuración del establecimiento (setup).
- Mensajes de desconexión:
 - o Finalización de la llamada completa (release complete).

- Otros mensajes:
 - o Estado (state)
 - o Estado de la búsqueda (state inquiry)
 - o Mensajes de información (information)

3.3.1.3.2 Media control H.245

Una vez establecida la llamada, esta se transmitirá sobre los protocolos RTP y RTCP, pero aún tendremos que negociar los canales a usar en la comunicación. Esto se consigue mediante H.245, cuyas funciones incluyen:

- **Evitar conflictos:** Determina que terminal podrá decidir quien y cuándo puede tomar una acción (maestro) a diferencia del resto de terminales (esclavos). Esto durará toda la llamada y evitará que surjan conflictos posteriores cuando los terminales quieran llevar a cabo acciones incompatibles a la vez.
- **Decidir qué transmitir y cómo:** Los terminales negociarán sus capacidades en cuanto a recepción y transmisión, informando del tipo de comunicación que soporta y los codificadores disponibles, velocidad de la comunicación (bit rate), etc. Permitirá también renegociar dichas capacidades en cualquier momento
- **Gestión de los canales:** estos pueden ser uni o bidireccionales, y vienen marcados por un identificador (son pues, canales lógicos). El protocolo decidirá que canales abrir o cerrar, manteniendo siempre el 0, para uso propio.

Al igual que en el caso del H.225.0, los mensajes de H.245 se transmitirán mediante TCP, para garantizar su recepción.

3.3.1.3.3 Establecimiento de una llamada con H.225 y H.245.

Veamos como se combinan los protocolos mencionados para realizar una llamada. Para simplificar, veremos el caso en que dos equipos se comunican directamente, sin hacer uso del gatekeeper. El caso con gatekeeper es muy parecido, y en realidad es bastante común, pues los equipos terminales a menudo incorporan un gatekeeper que, por H.323, debe ser deshabilitable para evitar que cada equipo quiera usar el suyo propio.

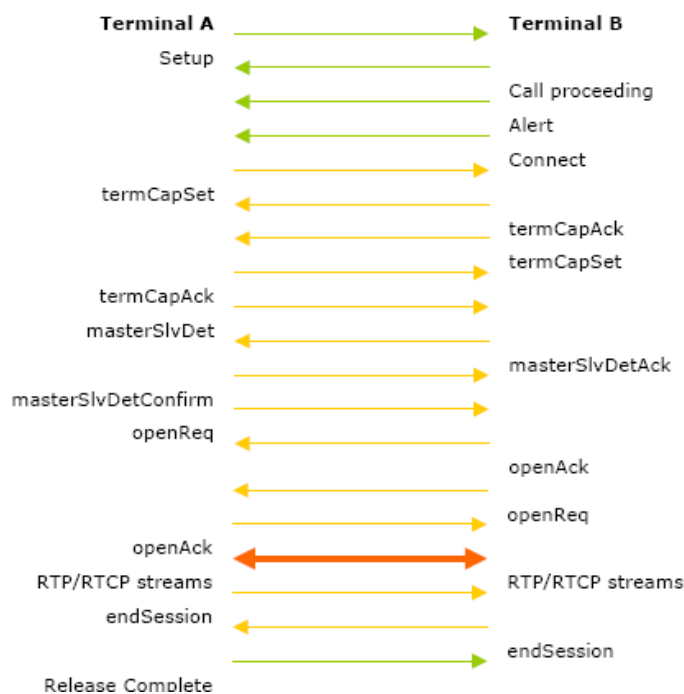


Figura 3.8 Llamada con H.225 y H.245

La Figura 3.8 muestra los mensajes correspondientes a H.225.0 en color verde, mientras que en color amarillo podemos ver las de H.245.

De acuerdo a lo anterior, analizamos la llamada iniciada por A:

Un mensaje de *setup* a B inicia la llamada. Éste incluye la petición TSAP (dirección de transporte) para la conexión H.245. B responderá con *call proceeding* que indica a A que está disponible y que la llamada sigue adelante. El mensaje *Alert* de B a A va a continuación

(opcional) y el de *connect*, indicando que se realizó la comunicación. Este es el que nos indica si el proceso tuvo éxito o no, y solo se envía si se acepta la petición TSAP.

A partir de aquí la conexión H.245 seguirá por la dirección TSAP, y negociará las capacidades con *TermCapSet* y *TermCapAck*. También fijará quien es el maestro y quien el esclavo con *masterSlvDet*, *masterSlvDetAck* y *masterSlvDetConfirm* y por último abrirá los canales lógicos con *openReg* y *OpenAck*. Hecho esto se inicia el flujo de datos sobre RTP y RTCP para la transmisión de voz video y datos, y finalmente *endSession* indica al terminal de destino que quiere terminar la llamada. Cuando este es correspondido, y de nuevo en H.225.0, se indica la finalización de conexión y la liberación de recursos con un *ReleaseComplete*

3.3.2 Protocolo SIP

SIP (Session Initiation Protocol) es un protocolo de señalización (situado en el nivel ISO / OSI de aplicación) para el establecimiento, mantenimiento y terminación de sesiones interactivas entre usuarios; estas sesiones pueden tratarse de conferencias multimedia, chat, sesiones de voz o distribución de contenidos multimedia. SIP, creado en 1996 por Mark Handley y Henning Schulzrinne, ha sido estandarizado por la IETF (Internet Engineering Task Force). La especificación más reciente de SIP se puede encontrar en el RFC 3261. SIP no define por si mismo un sistema de comunicaciones ni ofrece servicio alguno; es un protocolo flexible que se limita a ofrecer una serie de primitivas que las aplicaciones pueden utilizar para implementar servicios.

SIP ofrece funciones tales como:

- Redirección de llamadas
- Resolución de direcciones
- Determinar la disponibilidad de un punto final
- Establecer llamadas punto a punto o multipunto

3.3.2.1 Componentes SIP

SIP define cinco componentes lógicos. Estos componentes se pueden implementar en dispositivos físicos, tal como teléfonos IP, o bien como aplicaciones software; en cualquier caso un mismo dispositivo físico puede incluir uno o más componentes lógicos.

Todos los elementos SIP deben implementar obligatoriamente TCP y UDP. En ambos protocolos escucha en el puerto 5060.

Los componentes presentes en SIP son:

- El **Agente de Usuario** es una aplicación con arquitectura cliente / servidor que se utiliza para iniciar y terminar las sesiones. El cliente usuario-agente (UAC) se encarga de realizar peticiones SIP, mientras que el servidor usuario-agente (UAS) notifica al usuario cuando se recibe una petición y responde a dicha petición dependiendo de la acción tomada por el usuario.
- El **Servidor de Redirecciones** acepta una petición SIP y envía una respuesta al cliente que contiene las direcciones de los servidores con los que debe contactar el cliente.
- El **Servidor Proxy**, que contiene funciones de servidor y cliente, actúa como un intermediario que realiza peticiones en nombre de otros clientes: para ello interpreta la cabecera del mensaje y la reescribe identificando al Proxy como el que inicia la solicitud, recibe la respuesta del destinatario y se la reenvía al cliente.
- Un **Servidor de Registro** almacena (o actualiza) en una base de datos la información de contacto del usuario que realiza la petición.
- Un **B2BUA (Back to Back User Agent)** es una entidad que recibe una petición INVITE y la procesa como un servidor usuario-agente (UAS). Para determinar la respuesta a la

petición, actúa como un cliente usuario-agente que determina cómo responder a la petición y cómo realizar llamadas salientes.

A diferencia de un proxy, un B2BUA debe mantener el estado de la llamada y participar activamente en ella, enviando peticiones y respuestas. Un B2BUA tiene un mayor control de la llamada que un proxy.

3.3.2.2 Protocolos especificados por SIP

3.3.2.2.1 SDP (Session Description Protocol)

SDP es el protocolo empleado para describir una sesión multimedia, que consiste en un conjunto de flujos de medios (audio, vídeo o datos) que existen durante un determinado tiempo. Los paquetes SDP contienen (entre otros campos) información acerca del ancho de banda, los protocolos de transporte empleados, los códecs utilizados en la sesión, y la dirección de contacto del iniciador de la sesión.

Se define dos tipos de mensajes SIP: Peticiones y Respuestas.

- Peticiones SIP. Se definen 6 métodos básicos:
 - a. INVITE: invita a un usuario a iniciar una sesión.
 - b. ACK: confirma una solicitud INVITE.
 - c. BYE: finaliza una sesión.
 - d. CANCEL: cancela el establecimiento de una sesión.
 - e. REGISTER: comunica la localización de usuario (nombre de equipo, IP).
 - f. OPTIONS: comunica la información acerca de las capacidades de envío y recepción de teléfonos SIP.
- Respuestas SIP: Existen también mensajes SIP como respuesta a las peticiones. Existen 6 tipos de respuestas, que se diferencian por el primer dígito de su código. Estas son:

- a. 1xx: Mensajes provisionales.
- b. 2xx: Respuestas de éxito.
- c. 3xx: Respuestas de redirección.
- d. 4xx: Respuestas de fallas de método.
- e. 5xx: Respuestas de fallas de servidor.
- f. 6xx: Respuestas de fallas globales.

Algunos de los mensajes que se dieron a conocer anteriormente, los podemos apreciar en el ejemplo de comunicación ilustrado en la Figura 3.9, que corresponde a un intercambio de mensajes bajo el protocolo SIP.

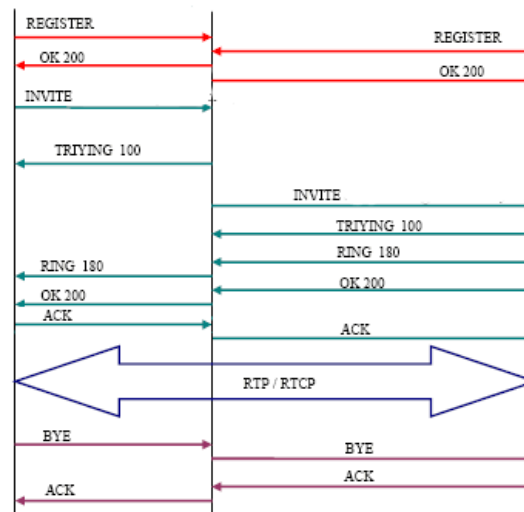


Figura 3.9 Intercambio de mensajes en SIP

- **Las dos primeras transacciones corresponden al registro de los usuarios.** Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición **REGISTER**, donde los campos **from** y **to** corresponden al usuario registrado. El servidor Proxy, que actúa como Register, consulta si el usuario puede ser autenticado y envía un mensaje de **OK** en caso positivo.
- **La siguiente transacción corresponde a un establecimiento de sesión.** Esta sesión consiste en una petición **INVITE** del usuario al proxy. Inmediatamente, el proxy envía un

TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario B envía un Ringing 180 cuando el teléfono empieza a sonar y también es reenviado por el proxy hacia el usuario A. Por último, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).

- **En este momento la llamada está establecida, pasa a funcionar el protocolo de transporte RTP** con los parámetros (puertos, direcciones, codecs, etc.) establecidos en la negociación mediante el protocolo SDP.
- **La última transacción corresponde a una finalización de sesión.** Esta finalización se lleva a cabo con una única petición BYE enviada al Proxy, y posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

3.4 Protocolos de Transporte

3.4.1 RTP/RTCP *Transmisión de datos durante la llamada*

El protocolo RTP trabaja sobre UDP, y se utilizará durante la llamada en sí para enviar los flujos de datos, voz y video. El protocolo da información que permitirá al receptor re-sincronizar los datos para poder sincronizar, por ejemplo, el movimiento de los labios con la voz, o para que un texto aparezca en el momento adecuado (como por ejemplo un subtítulo). Dado que RTP se puede configurar para tener una muy baja latencia, es muy útil para conversaciones interactivas o para envío de contenidos multimedia.

Por otra parte, RTCP trabaja con RTP para realizar estadísticas del tráfico, como por ejemplo el número de bytes enviados, los paquetes enviados y perdidos, el jitter o desorden de llegada, o el tiempo de latencia. Con ello, las aplicaciones extremas podrán juzgar la calidad de la conexión y ajustarlas según sea necesaria, cambiando entre codecs de alta compresión para malos canales a otros de mayor calidad cuando mejoren las condiciones.

Detallemos ambos protocolos mirando sus tramas. La Figura 3.10 muestra la trama RTP.

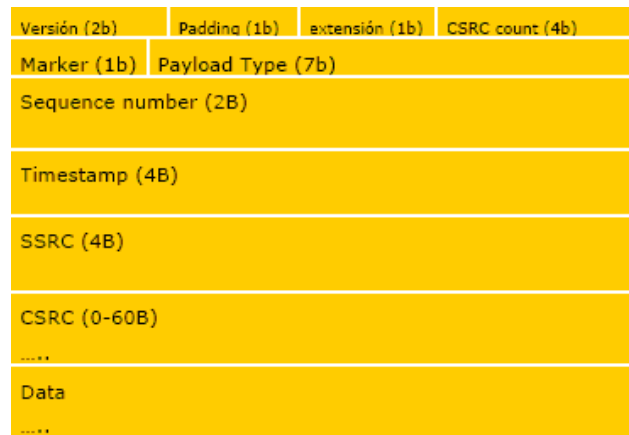


Figura 3.10 Trama RTP

Los campos corresponden a:

- Versión: actualmente, la 6
- Padding bit/Extensión bit: Indica si hay bits de relleno o de Extensión
- CSRC count: indica el nombre de contribuyentes en el flujo, con un máximo de 15.
- Marker: podría ser usado arbitrariamente por las aplicaciones.
- Payload type: indica si el paquete lleva datos, voz o audio, y con qué códecs
- Timestamp: indica el tiempo de envío, que podrá ser usado en el receptor para resincronizarse
- SSRC: indica quien es el emisor del mensaje
- CSRC: indica quienes son cada uno de los contribuyentes. A 4B por contribuyente, tendremos un máximo de 60B
- Data: los datos en sí.

Para el caso RTCP observamos su trama en la Figura 3.11

Versión (2b)	Padding (1b)	Reception report count (5 bits)
Packet type		
Length		
Data Report		

Figura 3.11 Trama RTCP

Tendrá los siguientes campos extras:

- Reception report count: indica cuantos informes se transmiten
- Packet type: indica el tipo de paquete RTCP
- Length: longitud del informe, en bytes
- Data Report: el informe en sí, con información sobre el jitter, los paquetes recibidos y perdidos, etc.
- RTP constituye el protocolo básico para la transmisión de los datos, y se verá complementado por los informes mediante RTCP.

3.5 Códecs

Se clasifican en dos tipos: Waveform Codecs o Vocoders. Los primeros van a tratar de comprimir la forma de onda que tengan a la entrada, muestreándola y tratando con dichos valores. Naturalmente, van a funcionar con cualquier voz, ruido o sonido que introduzcamos. Los Vocoders en cambio van a ser capaces de “entender” la voz humana, adaptando la onda de entrada a un modelo vocal. Los parámetros de dicho modelo se enviarán al receptor, el cual sintetizará una voz basada en ese modelo vocal. Típicamente, los Vocoders van a basar su funcionamiento en filtrar una señal base. Esto es análogo a tomar el sonido emitido por las cuerdas vocales y filtrarlos con labios, dientes o posición de la lengua). Los Vocoders tendrán pues problemas para adaptar sonidos que no sean voces a su modelo vocal.

3.5.1 Waveform códecs

Destacaremos de estos que:

- Se utilizan circuitos estándar muy conocidos, rápidos y poco complejos.
- No introducen prácticamente retardo algorítmico.
- Son muy adecuados para emplear en sistemas TDM.
- No son tan útiles para voz paquetizada, ya que una sola muestra es demasiada poca información como para justificar la cabecera de un paquete entero, y tener que reunir varias muestras implica introducir un retardo.

De este tipo se permiten G.711 y G.722

3.5.1.1 G.711

Es el estándar para enviar audio en un canal de 64kbps. Muestrea la señal a 8Khz, es decir, transmitirá la banda de 0 a 4KHz de la voz. A una muestra cada 0.125ms es comprensible que no podamos esperar mucho para llenar varios paquetes. Se usan 8 bits por muestra, de forma fija. Trabaja en PCM (Pulse Code Modulation)

Sobre paquetes, se suelen usar tramas de 40 muestras (5 ms. de voz) o de 80 (10ms).

3.5.1.2 G.722

También conocido como SB-ADPCM (SubBand – Adaptive Differential Pulse Code Modulation), nos aportará mejores respecto al G.711. Su velocidad de muestreo se dobla, a 16KHz, ofreciendo un ancho de banda de 8KHz. En realidad, la señal se va a dividir en dos bandas, y cada una de ellas se enviará mediante un ADPCM (Adaptive Differential Pulse Code Modulation), que al ser diferencial, funciona mejor para bandas reducidas. Encontraremos tres velocidades posibles:

- 64 Kbps (2 bpm para la banda inferior y 6 bpm para la banda superior).
- 56 Kbps (con 8 Kbps libres opcionales para datos) (2 y 5 bits/muestra).
- 48 Kbps (con 16 Kbps para datos) (2 y 4 bits/ muestra).

3.5.2 Codificadores mediante vocoders

Resultan mucho más eficaces con el ancho de banda, puesto que nos permitirán eliminar o comprimir los silencios, generar ruido de comfort (hace la conversación más apacible al usuario) y ocultar las tramas perdidas. Sin embargo, a veces la voz se oirá mal, debido a la mala codificación o a la falta de recursos de envío, y definitivamente tendremos problemas con otros sonidos que no sean voz. En concreto, no vamos a poder transmitir fax o datos de MODEM. Encontraremos típicamente, los siguientes algoritmos:

- **LPC (Linear Predictive Coding):** Este modelo convierte el trato vocal en un filtro excitado por una señal de entrada. La señal generada será simplemente el resultado de filtrar dicha señal. Así pues, el LPC codificará la señal de excitación y el filtro.
- **CELP (Code Excited Linear Predictor):** La idea básica es la del LPC, pero la señal de excitación se codifica mejor, diferenciando entre sonidos sonoros, con intervención de las cuerdas vocales, de las sordas, que no son más que ruido blanco. Para las excitaciones sonoras definimos un *codebook* de señales de excitación, de modo que tan solo tendremos que enviar el índice dentro de dicha tabla. Por otro lado, el filtro se codifica con predicción lineal, es decir, como variación respecto al filtro anterior.
- **ACELP (Algebraic CELP):** Se trata de un CELP para DSP's más simples, y usa un *codebook* simplificado.
- **CS-ACELP (Conjugate Structure - ACELP):** Divide la señal de excitación en dos contribuciones: "adaptative codebook" (una versión retrasada de la excitación usada en la trama anterior) y "fixed codebook" (tabla prefijada).

- **MP-MLQ (Multipulse Maximum Likelihood Quantization):** Usa un conjunto de pulsos (o ruido) como señal de excitación.

Los permitidos por el estándar son: G.723.1, G.728 y G.729.

3.5.2.1 G.723.1

Usa dos algoritmos, en función de si es la versión de 5.3Kbps o 6.3Kbps. Para la primera, un MP-MLQ, y para el segundo un ACELP. El bloque de voz codificado es de 30ms y 158bits o 189bits para 5.3Kbps o 6.3Kbps respectivamente.

De por sí, el algoritmo introduce un retardo de 47.5ms, a los que habrá que añadir los retardos de transmisión.

Por otro lado, el algoritmo incluye VAD (Voice Activity Detection) que detectará cuando no se está hablando, para ahorrar el ancho de banda; CNG (Comfort Noise Generation) que generará ruido aleatorio de fondo durante esos instantes de silencio, en beneficio del oyente. Durante los silencios se mandarán tramas SID (Silence Insertion Descriptor) que solo ocupan 5 bytes por trama, y llevan los parámetros necesarios para generar el ruido de confort.

3.5.2.2 G.728

Usará algoritmo Low Delay CELP (LD-CELP) con un bitrate de 16 Kbps, 12.8 Kbps o 9.6 Kbps. La trama es de 0.625 ms. y 10 bits. El retardo algorítmico es mínimo: 0.625ms y a la práctica nunca es mayor que 2 o 3 ms.

3.5.2.3 G.729

Dispone de varios bit rates: (8Kbps: G.729, G.729A. 6.4Kbps: G.729D. 11.8Kbps G.729E). Usa el algoritmo CS-ACELP. G.729A es una versión ligeramente más simple de G.729. D y E son extensiones para otros bit rates.

