ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA

"ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE UNA RED INALÁMBRICA MIXTA VOZ Y DATOS PARA EL SISTEMA DE COMUNICACIONES INTERNO DE LA ADMINISTRACIÓN ZONAL VALLE DE LOS CHILLOS DEL MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO"

JORGE LUIS CÁRDENAS CÁRDENAS

SANGOLQUÍ – ECUADOR

2006

CERTIFICACIÓN

CERTIFICAMOS QUE EL PRESENTE PROYECTO DE GRADO FUE REALIZADO EN SU TOTALIDAD POR EL SEÑOR JORGE LUIS CARDENAS CARDENAS BAJO NUESTRA DIRECCIÓN.

Ing. Carlos Romero **DIRECTOR**	Ing. Derlin Morocho **CODIRECTOR**

RESUMEN

En el Proyecto de Grado “Estudio de Factibilidad para la implantación de una red inalámbrica mixta voz y datos para el sistema de comunicaciones interno de la A.Z.V.CH. del Municipio de Quito” se analizo la solución de implementar una Intranet en la infraestructura de esta institución, para solucionar el problema de distribución de red que posee y además incursionar en una nueva tecnología como es la voz sobre IP que permita la comunicación interna y externa de esta entidad.

El diseño propuesto de redes LAN, WI-FI y VOIP, combina estas tecnologías para crear una solución híbrida, en donde se usaron herramientas para planificación de redes inalámbricas, como el modelo de predicción de propagación de ondas “Dominant Path” y la suite de software “WinProp”; ambas desarrolladas en Alemania. Estos aspectos integran una solución total, optimizando el espacio físico y reduciendo costos de llamadas telefónicas internas. También se determinaron las plataformas de software para la operación de la Intranet, así como sus sistemas informáticos aplicados.

Se utilizo el software WinProp lo que permitió establecer un diseño sustentado en simulaciones del desempeño de la red WI-FI, optimizando el número de equipos, disminuyendo los puntos de red y por tanto la inversión económica.

AGRADECIMIENTO

Quiero agradecer sinceramente a todas las personas que colaboraron con la realización del presente trabajo, de quienes encontré la mejor predisposición para brindarme su ayuda desinteresada, y que resultó ser de invalorable utilidad para la culminación exitosa de mi Proyecto de Grado:

A los Ingenieros Carlos Romero y Derlin Morocho, quienes me han dirigido concediéndome una especial prioridad y brindándome todo su tiempo, siempre estuvieron dispuestos a recibirme para orientarme y ayudarme. Para ellos, todo mi reconocimiento.

Al Dr. Jorge Carvajal e Ing. Gonzalo Olmedo, Secretario Académico y Coordinador de la carrera de Telecomunicaciones, de quienes siempre recibí colaboración.

Al Arq. Ramiro Tobar e Ing. Galo Medina, que, por parte de la A.Z.V.CH., me abrieron todas las puertas y dieron el mejor apoyo que pude haber encontrado ahí.

A Tomas Hager, de AWE Communications, de quien recibí especial colaboración, atención preferencial e incluso amistad, olvidando las diferencias de cultura, idioma y demás. Prácticamente no importó que él y los demás "Arquitectos" estuvieran en Alemania, y yo, con mi pequeño proyecto, aquí en Ecuador.

"Agradezco primero a DIOS quien es el que me guía e ilumina en todos los pasos que doy en mi vida.
A mi madre, porque ha sido un apoyo incomparable brindándome siempre su amor, cariño, comprensión y sobre todo su confianza. Además, sus enseñanzas y valores me han permitido alcanzar metas planteadas y ahora se reflejan en esfuerzo, dedicación y trabajo.

A mi familia, quienes siempre me depositan su apoyo y confianza. En especial a mi tío, Chicho, quien durante este tiempo me ha brindado un apoyo incalculable.

A la ESPE, en donde no solo llegué a formarme como profesional sino como una persona responsable, a mis profesores quienes nos impartieron los conocimientos, pero sobre todo la calidad humana y la amistad que me brindaron.

A mis grandes amigos y compañeros, con los que compartimos grandiosos momentos que mes permitieron seguir adelante.

Finalmente de todo corazón agradezco a todas las personas que confían en mí, realmente MUCHAS GRACIAS..."

Jorge Luis

El esfuerzo, la constancia y la humildad me han llevado a conseguir mis metas e ideales, por eso este proyecto está dedicado a todas las personas que han influido en mi vida, llegando a ser muy importantes para mí.

PRÓLOGO

El presente proyecto surgió como una alternativa tecnológica frente a la necesidad de la Administración Zonal Valle de los Chillos del Municipio de Quito de mejorar su sistema de comunicaciones interno para brindar conectividad con la red de voz y datos, a todas las dependencias de esta institución.

Se trata de un estudio de factibilidad que detalla paso a paso los procesos de análisis, y diseño del proyecto integral, donde en todo momento se pretende priorizar la Ingeniería desde una perspectiva de aplicación profesional, con enfoque plenamente realista.

Sobre el contenido, han sido tratados temas relacionados con las redes de comunicación de datos, compuestas por medios guiados e inalámbricos. También se han abordado tópicos concernientes a plataformas de software para operación de redes de voz, así como sistemas informáticos aplicados. Los puntos anteriores fueron integrados para converger hacia una solución global para el problema de distribución de red y altas planillas de telefonía de la entidad beneficiaria, la A.Z.V.CH.

El aporte más significativo a nuestro medio ha sido la introducción de novedosas e interesantes herramientas de planificación y diseño de redes de comunicaciones inalámbricas, tanto celulares como WirelessLAN, al estilo de la más moderna Ingeniería alemana y europea. Estas herramientas permiten realizar un verdadero análisis de desempeño de tales sistemas, en base a predicciones y simulaciones de funcionamiento.

Ese análisis evidencia las correcciones, cambios y mejoras que pueden aplicarse a las ideas originales, a fin de afinar la red hasta obtener un producto óptimo. Lo anterior constituye la ejecución de un auténtico método de diseño, exacto y confiable.

Todo el documento se halla ampliamente ilustrado. Se han incluido gráficos, planos, diagramas, fotografías, tablas, cuadros comparativos, etc. Por tanto, la comprensión del texto se ve ampliamente facilitada y respaldada por todo ese material didáctico.

Finalmente, la concepción de todo el trabajo ha sido, en términos generales, completa. Han sido considerados aspectos técnicos, en el diseño propiamente dicho; financieros, al momento de valorar el proyecto y viabilizarlo desde el punto de vista económico. De todos modos, de no haber considerado tales aspectos, difícilmente hubiera podido culminarse con éxito el proyecto de la Intranet de la A.Z.V.CH.

Sangolquí, Noviembre de 2006

ÍNDICE

CAPÍTULO I **1**

INTRODUCCIÓN **1**

1.1 Antecedentes 1

1.2 Importancia 3

1.3 Objetivo 4

1.4 Alcance 4

CAPÍTULO II **6**

REDES INALÁMBRICAS **6**

2.1 Qué es una red inalámbrica 6

2.2 Estándar IEEE 802.11 7

2.2.1 IEEE 802.11b 9

2.2.1.1 Canales 9

2.2.1.2 Análisis Costo Beneficio 10

2.2.2 IEEE 802.11a 11

2.2.2.1 Canales 12

2.2.2.2 Análisis Costo Beneficio 13

2.2.3 IEEE 802.11g 14

2.2.3.1 Análisis Costo Beneficio 15

2.3 Operación Básica de Wi-Fi 16

2.4 Visión General del protocolo Wi-Fi 17

2.5 Seguridad de la red inalámbrica 20

2.5.1 Introducción 20

2.5.2 Métodos de Autenticación 21

2.5.2.1 Filtrado de direcciones MAC 22

2.5.2.2 SSID Service Set Identifier 23

2.5.2.3 802.1x 24

2.5.2.4 WEP 27

2.5.2.4.1 Limitaciones 29

2.5.2.5 Protocolo de autenticación extensible EAP 30
2.5.3 Métodos de Encriptación de datos 32
2.5.3.1 Wi-Fi Protected Access WPA 33
2.5.4 Medidas de seguridad adicionales 34
2.5.4.1 Red Privada Virtual VPN 34
2.5.4.2 Firewalls 36
2.5.4.3 Configuración del punto de acceso 37
2.6 Voz sobre IP 37
2.6.1 Componentes de voz sobre IP 38
2.6.2 Protocolos de VOIP 39
2.6.2.1 Protocolo H.323 41
2.6.2.2 Protocolo SIP 42
2.6.2.3 Protocolo IAX 42
2.6.2.4 Protocolo MGCP 43

CAPITULO III 44
SITUACIÓN ACTUAL DEL SISTEMA DE COMUNICACIONES INTERNO 44
3.1 Administración Zonal Valle de los Chillos 44
3.2 Situación Actual: Logística e infraestructura 46
3.2.1 Infraestructura fisica 46
3.2.2 Infraestructura tecnológica 50
3.2.2.1. Equipos de computación 50
3.3 Proyecto de Modernización 51
3.3.1 Necesidad Específica 51

CAPÍTULO IV 53
DISEÑO DE LA RED INALÁMBRICA 53
4.1 Análisis de requerimientos 54
4.1.1 Cobertura 54
4.1.2 Seguridad 54
4.1.3 Escalabilidad 55
4.1.4 Calidad de Servicio 55
4.2 Planificación de la WLAN 56
4.2.1 El modelo de predicción Dominant Path 57

4.2.2 La suite de software Winprop 58
4.3 Determinación de número y ubicación de Access points 61
4.3.1 Creación de la base de datos 63
4.3.2 Ubicación de los Access Points 65
4.3.2.1 Primera Planta 66
4.3.2.2 Segunda Planta 69
4.3.2.3 Tercera Planta 70
4.3.3 Bases técnicas de los equipos WLAN 71
4.3.3.1 Access Points 72
4.3.3.2 Adaptadores de red WLAN 72
4.4 Arquitectura de la red Ethernet 72
4.4.1 Dimensionamiento de la Intranet 73
4.4.1.1 Voz sobre una red inalámbrica 74
4.4.1.1.1 Calidad de servicio QoS 75
4.4.1.1.1.1 WMM 75
4.4.1.1.2 Control de admisión de llamadas 78
4.4.1.1.3 Evaluación Experimental 79
4.4.1.1.4 Solución para VOIP 89
4.4.1.1.4.1 Servidor Asterisk 90
4.4.2 Backbone de la red LAN 92
4.4.3 Bases técnicas de los equipos de la red LAN 95
4.4.3.1 Switch de backbone 95
4.4.3.2 Router de backbone 95
4.4.3.3 Tarjetas de red NIC para servidor 95
4.4.3.4 Servidor de voz 95
4.4.3.5 Tarjetas análogas 95
4.5 Funcionamiento general de la red mixta voz y datos 95
4.6 Funcionamiento lógico de la red 97

CAPÍTULO V 101
ANÁLISIS ECONÓMICO 101
5.1 Selección de equipos y materiales para la Intranet de la A.Z.V.CH. segu análisis de relación costo beneficio 101
5.1.1 Dispositivos de red 103

5.1.2 Cableado Estructurado 106
5.1.3 Servidores de red y software 107
5.1.4 Mano de Obra 108
5.2 Presupuesto final 109

CAPÍTULO VI 111
CONCLUSIONES Y RECOMENDACIONES 111
6.1 Conclusiones 111
6.2 Recomendaciones 115

REFERENCIAS BIBIOGRÁFICAS 117

ANEXOS 119

ÍNDICE DE FIGURAS

Figura. 2. 1. Red Inalámbrica…..……6
Figura. 2. 2. Espectro de frecuencias para estándar 802.11b…..……10
Figura. 2. 3. Espectro de frecuencias para estándar 802.11a……13
Figura. 2. 4. Estructura Típica de una red Wi-Fi……..……....18
Figura. 2. 5. Arquitectura de un sistema de autenticación 802.1x..…….25
Figura. 2. 6. Estructura de una VPN para acceso inalámbrico…....……35
Figura. 2. 7. Servidor de procesamiento de llamadas……...…..……..39
Figura. 2. 8. Pila de protocolos RTP…...…….……40
Figura. 2. 9. Modelo de red TCP/IP & OSI y protocolos principales……..41
Figura. 3. 1. Administración Zonal Valle de los Chillos…….……46
Figura. 3. 2. Planta baja de la A.Z.V.CH……...…….……47
Figura. 3. 3. Segunda Planta de la A.Z.V.CH……...……...……48
Figura. 3. 4. Tercera planta de la A.Z.V.CH. ...……..……49
Figura. 4. 1. Potencia recibida en la primera planta con un transmisor de 19 dBm….……66
Figura. 4. 2. Potencia recibida en la primera planta con un transmisor de 19 dBm….……67
Ubicado en otro lugar.
Figura. 4. 3. Potencia recibida en la primera planta con dos transmisores de 19 dBm…....67
Figura. 4. 4. Tasa máx. de datos recibida en la primera planta con dos transmisores…….69
De 19 dBm.
Figura. 4. 5. Potencia recibida en la segunda planta con un transmisor de 19 dBm…….69
Figura. 4. 6. Potencia recibida en la segunda planta con dos transmisores de 19 dBm…..70
Figura. 4. 7. Tasa máx. de datos recibida en la segunda planta con dos transmisores…....70
De 19 dbm.
Figura. 4. 8. Potencia recibida en la tercera planta con dos transmisores de 19 dBm……71
Figura. 4. 9. Tasa máx. de datos recibida en la tercera planta con dos transmisores…….71

De 19 dBm.
Figura. 4. 10. Lógica interna de cola en Wi-Fi Multimedia…….……77
Figura. 4. 11. Throughput de una llamada de voz vs. Numero de estaciones….……80
Figura. 4. 12. Impacto de TXOP sobre dos estaciones saturadas…….……81
Figura. 4. 13. Impacto de TXOP sobre dos estaciones saturadas.(2)……...82
Figura. 4. 14. Impacto de Cwmin sobre dos estaciones saturadas……...…….……...83
Figura. 4. 15. Impacto de Cwmin sobre dos estaciones saturadas.(2)……..83
Figura. 4. 16. Impacto de AIFS sobre dos estaciones saturadas……..84
Figura. 4. 17. Impacto de AIFS sobre dos estaciones saturadas. (2)……85
Figura. 4. 18. Delay promedio para una llamada de voz con estaciones saturadas……..86
Figura. 4. 19. CDF para el delay de una llamada no priorizada, priorizada con …….88
AIFS = 4, priorizada con AIFS = 6.
Figura. 4. 20. Porción de tiempo que la capa MAC esta ocupada……89
Figura. 4. 21. Esquema de funcionamiento de Asterisk……...90
Figura. 4. 22. Esquema general de la Intranet……..94
Figura. 4. 23. Ajuste de los parámetros MAC del estándar 802.11e……96
Figura. 4. 24. Diagrama Lógico de la Intranet…….99

ÍNDICE DE TABLAS

Tabla. 2. 1. Familia del estándar IEEE 802.11……...8
Tabla. 2. 2. Características del estándar 802.11b……...9
Tabla. 2. 3. Características del estándar 802.11a……..……..12
Tabla. 2. 4. Características del estándar 802.11g…….15
Tabla. 3. 1. Dependencias del primer piso de la A.Z.V.CH…….47
Tabla. 3. 2. Dependencias del segundo piso de la A.Z.V.CH……..48
Tabla. 3. 3. Dependencias del tercer piso de la A.Z.V.CH……..49
Tabla. 3. 4. Listado de equipos de computación existentes…….50
Tabla. 3. 5. Detalle de tipos de procesador de computadoras tipo desktop…….51
Tabla. 4. 1. Propiedades físicas y eléctricas de las paredes componentes de la database……63
Tabla. 4. 2. Propiedades físicas y eléctricas de las puertas componentes de la database……64
Tabla. 4. 3. Propiedades físicas y eléctricas de elementos de vidrio en la database……64
Tabla. 4. 4. Propiedades físicas y eléctricas de pisos, columnas y techos en la database……65
Tabla. 4. 5. Categorías de acceso de Wi-Fi Multimedia……..76
Tabla. 5. 1. Cuadro Comparativo de Puntos de Acceso…….104
Tabla. 5. 2. Cuadro Comparativo de Adaptadores de red PCI……...104
Tabla. 5. 3. Cuadro Comparativo de adaptadores de red USB……...105
Tabla. 5. 4. Cuadro Comparativo de Servidores para comunicación de voz…….107
Tabla. 5. 5. Precio de Asterisk Business Edition……108
Tabla. 5. 6. Licencia para codec G.729……..108
Tabla. 5. 7. Tarjetas Análogas……108
Tabla. 5. 8. Detalle de precios de mano de obra especializada……..109

Tabla. 5. 9. Determinación del monto total de inversión estimado para la intranet de la A.Z.V.CH……110

GLOSARIO DE TÉRMINOS

Access Point	Punto de acceso a una WirelessLAN. Es la interfase entre el medio inalámbrico del usuario y el medio guiado de la red.
Ancho de banda	Capacidad máxima de un medio de transmisión y/o enlace
Backbone	Medio troncal de transmisión, en una red de comunicaciones. Soporta la comunicación de las ramificaciones, especialmente en topologías de árbol y estrella extendida.
Bridge	Dispositivo que interconecta redes de área local en la capa de enlace de datos.
Broadcast	Paquete enviado por una estación a todas las estaciones de la red.
Carrier	Operador de telefonía que proporciona conexión a Internet a alto nivel.

CSMA/CA	Carrier Sense Multiple Access / Colltion Avoidance
Ethernet	Tecnología de redes similar al estándar IEEE 802.3, que constituye una técnica de control de acceso a un medio de transmisión guiado.
Firmware	Software residente en equipos de red y computación en general. Permite el funcionamiento y administración del dispositivo.
Gateway	Puerta de acceso, dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.
Hacking	Ejecución de acciones para violentar el acceso y la seguridad de redes de comunicaciones, con diversos fines negativos como robo de información, saboteo, etc.
Intranet	Red privada e interna, conformada por una o más redes LAN.
MAC	Media Access Control
NIC	Del inglés Network Interface Card, tarjeta para conexión a una red.
OSI	Del inglés Open System Interconnection, o interconexión de sistema abierto. Modelo referencial

	para desarrollo de redes de comunicaciones, establecido por la ISO.
Red LAN	Del inglés Local Area Network. Red de datos de área local. Se caracteriza por tener relativamente pequeñas extensiones, pero muy altas velocidades de transmisión.
Service Packet 2 (SP2)	Paquete de Servicios No. 2, del fabricante Microsoft. Actualización para Windows XP que incluye correcciones de seguridad, nuevos protocolos, actualizaciones de software, etc.
Spam	Recepción de correo "basura" o no solicitado.
Spoof	Suplantación de dominio, para envío de correo spam.
Spyware	Software malicioso que se hospeda secretamente en un computador para publicar datos de éste al Internet.
Subcapa MAC	Del inglés Medium Access Control. Parte de la capa 2 del modelo OSI, encargada de controlar el acceso al medio de transmisión.
SSID	Service Set Identifier. Se refiere al nombre identificador que tienen los AP en una red 802.11.

Suite de software	Familia de programas de software agrupados en un solo paquete.
Switch	Dispositivo concentrador de conexiones de red, trabaja a nivel de capa 2 o 3 del modelo referencial OSI, según el tipo.
TCP/IP	Transmisión Control Protocol / Internet Protocol
Throughput	Transferencia real de cantidad de datos que son transmitidos a algún punto de la red.
WirelessLAN	LAN inalámbrica, red de datos sobre área local, que utiliza ondas radioeléctricas como medio de transmisión.
Wireless Fidelity (WI-FI)	Fidelidad inalámbrica. Se refiere al cumplimiento de normas de la familia IEEE 802.11, de una manera certificada, para asegurar compatibilidad e interoperatividad.