En G.729, la trama es de 10ms, o sea, 10bytes. El retardo algorítmico es de 15ms, y una vez implementado en la realidad, de unos 20ms. En caso de perder una trama, el algoritmo repite la última trama, pero ligeramente atenuada para que no se note tanto. Usa también VAD, CNG y SID.

Las tramas SID, en este caso, serán de 15 bits (contra los 80 de la trama de voz) pero solo se envían si el ruido de fondo ha cambiado.

3.6 Aspectos importantes de VoIP

3.6.1 Seguridad

VoIP es una tecnología que ha de apoyarse necesariamente en muchas otras capas y protocolos ya existentes de las redes de datos. De esta manera VoIP va a heredar ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes problemas clásicos de seguridad que afectan al mundo de las redes de datos.

Como vemos en la Figura 3.12 la seguridad de VoIP se construye sobre muchas otras capas tradicionales de seguridad de la información.



Figura 3.12 Capas tradicionales de seguridad de la información

En la Tabla 3.1 se detallan algunos de los puntos débiles y ataques que afectan a cada una de las capas.

Capa	Ataques y vulnerabilidades
Políticas y Procedimientos	Contraseñas débiles. Ej: Contraseña del VoiceMail Mala política de privilegios Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Ej: Acceso físico a un gatekeeper. Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP unreachable SYN floods
Seguridad en los Servicios	SQL injections Denegación en DHCP DoS
Seguridad en el S.O.	Buffer overflows Gusanos y virus Malas configuraciones
Seguridad en las Aplicaciones y protocolos de VoIP	Fraudes SPIT (SPAM) Vishing (Phishing) Floods (INVITE, REGISTER, etc..) Secuestro de sesiones (Hijacking) Interceptación (Eavesdropping) Redirección de llamadas (CALL redirection) Reproducción de llamadas (CALL replay)

Tabla 3.1 Puntos débiles y ataques que afectan a cada una de las capas

3.6.2 QoS en redes IP

Antes de iniciar el análisis de la QoS en VoIP, debemos remarcar que las redes IP no están orientadas a conexión, como lo están las redes ATM. Debido a esta principal diferencia ya podemos decir que el retardo total suele ser mayor que en redes ATM, ya que es más lento “enrutar” que “conmutar”. Además a esto contribuye el que no exista un “control de admisión”, generando una gran variabilidad en el nivel de congestión de la red, con paquetes que se enrutan por separado. Estos tendrán diferentes prioridades asignadas mediante el byte de TOS (Type Of Service), único mecanismo para controlarla calidad de servicio.

Los parámetros de QoS que se deben considerar cuando se habla de VoIP, son el retardo, jitter, eco y pérdida de paquetes.

3.6.2.1 Retardo

El retardo, que esta causado por distintas fuentes, es presumiblemente el efecto más notorio y perjudicial para este tipo de redes. En el G.114 de la ITU-T se especifica que el retardo máximo permisible en una comunicación extremo a extremo en una llamada de voz debe de ser menor que 150ms. Así pues podemos ya establecer una cierta distinción de zonas de retardo, como la siguiente:

- 25 ms. no existen dificultades para mantener una conversación normal.
- 25-150 ms. la calidad es aceptable para la mayoría de los usuarios pero se hace necesaria la utilización de canceladores de eco.
- 150-400 ms. hay dificultades para seguir una conversación (caso de las comunicaciones vía satélite). Es necesaria la utilización de canceladores de eco de gran rendimiento (supresores de eco).
- ≥ 400 ms. las dificultades para mantener una conversación interactiva hacen que la calidad sea inaceptable para la mayoría de los usuarios.

3.6.2.1.1 Fuentes de retardo

Para el retardo de extremo a extremo en una transmisión de voz en una red de paquetes, tenemos los siguientes tipos de retardo:

- Retardo del Codec.
- Retardo algorítmico (Algorithmic delay).
- Retardo de procesado (Processing delay).
- Retardo de propagación (Propagation delay).
- Retardo de serialización (Serialization delay).
- Retardo introducido por la red (Network delay).

Su importancia y sus valores variarán en función de la red que tengamos; pese a este hecho siempre siguen un mismo patrón. Un ejemplo bien podría ser la gráfica mostrada en la Figura 3.13 basada una red del tipo G.729A:

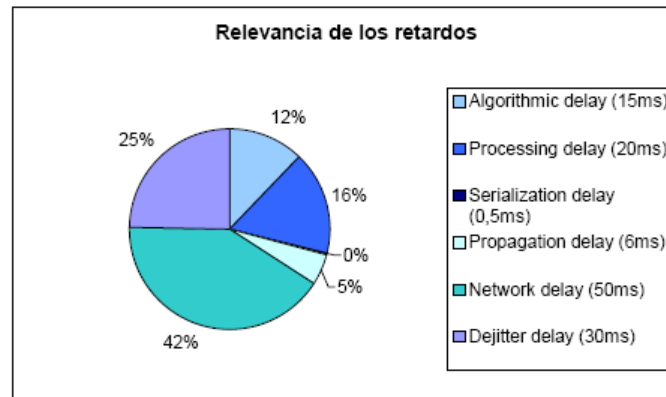


Figura 3.13 Retardo en Codec G729A

a) Retardo del códec

Este tipo de retardo se haya a partir de una contribución de dos tipos diferentes de retardo, el que introduce el propio códec, denominado retardo algorítmico, y el retardo de procesado, que incluye el tiempo que se tarda en codificar las muestras de voz y empaquetarlas adecuadamente. A su vez el retardo algorítmico consta de dos contribuciones. Tenemos el retardo de acumulación (accumulation delay), basado en el almacenaje de las muestras de la voz de la trama, y el retardo de previsión (look ahead delay), sólo presente en aquellos codecs que tengan presentes algunas muestras posteriores durante la codificación.

Queda por lo tanto establecido la principal diferencia entre las dos grandes contribuciones al total del retardo del códec (ver Figura 3.14), ya que mientras el retardo algorítmico sólo depende del propio códec, el retardo de procesado depende directamente de la propia red, tanto del hardware como software de implementación.

Coder	Rate	Required block	Best case delay	Worst case delay
ADPCM, G.726	32 Kbps	10ms	2.5ms	10ms
CS-ACELP, G.729A	8 Kbps	10ms	2.5ms	10ms
MP-MLQ, G.723.1	6.3 Kbps	30ms	5ms	20ms
MP-ACELP, G.723.1	5.3 Kbps	30ms	5ms	20ms

Figura 3.14 Retardos de códecs

b) Retardo de propagación

El retardo de propagación es el tiempo que tardan los paquetes en circular o viajar por el medio físico de transporte de un extremo a extremo. Por lo tanto, su valor dependerá directamente del medio físico en el que nos encontremos: aire, cable, fibra óptica,..., por ejemplo podemos encontrarnos con: 6 μ s./Km. para cable eléctrico y 3 μ s./Km. para fibra óptica.

c) Retardo de serialización

Este retardo se basa en el tiempo que se requiere para pasar un paquete de un buffer a un enlace o viceversa. Se hace evidente que este tipo de retardo nos presentará valores diferentes en función tanto del tamaño del paquete como por la velocidad del enlace que se use.

d) Retardo introducido por la red

El network delay es uno de los eventos que participan en la congestión de la red. Por ello, es uno de los retardos más significativos por su gran relevancia, llegando hasta cuotas de los 100ms en algunas redes de tipo Frame Relay.

3.6.2.2 Jitter

El Jitter, tiempo variable entre llegadas de paquetes causado por la red, es otro de los problemas de retardo a analizar en temas de calidad de servicio. Con ese motivo se hace evidente que los

paquetes deberán ser almacenados y retenidos lo suficiente como para ordenarlos y reproducirlos en su secuencia correcta. Queda claro, entonces, que este proceso conlleva un retardo adicional y precisa de un diseño o adaptación del tamaño del buffer de “de-jitter”.

Para poder adaptar el tamaño del buffer existen dos soluciones diferentes, escogiendo la mejor en función del tipo de red de paquetes que se use:

- La primera solución consiste en medir cuanto varia el nivel de los diferentes paquetes en un corto periodo de tiempo en el buffer de “de-jitter” y de forma gradual iremos adaptándolo hasta llegar al jitter óptimo. Esta versión es la correcta sobretodo para redes como ATM, que presentan un jitter poco variable o consistente.
- En cambio la segunda solución se basa en contar los paquetes que lleguen tarde y crear así una relación entre estos paquetes y el número de paquetes que sí se han procesado correctamente. Dicha relación es la que posteriormente se usará para poder ajustar el tamaño del buffer correctamente en función, eso sí, de la relación de paquetes tardíos permitida. Esta versión es mejor para redes con alta variabilidad de jitter, es decir, para redes IP.

3.6.2.3 Eco

El eco se produce por un fenómeno técnico que es la conversión de 2 a 4 hilos de los sistemas telefónicos o por un retorno de la señal que se escucha por los altavoces y se cuela de nuevo por el micrófono.

El eco es especialmente molesto cuanto mayor es el retardo y cuanto mayor es su intensidad con lo cual se convierte en un problema en VoIP puesto que los retardos suelen ser mayores que en la red de telefonía tradicional.

- **Valores recomendados**

El oído humano es capaz de detectar el eco cuando su retardo con la señal original es igual o superior a 10 ms. Pero otro factor importante es la intensidad del eco ya que normalmente la señal de vuelta tiene menor potencia que la original. Es tolerable que llegue a 65 ms. y una atenuación de 25 a 30 dB.

- **Posibles soluciones**

En este caso hay dos posibles soluciones para evitar este efecto tan molesto:

Supresores de eco: Consiste en evitar que la señal emitida sea devuelta convirtiendo por momentos la línea full-duplex en una línea half-duplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario. El tiempo de conmutación de los supresores de eco es muy pequeño. Impide una comunicación full-duplex plena.

Canceladores de eco: Es el sistema por el cual el dispositivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido). El dispositivo filtra esa información y cancela esas componentes de la voz. Requiere mayor tiempo de procesamiento.

3.6.2.4 Pérdida de paquetes

Como último factor nos encontramos la eficiencia, que no es más que la tasa o porcentaje de paquetes recibidos correctamente. De hecho para un buen cómputo del “*accuracy*” se deben tener en cuenta tanto los paquetes que se pierden como los que se reciben erróneamente y los paquetes que se descartan al retrasarse más de lo permisible.

La pérdida de paquetes, cuyo origen está en la congestión propia de la red, depende de la capacidad de los buffers y de los retrasos de los paquetes. Su efecto varia, ya que podemos pasar de una total transparencia de cara al usuario, a considerarse intolerable con la presencia de ráfagas de errores, que perjudican aún más la tasa de error que los simples errores intermitentes o más distribuidos. De hecho existen los siguientes intervalos:

- Menos del 5% → no detectable por el usuario.
- Entre el 5% y el 10% → puede ser tolerable en función de la estrategia de reemplazo de paquetes (loss concealment).
- Más del 10% → intolerable.

CAPÍTULO IV

EQUIPOS UTILIZADOS Y PROPUESTA E IMPLEMENTACIÓN DE ENLACE WiMAX

4.1 Antecedentes

Dentro de lo que es la parte práctica de ésta tesis, lo primero, es conocer e identificar los elementos y equipos utilizados para establecer la comunicación WiMAX, los que principalmente son la estación base y estaciones suscriptoras, donde todos los equipos y elementos asociados son distribuidos por la empresa Airspan.

A continuación se entrega una descripción de las principales características técnicas de cada equipo y finalmente la implementación del enlace WiMAX realizado.

4.2 Estación Base (BS)

En la Figura 4.1 apreciamos la apariencia física de la estación base utilizada, la MicroMAX-SOC, la cual tiene un diseño altamente modular, y se compone de una parte externa de radio frecuencia (BSR, Base Station Radio) que es la que proporciona un enlace inalámbrico con los abonados y las interfaces con el proveedor del backbone, y una interna, que consiste en un adaptador de datos denominada SDA-4S que podemos ver en la Figura 4.2, que es el utilizado en nuestro caso, debido a que nuestra estación base funcionara con un único BSR, en caso contrario, sería necesario una (BSDU, Unidad de Distribución de Estación Base) para la conexión de múltiples BSR. La conexión del BSR al SDA-4S es hecha a través de una interfaz 100baseT operando sobre cable UTP categoría 5, el cual conduce datos y alimentación.

MicroMAX-SOC ha sido diseñada para soportar baja densidad de tráfico, acceso de banda ancha rural, aplicaciones empresariales y DSL operando en bandas licenciadas y no licenciadas. MicroMAX ha sido considerada para zonas en las que la concentración de usuarios no es muy grande y el tráfico que generan no es muy alto.

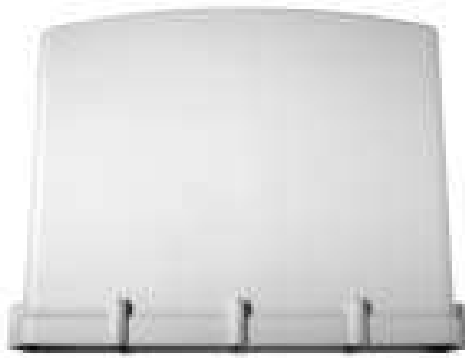


Figura 4.1 MicroMAX-SOC Base Station Radio (BSR)



Figura 4.2 SDA-4S

4.2.1 Interfaz física

En esta sección se definen todas las interfaces de un equipo externo para conexiones de red y mantenimiento.

4.2.1.1 Interfaz SDA-4S

El SDA-4S cuenta con cuatro interfaces de usuario, utilizados para conectar la estación base al backbone o conexión de vuelta a terceros por medio de conmutadores, routers, y/o unidades SDA-4S adicionales conectados en cascada. Cada puerto es RJ45 para conexión 10baseT/100baseT. Además, el SDA-4S cuenta con un conector DB15 para la conectividad a través de un adaptador de RJ45 a DB15, de alimentación y datos con la BSR.

4.2.1.2 Interfaz BSR

La BSR tiene un conector DB15 para conectividad a través de un adaptador de RJ45 a DB15 con el SDA-4S. También tiene un conector DB9 para el uso de personal específico de Airspan y un conector RJ45 para un posible uso futuro. La BSR se conecta a través de un conector hembra de 50 ohm a una antena externa por medio de cable coaxial.

La conexión entre estos dos elementos la vemos en la Figura 4.3.

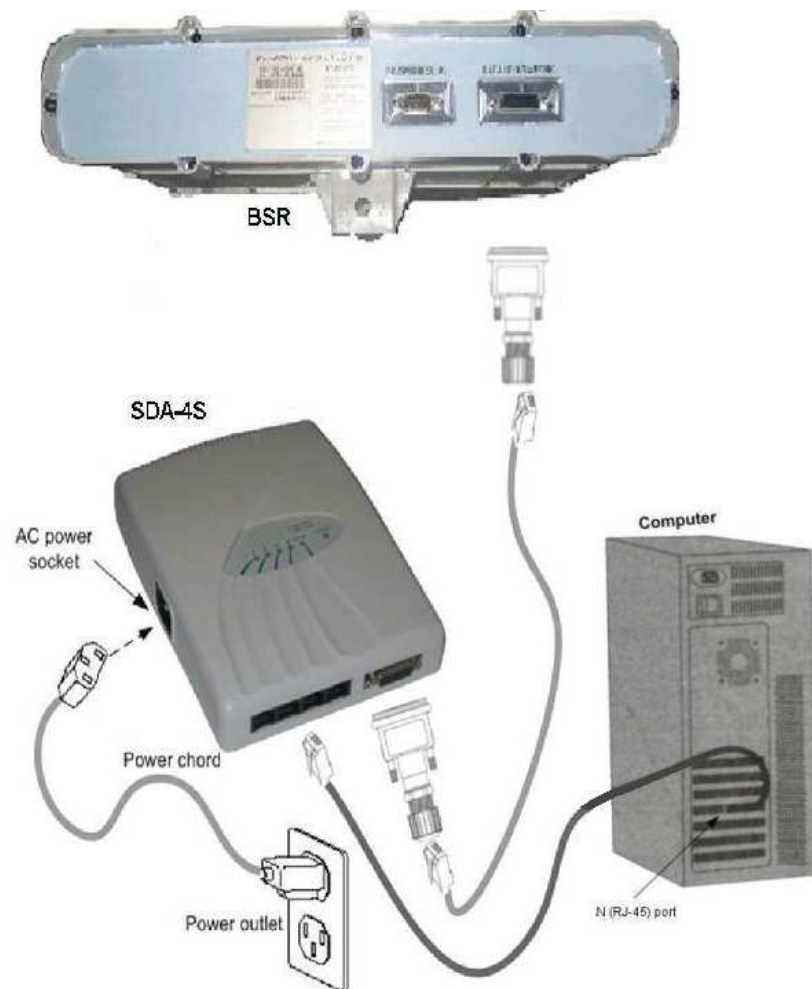


Figura 4.3 Conexión BSR a SDA-4S

4.2.2 Interfaz aire

- La comunicación del enlace WiMAX es realizado por medio de TDMA (Acceso múltiple por división de tiempo) adaptativa, con un ancho de banda máximo 3.5 MHz. por canal, cada uno con una capacidad de 256 suscriptores.
- Las frecuencias de operación y métodos duplex los podemos apreciar en la Tabla 4.1:

Frecuencia / Duplex Variante	Perfil aplicable WiMAX	Duplex	Rango de frecuencias Uplink	Rango de frecuencias Downlink
3.5GHz FDD Low	3.5F1	100MHz Full Duplex	3400 a 3452MHz	3500 a 3552MHz
3.5GHz FDD High	3.5F1	100MHz Full Duplex	3450 a 3500MHz	3550 a 3600MHz

Tabla 4.1 Frecuencias de operación y métodos duplex BSR

- Las modulaciones y correcciones de errores FEC de funcionamiento se aprecian en la Tabla 4.2.

Modulación	FEC
64QAM	3/4
64QAM	2/3
16QAM	3/4
16QAM	1/2
QPSK	3/4
QPSK	1/2
BPSK	1/2

Tabla 4.2 Modulaciones y FEC

- El nivel máximo de transmisión MicroMAX-SOC se detalla en la Tabla 4.3 de acuerdo a la diversidad de modulación utilizada. Esta es la medida en el del puerto del transceptor RF.

Máxima potencia Tx	Modulaciones soportadas
+27 dBm	BPSK, QPSK, 16QAM, 64QAM

Tabla 4.3 Potencia máxima de transmisión BSR

- La sensibilidad del receptor y el CINR (Carrier to Interference Noise Ratio) en el MicroMAX-SOC se detallan en la Tabla 4.4 para cada modulación y combinación FEC/CINR, medida en el puerto del transceptor RF.

Modulación	FEC	Niveles típicos BER < 1×10^{-6}	
		Sensibilidad Rx	CINR
64QAM	3/4	-80.0 dBm	23.0 dBm
64QAM	2/3	-82.0 dBm	21.0 dBm
16QAM	3/4	-86.0 dBm	17.0 dBm
16QAM	1/2	-88.0 dBm	15.0 dBm
QPSK	3/4	-92.0 dBm	11.0 dBm
QPSK	1/2	-94.0 dBm	9.0 dBm
BPSK	1/2	-98.0 dBm	5.0 dBm

Tabla 4.4 Niveles de sensibilidad y CINR en BSR

4.3 Estaciones Suscriptoras (SS)

Las estaciones suscriptoras, también conocidos como CPE (Customer Premises Equipment), son los equipos terminales de los abonados WiMAX. Un CPE es un terminal simple “plug and play”, similar a un módem xDSL el cual proporciona la conectividad.

Para la implementación de nuestro enlace WiMAX, el CPE utilizado es un EasyST, el cual podemos ver en la Figura 4.4, siendo éste diseñado para ser instalado fácilmente a un costado del PC del usuario final, como se puede apreciar en la Figura 4.5.