CAPITULO I

INTRODUCCION

1.1. ANTECEDENTES

La historia de la comunicaciones por radio (o inalámbricas) es bastante reciente (de aproximadamente 150 años), y constituye la base de las comunicaciones por medio de redes Wi-Fi o LAN Inalámbricos**.**

El físico teórico escocés James C. Maxwell y el físico alemán Heinrich Hertz fueron los principales pioneros y realizaron los descubrimientos científicos sobre la transmisión de ondas electromagnéticas, y de RF (radio-frecuencia) en la segunda mitad de los años 1800s. Normalmente, descubrimientos científicos son seguidos por innovaciones tecnológicas, que traducen los descubrimientos en aplicaciones y usos prácticos comerciales para el beneficio de la sociedad. Estas innovaciones pueden reportar distinción y recompensas personales para los innovadores/empresarios.

Por ejemplo en Estados Unidos, la introducción de las comunicaciones inalámbricas provocó una actividad febril de innovaciones tecnológicas durante las primeras décadas de los años 1900s. Estas innovaciones resultaron en una serie de nuevos productos militares, profesionales y de consumo tales como comunicación de radio bi-direccionales (usada por primera vez durante la Segunda Guerra Mundial), la radio (AM y después FM) y eventualmente la televisión (blanco y negro y después a color).

La comunicación inalámbrica es una experiencia diaria en nuestro mundo moderno. Ya sea que escuchemos la radio o miremos la televisión, ambas representan dos tipos de comunicaciones inalámbricas. Las señales de radio se propagan desde su fuente (un transmisor) a su destino (un receptor) – de una manera invisible.

El valor de una computadora se potencia enormemente si está conectada a una red de computadoras. A su vez, el valor de la red de computadoras aumenta a medida que aumenta velocidad de interconexión y la movilidad de los usuarios conectados a la red. La tecnología usada por las redes LAN inalámbricas (WLANs) para interconectar computadoras, aumenta el valor para todos los usuarios en todas estas dimensiones. Para comenzar, debido a su propia naturaleza permite la movilidad de sus usuarios (no requiere cables que lo tengan sujeto a la pared) y alta velocidades de interconexión (o velocidades de banda ancha o broadband). Por otra parte su adopción masiva estimulado por el uso del espectro de uso libre, reduce las barreras de adopción aumentando el numero de usuarios conectados en red y por consiguiente aumentado aun más su valor.

En los últimos años (1999) ha surgido una nueva tecnología de interconexión inalámbrica, llamada Wi-Fi (o Fidelidad Inalámbrica del ingles Wireless Fidelity); que ofrece la posibilidad de conectarse sin cables a velocidades que van desde 1Mbps hasta más de 50Mbps. Wi-Fi es el nombre comercial dado al estándar técnico IEEE 802.11. Esta tecnología extiende la interconexión de las redes actuales cableadas (o también llamadas Ethernet), evitando el uso de cables adicionales mediante la transmisión de ondas de radio por el espacio. Los gobiernos imponen reglas muy claras para su uso, legislando la potencia máxima transmitida permitida en cada una de las bandas, el tipo de uso, el uso de antenas y amplificadores externos.

Esta tecnología ofrece las siguientes ventajas:

- Estandarización e Interoperabilidad
- Movilidad

- Ahorro de costos de cableados fijos
- Escalabilidad actual
- Respeto a los bienes de interés cultural, monumentos,
- Ahorro de costos sobre líneas dedicadas
- Facilidad de instalación, gestión, flexibilidad, ahorro de espacio y bajo costo.

Las redes inalámbricas han crecido enormemente en países industrializados como Estados Unidos donde existe infraestructura de alta calidad. Con más razón deben crecer en América Latina, y especialmente aquí en nuestro país, donde se busca economizar y facilitar las comunicaciones internas de las empresas, manteniendo eficiencia y productividad.

1.2. IMPORTANCIA

La utilización de una red inalámbrica para el sistema de comunicaciones interno del Municipio de Quito – Administración Zonal del Valle de los Chillos, implica sobre todo, el aprovechamiento del espacio físico con el que cuenta, para el desarrollo y avance tecnológico del mismo, con un servicio confiable y de calidad, para brindar el servicio de transmisión de voz y datos a todos los departamentos de esta institución.

Se conoce además que la comunicación inalámbrica tiene algunas ventajas frente a las comunicaciones cableadas, por ejemplo: facilidad de instalación, bajo costo de expansión, ya que en muchas ocasiones la demanda aumenta, rápido despliegue sin pérdida de tiempo y sobre todo que la inversión hecha se la recupera rápidamente, esto ha sido ratificado por un estudio realizado por la Wíreless LAN Association (WLANA) que indica que la instalación de una WLAN se paga por sí misma dentro de 12 meses de operación.

Con este proyecto se quiere dar servicio todos los departamentos de esta institución, con el fin de que haya una comunicación rápida y eficiente entre ellos. Además se pretende

brindar servicios tales como: transferencia de archivos, aplicaciones web, mensajería e Internet.

1.3. OBJETIVO

Analizar la factibilidad de implementación de una red inalámbrica para el sistema de comunicaciones interno de el Municipio de Quito – Administración Valle de los Chillos, con tecnología de punta y bajo costo operacional que sirva de apoyo a las comunicaciones de datos y voz, mejorando el tipo de servicios ofrecidos y en muchos casos dando servicios por primera vez a ciertos departamentos que carecen de ellos en estos momentos.

1.4. ALCANCE

Los adelantos técnicos y otros cambios de la industria de telecomunicaciones han producido el crecimiento de la tecnología inalámbrica durante los últimos años. El advenimiento de servicios adicionales, dispositivos más pequeños, más poderosos, el aumento de demanda para la conectividad ha llevado a más compañías a considerar el uso de tecnología inalámbrica para sus necesidades de comunicaciones.

Con la ayuda de esta tecnología, se va analizar y diseñar una red inalámbrica que soporte tráfico de voz y de datos. Para la red de voz, se quiere investigar sobre la factibilidad de poner en marcha esta sobre una red inalámbrica, analizando todos los parámetros necesarios que permitan tener una comunicación de calidad tanto entre los departamentos de la institución como fuera de ellos.

En cuanto a la red de datos, es necesario cambiar la red cableada existente, por una red inalámbrica que permita solucionar el problema de distribución que posee actualmente la administración, además de brindar una característica de escalabilidad, tan necesaria en una institución publica.

Para los casos, primero se va a realizar un estudio de cobertura, seguidamente se procederá a diseñar la red en si, y finalmente establecer los equipos necesarios para instalar la red mencionada.

CAPITULO II

REDES INALAMBRICAS

2.1 QUE ES UNA RED INALAMBRICA

Una red inalámbrica es simplemente una colección de computadoras, impresoras y otros dispositivos interconectados entre sí por enlaces de radio.

Una red básica se construye alrededor de una estación base llamada Punto de Acceso (Access Point). Este punto es el dispositivo central que permite que dos o más computadoras compartan el acceso a Internet, así como también archivos e impresoras.

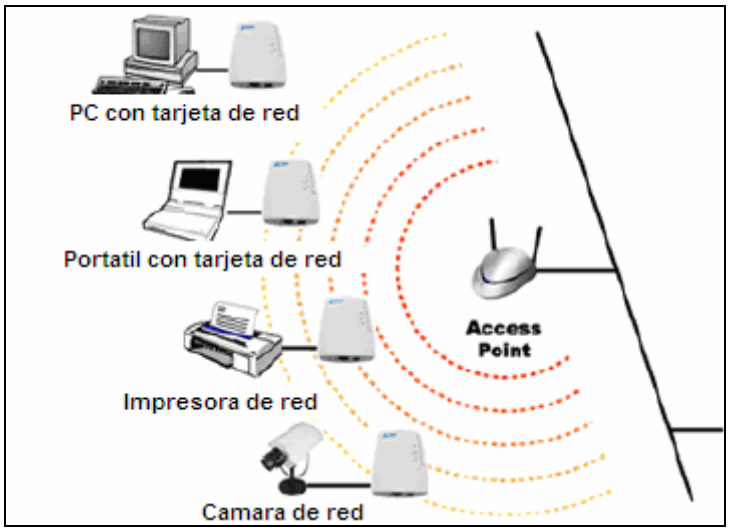


Figura 2.1. Red inalámbrica

En la figura 2.1, se muestra como la estación base (Access Point) actúa como el centro de todo el funcionamiento de una red básica entre computadoras personales, de escritorio, impresoras y otros dispositivos inalámbricos.

Esta red de computadoras se conecta al dispositivo central (Access Point) usando el estándar ***WiFi (802.11),*** que es un conjunto de reglas que proveen seguridad, confiabilidad y rapidez de conectividad inalámbrica. Más adelante se detallara su funcionamiento.

2.2 ESTÁNDAR IEEE 802.11

Es un tipo de tecnología de radio usado para redes inalámbricas de área local (WLANs). Este es un estándar que ha sido desarrollado por la IEEE (Institute of Electrical and Electronics Engineers). La IEEE es una organización internacional que desarrolla estándares de tecnologías eléctricas y electrónicas por varias décadas.

En el año 1997, la IEEE aprobó el estándar para WLAN conocido como 802.11, el cual especifica características de dispositivos con tasas de señal de 1 y 2 Mbps. El estándar especifica la capa física y MAC del modelo OSI para transmisiones en la banda de los 2.4 GHz. Los rangos utilizados en esta banda van desde los 2.4 a los 2.4835 GHz en EEUU y Europa, mientras que en Japón, los rangos son desde los 2.471 a los 2.497 GHz. Después de obtener buenos resultados por compañías tales como Lucent Technologies y Harris Semiconductors, la IEEE ratificó un nuevo ajuste con mejor desempeño, llamado 802.11b, que trabaja adicionalmente con tasas de transmisión de 5.5 y 11 Mbps; muchos dispositivos actuales en el mercado están basados en esta tecnología. Este estándar especifica algunas modificaciones en la codificación, en las capas inferiores las características de radio no fueron modificadas y se realizaron unos pequeños cambios sobre la capa MAC, para facilitar la compatibilidad con dispositivos IEEE 802.11. De aquí, que este estándar tuvo que ser referido como Wi-Fi o Wireless Fidelity, que se constituyó en marca registrada de dispositivos que operarían con este estándar, soportado e impulsado por la Wi-Fi Alliance.

En el año 1999, la IEEE publico las especificaciones de nuevas mejoras de la familia 802.11, la 802.11a. Estas especificaciones se refieren a la capa física y a la capa MAC del modelo OSI, y la banda usada en 5 GHz, que no tiene licencia en EEUU, pero si en otros países. Las tasas de señal son de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Los siguientes dispositivos de este estándar deberán ser utilizados en pequeñas partes de Europa donde la "Dynamic frequency Selecion" (DFS) y la "Adaptative Power Control" (APC), como se especifican en las reformas del 802.11h, son usadas.

En el 2003, la IEEE aprobó el 802.11g como una futura evolución de los estándares 802.11. Este estándar provee iguales desempeños que el 802.11a, pero trabaja en la banda de 2.4 GHz, lo que hace desplegarse en Europa. Además la compatibilidad con dispositivos 802.11b esta garantizada.

En la tabla 2.1. se presenta una tabla que resume a toda la familia del estándar 802.11:

Tabla 2.1. Familia del estándar IEEE 802.11

Familia del Estándar IEEE 802.11		
Estándar	**Descripción**	**Estado**
IEEE 802.11	WLAN, 1 a 2 Mbps, 2.4 GHz	Aprobado 1997
IEEE 802.11ª	WLAN, 1 a 54 Mbps, 5 GHz	Aprobado 1999
IEEE 802.11b	WLAN, 1 a 11 Mbps, 2.4 GHz	Aprobado 1999
IEEE 802.11g	WLAN, 1 a 54 Mbps, 2.4 GHz	Aprobado 2003
IEEE 802.11e	QoS	Aprobado 2005
IEEE 802.11f	IAPP (Inter AP Protocol)	Aprobado 2003
IEEE 802.11h	Usado en 5 GHz en Europa	Aprobado 2003
IEEE 802.11i	Estándar encriptación	Aprobado 2004

IEEE 802.11n	MIMO capa Física	Aprobado 2005

2.2.1. IEEE 802.11 b

Fue la primera gran revisión del estándar básico aprobada y revisada por la IEEE en 1999.

Este estándar define el Carrier Sense Multiple Access with Collision Avoidance (CSMA / CA) como protocolo de acceso al medio. Un gran porcentaje de la capacidad de canal disponible ha sido sacrificado (debido al uso de CSMA/CA) para incrementar la seguridad en las transmisiones de datos bajo condiciones diversas y adversas del ambiente.

En la tabla 2.2. se presentan las características principales de este estándar.

Tabla 2.2. Características de estándar 802.11b

Frecuencia de operación	2.4 GHz ISM
Tasa de transferencia (teórica)	1, 2, 5.5, 11 Mbps
Tasa de transferencia (Tx de Ix)	4 Mbps (promedio)
Mecanismo	DSSS (Direct Sequence Spread Spectrum)
Canales disponibles	11 (3 no traslapados)
Rango máximo	90 m (promedio)

2.2.1.1 Canales. 802.11b y 802.11g dividen el canal en 14 canales traslapados y escalonados, cuyas frecuencias están fuera de los 5 MHz. La división del espectro se detalla en la figura 2.2.

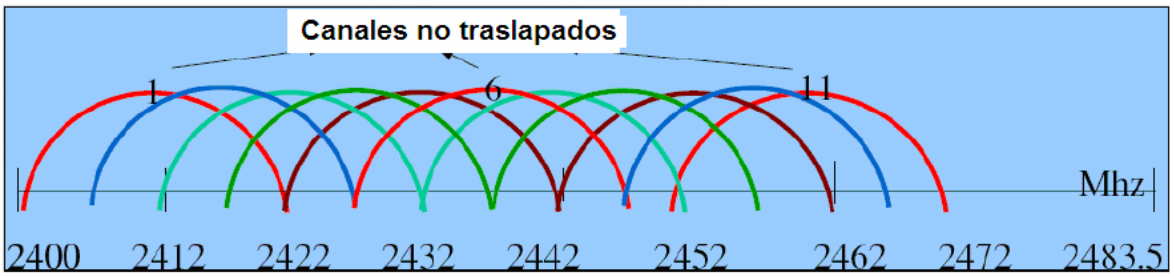


Figura 2.2. Espectro de frecuencias para estándar 802.11b

Es común escuchar que los canales 1, 6 y 11 no se traslapan y pueden ser usados tal que múltiples redes pueden operar muy cercanamente sin interferir una con otra, pero este argumento no es tan simple. Los estándares 802.11 b y 802.11g no especifican el ancho de cada canal. Ellos especifican la frecuencia central del canal y una máscara espectral para ese canal. El ancho de banda es 22MHz. Puesto que la máscara espectral solo define restricciones para la potencia de salida de +/- 22MHz de la frecuencia central, la gente asume que la energía del canal no se extiende más allá de eso, pero eso no ocurre. De hecho si el transmisor es suficientemente potente la señal puede estar más allá del punto de +/- 22 MHz. Por tanto, es incorrecto decir que estos canales no se traslapan. Es mejor decir que dada la separación entre los canales 1, 6 y 11, la señal sobre cualquier canal debe estar suficientemente atenuada para minimizar la interferencia con un transmisor sobre otro canal.

802.11g es visto actualmente por muchos usuarios como una alternativa práctica y funcional a las redes cableadas. El costo de instalación barato y la facilidad de aprendizaje de la instalación, han ayudado hacer de éste el favorito de hogares y oficinas pequeñas. Con un buen planeamiento y suerte, es fácil implementar una red en el hogar u oficina pequeña cubriendo un área de aproximadamente de 3000m2.

2.2.1.2. Análisis Costo Beneficio. A pesar de que los beneficios de este estándar son su costo y su rango de acción, existen algunas serias limitaciones para su uso. Por ejemplo, un gran problema es su operación en el espectro de 2.4 GHz. Debido a la falta de restricciones

para el uso de esta banda, ésta ha llegado a estar sobrecargada. La transmisión de datos inalámbricamente pude sufrir un severo daño, desde dispositivos como hornos microonda, teléfonos inalámbricos o dispositivos Bluetooth que también utilizan esta banda de 2.4GHz.

Otro inconveniente es el ancho de banda a utilizar. Con un throughput promedio de 4-5 Mbps, 4 usuarios tendrían un margen relativamente estrecho de ancho de banda disponible. Estas tasas de transferencia no son un problema para la conexión de un hogar que usualmente se usa para navegar en Internet. Pero para oficinas pequeñas, donde existen archivos grandes para transferir de una máquina a otra, aparece un gran problema. En tal situación, la solución sería aumentar más Access points para mejorar la carga, pero esta acción se torna relativamente difícil cuando solo existen tres canales que no se traslapan.

El trabajo de configurar varios Access points bajo el mismo protocolo y evitar el traslapamiento de canales es una tarea que requiere mucha técnica y tiempo.

El estándar 802.11g es una muy buena elección para casas y oficinas pequeñas y provee un buen grado del rango de la señal a un costo asequible.

2.2.2 IEEE 802.11 a

Es la segunda revisión del estándar básico 802.11, y fue ratificado y aprobado en el 2001. Aunque el grupo de trabajo para este estándar arrancó antes del 802.11b, sus objetivos fueron más ambiciosos y difíciles, de ahí su tardía ratificación.

802.11a representa un incremento significativo en la tasa de transferencia con una velocidad máxima teórica de 54 Mbps, casi cinco veces la velocidad del estándar 802.11b.

En la tabla 2.3. se presenta las características principales de este estándar.

Tabla 2.3. Características del estándar 802.11a.

Frecuencia de operación	5.8 GHz UNII
Tasa de transferencia (teórica)	54 Mbps
Tasa de transferencia (Tx de Ix)	20 -36 Mbps (promedio)
Mecanismo	OFDM (Orthogonal Frequency Division Multiplexing)
Canales disponibles	12 (todos no traslapados)
Rango máximo	24 m (promedio)

La tasa de datos es reducida a 48, 36, 24, 18, 12, 9 y 6 Mbps si se requiere. Dentro de los doce canales, ocho son dedicados para enlaces interiores y cuatro para enlaces punto a punto.

Desde que la banda de 2.4 GHz está ampliamente usada, usar la banda de 5 GHz le da a este estándar la ventaja de sufrir menos interferencias de otros dispositivos. En contraste, su alta frecuencia también trae algunas desventajas.

2.2.2.1 Canales. En la figura 2.3. se indica una gráfica, en la cual se observa la distribución de los canales para el estándar 802.11a.