Figura 4.4 EasyST

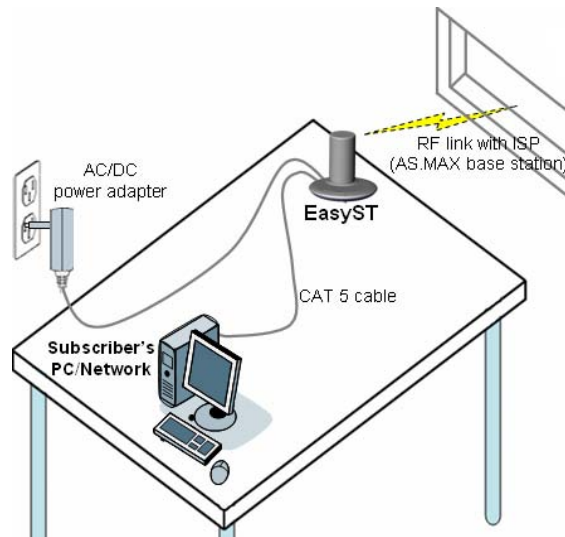


Figura 4.5 Arquitectura EasyST

El EasyST está diseñado para la vivienda y los mercados de la pequeña empresa, proporcionando alta velocidad acceso a Internet de banda ancha y una rápida conexión Ethernet al abonado de la red de área local (LAN).

4.3.1 Interfaz física

El EasyST cuenta con un puerto RJ45 para conexión Ethernet 10baseT/100baseT conectada al PC, una antena desmontable auto selectiva de 6 dBi con un controlador integrado de 6 pines, y un conector de alimentación de 6 VDC.

4.3.2 Interfaz aire

- La comunicación del EasyST con la BSR para el caso Downlink, utiliza TDMA adaptativa, mientras que para el caso Uplink, utiliza TDMA adaptativa o OFDMA (subcanalización de enlace ascendente), con soportes de anchos de banda por canal de 1.75 MHz. y 3.5 MHz.

- Las frecuencias de operación y métodos duplex los podemos apreciar en la Tabla 4.5.

Frecuencia / Duplex Variante	Perfil aplicable WiMAX	Duplex	Rango de frecuencias Uplink	Rango de frecuencias Downlink
3.5GHz HFDD	3.5F1	100MHz Full Duplex	3400 a 3500MHz	3500 a 3600MHz

Tabla 4.5 Frecuencias de operación y métodos duplex EasyST

- Las modulaciones y correcciones de errores FEC de funcionamiento se visualizan en la Tabla 4.6.

Modulación	FEC	Soporte	
		Downlink	Uplink
64QAM	3/4	Si	Si
64QAM	2/3	Si	Si
16QAM	3/4	Si	Si
16QAM	1/2	Si	Si
QPSK	3/4	Si	Si
QPSK	1/2	Si	Si
BPSK	1/2	Si	Si

Tabla 4.6 Modulaciones y FEC EasyST

- De acuerdo a las distintas modulaciones, se detalla en la Tabla 4.7 los niveles de transmisión máximos de energía en el EasyST.

Máxima potencia Tx	Modulación
24 dBm	BPSK
23 dBm	QPSK
21 dBm	16QAM
19 dBm	64QAM

Tabla 4.7 Potencia Tx EasyST según modulación

- Otro factor importante es la sensibilidad del receptor. La Tabla 4.8 detalla la sensibilidad del receptor y $C/I + n$ para cada combinación de modulación y FEC.

Modulación	FEC	Niveles típicos $BER \leq 1 \times 10^{-6}$	
		Sensibilidad Rx	$C/I + n$
64QAM	3/4	-82.0 dBm	21.0 dBm
64QAM	2/3	-83.5 dBm	19.5 dBm
16QAM	3/4	-87.7 dBm	15.5 dBm
16QAM	1/2	-91.0 dBm	12.0 dBm
QPSK	3/4	-94.0 dBm	9.0 dBm
QPSK	1/2	-96.5 dBm	6.5 dBm
BPSK	1/2	-99.0 dBm	4.0 dBm

Tabla 4.8 Niveles de sensibilidad y $C/I + n$ en *EasyST*

4.4 Enlace WiMAX propuesto

El enlace final implementado, comunica dos usuarios finales con una BSR (estación base), por medio de sus respectivos CPE (estaciones suscriptoras), las cuales en conjunto, son conectada a un servidor de gestión, de donde se controlan todos los parámetros de comunicación, como frecuencias, canales, potencia, etc.

El enlace, y la configuración gráfica, por la cual se transmitirá la voz en IPv6, la podemos observar en la Figura 4.6.

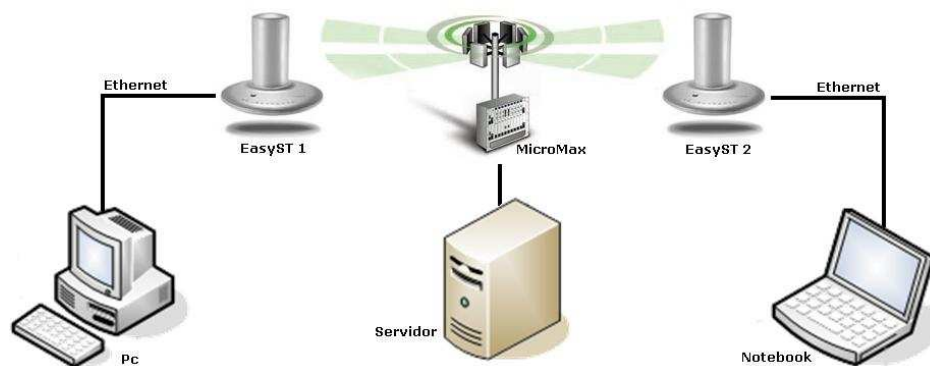


Figura 4.6 Arquitectura enlace WiMAX

CAPÍTULO V

CONFIGURACION DE SERVIDOR WIMAX Y EQUIPOS ABONADOS

5.1 Antecedentes

Como ya es sabido, en todo enlace de radio son requeridas configuraciones y ajustes necesarios para que dicho enlace funcione: ajuste de frecuencias, identificadores, autorizaciones, direcciones. Así también WiMAX requiere cierta configuración propia de la misma, elección de canal, ancho de banda, modulación, potencia Tx y además un servidor que sea capaz de gestionar la red, y el registro de equipos abonados y estaciones bases en la red. A continuación se describen más detalladamente estas configuraciones.

5.2 Configuración de la estación base (BS)

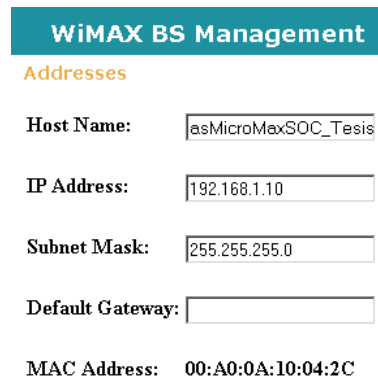
La configuración de la BS se realiza mediante dos maneras complementarias, inicialmente se realiza dentro de la Web Page que se encuentra empuetrada en la BS y posteriormente para funciones adicionales mediante el servidor Netspan.

5.2.1 Web Page de la estación base (BS)

El acceso a la Web Page de la estación base, se realiza por medio un navegador Web como Internet Explorer, ingresando la dirección IP por defecto de dicha estación en la barra de dirección, para nuestro caso la dirección 192.168.1.10 como se puede ver en la Figura 5.1, solicitando posteriormente un nombre de usuario y password de acceso. Estando en la Web Page es posible modificar el nombre de Host y dirección IP de la BS dentro de la jerarquía la cual se va a trabajar, esto se muestra en la Figura 5.2.



Figura 5.1 Acceso a BS vía Web Page



WiMAX BS Management

Addresses

Host Name:

IP Address:

Subnet Mask:

Default Gateway:

MAC Address: 00:A0:0A:10:04:2C

Figura 5.2 Host Name e IP de estación base

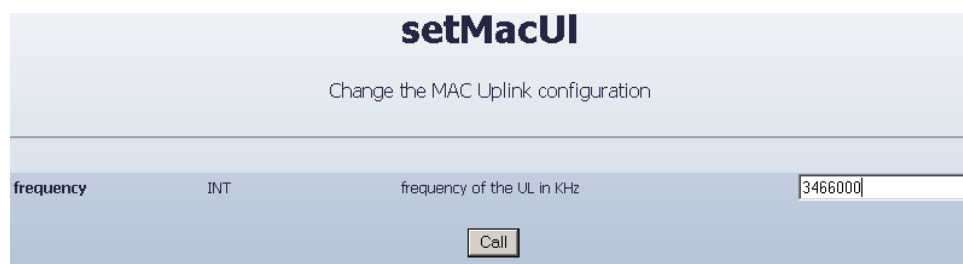
Después de haber realizado este procedimiento se debe configurar las opciones avanzadas de la BS. Esto se describe a continuación.

5.2.2 Configuraciones avanzadas de la BS

Dentro de las configuraciones avanzadas existe una serie de opciones de monitoreo de estado de la BS y otras opciones que pueden ser modificables, sin embargo las opciones necesarias para poner en funcionamiento a la BS son sólo algunas y se describen a continuación.

5.2.2.1 Configuración de enlace de subida

Para configurar el enlace de subida se debe introducir la frecuencia del canal que debe estar entre 3450 Mhz y 3500 Mhz, (Rango Uplink), en este caso se eligió la frecuencia 3466 Mhz. Como se aprecia en la Figura 5.3.



setMacUI

Change the MAC Uplink configuration

frequency	INT	frequency of the UL in KHz
		3466000

Figura 5.3 Ajuste de frecuencia Uplink del canal

Para comprobar lo anterior se puede visualizar la configuración del controlador Rx como se muestra en la Figura 5.4.

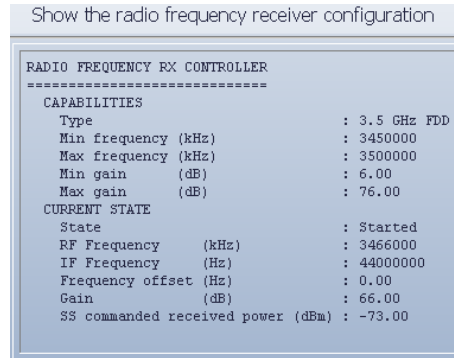


Figura 5.4 Configuración Rx (canal Uplink)

También se pueden ver otros datos interesantes tales como la capacidad del canal Rx, frecuencia intermedia, ganancias, etc.

5.2.2.2 Configuración de enlace de bajada

Para configurar el enlace de bajada se debe introducir la frecuencia del canal que debe estar entre 3550 Mhz y 3600 Mhz, la potencia del controlador de radio Tx cuya capacidad máxima es 27 dBm y un identificador de estación base (bs-id) como vemos en la Figura 5.5.

Change the MAC Downlink configuration			
tx-power	INT [0->28]	BS transmission power (dBm)	0
frequency	INT [3550000->3600000]	frequency of the DL in KHz (Invalid in license-exempts operations)	3566000
bs-id	STRING	BS ID (MAC Address)	00:A0:0A:10:04:2C
Call			

Figura 5.5 Ajuste de salida Tx, frecuencia Downlink y bs-id

La potencia fue fijada en 0 dBm para fines de prueba ya que los equipos CPE se encontraban inicialmente al lado de esta, la frecuencia se fijó en 3566 Mhz ya que el enlace de subida estaba en 4566 Mhz y en el bs-id se introdujo la Mac address de la estación base.

Para comprobar lo anterior se puede visualizar la configuración del controlador Tx en la Figura 5.6.

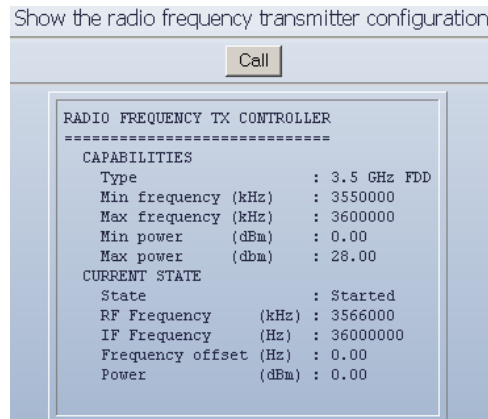


Figura 5.6 Configuración Tx (canal Downlink)

Cabe destacar que la BS soporta canales de hasta 3.5 Mhz de ancho de banda así como también los equipos CPE en la cual se dejó trabajando la estación base, y así como la estación base fue configurada con el canal Uplink de 3466 MHz. y Downlink de 3566 MHz. también deben ser configurados los equipos CPE, esto se demuestra a continuación.

5.3 Configuración de los equipos suscriptores CPE

Una vez ingresado a la Web Page se fijan las direcciones IP de ambos equipos CPE. Para nuestro CPE (1) la dirección IP será 192.168.1.1 y CPE (2), 192.168.1.2. La Figura 5.7 corresponde al CPE 1:

WiMAX Modem Management	
System	Signal Parameters
Addresses	Log
Advanced	
Addresses	
MAC Address #1	00:A0:0A:C1:96:b2
MAC Address #2	00:A0:0A:C1:96:b3
LAN Port Default IP Address	10.0.0.1
Default Subnet Mask	255.255.255.240
IP Address (static)	192.168.1.1
IP Mask (static)	255.255.255.0
Default GW (static)	0.0.0.0
DHCP Server IP Address	N/A

Figura 5.7 Configuración IP de CPE EasyST

Después del procedimiento anterior se debe fijar el canal en el cual vamos a operar, los EasyST tienen como característica el poder operar bajo dos anchos de banda, 1.75 Mhz llamado canal de banda ancha baja y 3.5 Mhz llamado canal de banda ancha alta, en este caso se eligió la banda de 3.5 Mhz y eligiendo el canal correspondiente al canal de la estación base, esto se muestra en la Figura 5.8.

High Bandwidth Channel Table

Status	Channel	Uplink Frequency (MHz)	Downlink Frequency (MHz)
☐	0	3452.000	3552.000
☐	1	3455.500	3555.500
☐	2	3459.000	3559.000
☐	3	3462.500	3562.500
☒	4	3466.000	3566.000
☐	5	3469.500	3569.500

Figura 5.8 Ajuste de canal de CPE

Base Station ID Settings

Base Station ID

00 A0 0A 10 04 2C

Base Station Mask

FF FF FF 00 00 00

Submit

Figura 5.9 Ingreso de bs-id en CPE

Posteriormente y para finalizar la configuración se debe ingresar el bs-id de la estación base como se muestra en la Figura 5.9, la cual se asociará el equipo CPE; este bs-id corresponde a la Mac address de la estación base.

Para comprobar la configuración y un correcto enlace entre estación base y CPE se puede visualizar en la misma Web Page del CPE, esto se muestra en la Figura 5.10.

Signal Parameters

Link Status
OPERATIONAL

Downlink Parameter	Value
BS Identifier	00A00A10042C
Downlink Frequency	3566.000 MHz
Downlink Channel Bandwidth	3.5 MHz
SNR	32.1 dB
Received Signal Strength	-66.0 dBm
Modulation	64QAM 3/4

Uplink Parameter	Value
Uplink Frequency	3466.000 MHz
Uplink Channel Bandwidth	3.5 MHz
Tx Power	-2.5 dBm
Modulation	64QAM 3/4

Figura 5.10 Parámetros de señal de CPE

La figura anterior describe gran parte de todo lo hecho anteriormente, se muestran las frecuencias de enlaces, el bs-id de la estación base, el ancho de banda, así como también otros parámetros de gran importancia como la relación señal a ruido, la sensibilidad, la potencia Tx y las modulaciones que se estaban utilizando para ese instante del enlace.

5.4 Configuración Servidor Netspan

5.4.1 Antecedentes

Como en todo sistema de telecomunicación al nivel de WiMAX es necesaria una plataforma de administración y monitoreo de red. Para este caso se utilizó la plataforma provista por el mismo fabricante Airspan llamada Netspan.

Netspan es un completo sistema de administración de red diseñado entorno a una arquitectura cliente-servidor (HTML a través de HTTP) y está basado en SNMP sobre TCP/IP. Se ejecuta en una plataforma PC con Windows Server 2003 y usa una base de datos SQL para almacenar la configuración, estadísticas e historial de alarmas de la red de radio.

5.4.2 Detección de estación base

A continuación se muestran los pasos para el descubrimiento automático del MicroMAX-SOC a través de Netspan.

Una vez ingresado a Netspan, se debe ir a Server donde se encuentra el Discovery Task y definir las comunidades destinatarias, el puerto 161 por el cual trabaja el protocolo SNMP que permite el descubrimiento de los equipos WiMAX (Anexo I) y el rango de direcciones IP en la que se encuentra la estación base, en este caso, como se muestra en la Figura 5.11 se fijó un rango de 192.168.1.10 a 192.168.1.10 ya que esa es la dirección IP fijada en la estación base.

Edit Discovery Task Parameters

Name: Estacion Base

General Properties

Enabled: ☐
 Discovery Type: BS
 Manager Timeout: 5000 ms
 Agent Timeout: 5000 ms
 Preferred SNMP Protocol: Version 2C

Discovery Target Communities And Ports

Write Community: private
 Read Only Community: public
 Port: 161

Discovery Target IP Address Ranges

	Start Address	End Address
1	192.168.1.10	192.168.1.10

Figura 5.11 Descubrimiento de estación base

Una vez creado el “Discovery Task” se puede ver la estación base descubierta en “Configuration Management” y después “Base Station” tal como se muestra en la Figura 5.12.

Base Stations

List

Filter: -- No Filter --

	BS Name	BSID	IP Address	Managed	Connection State	Provisioning State	Discovered
1	BS:00A00A:10042C	00A00A:10042C	192.168.1.10	☒	On Line	OK	☒

Figura 5.12 Estación base descubierta

Haciendo doble click sobre la estación base se puede ver opciones de configuración y monitoreo que se muestran en la Figura 5.13 en este caso son dejadas por defecto ya que para este caso de configuración de red WiMAX mínimo no se requiere mayor configuración.

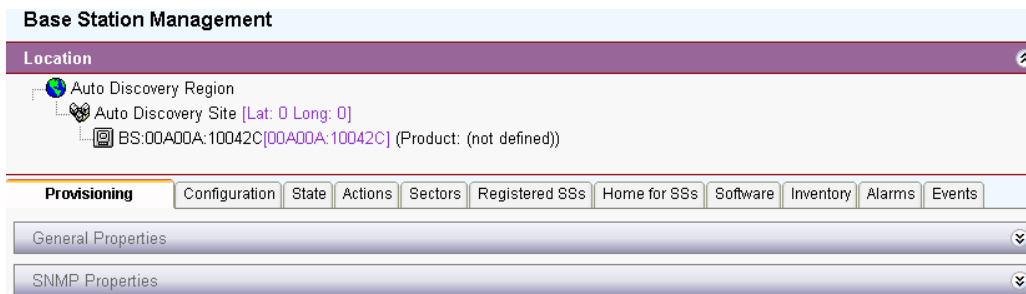


Figura 5.13 Administrador de estación base

5.4.3 Detección de estaciones suscriptoras (CPE)

Una vez detectada la estación base y de haber hecho la configuración de canales de equipos CPE y estación base se produce el auto descubrimiento de equipos CPE, cada vez que se encienda un CPE escanea buscando la frecuencia, sincroniza los enlaces y pide autorización a la estación base para su auto descubrimiento.

En la Figura 5.14 se pueden ver los equipos CPE registrados y habilitados en la interfaz Netspan.

Subscriber Stations									
List									
Filter		-- No Filter --	Edit		List...				
	MAC Address	IP Address	Registered	Service Enabled	Service Product	Configuration Profile	Service Home	Last seen on Sector	Provisioning Error Count
1	00:A0:0A:C1:9E:3C	192.168.1.2	☒	☒	Tesis	Dynamic Modul...		Sector:00A00A...0	0
2	00:A0:0A:C1:96:B2	192.168.1.1	☒	☒	Tesis	Dynamic Modul...		Sector:00A00A...0	0

Figura 5.14 Equipos CPE registrados

5.4.4 Configuración de comunicación

En toda red de datos se requiere, una configuración correspondiente, la cual será ajustada según al servicio o la aplicación que en esta se ejecutará. Como en este caso se entregará servicio de VoIP, se debe ajustar la configuración de la comunicación buscando las opciones de QoS que hagan más efectiva dicha comunicación.

5.4.4.1 Clase de servicio

La Figura 5.15 muestra el conjunto de parámetros de QoS que están asociados a un flujo de servicio (SF) de un suscriptor, a esta clase de servicio se le dio el nombre de “Normal Traffic”.

Figura 5.15 Editor de Clase de Servicio

Como se ve en la Figura 5.15 se usó el protocolo UGS (Unsolicited Grant Service) que es el más adecuado para el servicio de VoIP.

Luego de esto, se está listo para configurar los flujos de servicio de ambas direcciones que serán guardadas dentro de un perfil de Service Products que se muestra en la Figura 5.16.