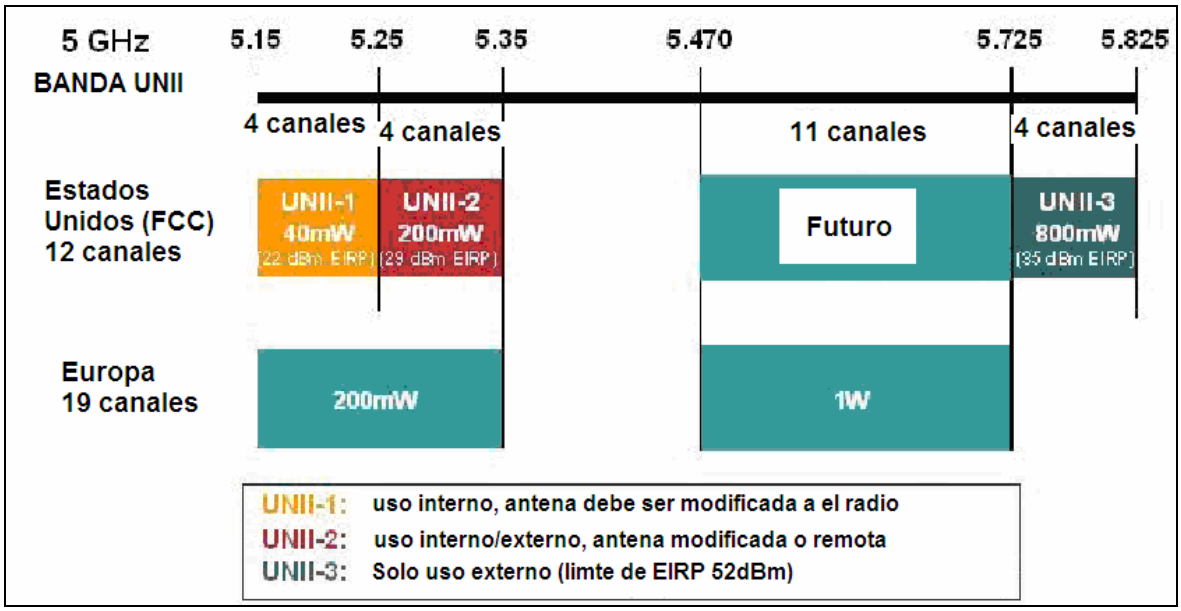


Figura 2.3. Espectro de frecuencias del estándar 802.11[a]

Como se dijo, existen 8 canales dedicados para enlaces interiores, y estos a su vez se dividen en dos grupos de cuatro acanales cada uno. La diferencia entre uno y otro a más del rango de frecuencias es la medida permitida de EIRP (potencia isotrópica radiada), 22 dBm y 29 dBm respectivamente.

2.2.2.2 Análisis Costo Beneficio. Mientras 802.11a es capaz de conseguir velocidades de transferencia altas, su mayor sacrificio es respecto al rango de acción disponible.

Esto es que este estándar tendrá una degradación extrema de la señal al bordear su límite máximo de 100 pies de cobertura si no existe línea de vista directa.

Las empresas que implementen este tipo de tecnología tendrán que hacer una fuerte inversión debido a la necesidad de un gran número de puntos de acceso para cubrir un área determinada.

Análogamente, su instalación resulta más fácil que la del estándar 802.11b, ya que se cuenta con doce canales separados, no traslapados para usar en una configuración de red.

Otra limitación es que esta tecnología es incompatible con su predecesora 802.11b. Por este motivo los administradores de red tienen la dura decisión de mantener una red 802.11b existente o empezar con una nueva red 802.11a.

Es muy claro, que haciendo a un lado las limitaciones, este estándar provee una clara ventaja para usuarios que requieren velocidades de transferencia altas considerando su costo, en contraste con usuarios casuales que verían a este estándar como nada beneficioso debido a su costo principalmente.

2.2.3 IEEE 802.11g

Es el estándar más actual de la IEEE aprobado en Junio de 2003. Este provee una tasa de transferencia de datos sobre los 54Mbps y tiene compatibilidad con los productos 802.11b, medida tomada como protección a las inversiones en las redes inalámbricas actuales.

En la tabla 2.4. se indican las características del estándar 802.11g.

Tabla 2.4. Características de estándar 802.11g

Frecuencia de operación	2.4 GHz ISM
Tasa de transferencia (teórica)	54 Mbps
Tasa de transferencia (Tx de Ix)	20 -30 Mbps (promedio)
Mecanismo	Modulación por Codificación Complementaria CCK, OFDM
Canales disponibles	3 (1, 6, 11)
Rango máximo	53 m (promedio)

La tecnología de este estándar soporta múltiples tasas de datos que permiten a los usuarios comunicarse a la mejor velocidad posible. La selección de la tasa de datos es una alternativa entre obtener la tasa de transmisión más alta y tratar de minimizar el número de errores en la comunicación. Los usuarios de 802.11g pueden seleccionar de un amplio rango posible de tasas de datos OFDM 54, 48, 36, 24, 18 ,12, 9 y 6 Mbps, o de tasas de datos CCK 11, 5.5, 2 y 1 Mbps.

En un entorno de red, como la distancia de los puntos de acceso aumenta, los productos basados en la tecnología 802.11 reducen las tasas de datos para mantener la conectividad. Este estándar tiene la misma característica de propagación que 802.11b porque transmite en la misma banda de frecuencia, 2.4 GHz.

2.2.3.1 Análisis Costo Beneficio. Una de las ventajas más grandes de este estándar es su increíble velocidad cuando se hace una comparación con los anteriores. Además de conseguir tal velocidad con un amplio rango de cobertura de la señal.

Actualmente no está claro si 802.11g es capaz de mantener esta alta tasa de datos en los límites de su rango. Varios laboratorios han puesto a prueba este parámetro, y coinciden en que es altamente susceptible a la degradación de la señal cuando alcanza su máximo rango posible.

Al igual que su predecesor 802.11b, este estándar sufre severas interferencias debido a la banda en la cual opera, 2.4GHz que está sobrecargada y en la que operan otros dispositivos.

Haciendo a un lado los problemas potenciales considerados con la interferencia, 802.11g provee muchos beneficios a una amplia variedad de usuarios y consumidores. La compatibilidad con las redes 802.11b, permite modernizar e integrar una nueva tecnología, más rápida, sin tener que eliminar los dispositivos ya existentes. Además los dispositivos 802.11g son más baratos que los del estándar 802.11a. Como resultado se tiene una alternativa de costo asequible y que ofrece altas velocidades.

2.3 OPERACION BASICA DE WI-FI

Cuando encendemos una estación Wi-Fi, deberá explorar los canales disponibles para poder activar una red donde las señales empiezan a transmitirse. Si esta selecciona una red, puede ser de dos tipos de topología: *Ad-Hoc* (estación a estación) o modo *Infraestructura* (con Access Points). Posterior a esto, se deberá autenticar a si mismo y con el Access point. Luego viene la asociación, si la seguridad WEP o WAP es activada, se debe realizar un paso futuro de autenticación. Después de esto, cualquiera de las estaciones puede participar en la red.

Wi-Fi provee diferentes acuerdos para brindar calidad de servicio QoS, los rangos van desde priorizar el mejor esfuerzo *Best effort* en la infraestructura de red y garantizar el servicio. Mientras se empieza a ser parte de una red, las estaciones pueden descubrir nuevas redes y pueden desasociarse de la actual y asociarse con una de las nuevas (tiene que ver con la potencia de la señal recibida). Las estaciones pueden deambular entre redes que comparten un sistema de distribución común, y en este caso es posible el "roaming", que permite mantener el esquema de celdas de cobertura, es decir, mantener el servicio cuando una estación cambia de un AP a otro. Además, una estación puede estar inactiva para ahorrar energía, y cuando esta finaliza su modo de operación de infraestructura, puede desasociarse y desanteuticarse del AP.

2.4 VISION GENERAL DEL PROTOCOLO WI-FI.

Una WLAN Wi-Fi se basa en una arquitectura de celdas, cada una de las cuales es llamada "*Basic Service Set*" (BSS).

Una BSS es un conjunto de estaciones Wi-Fi fijas o móviles. Para acceder a la transmisión, el medio es controlado por cierto conjunto de reglas llamadas "Coordination Function". Wi-Fi define una función de coordinación distribuida o "Distributed Coordination Function" (DCF) y "Point Coordination Function" (PCF).

Alternativamente, una infraestructura BSS puede ser parte de una red extensa, a esto se lo llama *Extended Service Set* (ESS). Un ESS es el conjunto de una o mas infraestructuras BSS conectadas vía distribución sistema, cuya naturaleza no esta especificada por el estándar, pudiendo ser una red cableada Ethernet o algún tipo de red inalámbrica, como la especificada en 802.11f, acerca de los protocolos entre AP. Las estaciones conectadas a un sistema de distribución son los AP.

El servicio ofrecido por las estaciones cae dentro de dos clases: stations service y distribution system service. La segunda clase es ofrecida por los AP, y permite la transferencia de datos entre estaciones que pertenecen a diferentes BSS. Ademas, el estándar define las funciones del portal, que es el puente para la interconexión de una WLAN con una red LAN genérica IEEE 802.3x.

En la figura 2.4. se muestra todos los componentes de una red Wi-Fi, en la que se presenta el esquema BSS, ESS que por medio de un portal pueden acceder a una red LAN genérica en la cual interactúan, compartiendo aplicaciones y archivos en un solo entorno de red.

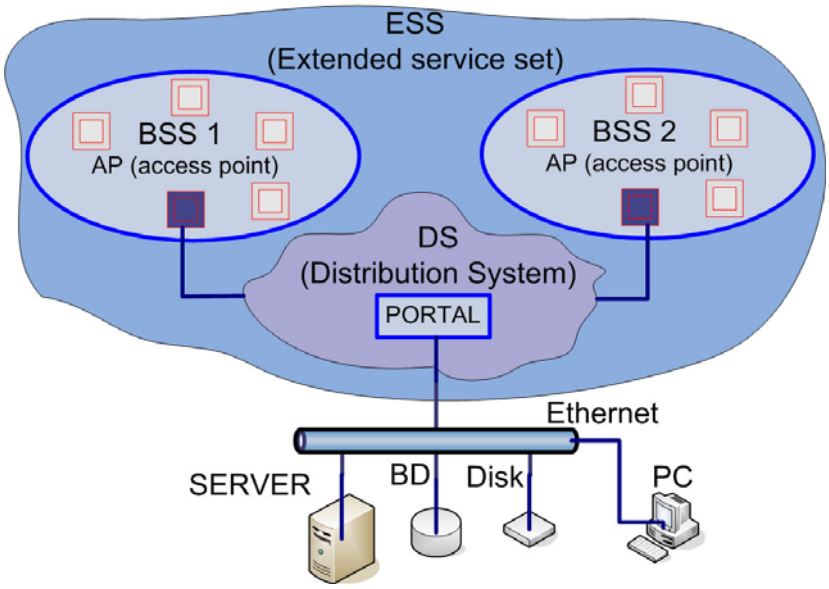


Figura 2.4. Estructura Típica de una red Wi-Fi.

El ancho de banda disponible es dividido dentro de 14 canales parcialmente traslapados, cada 22 MHz de ancho. Solamente 11 de estos canales están disponibles en EEUU, 13 en Europa y solamente 1 en Japón. Todos los dispositivos en la misma BSS (infraestructura o ad-hoc) usan el mismo canal.

Para multiplexar la señal se utilizan tres técnicas:

- **DSSS (Direct Sequence Spread Spectrum):** la cual usa una secuencia, es adoptada para tasas de 1 y 2 Mbps.
- **CCK (Complementary Code Keying):** definida en 802.11b, es usada para tasas de 5.5 y 11Mbps.
- **OFDM (Orthogonal frequency division multiplexing):** definida en 802.11a, y ademas utilizada en 802.11g, es usada para tasas de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

DSSS usa una secuencia de 11 bit, además, cada secuencia de 11 chips es codificado a un solo bit de información. La tasa desmodulación es 1 Msymbol/s usando BPSK o QPSK para tasas de transmisión de 1 y 2 Mbps respectivamente.

Con CCK, una secuencia de 16 bit es transmitida en el canal, codificando a 4 u 8 los bits de información. La modulación es QPSK a 1.375 Msymbols/s para tasas de 5.5 y 11 Mbps. Nótese que ambos casos, DSSS y CCK, la tasa de chip es de 11 Mchips/s, lo cual significa que la capa física (radiofrecuencia) es la misma; la diferencia esta en la modulación y en la múltiplexación.

OFDM utiliza un canal de 52 subportadoras (48 para datos) con un espaciamiento de 0.3125 MHz y una duración de símbolo de 4 us, para un total de 12 Msymbol/s. Cada símbolo es protegido con un código convolucional de cualquiera de estas tres tasas: ¾, 2/3 o ½, utilizando modulación M-QAM con M de 2, 4, 16 o 64. El resultado de estas combinaciones provee tasas de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

El protocolo fundamental de Wi-Fi es la capa 2 del modelo OSI, es decir, la capa MAC, la cual debe ser implantada por cada estación, y es el DCF, que para acceder al canal utiliza *CSMA/CA* (Carrier Sense Multiple Access/Collision Avoidance) y es utilizado tanto en el modo Ad-Hoc como en el modo infraestructura. Wi-Fi define también un protocolo opcional de acceso al medio llamado PCF, el cual solo puede ser usado en el modo infraestructura. PCF, tiene muchos inconvenientes, por lo que no es usado comercialmente.

El estándar IEEE 802.11e esta mejorando esta situación para redefinir los aspectos de QoS del protocolo de acceso al medio. Estas nuevas funciones de coordinación son llamadas "Enhanced distributed channel access" (EDCA) y HCF controlled channel Access (HCCA), junto con el cual se constituye el nuevo "Hybrid coordination function" (HCF). Estos nuevos mecanismos pueden operar con los anteriores.

La especificación de seguridad de Wi-Fi es el protocolo llamado *Wireless Equivalent Privacy* WEP, aunque es de calidad cuestionable. A finales del 2002, la Wi-Fi Alliance definió el *Wireless Protected Access* WPA, una notable mejora sobre la seguridad WEP. El estándar IEEE 802.11i trabajo en este nuevo estándar de encriptación, el cual utiliza tramas 802.1x/EAP con Temporal Key Integrity Protocol (TKIP) para el chip y un método *Extensible Authentication Protocol* (EAP) para la autenticación. Este mecanismo esta disponible actualmente en los nuevos dispositivos y se conoce como WPA2.

2.5 SEGURIDAD DE LA RED INALÁMBRICA

2.5.1 Introducción

Se han expuesto los grandes beneficios que la WLANs ofrece a las empresas. Sin embargo, todos estos beneficios no son aporte cuando la LAN inalámbrica provoca una

brecha en la seguridad a lo largo de toda la empresa que finalmente impida o detenga su implementación.

Las LAN Wi-Fi pueden tener un tremendo impacto positivo en una organización. Y también pueden tener un impacto negativo grande correspondiente, uno que ponga en riesgo la seguridad de la WLAN. Distintos comercios y negocios han mencionado estas preocupaciones para captar la atención del público. Sin embargo se ha malinterpretado las WLAN afirmando que son fundamentalmente incapaces de ofrecer seguridad.

La realidad es que a pesar de que la naturaleza inalámbrica de Wi-Fi presenta problemas en la seguridad que no se encuentran en las LANs cableadas, se puede desplegar una WLAN de cualquier tamaño que proporcione un nivel general de seguridad que se igual, o más alto, que el de una LAN cableada.

A continuación se describen las distintas herramientas de seguridad que están disponibles actualmente para el mercado en general.

2.5.2 Métodos de Autenticación

La autenticación es usada para regular el acceso y control de quien o quienes quieran usar nuestra red inalámbrica. Actualmente hay algunas técnicas que pueden ser usadas y cada una tiene sus ventajas y desventajas.

Los métodos más comunes para autenticación para redes inalámbricas incluyen:

- Filtrado de direcciones MAC

- SSID (Service Set Identifier)
- Clave WEP compartida
- 802.1x

Algunos de estos métodos pueden combinarse para crear una fuerte solución de seguridad.

El filtraje de direcciones MAC es una capa separada de autenticación que puede ser aplicada a cualquier otro método de autenticación. Por ejemplo, para implementaciones inalámbricas pequeñas, que no necesitan la complejidad de un servidor RADIUS, se puede escoger la autenticación por contraseña WEP combinado con el filtraje de direcciones MAC para controlar el acceso de usuarios.

Para usar un esquema de seguridad con 802.1x se requiere la selección de un Protocolo de Autenticación Extensible (EAP). Dependiendo de los requerimientos de seguridad, este protocolo EAP complicará el trabajo a seguir. Los tipos de EAP más comunes incluyen:

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- PEAP

2.5.2.1 Filtrado de direcciones MAC. Es uno de los métodos que se utiliza para proteger las redes inalámbricas.

Una dirección MAC es un número hexadecimal de 12 dígitos que es único para cada dispositivo LAN. Debido a que cada tarjeta Ethernet tiene su propia dirección MAC, si se limita el acceso al punto de acceso de solo las direcciones MAC de los dispositivos autorizados, se puede impedir fácilmente la entrada de intrusos a la red.

Sin embargo el filtrado de direcciones MAC no es completamente seguro, y si se instala solamente este mecanismo se tendrá un falso sentido de seguridad. Se debe considerar lo siguiente:

- Las direcciones MAC pueden ser falsificadas. Algunos adaptadores de cliente utilizan la Dirección de Administración Universal (UAA), que definen los fabricantes de tal forma que sobrescribe una dirección administrada localmente (LAA). Un hacker puede usar un analizador de protocolo inalámbrico para husmear el tráfico y encontrar una dirección MAC válida y luego simplemente copiarla en un adaptador de cliente compatible con LAA, por lo tanto, hacerse pasar por cliente legítimo.
- Las bases de datos separadas crean problemas administrativos. Cada tabla de direcciones MAC que se ubica en puntos de acceso individuales representa una base de datos separada. A pesar de que algunos fabricantes proporcionan medios para replicar estas tablas a lo largo de un grupo de puntos de acceso, esta solución rompe la sincronización y crea problemas de actualización.

2.5.2.2 SSID Service Set Identifier. Los puntos de acceso se pueden configurar de manera que usen contraseñas. A estos se les conoce como *Identificadores de servicio* SSID.

A menudo se considera a este método como un medio rudimentario de seguridad, pero en la realidad son bastante seguros.

Los puntos de acceso normalmente se distribuyen con un SSID determinado, que es específico del fabricante, que se emite como parte de las balizas a los puntos de acceso. Cuando este es el caso, y un adaptador de cliente tiene configurado un SSID nulo, al dejar el SSID en blanco en la utilidad del cliente, será capaz de asociarse al punto de acceso.

Las herramientas administrativas como Windows XP proporcionan la capacidad de registrar todos los SSIDs que se puedan percibir de un cliente y luego permitir que éste se asocie al punto de acceso seleccionado.

Algunos fabricantes permiten eliminar el SSID; por un lado, resuelve el problema de seguridad, pero deshabilita la capacidad de que un cliente pueda encontrar la red adecuada con la que desea conectarse.

En resumen, un SSID debe considerarse más como un nombre de red que una contraseña. Debe actuar como un medio de identificación del punto de acceso o, cuando el mismo SSID se añade a múltiples puntos de acceso de una LAN Wi-Fi. Es muy normal que una empresa use el mismo SSID en todos los puntos de acceso sin importar su ubicación.

2.5.2.3 802.1x. Es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados de autenticar y autorizar a los clientes a una red.

El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes:

- El equipo del cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores *RADIUS (Remote Authentication Dial-In User Service),* cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del cliente. El autenticador actúa como intermediario entre el cliente y el servidor de autenticación, y solamente permite el acceso del cliente a la red cuando el servidor de autenticación así lo autoriza.