	Description	Service Class	Scheduling Type	Traffic Priority	Direction	Initial State	Convergence Sublayer Type
1	Downlink	Normal Traffic(N/A)	7	Downlink	Active	Packet 802.3 Ethernet	
2	Uplink	Normal TrafficUGS	7	Uplink	Active	Packet 802.3 Ethernet	

Figura 5.16 Configuración de Flujos de Servicios

Como se observa en la figura 5.16 cada flujo de servicio tiene como clase de servicio a “Normal Traffic” creada anteriormente y la sub capa de convergencia “Packet 802.3 Ethernet” que es el estándar que utilizamos para realizar la aplicación.

5.4.4.2 Perfil de Estación Suscriptora

La modulación de subida y bajada se puede configurar independientemente, dependiendo de las condiciones de propagación y aplicación, en este caso fue dejado en “modulación dinámica” como se observa en la Figura 5.17 en donde el mismo sistema de radio enlace fija la modulación según su criterio.

Edit Subscriber Station Custom Configuration Profile	
Identity	
Name	Dynamic Modulation
Description	
Properties	
Dynamic Services	Allow Add Allow Change Allow Delete
VLAN Port Mode	Check And Untag
Requested Downlink Modulation	Dynamic Modulation
Requested Uplink Modulation	Dynamic Modulation
Minimum SubChannel Width	Dynamic Modulation
BPSK (CC) 1/2 QPSK (RS+CC/CC) 1/2 QPSK (RS+CC/CC) 3/4 16-QAM (RS+CC/CC) 1/2 16-QAM (RS+CC/CC) 3/4 64-QAM (RS+CC/CC) 2/3 64-QAM (RS+CC/CC) 3/4 QPSK (BTC) 1/2 QPSK (BTC) 3/4 16-QAM (BTC) 3/4	

Figura 5.17 Perfil de configuración de estaciones suscriptoras

CAPÍTULO VI

CONECTIVIDAD WIMAX IPV6

6.1 Antecedentes

En el presente capítulo, se describirá el proceso realizado de forma sistemática para llegar a la conexión IPv6 en el enlace WiMAX en el cual transmitiremos la voz. Se hará alusión al sistema operativo utilizado en los equipos finales, comprobación de conectividad entre los extremos WiMax para el caso IPv4 y posteriormente para el caso IPv6, éste último, hecho por tunelización IPv6 sobre IPv4, debido a la restricción de los equipos para la utilización de IPv6 nativo.

6.2 Configuración IPv4 en equipos terminales

Antes de establecer una comunicación WiMAX de voz en IPv6, es indispensable comprobar el correcto funcionamiento de nuestro enlace, lo cual se hace por medio de IPv4, protocolo soportado por todos los equipos, los cuales ya cuentan con una configuración de identificadores o direcciones establecidas anteriormente, restando los PC finales para completar dicho proceso de comunicación.

Para un manejo de red más amigable, que permita la visualización de los equipos entre si, ésta configuración se estableció bajo la jerarquía IP 192.168.1.X, de las cuales ya contamos con las direcciones para el servidor, estación base y estaciones suscriptoras como se detalla a continuación:

Dispositivo en la red	Identificador IPv4	Mascara de Subred
Servidor Netspan	192.168.1.15	255.255.255.0
Estación Base (MicroMax)	192.168.1.10	255.255.255.0
Suscriptor 1 (EasyST 1)	192.168.1.1	255.255.255.0
Suscriptor 2 (EasyST 2)	192.168.1.2	255.255.255.0

Tabla 6.1 Identificadores IPv4 para los dispositivos en la red

Para la conexión de los equipos finales, se utilizó la plataforma Windows en su versión XP Profesional Service Pack 3. La asignación de direcciones IP se realiza dirigiéndonos a Panel de Control, Conexiones de red y Conexión de área local. Aquí vamos la opción propiedades, seleccionamos la categoría Protocolo Internet (TCP/IP) y finalmente propiedades como podemos ver en la Figura 6.1.

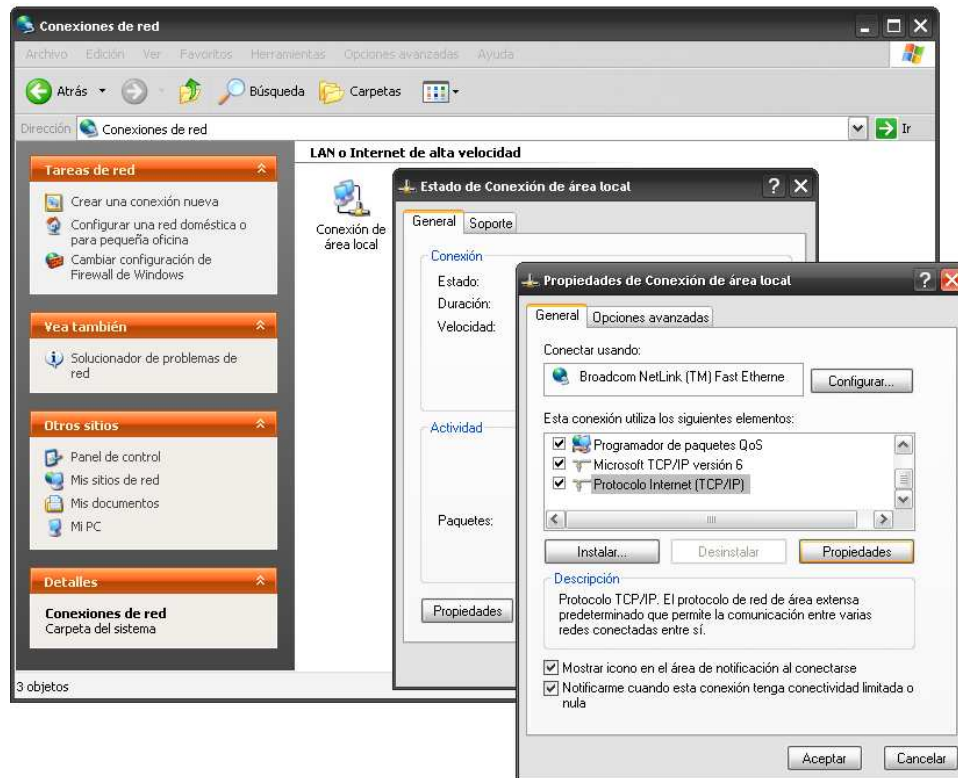


Figura 6.1 Propiedades Conexión área local para IPv4

Para la configuración de la primera máquina, conectada al EasyST 1, ingresamos una IP de la misma jerarquía que para los equipos conectados en la red, asignándole la IP estática 192.168.1.5 y máscara de subred 255.255.255.0. De la misma manera, se configuró la segunda máquina conectada al EasyST 2, con la dirección IP estática 192.168.1.6 cuya máscara de subred es 255.255.255.0. Los cambios realizados para el primer caso lo vemos en la Figura 6.2, siendo de forma análoga para el segundo con sus respectivos valores:

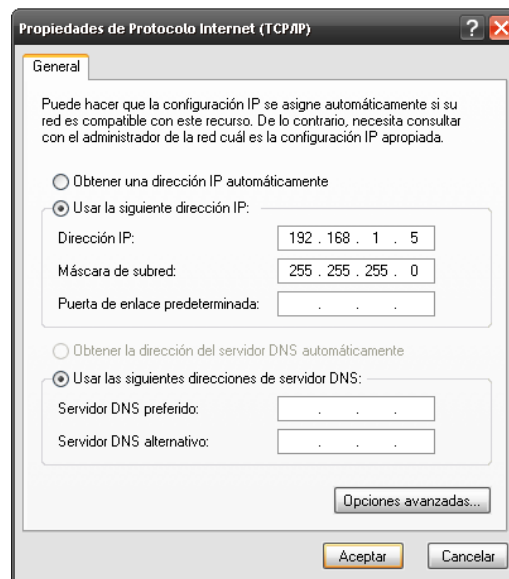
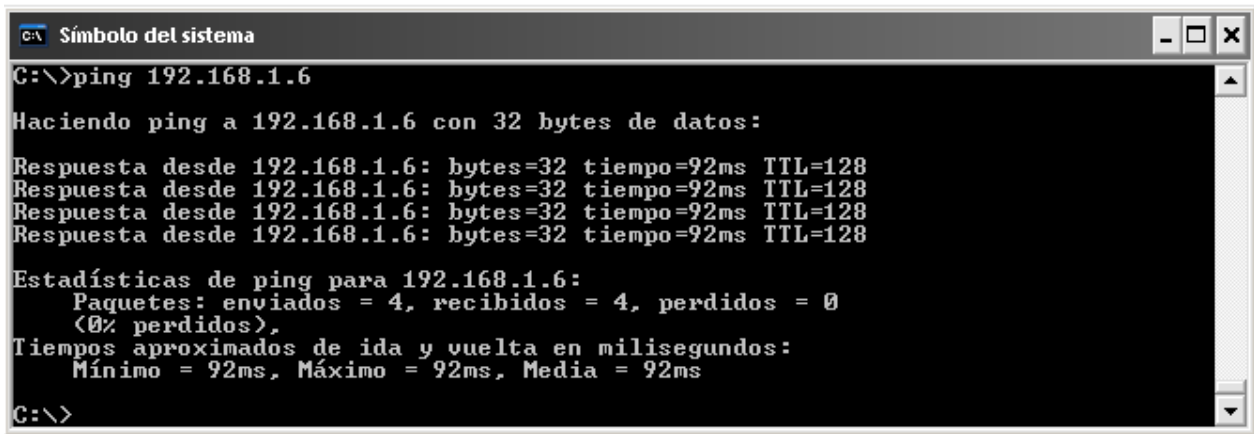


Figura 6.2 Configuración IP equipos terminales

6.3 Conectividad IPv4 (Ping)

Una vez configurado ambos terminales, deberían ser capaces de verse mutuamente a través de la red, debido a que todos los elementos de la red se encuentran en una misma jerarquía de red. Para verificar dicha afirmación, hacemos uso de la utilidad *ping*, la cual permite comprobar el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (ambos definidos en el protocolo de red ICMP) para determinar si el sistema IP específico es accesible en la red. Para comprobar esto, abrimos la consola de Windows ejecutando: Menú Inicio – Ejecutar – CMD – Enter, y nos disponemos a realizar las pruebas de conectividad.

El primer ping realizado se efectúa desde el primer PC con IP 192.168.1.5 al segundo PC con la dirección 192.168.1.6 y el segundo de forma inversa, desde la dirección IP 192.168.1.6 a la 192.168.1.5 como en las Figuras 6.3 y 6.4 respectivamente.



```

C:\>ping 192.168.1.6

Haciendo ping a 192.168.1.6 con 32 bytes de datos:

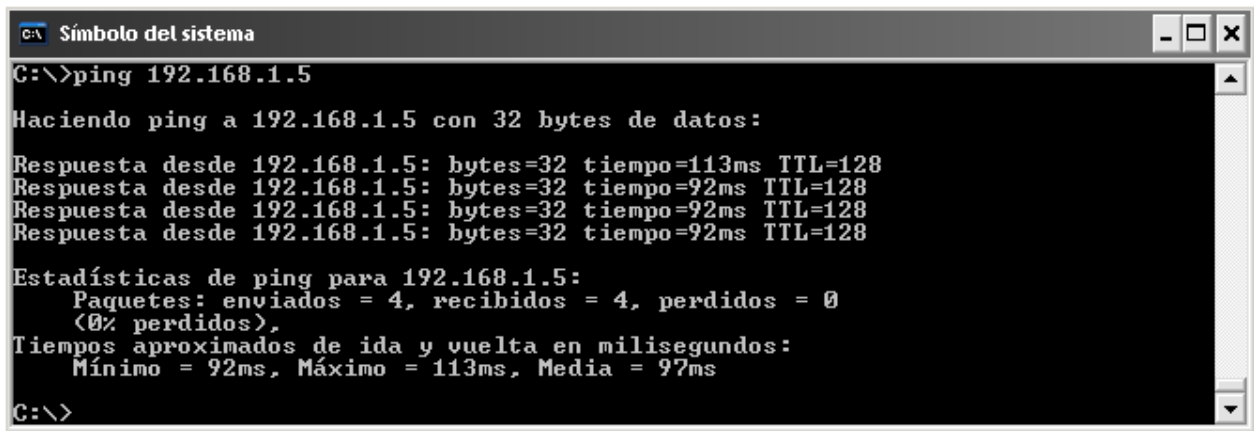
Respuesta desde 192.168.1.6: bytes=32 tiempo=92ms TTL=128
Respuesta desde 192.168.1.6: bytes=32 tiempo=92ms TTL=128
Respuesta desde 192.168.1.6: bytes=32 tiempo=92ms TTL=128
Respuesta desde 192.168.1.6: bytes=32 tiempo=92ms TTL=128

Estadísticas de ping para 192.168.1.6:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 92ms, Máximo = 92ms, Media = 92ms

C:\>

```

Figura 6.3 Ping desde 192.168.1.5 a 192.168.1.6



```

C:\>ping 192.168.1.5

Haciendo ping a 192.168.1.5 con 32 bytes de datos:

Respuesta desde 192.168.1.5: bytes=32 tiempo=113ms TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo=92ms TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo=92ms TTL=128
Respuesta desde 192.168.1.5: bytes=32 tiempo=92ms TTL=128

Estadísticas de ping para 192.168.1.5:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 92ms, Máximo = 113ms, Media = 97ms

C:\>

```

Figura 6.4 Ping desde 192.168.1.6 a 192.168.1.5

De esta manera podemos corroborar nuestra afirmación que existe efectivamente conectividad WiMax en IPv4 al existir envío y respuesta de todos los paquetes entre los extremos de red. Podemos extraer de esta prueba un cierto retardo, el que es asociado a la red misma, influida por características propias de los equipos utilizados.

6.4 Tunelización IPv6 en IPv4

Una vez comprobada la conectividad WiMax IPv4 de nuestro enlace, procedemos a establecer la comunicación en IPv6.

Para establecer una comunicación IPv6 entre terminales, es indispensable el uso de túneles IPv6 sobre IPv4, debido a que el protocolo IPv6 nativo, no es soportado por los equipos de la red.

6.4.1 Descripción y configuración del túnel

Primero que todo, debemos comprobar si está activada la pila IPv6 en nuestro sistema operativo, para esto abrimos una consola de Windows “CMD” y hacemos un ping a la dirección ::1 correspondiente a la dirección loopback. Si obtenemos un resultado de ida y vuelta de paquetes, y no hay pérdida de estos, es porque la pila esta funcionando correctamente, en caso contrario, habrá que habilitarla desde la misma consola escribiendo “ipv6 install”, ya que viene instalada por defecto en Windows XP SP1 o posterior.

Teniendo nuestra máquina operativa para el funcionamiento del protocolo IPv6, procedemos a la configuración del túnel manual, de Host a Host, es decir, establece conectividad IPv6 entre los extremos de red. El túnel escogido es “v6v4tunnel” configurándolo en ambos PCs de la siguiente manera:

PC 1:

```
netsh interface ipv6 add v6v4tunnel "Túnel Wimax IPv6" 192.168.1.5 192.168.1.6
netsh interface ipv6 add address "Túnel Wimax IPv6" 2001:10:10::1
netsh interface ipv6 add route ::/0 "Túnel Wimax IPv6" 2001:10:10::2
```

PC 2:

```
netsh interface ipv6 add v6v4tunnel "Túnel Wimax IPv6" 192.168.1.6 192.168.1.5
netsh interface ipv6 add address "Túnel Wimax IPv6" 2001:10:10::2
netsh interface ipv6 add route ::/0 "Túnel Wimax IPv6" 2001:10:10::1
```

En donde:

- ***netsh interface ipv6 add v6v4tunnel "Túnel Wimax IPv6" 192.168.1.5 192.168.1.6***
Crea un túnel IPv6 en IPv4 con el nombre Túnel WiMAX IPv6 entre las direcciones 192.168.1.5 y 192.168.1.6
- ***netsh interface ipv6 add address "Túnel Wimax IPv6" 2001:10:10::1***
Agrega la dirección IPv6 2001:10:10::1 a la interfaz Túnel WiMAX IPv6.
- ***netsh interface ipv6 add route ::/0 "Túnel Wimax IPv6" 2001:10:10::2***
Agrega la ruta 2001:10:10::2 correspondiente al PC 2, al prefijo ::/0 de la interfaz WiMAX IPv6.

6.4.2 Conectividad IPv6 (Ping)

De forma análoga que para el caso de conectividad en IPv4, teniendo configurado ambos terminales, deberían ser capaces de verse mutuamente a través de la red, esta vez en IPv6 gracias al túnel recientemente configurado. Comprobamos conectividad haciendo uso nuevamente de la utilidad ping ahora para su versión IPv6.

El primer ping realizado se efectúa desde el primer PC con IP 2001:10:10::1 al segundo PC con la dirección 2001:10:10::2 y el segundo de forma inversa, desde la dirección IP 2001:10:10::2 a la 2001:10:10::1 como vemos en las Figura 6.5 y 6.6 respectivamente.


```

C:\>ping6 2001:10:10::2

Haciendo ping 2001:10:10::2
de 2001:10:10::1 con 32 bytes de datos:

Respuesta desde 2001:10:10::2: bytes=32 tiempo=92ms
Respuesta desde 2001:10:10::2: bytes=32 tiempo=93ms
Respuesta desde 2001:10:10::2: bytes=32 tiempo=93ms
Respuesta desde 2001:10:10::2: bytes=32 tiempo=93ms

Estadísticas de ping para 2001:10:10::2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 92ms, Máximo = 93ms, Media = 92ms

C:\>

```

Figura 6.5 Ping desde 2001:10:10::1 a 2001:10:10::2

```

C:\>ping6 2001:10:10::1

Haciendo ping 2001:10:10::1
de 2001:10:10::2 con 32 bytes de datos:

Respuesta desde 2001:10:10::1: bytes=32 tiempo=97ms
Respuesta desde 2001:10:10::1: bytes=32 tiempo=96ms
Respuesta desde 2001:10:10::1: bytes=32 tiempo=96ms
Respuesta desde 2001:10:10::1: bytes=32 tiempo=95ms

Estadísticas de ping para 2001:10:10::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 95ms, Máximo = 97ms, Media = 96ms

C:\>

```

Figura 6.6 Ping desde 2001:10:10::2 a 2001:10:10::1

Al igual que para el caso IPv4, corroboramos que existe efectivamente conectividad WiMAX en IPv6 al existir envío y respuesta de todos los paquetes entre los extremos de red. El retardo es asociado nuevamente a la red, influida por características propias de los equipos utilizados.

En la Tabla 6.2 podemos ver la configuración de direcciones IP para los PC 1 y PC 2 en sus versiones 4 y 6 de forma resumida.

Enlace WiMAX	Dirección IPv4	Dirección IPv6
PC 1	192.168.1.5	2001:10:10::1
PC 2	192.168.1.6	2001:10:10::2

Tabla 6.2 Resumen direcciones IPv4 e IPv6 equipos finales

CAPÍTULO VII

COMUNICACION VOIP EN IPV6

7.1 Antecedentes

Es sabido que para realizar una comunicación de VoIP se necesitan elementos básicos para poder establecer la comunicación, llámense elementos básicos a códecs, protocolos de señalización y transporte, IPv4 e IPv6, etc. Todos estos elementos hoy en día se pueden encontrar en conjunto, empujados en un mismo software más comúnmente llamado “softphone”. Para este caso de VoIP en IPv6, el softphone más adecuado y asequible encontrado es el llamado Eyebeam que será descrito a continuación.

7.1.1 Softphone utilizado

El softphone utilizado fue el Eyebeam, el cual no sólo tiene características de VoIP, sino también, video conferencia y mensajería instantánea. Está basado en el protocolo SIP, soporta direcciones IPv6, posee una amplia gama de códecs, y también cambio dinámico de códecs durante la llamada según el ancho de banda disponible, pérdida de paquetes y jitter de la red.

Los códecs que maneja son:

- Códecs de banda estrecha:
 - o iLBC, Speex, DVI4, G711 aLaw, G711 uLaw, GSM, Speex FEC.
- Códecs de banda ancha:
 - o BroadVoice-32, BroadVoice-32 FEC, L16 PCM Wideband, DVI4 Wideband, Speex Wideband, Speex Wideband FEC.