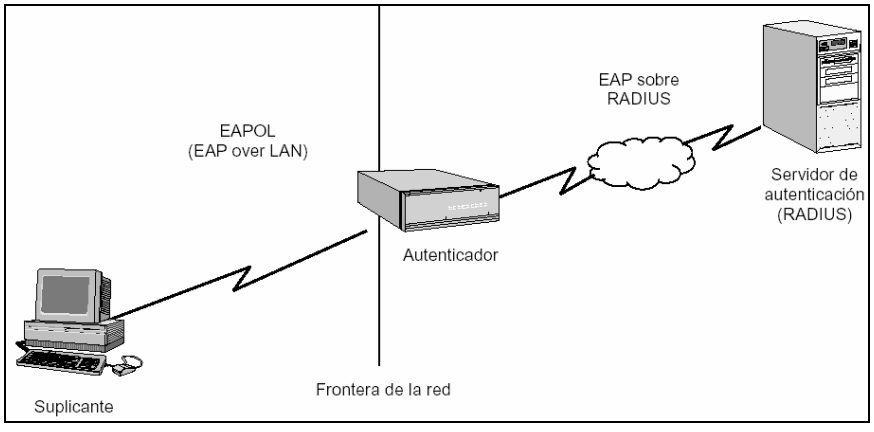


Figura 2.5. Arquitectura de un sistema de autenticación 802.1x

La autenticación del cliente se lleva a cabo mediante el protocolo *EAP (Extensible Authentication Protocol)* y el servicio RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.

- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.

- El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/ Identity.

- La estación se identifica mediante un mensaje EAP- Response/Identity.

- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access-Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.

- El servidor de autenticación responde con un mensaje RADIUSAccess- Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una

contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP- Request.

- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.

- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.

- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

En el caso del acceso inalámbrico, el servidor RADIUS despacha en el mensaje RADIUS-Access-Accept un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente (por ejemplo, cada cinco minutos), para evitar el ataque de rompimiento de la clave.

2.5.2.4 WEP. El estándar WEP proporciona el cifrado de paquetes usando claves de cifrado estáticas que comparten todos los dispositivos en la WLAN, inclusive los puntos de acceso y los clientes.

Puede estar configurado en tres posibles modos:

- No encriptación
- Encriptación de 40 bits
- Encriptación de 128 bits.

Este estándar adolece del problema de escalabilidad, ya que la instalación de claves de cifrado de manera manual en una cantidad extensa de dispositivos requiere bastante tiempo. La arquitectura de clave de cifrado estática y compartida es incompatible con las redes del tamaño de despliegues empresariales.

La robustez de las claves de cifrado ha sido muy cuestionada. Las claves de cifrado que usa WEP están basadas en el algoritmo de cifrado de *RC4,* que es un cifrado de flujo y se puede implementar usando varias longitudes de clave.

La implementación en WEP del algoritmo RC4 ofrece claves de cifrado de 40 bits de largo y tienen un vector de inicialización de 24 bits, lo cual da como resultado una clave de 64 bits de longitud. Muchos fabricantes ahora proporcionan claves de 104 bits, lo que da como resultado una longitud de clave total de 128 bits.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack,8 que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer.

La herramienta AirSnort9 hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

2.5.2.4.1 Limitaciones. WEP protege el tráfico inalámbrico combinando la clave secreta WEP con un número de 24 bits generado randómicamente para proveer la encriptación. A este vector de inicialización de 24 bits se le añade otra clave de 40 o 104 bits para dar una encriptación posible de 128 bits.

Existen algunos parámetros que complican la implementación de WEP, así:

- La limitación numérica del vector de inicialización del cual resultan 2^24 valores posibles. Aparentemente es una gran cantidad, pero el problema es que eventualmente los valores y las claves comenzarán a repetirse; de esta manera es como los hackers pueden capturar la clave WEP.

- De los 16 millones de valores posibles, no todos son adecuados, por ejemplo el número 1. Si un hacker puede usar una herramienta para buscar los valores, el WEP puede ser forzado.

- La diferencia entre la encriptación de 64 bits y 128 bits. Si se piensa que la encriptación de 128 bits es mejor, es totalmente incorrecto, ya que los dos niveles de encriptación utilizan el mismo vector de inicialización de 24 bits.

2.5.2.5 Protocolo de Autenticación Extensible EAP. Es un protocolo de seguridad Capa 2 (capa direcciones MAC) que existe en el estado de autenticación de un proceso de seguridad, que acompañado con otras medidas de seguridad, provee una capa final de seguridad para la red inalámbrica.

Usando 802.1x, cuando un dispositivo solicita acceso a un punto de acceso, ocurre lo siguiente con EAP:

- El punto de acceso solicita información de autenticación del cliente.
- El usuario envía la información de autenticación requerida.
- El punto de acceso envía la información del cliente a un servidor RADIUS para su autenticación y autorización.
- Una vez autorizado, el cliente puede conectarse y transmitir datos.

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

- **EAP-TLS:** Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

- **EAP-TTLS:** Desarrollada por Funk Software y Certicom. Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor. Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2.
- **PEAP:** Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

Las variantes de EAP que utilizan contraseñas son las siguientes:

- **EAP-MD5:** Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

- **LEAP:** Esta variante es propietaria de Cisco. Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

- **EAP-SPEKE:** Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

2.5.3 Métodos de Encriptación de datos

Una vez seleccionado el método de autenticación para la red inalámbrica, es necesario seleccionar un esquema de encriptación para proteger los datos que viajan a través del aire. Algunos de estos esquemas de encriptación pueden ser solo usados con un método de autenticación específico.

No todas las tarjetas de red inalámbricas soportarán los últimos estándares de seguridad, por lo que es imprescindible verificar que tengan capacidad de actualización.

No todos los sistemas operativos soportan los últimos métodos de encriptación. Por ejemplo WPA no es soportado por todos los sistemas operativos de Windows o Unix.

Cada método de autenticación puede ser combinado con un método de encriptación de datos para asegurar la red inalámbrica. Los esquemas disponibles más comunes de encriptación de datos incluyen:

- WEP estática

- WEP dinámica
- Wi-Fi Protected Access WPA

2.5.3.1 Wi-Fi Protected Access WPA. WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como *TKIP (Temporary Key Integrity Protocol).* Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP, que fueron discutidos en la sección anterior.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- **Modalidad de red empresarial**: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- **Modalidad de red casera (Pre-Shared Key**): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello "Wi- Fi Certified" podrá ser actualizado por software para que cumpla con la especificación WPA.

2.5.4 Medidas de seguridad adicionales

2.5.4.1 Red Privada Virtual VPN. Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en

una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

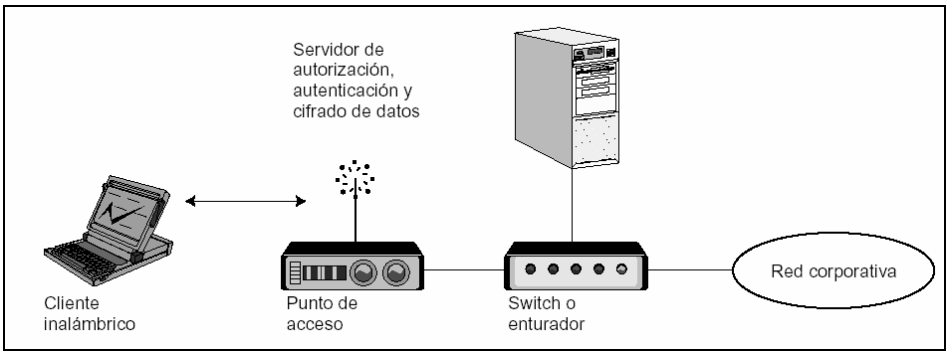


Figura 2.6. Estructura de una VPN para acceso inalámbrico

Muchas organizaciones han optado por ignorar los desarrollos que se ha realizado en la seguridad específica para Wi-Fi y simplemente despliegan una VPN sobre la capa física Wi-Fi que es completamente insegura.

Existe una variedad de ventajas en este enfoque:

- La tecnología VPN es relativamente madura. Actualmente, las VPN proporcionan una variedad de métodos de autenticación que integran los cifrados DES, 3DES y AES.

- El enfoque VPN aprovecha la infraestructura de seguridad existente y el conocimiento del personal. Muchas empresas se han basado en esto para ofrecer acceso remoto en lugar de líneas contratadas costosas. Es decir, estos esfuerzos se

pueden aprovechar para resolver también los problemas de los clientes inalámbricos.

- Con las VPN, existe cierta capacidad de interoperatibilidad. Las soluciones VPN están formadas por una aplicación del lado del cliente y un concentrador (hardware) en el otro extremo, o una aplicación de servidor basada en software. La mayoría de aplicaciones VPN del lado del cliente operan en un rango muy amplio de sistemas operativos y están disponibles a un costo muy bajo o gratuitamente.

Sin embargo, existen algunas desventajas cuando se usa una solución VPN para resolver la seguridad WLAN:

- Las ventajas de interoperatibilidad de las VPN son su desventaja. Es decir, debido a que los clientes VPN residen en el software y usan el procesador del anfitrión, su operación implicará un impacto en el desempeño mucho mayor al que ocasionan las soluciones que implementan el cifrado en el hardware. A pesar de que esto es cierto en el lado del cliente, es mucho más visible en el software del servidor VPN dentro de la infraestructura.
- Las VPN están limitadas ya que no proporcionan la capacidad de priorizar el flujo de paquetes que se requiere para el tráfico sensible al tiempo, como el de voz y video. Las VPN solo dan soporte para el tráfico unidifusión IP y no soportan otros protocolos, por ejemplo, IPX y AppleTalk.

2.5.4.2 Firewalls. Si la red inalámbrica está conectada a una LAN cableada, es conveniente colocar un firewall entre ellas.

Considerar a la red inalámbrica como pública, asegura que cualquier intruso dentro de ella, no tendrá fácil acceso a la LAN cableada.

2.5.4.3 Configuración del Punto de acceso. Cuando se configura un punto de acceso, se debe tener en cuenta los siguientes parámetros:

- Asegurarse de que solo las conexiones aceptadas tengan el SSID correcto.
- Cambiar la contraseña por defecto del punto de acceso.
- Comparta las direcciones IP solo a los clientes autenticados.
- Mantener una lista de direcciones MAC permitidas y solo permitir que esos clientes se conecten a la WLAN.