7.2 Configuración del Softphone

La instalación del softphone se realiza mediante un fichero ejecutable sobre Windows XP. Luego de esto el softphone ejecutado tiene la siguiente interfaz gráfica mostrada en la Figura 7.1



Figura 7.1 Apariencia de Eyebeam

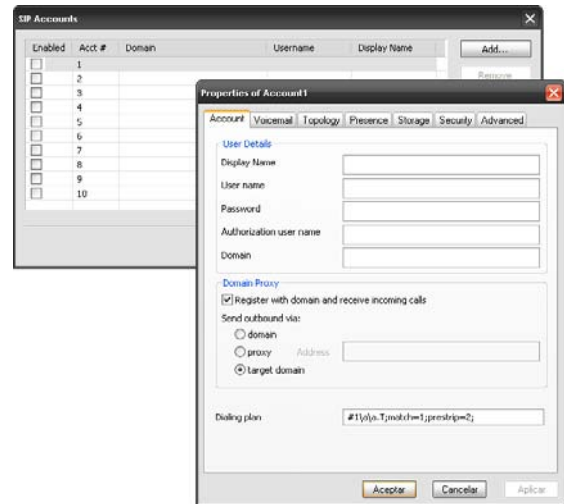


Figura 7.2 Propiedades de cuenta SIP

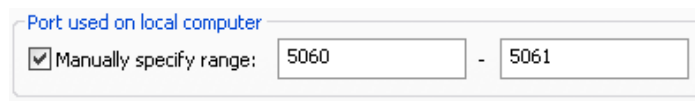
7.2.1 Configuración PC1

Una vez instalado el software, procedemos a la configuración de éste. Lo primero es configurar las cuentas SIP en cada computador respectivamente, encontrándonos con en el cuadro de diálogo que vemos en la Figura 7.2 en donde para el PC1 tenemos:

- **Display Name:** nombre cualquiera que reconozca al usuario. Para nuestro caso los nombres asignados fueron (PC1 IPv4/PC1 IPv6).
- **User Name:** nombre de usuario asignado por la central. Normalmente es el identificador de número de teléfono, lo que para nuestro caso, dado a la ausencia de un servidor, corresponden a los mismos nombres propios que para el caso Display Name.
- **Password:** esta casilla es un password registrado en el servidor para cada usuario, el cual se omite nuevamente en nuestro caso por la inexistencia del mismo.
- **Athorization user name:** autorización validada por el servidor. No aplica a nuestro caso.
- **Domain:** corresponde a la dirección IP o enlace donde se encuentra alojado el servidor de VoIP, para nuestro caso la dirección usada como servidor será la IP del PC2 192.168.1.6 para IPv4 y 2001:10:10::2 para IPv6, que es en donde seremos registrados de forma

automática mientras se efectúa la llamada, sin tener la necesidad de crear un servidor debido a que realizaremos una configuración punto a punto.

Posteriormente es necesario configurar el puerto que se usará para la comunicación SIP, el que por defecto es el 5060 en TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) para recibir las peticiones de los clientes SIP y lo podemos especificar en la pestaña “Topology” en donde se dará un rango de puertos para ambos PC como se muestra en la Figura 7.3

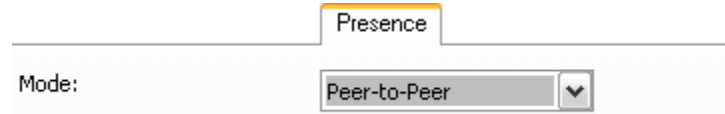


Port used on local computer

☒ Manually specify range: 5060 - 5061

Figura 7.3 Configuración de puertos

Como la llamada será en modo Peer-to-peer también se tendrá que configurar de esta forma como se muestra en la Figura 7.4



Presence

Mode: Peer-to-Peer

Figura 7.4 Modo Peer to Peer

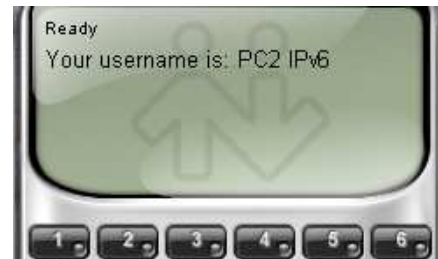
7.2.2 Configuración PC2

De la misma forma como se configuró el PC1 se hace con el PC2 teniendo la siguiente configuración de cuenta SIP:

- **Display Name:** PC2 IPv4/PC2 IPv6.
- **User Name:** PC2 IPv4/PC2 IPv6
- **Domain:** 192.168.1.5/2001:10:10::1

De esta manera se encuentran listos los softphones en ambos PC para realizar llamadas como podemos ver a continuación.

Figura 7.5 Propiedades de cuenta SIP PC1**Figura 7.6** Softphone listo para usar PC1

Figura 7.7 Propiedades de cuenta SIP PC2**Figura 7.8** Softphone listo para usar PC2

Como se puede ver en la figuras 7.5 y 7.7 el dominio para cada PC, es la del punto extremo, donde será registrado dicho usuario mientras se sostenga la llamada, y en las figuras 7.6 y 7.8, los softphones listos para establecer comunicación. Para el caso IPv4 se realizará de forma análoga.

7.3 Pruebas de llamadas

7.3.1 Llamadas en IPv4

Después de haber hecho las configuraciones ya descritas se podrá realizar llamadas. Primero se empezará con llamadas en IPv4. En la Tabla 7.1 se muestran las direcciones IP de cada PC.

PC	Dirección IP PC	Dirección IP EasyST
PC1	192.168.1.5	192.168.1.1
PC2	192.168.1.6	192.168.1.2

Tabla 7.1 Direcciones IP de cada PC

7.3.1.1 Llamada de PC1 a PC2

Al realizar la llamada desde el PC1 al PC2 se obtiene una llamada entrante en el PC2 como se muestra en la Figura 7.9.

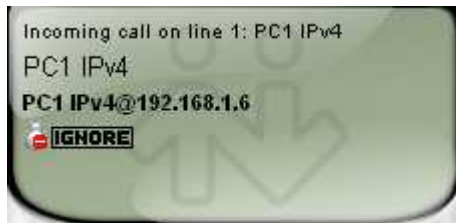


Figura 7.9 Llamada entrante en PC2



Figura 7.10 Llamada contestada en PC2

Al contestar la llamada queda establecida la conexión VoIP entre ambos PC, como vemos en la Figura 7.10.

7.3.1.2 Llamada de PC2 a PC1

Al realizar la llamada desde PC2 a PC1 se obtiene una llamada entrante en el PC1 como se muestra en la Figura 7.11.

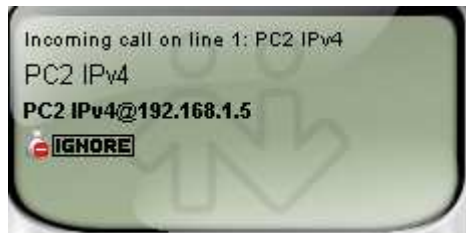


Figura 7.11 Llamada entrante en PC1

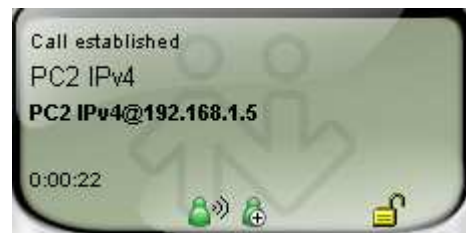


Figura 7.12 Llamada contestada en PC1

Al contestar la llamada queda establecida la conexión VoIP entre ambos PC, como vemos en la Figura 7.12.

7.3.2 Llamada en IPv6

Para realizar llamadas en IPv6 se debe fijar las direcciones IPv6 en las cuentas de Eyebeam como se demostró en la “Configuración de Eyebeam”. Además de esto, teniendo el túnel IPv6 correctamente configurado dentro de la comunicación WiMAX podremos hacer llamadas en IPv6. La Tabla 7.2 muestra las direcciones IP de cada PC.

PC	Dirección IP EasyST	Dirección IPv4 PC	Dirección IPv6 PC
PC1	192.168.1.1	192.168.1.5	2001:10:10::1
PC2	192.168.1.2	192.168.1.6	2001:10:10::2

Tabla 7.2 Direcciones IPv6 de ambos PC

7.3.2.1 Llamada de PC1 a PC2

A continuación podemos apreciar en la Figura 7.13 una llamada en IPv6 del PC1 al PC2, y en la Figura 7.14 la llamada establecida entre ambos PCs.

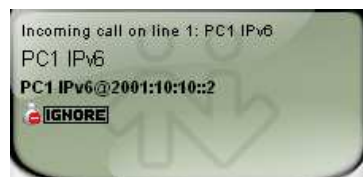


Figura 7.13 Llamada entrante en PC2

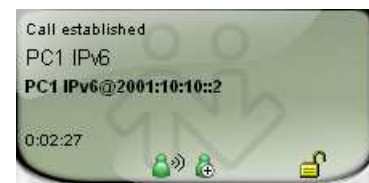


Figura 7.14 Llamada contestada en PC2

7.3.2.2 Llamada de PC2 a PC1

De la misma manera, ahora de PC2 a PC1 se muestra en la Figura 7.15, mientras que la Figura 7.16 muestra la llamada establecida.

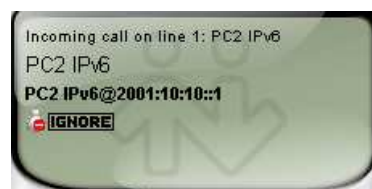


Figura 7.15 Llamada entrante en PC1

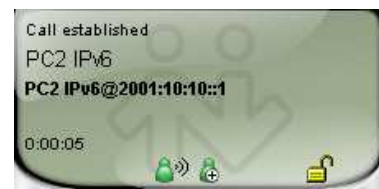


Figura 7.16 Llamada contestada en PC1

7.4 Monitoreo por Ethereal

Una vez establecidas las llamadas en el enlace WiMAX para IPv4 e IPv6, procedemos a visualizar el tráfico de paquetes en la comunicación, observando los protocolos involucrados. Este monitoreo se realizó haciendo uso del software analizador de red Ethereal, para el cual vemos continuación los siguientes tráficos para las distintas pruebas de comunicación de voz sobre IP.

7.4.1 Monitoreo VoIPv4

- **Tráfico IPv4 de: PC1: 192.168.1.5 a PC2: 192.168.1.6**

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.5	192.168.1.6	SIP/SD	Request: INVITE sip:10192.168.1.6, with session description
2	0.199854	192.168.1.6	192.168.1.5	SIP	Status: 180 Ringing
3	1.989596	192.168.1.6	192.168.1.5	RTP	Unknown RTP version 0
4	1.989665	192.168.1.6	192.168.1.5	RTCP	Receiver Report
5	1.991889	192.168.1.5	192.168.1.6	RTP	Unknown RTP version 0
6	2.000209	192.168.1.6	192.168.1.5	SIP/SD	Status: 200 OK, with session description
7	2.021165	192.168.1.5	192.168.1.6	RTP	Unknown RTP version 0
8	2.021454	192.168.1.5	192.168.1.6	RTCP	Receiver Report
10	2.029555	192.168.1.6	192.168.1.5	RTP	Payload type=BV32, SSRC=2946187379, Seq=6624, Time=52000, Mark
11	2.034637	192.168.1.5	192.168.1.6	RTCP	Unknown packet type
12	2.045044	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=1090710326, Seq=2817, Time=3270500, Mark
13	2.049579	192.168.1.6	192.168.1.5	RTP	Payload type=BV32, SSRC=2946187379, Seq=6625, Time=52320
14	2.049647	192.168.1.6	192.168.1.5	RTP	Payload type=BV32, SSRC=2946187379, Seq=6626, Time=52640
15	2.064231	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=1090710326, Seq=2818, Time=3270820

#	Frame 1 (1086 bytes on wire, 1086 bytes captured)
#	Ethernet II, Src: Intel_dd:e8:2e (00:16:76:dd:e8:2e), Dst: Intel_dd:e8:b9 (00:16:76:dd:e8:b9)
#	Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.6 (192.168.1.6)
#	User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
	Source port: 5060 (5060)
	Destination port: 5060 (5060)
	Length: 1052
	Checksum: 0xa954 [correct]
#	Session Initiation Protocol
	+ Request-Line: INVITE sip:10192.168.1.6 SIP/2.0
#	Message Header
#	Message body

Figura 7.17 Paquetes IPv4 monitoreados de PC1 a PC2 (inicio de llamada)

Como podemos apreciar en la Figura 7.17, el tráfico se inicia con la invitación (INVITE la cual establece una sesión) de iniciar una llamada desde la dirección 192.168.1.5 a la dirección 192.168.1.6 por medio de los protocolos SIP y SDP. Posteriormente el PC2 envía al PC1 una respuesta 180, la cual significa que su teléfono esta sonando y se encuentra lista para ser contestada. Una vez que esta llamada es aceptada, es decir, cuando el receptor levanta el teléfono, este envía al teléfono del cual sale la llamada una respuesta 200 (OK), declarando la respuesta exitosa y establecimiento de la comunicación. Luego podemos ver el inicio de la captura de los

paquetes de VoIP que se encuentran en el protocolo RTP, encapsulados en paquetes UDP comunicándose por el puerto 5060 como se configuró anteriormente para SIP.

Posteriormente visualizamos el fin de la llamada SIP, la cual comienza cuando el teléfono del PC2 cuelga, enviando al PC1 un mensaje BYE como se aprecia en la Figura 7.18, concretándose con una respuesta 200 (OK) de la aceptación de fin de llamada.

No. -	Time	Source	Destination	Protocol	Info
290	4.684892	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=1090710326, Seq=2949, Time=3312740
292	4.704894	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=1090710326, Seq=2950, Time=3313060
293	4.724004	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=1090710326, Seq=2951, Time=3313380
294	4.729998	192.168.1.6	192.168.1.5	SIP	Request: BYE sip:PC1%20IPv4@192.168.1.5:5060
296	4.731377	192.168.1.5	192.168.1.6	RTCP	Sender Report
298	4.833192	192.168.1.5	192.168.1.6	SIP	Status: 200 OK

Frame 294 (502 bytes on wire, 502 bytes captured)
Ethernet II, Src: Intel_dd:e8:b9 (00:16:76:dd:e8:b9), Dst: Intel_dd:e8:2e (00:16:76:dd:e8:2e)
Internet Protocol, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.5 (192.168.1.5)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
Source port: 5060 (5060)
Destination port: 5060 (5060)
Length: 468
Checksum: 0xca02 [correct]
Session Initiation Protocol
Request-Line: BYE sip:PC1%20IPv4@192.168.1.5:5060 SIP/2.0
Message Header

Figura 7.18 Paquetes IPv4 monitoreados de PC1 a PC2 (fin de llamada)

La transferencia de paquetes monitoreada anteriormente entre PCs, podemos visualizarla de forma más clara en un diagrama de flujo extraído del mismo Ethereal como muestra la Figura 7.19, observando el protocolo SIP y códec BV32 usado para la compresión de voz.

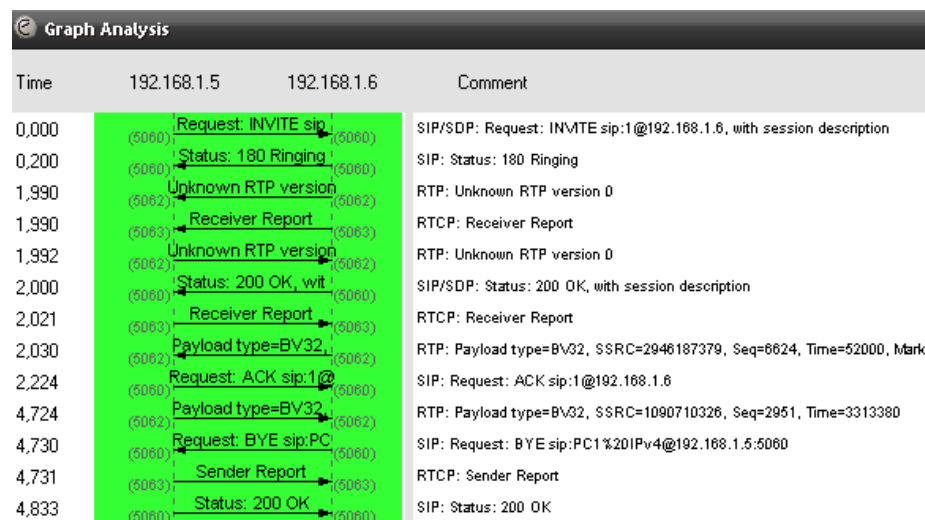


Figura 7.19 Diagrama de flujo VoIPv4 entre PC1 y PC2

- **Tráfico IPv4 de: PC2: 192.168.1.6 a PC1: 192.168.5**

Al igual que para el caso anterior de llamada de PC1: 192.168.1.5 a PC2: 192.168.1.6, monitoreamos los paquetes de comunicación para la llamada de: PC2: 192.168.1.6 a PC1: 192.168.5, para el cual se obtienen resultados similares, esta vez de forma invertida al primer caso para fuente y destino.

En las Figuras 7.20 y 7.21, se muestran el tráfico de paquetes al inicio de sesión y fin de sesión de comunicación de VoIP, y en la Figura 7.22 el gráfico de flujo para el protocolo SIP entre PC2 y PC1.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.6	192.168.1.5	SIP/SD	Request: INVITE sip:1@192.168.1.5, with session description
2	0.196104	192.168.1.5	192.168.1.6	SIP	Status: 180 Ringing
3	1.465962	192.168.1.5	192.168.1.6	RTP	Unknown RTP version 0
4	1.466120	192.168.1.5	192.168.1.6	RTCP	Receiver Report
5	1.469564	192.168.1.6	192.168.1.5	RTP	Unknown RTP version 0
7	1.486312	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=4002797603, Seq=5302, Time=2679300, Mark
8	1.516672	192.168.1.5	192.168.1.6	SIP/SD	Status: 200 OK, with session description
9	1.516781	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=4002797603, Seq=5303, Time=2679620
10	1.516855	192.168.1.5	192.168.1.6	RTP	Payload type=BV32, SSRC=4002797603, Seq=5304, Time=2679940

[+] Frame 8 (1054 bytes on wire, 1054 bytes captured)
 [+] Ethernet II, Src: Intel_dd:e8:2e (00:16:76:dd:e8:2e), Dst: Intel_dd:e8:b9 (00:16:76:dd:e8:b9)
 [+] Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.6 (192.168.1.6)
 [+] User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
 Source port: 5060 (5060)
 Destination port: 5060 (5060)
 Length: 1020
 Checksum: 0x89b5 [correct]
 [+] Session Initiation Protocol
 + Status-Line: SIP/2.0 200 OK
 + Message Header
 + Message body

Figura 7.20 Paquetes IPv4 monitoreados de PC2 a PC1 (inicio de llamada)

No. -	Time	Source	Destination	Protocol	Info
348	4.736819	192.168.1.6	192.168.1.5	RTP	Payload type=BV32, SSRC=922193536, Seq=2862, Time=2760080
350	4.756415	192.168.1.6	192.168.1.5	RTP	Payload type=BV32, SSRC=922193536, Seq=2863, Time=2760400
351	4.776047	192.168.1.5	192.168.1.6	SIP	Request: BYE sip:PC2%20IPv4@192.168.1.6:5060
353	4.777426	192.168.1.6	192.168.1.5	RTP	Payload type=BV32, SSRC=922193536, Seq=2864, Time=2760720
354	4.777861	192.168.1.6	192.168.1.5	RTCP	Sender Report
359	4.880211	192.168.1.6	192.168.1.5	SIP	Status: 200 OK

[+] Frame 359 (434 bytes on wire, 434 bytes captured)
 [+] Ethernet II, Src: Intel_dd:e8:b9 (00:16:76:dd:e8:b9), Dst: Intel_dd:e8:2e (00:16:76:dd:e8:2e)
 [+] Internet Protocol, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.5 (192.168.1.5)
 [+] User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
 Source port: 5060 (5060)
 Destination port: 5060 (5060)
 Length: 400
 Checksum: 0xab71 [correct]
 [+] Session Initiation Protocol
 + Status-Line: SIP/2.0 200 OK
 + Message Header

Figura 7.21 Paquetes IPv4 monitoreados de PC2 a PC1 (fin de llamada)

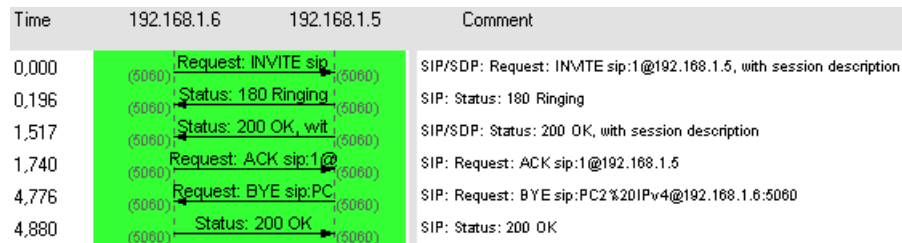


Figura 7.22 Diagrama de flujo VoIPv4 entre PC2 y PC1

7.4.2 Monitoreo VoIPv6

- **Tráfico IPv6 de: PC1: 2001:10:10::1 a PC2: 2001:10:10::2**

Para el caso IPv6, podemos apreciar en las Figura 7.23 y 7.24, el tráfico se inicia con la invitación (INVITE la cual establece una sesión) de iniciar una llamada desde la dirección 2001:10:10::1 a la dirección 2001:10:10::2 por medio de los protocolos SIP y SDP. Posteriormente el tráfico producido es similar al descrito para el caso IPv4 resumiéndolos en los siguientes pasos:

- PC1 a PC2, solicitud INVITE, negociación SIP y SDP encapsulados en UDP.
- PC2 a PC1, respuesta 180, la cual significa que su teléfono esta sonando.
- PC2 a PC1, respuesta 200 (OK), respuesta exitosa.
- PC1 a PC2 mensaje ACK de confirmación de negociación.
- Trafico de paquetes de VoIP por el protocolo RTP, encapsulados en paquetes UDP.
- PC2 a PC1, mensaje BYE.
- PC1 a PC2, respuesta 200 (OK), de la aceptación de fin de llamada.

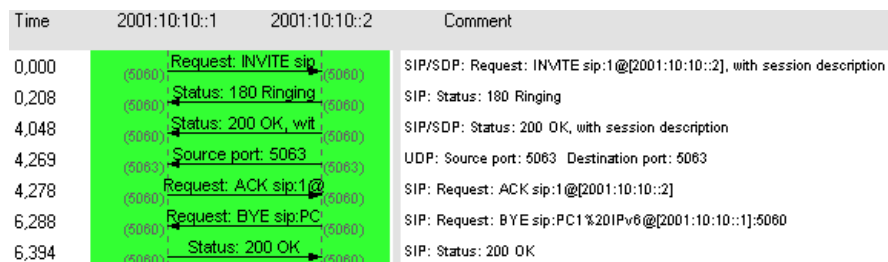


Figura 7.23 Diagrama de flujo VoIPv6 entre PC1 y PC2

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	2001:10:10::1	2001:10:10::2	SIP/SDP	Request: INVITE sip:1@[2001:10:10::2], with session description
2	0.207587	2001:10:10::2	2001:10:10::1	SIP	Status: 180 Ringing
7	4.048288	2001:10:10::2	2001:10:10::1	SIP/SDP	Status: 200 OK, with session description
40	4.269005	2001:10:10::2	2001:10:10::1	UDP	Source port: 5063 Destination port: 5063
52	4.277693	2001:10:10::1	2001:10:10::2	SIP	Request: ACK sip:1@[2001:10:10::2]
256	6.287522	2001:10:10::2	2001:10:10::1	SIP	Request: BYE sip:PC1%20IPv6@[2001:10:10::1]:5060
262	6.393952	2001:10:10::1	2001:10:10::2	SIP	Status: 200 OK

[-] Frame 1 (1148 bytes on wire, 1148 bytes captured)
[-] Ethernet II, Src: Intel_dd:e8:2e (00:16:76:dd:e8:2e), Dst: Intel_dd:e8:b9 (00:16:76:dd:e8:b9)
[-] Internet Protocol, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.6 (192.168.1.6)
[-] Internet Protocol version 6
[-] Version: 6
[-] Traffic class: 0x00
[-] Flowlabel: 0x000000
[-] Payload length: 1074
[-] Next header: UDP (0x11)
[-] Hop limit: 128
[-] Source address: 2001:10:10::1
[-] Destination address: 2001:10:10::2
[-] User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
[-] Session Initiation Protocol
[-] Request-Line: INVITE sip:1@[2001:10:10::2] SIP/2.0
[-] Message Header
[-] Message body

Figura 7.24 Paquetes IPv6 monitoreados de PC1 a PC2 (inicio y fin de llamada)

- **Tráfico IPv6 de: PC2: 2001:10:10::2 a PC1: 2001:10:10::1**

De forma análoga para la llamada IPv6 de PC2 a PC1, observamos en la Figura 7.25 el monitoreo de paquetes SIP y en la Figura 7.26 el diagrama de flujo de dicha comunicación.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	2001:10:10::2	2001:10:10::1	SIP/SD	Request: INVITE sip:1@[2001:10:10::1], with session description
2	0.195000	2001:10:10::1	2001:10:10::2	SIP	Status: 180 Ringing
14	2.725205	2001:10:10::1	2001:10:10::2	SIP/SD	Status: 200 OK, with session description
47	2.956697	2001:10:10::2	2001:10:10::1	SIP	Request: ACK sip:1@[2001:10:10::1]
292	5.385234	2001:10:10::1	2001:10:10::2	SIP	Request: BYE sip:PC2%20IPv6@[2001:10:10::2]:5060
299	5.492865	2001:10:10::2	2001:10:10::1	SIP	Status: 200 OK

[-] Frame 1 (1148 bytes on wire, 1148 bytes captured)
[-] Ethernet II, Src: Intel_dd:e8:b9 (00:16:76:dd:e8:b9), Dst: Intel_dd:e8:2e (00:16:76:dd:e8:2e)
[-] Internet Protocol, Src: 192.168.1.6 (192.168.1.6), Dst: 192.168.1.5 (192.168.1.5)
[-] Internet Protocol version 6
[-] Version: 6
[-] Traffic class: 0x00
[-] Flowlabel: 0x000000
[-] Payload length: 1074
[-] Next header: UDP (0x11)
[-] Hop limit: 128
[-] Source address: 2001:10:10::2
[-] Destination address: 2001:10:10::1
[-] User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
[-] Session Initiation Protocol
[-] Request-Line: INVITE sip:1@[2001:10:10::1] SIP/2.0
[-] Message Header
[-] Message body

Figura 7.25 Paquetes IPv6 monitoreados de PC2 a PC1 (inicio y fin de llamada)

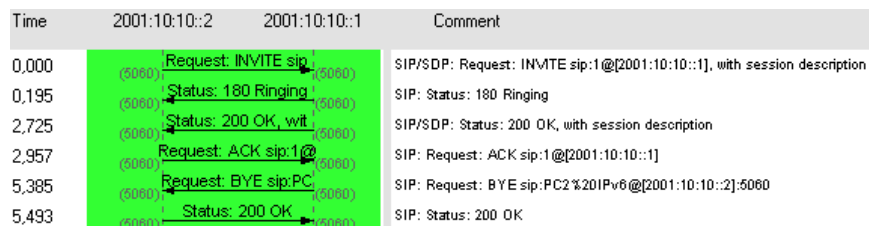


Figura 7.26 Diagrama de flujo VoIPv6 entre PC2 y PC1

CAPÍTULO VIII

PRUEBAS ADICIONALES Y RESULTADOS

8.1 Antecedentes

Como fue dicho en capítulos anteriores, una de las grandes ventajas de WiMAX frente a otros estándares de transmisión como WiFi u otros es el largo alcance que puede ofrecernos, el cual varía según la especificación de cada equipo y por supuesto del medio de propagación (LOS, NLOS), y diseño del enlace inalámbrico. Lo que se pretende a continuación es demostrar las promesas de WiMAX, realizando el proyecto de VoIP en IPv6 utilizando el estándar ya mencionado, en una red de topología PMP (Punto a multipunto) que es la topología que soportan los equipos de Airspan comunicando a dos equipos suscriptores entre si. Así también se realizarán pruebas de VoIP en IPv6 con otras normas de transmisión como lo son Ethernet y WiFi para obtener una comparación entre estas y WiMAX.

8.2 Comparación de VoIP IPv6 en WiMAX con Ethernet y WiFi

Para llevar a cabo este procedimiento, antes que nada se debió establecer una comunicación IPv6 entre ambos PC. Esto se realizó mediante dos portátiles haciendo uso de la Ethernet y WiFi de cada uno. Ya que no se usó ningún router de por medio o algún otro elemento de red que limite el protocolo IP, no fue necesario realizar un túnel IPv6. Las direcciones IPv6 fueron configuradas manualmente y en modo nativo.

En la Figura 8.1 podemos apreciar las interfaces de “Conexión de área local” y “Conexiones de red inalámbrica” con las respectivas direcciones IPv6 asignadas al PC1.

```

C:\>netsh interface ipv6 show address
Consultando el estado activo...

Interfaz 6: Teredo Tunneling Pseudo-Interface
-----
Tipo dir. Estado DAD Vida válida Vida pref. Dirección
-----
Vínculo Preferida infinite infinite fe80::ffff:ffff:fffd

Interfaz 5: Conexiones de red inalámbricas
-----
Tipo dir. Estado DAD Vida válida Vida pref. Dirección
-----
Manual Preferida infinite infinite 2001:10:100::1
Vínculo Preferida infinite infinite fe80::219:7dff:fe5c:ec01

Interfaz 4: Conexión de área local
-----
Tipo dir. Estado DAD Vida válida Vida pref. Dirección
-----
Manual Preferida infinite infinite 2001:10:10::1
Vínculo Preferida infinite infinite fe80::216:36ff:fedd:5e06

Interfaz 2: Automatic Tunneling Pseudo-Interface
-----
Tipo dir. Estado DAD Vida válida Vida pref. Dirección
-----
Vínculo Preferida infinite infinite fe80::5efe:192.168.0.1

Interfaz 1: Loopback Pseudo-Interface
-----
Tipo dir. Estado DAD Vida válida Vida pref. Dirección
-----
Bucle inv. Preferida infinite infinite ::1
Vínculo Preferida infinite infinite fe80::1

C:\>

```

Figura 8.1 Direcciones IPv6 de PC1

El mismo proceso se realizó en el segundo portátil. En la Tabla 8.1 se muestra un resumen con las direcciones IPv6 configuradas para ambos portátiles.

Comunicación	PC1	PC2
IPv6 Ethernet (802.3)	2001:10:10::1	2001:10:10::2
IPv6 WiFi (802.11)	2001:10:100::1	2001:10:100::2

Tabla 8.1 IPv6 de ambos portátiles

Teniendo la configuración IPv6 en ambos PCs, procedemos a realizar las pruebas de voz siguiendo los diagramas de conexión de las Figura 8.2 para el caso de Ethernet y Figura 8.3 para el caso de WiFi.

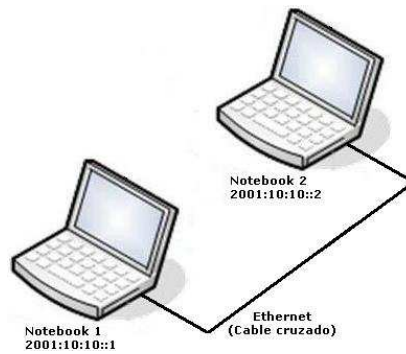


Figura 8.2 Conexión VoIP Ethernet IPv6 nativo

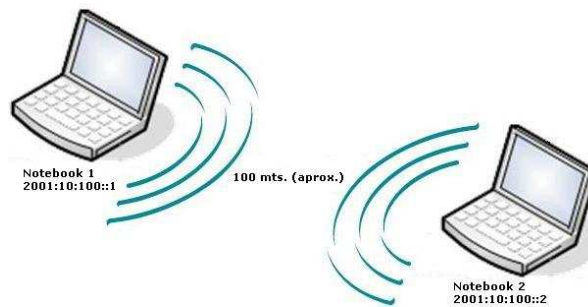


Figura 8.3 Conexión VoIP WiFi IPv6 nativo (100 mts. Aprox.)

8.2.1 Prueba VoIP en Ethernet

La prueba de conectividad IPv6 nativo en Ethernet, se realiza haciendo uso de la herramienta ping6 como se ha explicado anteriormente, el resultado se visualiza en la Figura 8.4.

```

C:\ Símbolo del sistema
C:\>ping6 2001:10:10::2
Haciendo ping 2001:10:10::2
de 2001:10:10::1 con 32 bytes de datos:
Respuesta desde 2001:10:10::2: bytes=32 tiempo<1m
Respuesta desde 2001:10:10::2: bytes=32 tiempo<1m
Respuesta desde 2001:10:10::2: bytes=32 tiempo<1m
Respuesta desde 2001:10:10::2: bytes=32 tiempo<1m
Estadísticas de ping para 2001:10:10::2:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\>

```

Figura 8.4 Ping por Ethernet desde PC1 a PC2

Al realizar la llamada, por medio de Ethereal podemos monitorear los paquetes y protocolos involucrados demostrando que la llamada ha sido satisfactoriamente realizada entre ambos portátiles como se puede ver en la Figura 8.5.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	2001:10:10::1	2001:10:10::2	SIP/SD	Request: INVITE sip:10[2001:10:10::2], with session description
2	0.172960	2001:10:10::2	2001:10:10::1	SIP	Status: 180 Ringing
11	1.044430	2001:10:10::2	2001:10:10::1	RTCP	Unknown packet type
12	1.046189	2001:10:10::1	2001:10:10::2	RTCP	Unknown packet type
13	1.046891	2001:10:10::2	2001:10:10::1	RTCP	Sender Report
16	1.088523	2001:10:10::2	2001:10:10::1	SIP/SD	Status: 200 OK, with session description
21	1.111337	2001:10:10::1	2001:10:10::2	RTCP	Receiver Report
24	1.118942	2001:10:10::1	2001:10:10::2	RTCP	Receiver Report
28	1.162462	2001:10:10::1	2001:10:10::2	RTCP	Unknown packet type
29	1.164351	2001:10:10::2	2001:10:10::1	RTCP	Unknown packet type
49	1.320622	2001:10:10::1	2001:10:10::2	SIP	Request: ACK sip:10[2001:10:10::2]
154	2.358270	2001:10:10::2	2001:10:10::1	SIP	Request: BYE sip:PC1%20IPv6@[2001:10:10::1]:5060
157	2.459715	2001:10:10::1	2001:10:10::2	SIP	Status: 200 OK

Frame 1 (1134 bytes on wire, 1134 bytes captured)
 # Ethernet II, Src: Quantaco_dd:5e:06 (00:16:36:dd:5e:06), Dst: Mitacint_93:a5:8f (00:40:d0:93:a5:8f)
 # Internet Protocol Version 6
 Version: 6
 Traffic class: 0x00
 Flowlabel: 0x00000
 Payload length: 1080
 Next header: UDP (0x11)
 Hop limit: 128
 Source address: 2001:10:10::1
 Destination address: 2001:10:10::2
 # User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
 # Session Initiation Protocol
 # Request-Line: INVITE sip:10[2001:10:10::2] SIP/2.0
 # Message Header
 # Message body

Figura 8.5 Captura de paquetes en llamada Ethernet desde PC1 a PC2

8.2.2 Prueba VoIP en WiFi

La prueba de conectividad IPv6 nativo en WiFi, se realiza a una distancia de 100 mts. aproximadamente, dado que a esta distancia se comienza a presentar interferencias. Haciendo uso de la herramienta ping6 como se ha explicado anteriormente, el resultado se visualiza en la Figura 8.6. Debemos mencionar que la red fue configurada en modo Ad-Hoc para poder realizar la conexión sin un access point de por medio, dejando a un portátil en modo Ad-Hoc y el otro en modo infraestructura.

```

C:\ Simbolo del sistema
C:\>ping6 2001:10:100::2
Haciendo ping 2001:10:100::2
de 2001:10:100::1 con 32 bytes de datos:
Respuesta desde 2001:10:100::2: bytes=32 tiempo=2ms
Respuesta desde 2001:10:100::2: bytes=32 tiempo=5ms
Respuesta desde 2001:10:100::2: bytes=32 tiempo=34ms
Respuesta desde 2001:10:100::2: bytes=32 tiempo=4ms
Estadísticas de ping para 2001:10:100::2:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 2ms, Máximo = 34ms, Media = 11ms
C:\>
  
```

Figura 8.6 Ping por WiFi desde PC1 a PC2

Al realizar la llamada, por medio de Ethereal podemos monitorear los paquetes y protocolos involucrados como podemos ver en la Figura 8.7 demostrando que la llamada ha sido satisfactoriamente realizada entre ambos portátiles.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	2001:10:100::1	2001:10:100::2	SIP/SD	Request: INVITE sip:k@[2001:10:100::2], with session description
2	0.508587	2001:10:100::1	2001:10:100::2	SIP/SD	Request: INVITE sip:k@[2001:10:100::2], with session description
3	1.083240	2001:10:100::2	2001:10:100::1	SIP	Status: 180 Ringing
4	2.963977	2001:10:100::2	2001:10:100::1	RTCP	Receiver Report
5	3.014796	2001:10:100::2	2001:10:100::1	RTP	Payload type=BV32, SSRC=3365947346, Seq=2614, Time=2754300, Mark
6	3.026715	2001:10:100::2	2001:10:100::1	RTP	Payload type=BV32, SSRC=3365947346, Seq=2615, Time=2754620
7	3.038004	2001:10:100::2	2001:10:100::1	SIP/SD	Status: 200 OK, with session description

Frame 1 (1144 bytes on wire, 1144 bytes captured)					
Ethernet II, Src: 00:19:7d:5c:ec:01 (00:19:7d:5c:ec:01), Dst: Billfont_65:ed:b1 (00:10:60:65:ed:b1)					
Internet Protocol Version 6					
Version: 6					
Traffic class: 0x00					
Flowlabel: 0x000000					
Payload length: 1090					
Next header: UDP (0x11)					
Hop limit: 128					
Source address: 2001:10:100::1					
Destination address: 2001:10:100::2					
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)					
Session Initiation Protocol					
Request-Line: INVITE sip:k@[2001:10:100::2] SIP/2.0					
Message Header					
Message body					

Figura 8.7 Captura de paquetes en llamada WiFi desde PC1 a PC2

8.3 Prueba de larga distancia WiMAX

Uno de los requisitos planteados dentro de los objetivos, es lograr comunicación inalámbrica de larga distancia, es decir, comunicación inalámbrica a más de un kilómetro como mínimo. Como se a descrito a lo largo de este trabajo, para establecer dicha comunicación se ha hecho de la tecnología WiMAX la cual de forma teórica tiene un alcance máximo de 50 Km., condición que quizás sea posible lograr con una antena de alta potencia de transmisión, ubicada a una altura considerable que permita línea vista donde la mayor parte de la primera zona de Fresnel se encuentre libre de obstáculos.

De acuerdo a las características técnicas de la estación base utilizada, BSR MicroMAX-SOC, y los equipos abonados, CPE EasyST, el alcance máximo disminuye considerablemente.

A continuación se describen las pruebas realizadas para comprobar y poder lograr el mayor alcance posible con línea a vista, para lo cual se ubicó la estación base con su respectiva antena, en el exterior de las dependencias del casino del Campus Miraflores de la Universidad Austral de

Chile, alejando los equipos receptores en dirección al “Puente Cruces”, para posteriormente alejarnos un poco mas, en dirección a los condominios “Alto del Cruces” y “Los Notros de Curiñanco”, ubicados por el “Camino los Pellines” orientado en dirección al “Parque Oncol”.

8.3.1 Prueba desde Casino de Miraflores a Puente Cruces (1.34 Km.)

La prueba de conectividad como se explicó anteriormente, se hizo entre Casino y Puente Cruces, para la cual se comenzó por la instalación de la estación base en el casino, como se puede apreciar en las Fotografía 8.1 y 8.2.



Fotografía 8.1 BS instalada, vista 1



Fotografía 8.2 BS instalada, vista 2

La orientación de la antena a la que fue dirigida la antena fue aproximadamente de unos 5°. La vista de enfoque la apreciamos en la Fotografía 8.3.



Fotografía 8.3 Orientación de la antena

La distancia entre Puente Cruces (ubicación de los CPEs) al Casino de Miraflores (estación base o BS), existe una distancia aproximada de 1.34 Km., como se puede apreciar en la Figura 8.8 extraída del software Google Earth Pro 4.2.

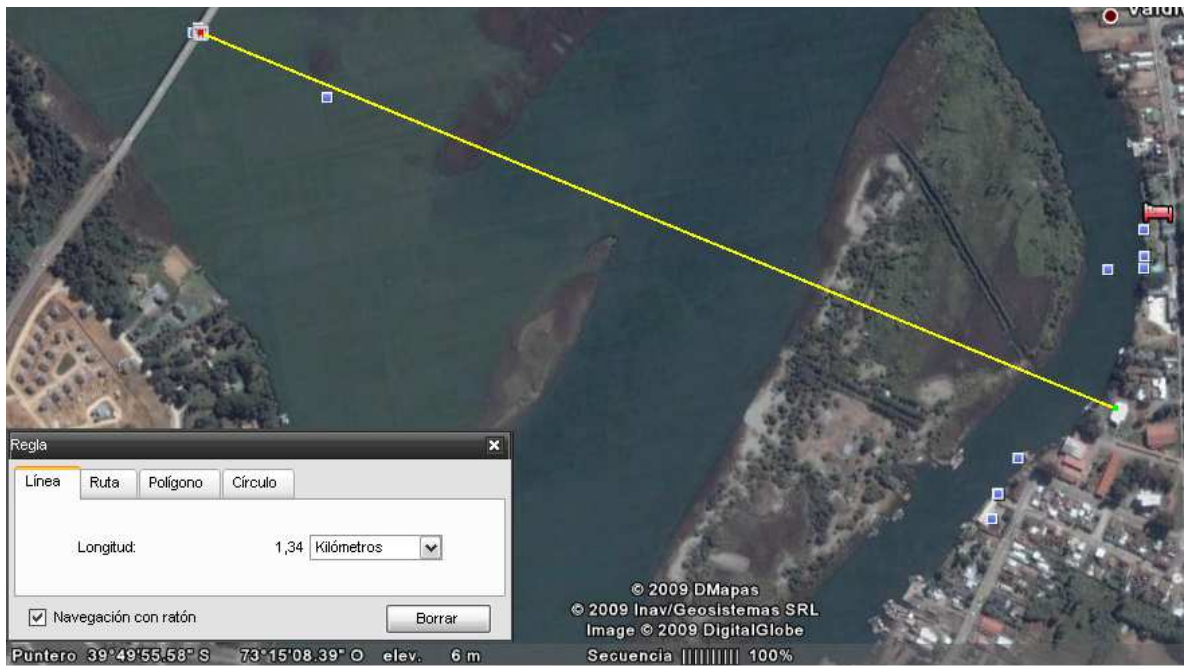


Figura 8.8 Distancia entre Casino Miraflores al Puente Cruces

Teniendo ya nuestra estación base instalada y la distancia aproximada entre BS y CPEs, procedemos a comprobar nuestro enlace, para lo cual solo nos resta alimentar los EasyST para probar la comunicación, hecho que fue posible por medio de una UPS que fue transportada por nosotros mismos juntos a los equipos terminales. Habiendo establecido comunicación comprobamos que la respuesta a nuestra conectividad fue satisfactoria, con una señal de recepción máxima en los EasyST, dando la posibilidad de pensar en poder alejarnos un poco más en la misma dirección en que fue orientada nuestra antena.

En las Fotografías 8.4 y 8.5 se aprecia la prueba en terreno de lo anteriormente comentado visualizando los portátiles finales, EasyST respectivos y la UPS utilizada como fuente de alimentación para los CPE.



Fotografía 8.4 Prueba 1 en terreno, vista 1



Fotografía 8.5 Prueba 1 en terreno, vista 2

8.3.2 Prueba desde Casino de Miraflores a Alto del Cruces (2.6 Km.)

Como anteriormente se mencionó, precedimos a alejarnos aun más de nuestra estación base para obtener mayor distancia de alcance, con la premisa de haber obtenido una calidad de recepción máxima en nuestros CPEs desde el Puente Cruces. Fue así que nos dirigimos caminando con nuestros terminales y UPS, en búsqueda de un lugar que nos brinde línea a vista con nuestra antena y nos permita mantener comunicación con esta. De esta manera fue donde nuestro segundo punto de prueba (Fotografía 8.6) fue en el condominio “Alto del Cruces”, obteniendo respuesta satisfactoria nuevamente.



Fotografía 8.6 Prueba 2 en terreno

Habiendo logrado respuesta satisfactoria una vez mas, nos alejamos un poco mas, al que sería nuestro punto final de prueba debido a que; geográficamente el “Camino los Pellines” continuaba con descenso haciéndonos perder línea vista con nuestra antena, no contábamos con movilización que nos permita la búsqueda de un punto de alcance a mayor lejanía, y finalmente el agotamiento de la carga de nuestra UPS.

De esta manera la distancia final lograda desde un sitio eriazo cerca del condominio Alto del Cruces situado a 80 mts. aproximadamente sobre el nivel del mar y el Casino Miraflores, fue de 2.6 Km. aproximadamente, visualizándola en la Figura 8.9 extraída nuevamente del Software Google Earth Pro.

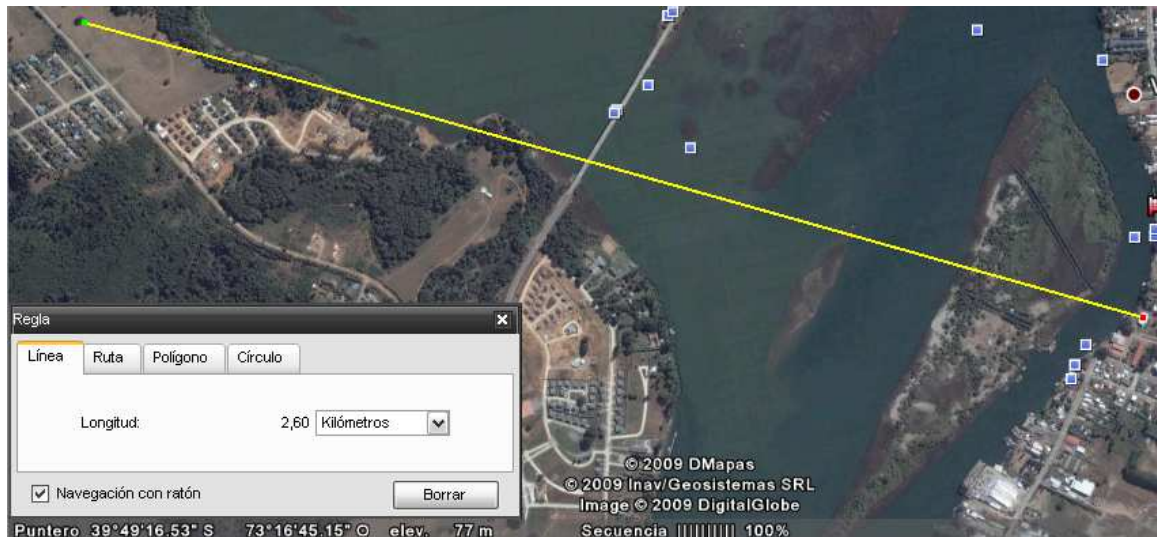


Figura 8.9 Distancia entre Casino Miraflores a Altos del Cruces

En las Fotografía 8.7 se aprecia la prueba en terreno de lo anteriormente comentado visualizando los portátiles finales, EasyST respectivos y la UPS utilizada como fuente de alimentación para los CPE.



Fotografía 8.7 Prueba 3 en terreno

8.3.3 Resultados técnicos del enlace.

Algunos resultados importantes del enlace pueden ser medidos y monitoreados por medio del mismo equipo abonado viendo los parámetros en la Web Page. En la Figura 8.10 se muestran algunos de estos casos.

Signal Parameters

Link Status
OPERATIONAL

Downlink Parameter	Value
BS Identifier	00A00A10042C
Downlink Frequency	3566.000 MHz
Downlink Channel Bandwidth	3.5 MHz
SNR	17.3 dB
Received Signal Strength	-79.6 dBm
Modulation	QPSK 3/4

Uplink Parameter	Value
Uplink Frequency	3466.000 MHz
Uplink Channel Bandwidth	3.5 MHz
Tx Power	24.0 dBm
Modulation	BPSK 1/2

Figura 8.10 CPE PC1 (NLOS)

Signal Parameters

Link Status
OPERATIONAL

Downlink Parameter	Value
BS Identifier	00A00A10042C
Downlink Frequency	3566.000 MHz
Downlink Channel Bandwidth	3.5 MHz
SNR	20.6 dB
Received Signal Strength	-78.4 dBm
Modulation	16QAM 1/2

Uplink Parameter	Value
Uplink Frequency	3466.000 MHz
Uplink Channel Bandwidth	3.5 MHz
Tx Power	24.0 dBm
Modulation	BPSK 1/2

Figura 8.11 CPE PC2 (NLOS)

Uno de los primeros detalles visto en los equipos abonado, es el cambio de modulación a una de nivel inferior a la que se podía ver dentro del laboratorio, la cual casi siempre se mantuvo en 64QAM en Downlink debido a la proximidad que se encontraban los equipos, en contraste a los resultados que se veían en el laboratorio, con respecto a larga distancia, los equipos abonados presentan modulaciones QPSK y 16QAM en Downlink y ambos BPSK 1/2 en Uplink, esto debido a la función adaptativa que WiMAX ofrece según las condiciones de propagación, para este caso anterior por la distancia considerable y la poca visibilidad directa en que se encontraban los equipos CPE en ese momento (Figura 8.10 y Figura 8.11).

Cabe mencionar también la auto regulación de la potencia TX del equipo CPE, en donde la estación base no sólo controla la modulación del equipo CPE, sino que también la potencia que este debe emitir para poder conectarse a la estación base. También puede apreciarse la disminución de la potencia recibida por el equipo CPE.

La Tabla 8.2 muestra los parámetros de señal para distintos casos:

Potencia Tx BS	Potencia Tx CPE	Distancia (mts.)	Señal recibida CPE	SNR	Modulación Uplink	Modulación Downlink
0 dBm	-1 dBm	1	-48.4 dBm	30.4 dB	16QAM ½	64QAM ¾
28 dBm	-12.5 dBm	1	-23.8 dBm	30.4 dB	16QAM ½	64QAM ¾
28 dBm	24 dBm	2600 (LOS)	-67.0 dB	30 dB	BPSK ½	64QAM ¾
28 dBm	24 dBm	2600 (NLOS)	-79.6 dB	17.3 dB	BPSK ½	QPSK ¾ y 16 QAM ½

Tabla 8.2 Parámetros de señal para diferentes condiciones de propagación

8.3.4 Balance de potencias

Antes de realizar nuestro balance de potencias de subida y de bajada, se comprobó que la primera zona de Fresnel estaba libre de obstáculos para establecer la comunicación.

Para establecer la primera zona de Fresnel, debemos determinar la línea de vista de RF "RF LOS", que en términos simples es una línea recta entre la antena transmisora y la receptora. Ahora la zona que rodea el RF LOS es la zona de Fresnel. El radio de la sección transversal de la primera zona de Fresnel tiene su máximo en el centro del enlace. En este punto, el radio r se puede calcular como sigue:

$$r = 547.723 \sqrt{\frac{d}{4f}}$$

Donde:

r = radio en metros (mts.)

d = distancia en kilómetros (Km.)

f = frecuencia en (MHz.).

De esta manera tenemos que la primera zona de Fresnel para el enlace de subida es:

$$r = 547.723 \sqrt{\frac{2.6}{4 \cdot 3466}}$$

$$r \approx 7.5(\text{mts.})$$

Y para el enlace de bajada tenemos que:

$$r = 547.723 \sqrt{\frac{2.6}{4 \cdot 3566}}$$

$$r \approx 7.39(\text{mts.})$$

De esta manera comprobamos que nuestra primera zona de Fresnel, que requiere al menos de un 60% libre de obstrucción, cuanta con un 100% libre, debido a que nuestra antena transmisora se encuentra a una altura aproximada de 6 mts. sobre el nivel del mar y nuestros equipos receptores a 80 mts. aproximadamente sobre el nivel del mar.

8.3.4.1 Balance de potencia Uplink

Primeramente comenzaremos calculando las atenuaciones de la comunicación desde estación suscriptora a estación base, para luego realizar el balance de potencia, mediante la diferencia entre ganancia y pérdidas del enlace.

- *Atenuación espacio libre*

$$A_0(\text{dB}) = 20 \cdot \log d(\text{Km}) + 20 \cdot \log f(\text{MHz}) + 32.5$$

$$A_0(\text{dB}) = 20 \cdot \log 2.6 + 20 \cdot \log 3466 + 32.5$$

$$A_0(\text{dB}) \approx -111.6$$

- ***Atenuación por apuntamiento***

Las pérdidas por apuntamiento fueron consideradas despreciables. Para este enlace se tomo la consideración que tanto el azimut y ángulo de elevación de la antena correspondían al caso ideal de direccionamiento.

- ***Perdidas por dispersión***

Anteriormente se explicaron las consideraciones de altura tanto para antena trasmisora como equipos receptores, dejando libre la primer zona de Fresnel por lo cual se asume que el enlace no cuenta con pérdidas por dispersión.

- ***Perdidas por lluvia***

Claramente este factor no es considerado, debido a que a la hora de comprobar la comunicación en nuestro enlace, el cual fue por unos breves instantes de tiempo, no se registraron precipitaciones.

- ***Absorción por gases***

En enlaces Troposfericos, existe la absorción y refracción por la incidencia de la troposfera con las ondas de radio. La atenuación por absorción molecular se debe principalmente a moléculas de oxígenos y vapor de agua, medidas en dB/Km. Para frecuencias bajo los 10 GHz., como es el caso nuestro, esta atenuación es minima y prácticamente despreciable para frecuencias dentro del rango de los 3.5 GHz. como podemos apreciar en la Figura 8.12, mientras que a frecuencias superiores se puede apreciar un considerable aumento de las atenuaciones producidas.

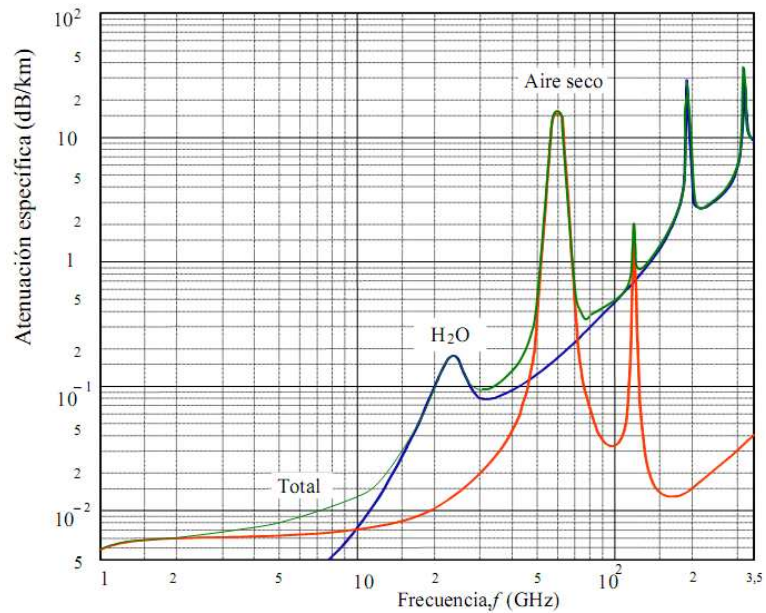


Figura 8.12 Absorción atmosférica de las ondas electromagnéticas

Las pérdidas en el cable que conecta la antena receptora al BSR es de tipo LMR-400 el cual presenta una atenuación de 0.267dB por metros a 3466 MHz, utilizando en nuestro caso 1.8 mts. correspondiente a una atenuación de 0.481dB.

Ahora con nuestras atenuaciones calculadas, realizaremos la aproximación para comprobar el comportamiento del enlace, y si la señal que llega a destino no sobrepasa los niveles de sensibilidad del receptor. Figura 8.13.

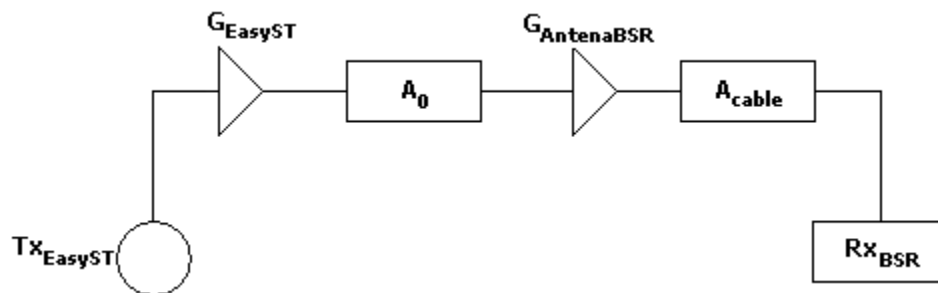


Figura 8.13 Diagrama balance potencias Uplink

$$Tx_{EasyST} = 24dBm$$

$$G_{AntenaTx} = 6dBi$$

$$A_0 = -111.6dB$$

$$G_{AntenaRx} = 14dBi$$

$$A_{cable} = -0.481dB$$

$$Rx_{BSR} = -98dBm$$

$$Rx_{BSR} = Tx_{EasyST} + G_{AntenaTx} + A_0 + G_{AntenaRx} + A_{cable}$$

$$Rx_{BSR} = 24dBm + 6dBi - 111.6dB + 14dBi - 0.481dB$$

$$Rx_{BSR} = -68.081dBm$$

Entonces como la sensibilidad del Rx es de -98dBm para una modulación BPSK 1/2, decimos que nuestro enlace cumple con su objetivo en esta primera zona.

8.3.4.2 Balance de potencia Downlink

Al igual que para el caso Uplink calculamos las atenuaciones de la comunicación esta vez desde estación base a estación suscriptora, para luego realizar el balance de potencia, mediante la diferencia entre ganancia y pérdidas del enlace.

Las consideraciones para el enlace Downlink son las mismas que para Uplink, por lo cual se consideran las mismas atenuaciones que para el caso anterior.

- **Atenuación espacio libre**

$$A_0(dB) = 20 \cdot \log d(Km) + 20 \cdot \log f(MHz) + 32.5$$

$$A_0(dB) = 20 \cdot \log 2.6 + 20 \cdot \log 3566 + 32.5$$

$$A_0(dB) \approx -111.84$$

Las pérdidas en el cable que conecta la antena receptora al BSR es de tipo LMR-400 el cual presenta una atenuación de 0.272dB por metros a 3566 MHz, utilizando en nuestro caso 1.8 mts. correspondiente a una atenuación de 0.49dB.

Ahora con nuestras atenuaciones calculadas, realizaremos la aproximación para comprobar el comportamiento del enlace, y si la señal que llega a destino no sobrepasa los niveles de sensibilidad del receptor. Figura 8.14.

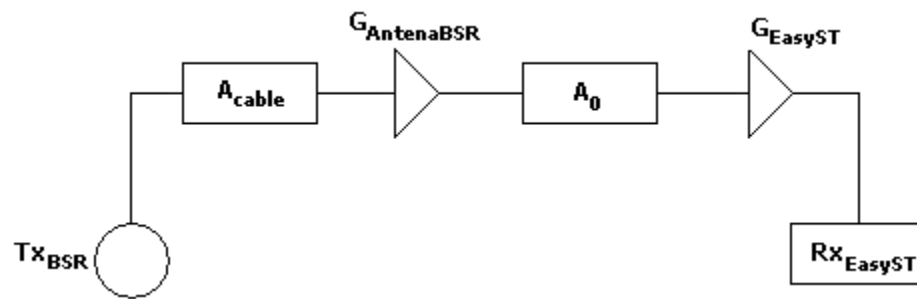


Figura 8.14 Diagrama balance potencias Downlink

$$Tx_{BSR} = 27dBm$$

$$A_{cable} = -0.49dB$$

$$G_{AntenaTx} = 14dBi$$

$$A_0 = -111.84dB$$

$$G_{AntenaRx} = 6dBi$$

$$Rx_{EasyST} = -82dBm$$

$$Rx_{EasyST} = Tx_{BSR} + A_{cable} + G_{AntenaTx} + A_0 + G_{AntenaRx}$$

$$Rx_{EasyST} = 27dBm - 0.49dB + 14dBi - 111.84dB + 6dBi$$

$$Rx_{EasyST} = -65.33dBm$$

Entonces como la sensibilidad del Rx es de -82dBm para una modulación 64QAM 3/4, decimos que nuestro enlace cumple con su objetivo en esta primera zona.

CONCLUSIONES

De acuerdo a las pruebas comparativas de VoIP realizadas en Ethernet y WiFi contra WiMAX, no se apreciaron grandes diferencias en la comunicación dentro de un radio menor a 100 mts. de distancia entre terminales, sin embargo, superada esta barrera, la comunicación se hizo imposible en WiFi, y es comprobado que las pérdidas para el caso de los cables en distancias superiores, son considerables para el caso de Ethernet, no satisfaciendo las necesidades ni prestaciones entregados por la tecnología inalámbrica de largo alcance WiMAX, que si fue capaz de transmitir paquetes de voz a largas distancias sin problemas.

Debido a que Ethernet y WiFi, son tecnologías ideadas para soluciones de redes de área local, estas no están diseñadas para permitir la interacción de una gran cantidad de usuarios, debido al mecanismo de detección de colisiones implementado en ambos casos, lo que se traduce como la ausencia de calidad de servicio, especialmente para servicios de tiempo real como la voz, soporte que si es entregado por WiMAX, por medio de VLANs, para seguridad entre usuarios conectados a una misma estación base, QoS que puede ser configurado dinámicamente en función del tráfico transportado, dando prioridad a los paquetes de voz como es nuestro caso y la principal ventaja de poder establecer comunicación NLOS a diferencia de WiFi.

Dentro del soporte de QoS que ofrece WiMAX, encontramos mecanismos correctores de errores como FEC, que permite de forma automática la corrección en el receptor sin retransmisión de la información original, y la alternativa de activación del protocolo ARQ que a diferencia del anterior, si se encarga de retransmitir paquetes perdidos en el camino, por lo cual es importante considerar muy bien estos parámetros a la hora de establecer un enlace dedicado como fue el nuestro para el caso de la voz, donde no fue, ni es conveniente activar el mecanismo ARQ, debido a que no es óptimo para transmisión de paquetes en tiempo real provocando posiblemente mayores interferencias que soluciones en la comunicación.

WiMAX, gracias a su modulación adaptativa, permite ajustar el orden de la modulación de la señal dependiendo de la relación señal a ruido. Cuando el enlace de radio es de alta calidad, se utiliza una modulación de mayor orden, dando al sistema más capacidad. Durante la pérdida de

señal, el sistema WiMAX puede cambiar la modulación a una de orden inferior con el fin de mantener la estabilidad de la calidad y el enlace de la conexión. Esto se pudo comprobar en terreno bajo diferentes perfiles de propagación, pasando desde condiciones muy favorables como distancias cortas en LOS y desfavorables como distancias largas tanto en LOS como NLOS, viendo así los cambios de modulación que los enlaces sufrían de acuerdo a su alejamiento y pérdida de línea vista.

Durante la mayor parte de las pruebas de enlaces se pudo comprobar siempre que la modulación empleada por el canal Uplink es de menor orden que la del canal Downlink, ya que el enlace descendente es siempre de mayor calidad que el ascendente. Esto es debido por propias características de los equipos empleados (Airspan), los equipos abonados EasyST poseen un transmisor Tx de menor potencia que la estación base MicroMAX (24 y 27 dBm respectivamente).

Una de las características de WiMAX comprobada en los enlaces realizados, es la integración de un algoritmo de control de potencia utilizado para mejorar el funcionamiento total del sistema, que es regulado por la propia estación base, enviando una información al equipo abonado CPE para que este regule la potencia de transmisión Tx, reduciéndola para condiciones favorables de propagación y aumentándola para condiciones desfavorables tales como NLOS.

Si bien WiMAX es una tecnología que soporta una topología de malla, es decir conectar equipos CPE entre sí a través de saltos hasta llegar a la estación base y de esta manera lograr un mayor alcance, no fue posible realizar esta configuración por limitaciones propias de los equipos, teniendo solamente la opción de topología PMP (Punto multipunto) que es la que nos permite comunicar los equipos CPE, pero pasando a través de la estación base.

En una llamada de VoIP, la voz analógica es digitalizada por la interfaz de sonido del PC y comprimida por los códec del softphone, siendo encapsulada en RTP y luego UDP antes de ser transmitida en la trama IP, esto se demostró en las llamadas establecidas y monitoreadas por el analizador de Red Ethereal, en donde cada RTP se mostraba dentro del protocolo UDP.

De acuerdo a los resultados obtenidos en WiMAX de estos equipos, se puede afirmar que son apropiados para realizar llamadas en VoIP ya que su latencia aún siendo alta, en promedio de 50 milisegundos, encontrándose dentro del rango para poder establecer una conversación sin molestia, sin embargo, es probable que si la llamada tuviera que realizar varios saltos entre nodos o estaciones bases, la latencia aumentaría considerablemente ofreciendo una pésima QoS e inhabilitándose para poder realizar llamadas sin molestias.

El protocolo SIP permite establecer la ubicación física de un usuario determinado y es independiente de donde se encuentre conectado este (Dirección IP), el usuario que inicia la llamada, envía una petición en modo register al servidor de registro SIP, informando a qué dirección física debe asociarse la dirección lógica del mismo. En nuestro caso se demuestra que no es necesario el uso de un servidor SIP, ya que las pruebas se realizaron entre dos usuarios solamente, esto se logro dejando como dominio a uno de ellos, haciendo creer por medio de la configuración del usuario que inicia la llamada, que el destino es el dominio o servidor, de esta forma se pudo establecer la comunicación de voz entre origen y destino sin tener que pasar por un servidor.

En esta experiencia se pudo demostrar la coexistencia entre el protocolo IPv6 e IPv4 mediante el mecanismo “dual stack”, que es el método de integración, donde el Host tiene implementado tanto IPv4 como IPv6 lo que permite a este tener la capacidad de enviar y recibir paquetes en ambos protocolos, tomando la decisión de cuando las conexiones deben realizarse en IPv6 o IPv4.

Una de las limitantes del hardware utilizado es que este no soporta el protocolo IPv6, sin embargo fue posible transmitir paquetes IPv6 mediante “Tunelización” que es el mecanismo de transición que permite encapsular datagramas IPv6 dentro de datagramas IPv4. Este mecanismo es muy útil para conectar dos islas informáticas bien conocidas y muy poco probable que cambien, como lo fue nuestra comunicación entre dos equipos CPE.

Como se vió en nuestro estudio teórico, IPv6 a diferencia de IPv4, cuenta con soporte de calidad de servicio QoS, trabajando con etiquetas en los campos de flujo, que son de gran utilidad para

manejar tráfico como lo es el de tiempo real, necesario para la VoIP. Si bien no se pudo apreciar con claridad esta ventaja en nuestro trabajo práctico, debido a la baja demanda de equipos suscriptores conectados simultáneamente, es concluyente decir que si podrían ser apreciadas tales ventajas en sistemas con mayor cantidad de usuarios

A la hora de hacer un enlace de larga distancia, es importante evaluar los equipos requeridos según las necesidades de servicio. Es importante considerar potencias de transmisión, recepción, y ganancias en las antenas, ya que son de vital importancia en el establecimiento de dicha comunicación y serán las limitantes del alcance de nuestro enlace.

Para el establecimiento de un backbone o una red de enlace WiMAX, es indispensable hacer un estudio detallado de la topografía, obstáculos y lugares propiamente tal para el emplazamiento de estaciones base, las cuales deben contar con la mayor línea a vista posible a otros nodos bases y/o nodos suscriptores, para lograr mejores rendimientos, tal como se realizó en nuestra prueba en terreno, donde previamente se hizo un estudio de estos factores, comprobado conectividad LOS y NLOS para los enlaces de 1.3 y 2.6 Km. aproximadamente.

Es importante evaluar las consideraciones técnicas de la máquina en donde alojaremos nuestro servidor WiMAX, en nuestro caso el software Netspan, debido a los requisitos de rendimiento, memoria, sistemas operativos y bases de datos que maneja, son de real importancia a la hora de expandir nuestro enlace punto a punto, a uno punto multipunto, donde las necesidades de diversos usuarios suscriptores puedan verse afectadas, debido a congestión de nuestra red.

A pesar de que nuestra estación base MicroMAX presenta ciertas limitaciones técnicas en comparación a otras BSR, pudimos alcanzar un distancia entre BS y SS de 2.6 Km., es decir, una distancia posible de 5.2 Km. entre puntos terminales con la posibilidad de haber tenido un alcance un poco mayor, sin embargo, es necesario aclarar que existe la posibilidad alcanzar distancias mucho mayores basadas en WiMAX, con mejores prestaciones y calidad de servicio, incluyendo movilidad, si es que se optara por estaciones base de primera jerarquía dentro de las distribuidas por Airspan como sería con una MacroMAX o HiperMAX.

REFERENCIAS BIBLIOGRAFICAS

- [1]. Silvia Hagen, IPv6 Essentials, 1º edición, Ed. O'Reilly Media, Inc, 2002.
- [2]. Daniel Minoli, Voice Over IPv6: Architectures for Next Generation VoIP Networks, 1º edición, Ed. Newnes, USA, 2006.
- [3]. 6SOS, El Protocolo IPv6, versión 4.0, Enero, 2004.
- [4]. 6SOS, Instalación de IPv6 en Plataformas Windows, versión 4.0, Enero, 2004.
- [5]. Salvador Fernández Fernández, Fundamentos de Migración IPv4 a IPv6, 2008.
- [6]. SR Telecom Inc., WiMAX Capacity White Paper, Agosto, 2006.
- [7]. SR Telecom Inc., WiMAX Technology: LOS and NLOS Environments , Agosto, 2004.
- [8]. Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed, Fundamentals of WiMAX: Understanding Broadband Wireless Networking, 1º edición, Ed. Prentice Hall PTR, 2007.
- [9]. Loutfi Nuaymi, WiMAX: Technology for Broadband Wireless Access, Ed. Wiley, 2007.
- [10]. Maybelline Reza Robles, Voz sobre IP: Análisis del Servicio Instalado en la Facultad de Telemática, Colombia, Junio, 2001.
- [11]. Airspan, MicroMAX-SOC Hardware Installation, 605-0000-742 Rev B.
- [12]. Airspan, EasyST Hardware Installation Guide, 605-0000-701 Rev I.
- [13]. Airspan, Netspan SR2.0 User's Guide, 605-0000-712 Rev D.
- [14]. Airspan, MicroMAX-SOC Setup vía Netspan.
- [15]. Airspan, Product Specification: AS.MAX MicroMAX-SOC, System Release 2.1.
- [16]. Airspan, Product Specification: AS.MAX EasyST, System Release 2.00.
- [17]. <http://www.ipv6forum.com/>
- [18]. <http://www.wimaxforum.org/>
- [19]. <http://www.voipforo.com/protocolosvoip.php>

ANEXO I

MONITOREO DE PAQUETES SNMP DESDE SERVIDOR NETSPAN

SNMP o Protocolo Simple de Administración de Red, es un protocolo de la familia de protocolos TCP/IP. SNMP trabaja en la capa de aplicación del modelo OSI, y se encarga de facilitar el intercambio de información de administración entre dispositivos de red, es decir, permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas.

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2) esta ultima, con algunas mejoras adicionales hechas a la primera versión.

Para el manejo de nuestra Red WiMAX, el software utilizado es Netspan, el cual es el encargado de administrar la Red y gestionar todos los paquetes por medio de este protocolo. Para enviar información o establecer parámetros entre estaciones suscriptoras (SS) y estaciones base (BS), SNMP en su versión 2 es el protocolo utilizado, el cual permite el reconocimiento de estos equipos entre si, y es el encargado de entregar las Bases de Información de Gestión o Management Information Bases (MIBs).

Una captura de tráfico extraído desde el software Ethereal, de paquetes SNMP entre el Servidor Netspan con IP 192.168.1.15 y la Estación Base 192.168.1.10, se aprecia en la Figura A1.1.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	D-Link_8c:b8:1d	Broadcast	ARP	who has 192.168.1.10? Tell 192.168.1.15
2	0.000795	RDCCommu_10:0a:a0	D-Link_8c:b8:1d	ARP	192.168.1.10 is at 00:a0:0a:10:0a:a0
3	0.000802	192.168.1.15	192.168.1.10	SNMP	GET-NEXT IF-MIB::ifNumber
4	0.001879	192.168.1.10	192.168.1.15	SNMP	RESPONSE IF-MIB::ifNumber.0
5	0.015093	192.168.1.15	192.168.1.10	SNMP	GET-NEXT SNMPv2-SMI::transmission.184.1.1.6 iso.0.8802.16.1.1.1 SNMPv2-SMI::transmission.1
6	0.018392	192.168.1.10	192.168.1.15	SNMP	RESPONSE SNMPv2-SMI::transmission.184.1.1.6.1.1.1.1 iso.0.8802.16.1.1.3.2.1.1.2.1 SNMPv2
7	0.032849	192.168.1.15	192.168.1.10	SNMP	GET-NEXT IF-MIB::ifEntry
8	0.033932	192.168.1.10	192.168.1.15	SNMP	RESPONSE IF-MIB::ifIndex.1
9	0.034500	192.168.1.15	192.168.1.10	SNMP	GETBULK IF-MIB::ifIndex
10	0.036566	192.168.1.10	192.168.1.15	SNMP	RESPONSE IF-MIB::ifIndex.1 IF-MIB::ifIndex.2 IF-MIB::ifDescr.1 IF-MIB::ifDescr.2 IF-MIB::if
11	0.038831	192.168.1.15	192.168.1.10	SNMP	GETBULK IF-MIB::ifType
12	0.041643	192.168.1.10	192.168.1.15	SNMP	RESPONSE IF-MIB::ifType.1 IF-MIB::ifType.2 IF-MIB::ifMTU.1 IF-MIB::ifMTU.2 IF-MIB::ifSpeec
13	0.043961	192.168.1.15	192.168.1.10	SNMP	GETBULK IF-MIB::ifPhysAddress
14	0.046099	192.168.1.10	192.168.1.15	SNMP	RESPONSE IF-MIB::ifPhysAddress.1 IF-MIB::ifPhysAddress.2 IF-MIB::ifAdminStatus.1 IF-MIB::if
15	0.048007	192.168.1.15	192.168.1.10	SNMP	GETBULK IF-MIB::ifAdminStatus

Frame 3 (82 bytes on wire (82 bytes captured)) # Ethernet II, Src: D-Link_8c:b8:1d (00:05:5d:8c:b8:1d), Dst: RDCCommu_10:0a:a0 (00:a0:0a:10:0a:a0) # Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.10 (192.168.1.10) # User Datagram Protocol, Src Port: 2573 (2573), Dst Port: snmp (161) # Simple Network Management Protocol Version: 2C (1) Community: public PDU type: GET-NEXT (1) Request Id: 0x000004d8 Error Status: NO ERROR (0) Error Index: 0 Object Identifier 1: 1.3.6.1.2.1.2.1 (IF-MIB::ifNumber) Value: NULL

Figura A1.1 Monitoreo de paquetes SNMP entre servidor Netspan y BS

ANEXO II

CONFIGURACION MODO AD-HOC

La configuración modo Ad-Hoc es donde los equipos clientes WiFi se conectan entre si para formar una red punto a punto sin necesidad de utilizar un punto de acceso, y en donde cada equipo funciona como cliente y a la vez como punto de acceso.

A continuación se describe los pasos para crear una red WiFi en modo Ad-Hoc:

Uno de los dos equipos será el que funcionará como servidor, para esto nos dirigimos a Propiedades de Conexiones de red inalámbricas y en la pestaña “Redes inalámbricas” vamos a opciones avanzadas y escogemos la opción “Sólo redes de equipo a equipo (ad hoc)”, Figura A2.1.

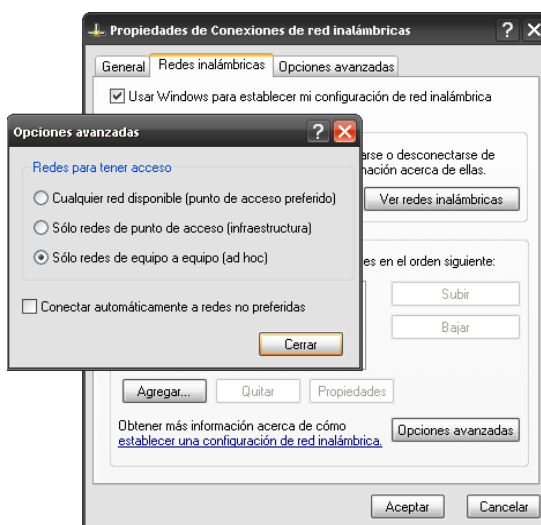


Figura A2.1 Opción modo Ad-Hoc

Después de haber fijado la red en modo (ad hoc) hacemos click en “Agregar...” para poder dar un “Nombre de red” a nuestra red, Figura A2.2.

En nuestro caso nuestro el (SSID) es “WiFi Ad-Hoc”, y la red es abierta sin clave de red.

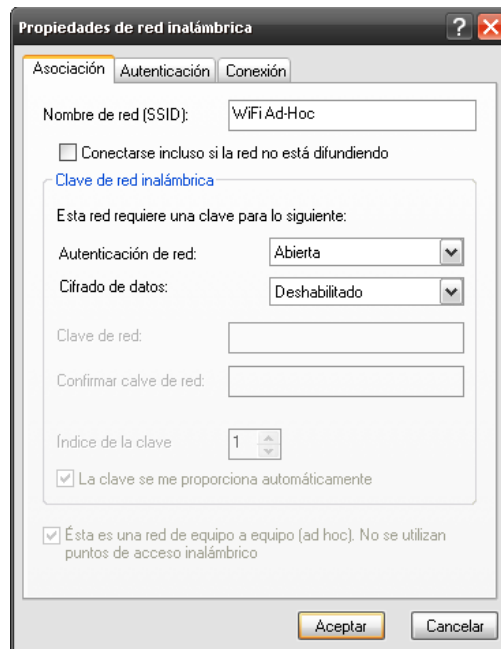


Figura A2.2 Nombre y seguridad de Red

Una vez creada la red con su respectivo SSID, la red se mostrara en lista de redes inalámbricas disponibles como se muestra en la Figura A2.3.

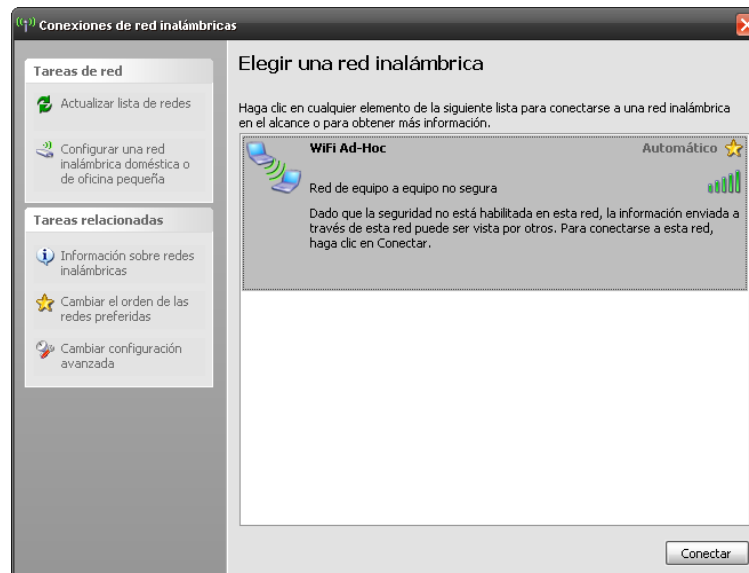


Figura A2.3 Red Ad-Hoc detectada

Tan sólo se necesita hacer un click en Conectar para poder acceder a la red Ad-Hoc configurada.

ANEXO III

ANTENA SECTORIAL DE BS

A continuación se darán los datos técnicos de la antena BS, datos que son de importancia al momento de realizar el diseño y estimación de un enlace.

La Tabla A3.1 muestra las características técnicas de la antena sectorial del fabricante “European Antennas” modelo “SA13-180V-35B-D3/800”, además de visualizar en las Figuras A3.1 y A3.2 el panel de la antena y su vista frontal respectivamente.

Tipo de antena	Direccional
Polarización	Vertical
Frecuencia	3.40 - 3.72 GHz.
Ganancia	14 dBi
HPBW Az°(área de cobertura)	180°
HPBW EI°	10°
Tipo de tecnología	Panel
Conector	(N) hembra
Dimensiones (Mm.)	840x159x206

Tabla A3.1 Características de la antena



Figura A3.1 Panel de antena



Figura A3.2 Vista frontal de antena