2.6 VOZ SOBRE IP

La voz sobre IP utiliza el método de conmutación de paquetes de las redes de datos para proveer una forma más eficiente de enviar comunicaciones de voz. La conmutación de paquetes optimiza el uso de los recursos de la red (ancho de banda) porque el canal solo esta ocupado durante el tiempo que el paquete esta siendo transmitido. Muchos usuarios pueden compartir el mismo canal porque los paquetes pueden ser enviados y recibidos en cualquier orden y la red puede balancear la carga a través de varios equipos. Esto permite que muchas llamadas telefónicas ocupen la cantidad de espacio que una sola en una red de conmutación de circuitos. Con la migración de las redes telefónicas hacia la tecnología de conmutación de paquetes, estas han ganado la habilidad de comunicarse mas eficientemente como las computadoras lo hacen.

En el mundo IP, la voz es otra aplicación de datos funcionando sobre una red IP. En un ambiente mixto, los PBX llegar a ser el equivalente a un super servidor que esta en la

red y es accesado por clientes remotos en cualquier lugar de la red sobre cualquier tipo de líneas de transmisión.

2.6.1 Componentes de voz sobre IP

Los tres componentes principales de una red de voz sobre IP son:

1. Servidor de procesamiento de llamadas, IP PBX: es el corazón de una solución IP. Maneja todas las conexiones de control VOIP. Es usualmente un software que puede ser instalado en un simple servidor.

Las comunicaciones VOIP necesitan un mecanismo de señalización para el establecimiento de las llamadas, conocido como control de tráfico, y para el tráfico actual de voz, conocido como carga VOIP. Este control de trafico sigue el modelo de cliente – servidor. El cliente es el dispositivo final VOIP como un teléfono IP, el cual comunica de regreso el control de tráfico hacia el servidor. La carga VOIP (trafico de voz actual) fluye en un modelo peer to peer entre cada teléfono IP. Es decir, el servidor negocia y habilita las llamadas, mientras que los teléfonos IP manejan la carga VOIP.

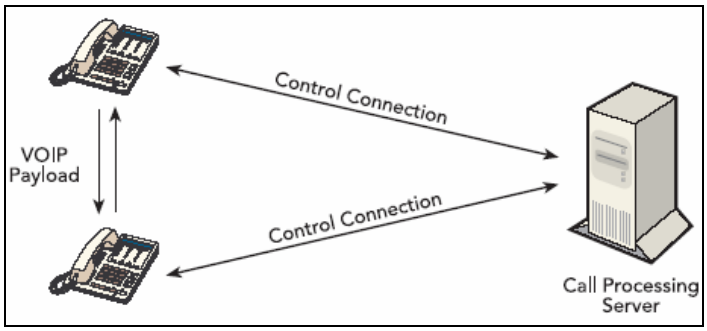


Figura 2.7. Servidor de procesamiento de llamadas.

2. Teléfonos IP: utilizan el protocolo TCP/IP para comunicarse con la red IP. Debe tener una dirección IP de la red en la que esta instalado. Típicamente, estos teléfonos usan DHCP, protocolo para asignamiento dinámico de direcciones IP a dispositivos en una red.

3. Gateways IP: es el dispositivo que conecta la red de datos con la red de voz. Su principal función es la conversión análoga – digital de las comunicaciones de voz y la creación de los paquetes IP de voz. Luego envía estos paquetes de voz sobre la red IP de datos. Llamados también media gateways, pueden ser equipos integrados de telecomunicaciones, o software corriendo sobre una PC.

2.6.2 Protocolos de VoIP

El conjunto de protocolos de Voz sobre IP (VoIP) se descompone en dos categorías:

- Protocolos del plano de datos
- Protocolos del plano de control

El **plano de datos (Voz)** es el protocolo necesario para llevar el tráfico de un usuario a otro.

RTP y cRTP son protocolos de plano de datos y están disponibles en cualquiera de las arquitecturas de VoIP. El tráfico propio de VoIP a veces va por caminos diferentes a la señalización, esto significa que pueden viajar de forma independiente. RTP es el protocolo que soporta la voz del usuario. Cada paquete RTP contiene una muestra pequeña de la conversación de voz. El tamaño del paquete y el tamaño de la muestra de voz, dentro de dicho paquete, dependerán del CODECs utilizados. En la figura se muestra la pila de protocolos RTP.

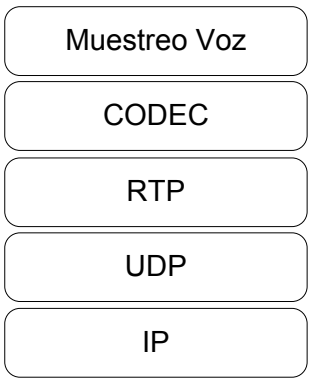


Figura 2.8. Pila de protocolos RTP

La parte del **plano de control de VoIP** es el tráfico necesario para conectar y mantener el tráfico actual de usuario. Es también responsable de mantener toda la operación de toda la red (comunicaciones router-router).

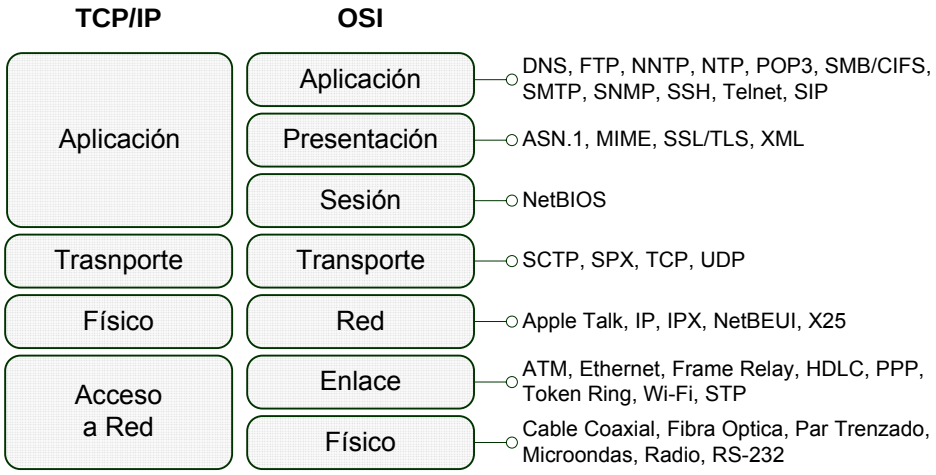


Figura 1.9. Modelo de red TCP/IP & OSI y protocolos principales

Hay muchos tipos de protocolos de señalización diferentes, IAX, SIP, H.323, MGCP, Skinny/SCCP, UNISTIM. Los más ampliamente utilizados son H.323 y SIP.

2.6.2.1 Protocolo H.323. El protocolo H.323 fue diseñado por la ITU (International Telecommunication Union) para proveer a los usuarios mecanismos para tele-conferencias que tienen capacidades de voz, video y datos sobre redes de conmutación de paquetes**.**

Un punto fuerte de H.323 era la relativa y temprana disponibilidad de un grupo de estándares, no solo definiendo el modelo básico de llamada, sino que además definía servicios suplementarios, necesarios para dirigir las expectativas de comunicaciones comerciales. H.323 fue el primer estándar de VoIP en adoptar el estándar de IETF de RTP para transportar audio y vídeo sobre redes IP.

H.323 está basado en el protocolo RDSI, Q.931 y está adaptado para situaciones en las que se combina el trabajo entre IP y RDSI, y respectivamente entre IP y QSIG (Protocolo de señalización en una Central PBX en una red PSTN). Un modelo de llamada, similar al modelo de RDSI, facilita la introducción de la Telefonía IP en las redes existentes de RDSI basadas en sistemas PBX. Por esto es posible el proyecto de una migración sin problemas hacia el IP basado en sistemas PBX.

2.6.2.2 Protocolo SIP. El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF (Internet Engineering Task Force), definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero del 1996 en la RFC 2543, ahora obsoleta con la publicación de la nueva versión RFC 3261 que se publicó en junio del 2002.

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP.

El protocolo RTP se usa para transportar los datos de voz en tiempo real, igual que para el protocolo H.323; mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.

SIP fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales. El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales.

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

2.6.2.3 Protocolo IAX. IAX (Inter-Asterisk Exchange protocol) es un protocolo abierto, lo cual significa que cualquier usuario puede a partir del código fuente seguir desarrollándolo, pero este no llega a ser aun un estándar.

El protocolo IAX, fue desarrollado por Digium con el propósito de establecer una comunicación entre servidores Asterisk. IAX es un protocolo de transporte que utiliza el

puerto UDP (4569) para ambos canales de señalización y cadenas de datos del protocolo de transporte en tiempo real (RTP).

IAX soporta Trunking, donde un simple enlace permite enviar datos y señalización por múltiples canales. Cuando se realiza Trunking, los datos de múltiples llamadas son manejados en un único conjunto de paquetes, lo que significa que un datagrama IP puede entregar información para más llamadas sin crear latencia adicional. Esto es una gran ventaja para los usuarios de VoIP, donde las cabeceras IP son un gran porcentaje del ancho de banda utilizado.

2.6.2.4 Protocolo MGCP. MGCP (Media Gateway Control Protocol), también fue desarrollado por el grupo IETF. Si bien MGCP aún se encuentra en desarrollo, éste protocolo es más difundido de lo que se imagina y está dejando atrás a otros protocolo como SIP y IAX. MGCP está definido en la RFC 3534 y fue diseñado para que los equipos terminales sean los más simple posible y que todo el procesamiento de la llamada se ejecute en los gateways y en otros agentes de control. A diferencia de SIP, MGCP utiliza un modelo centralizado. Los teléfonos MGCP no pueden establecer una llamada directamente.

MGCP separa conceptualmente estas funciones en los tres elementos: un MGC (*Media Gateway Controller*), uno o más MG (*Media Gateway*), y uno o más SG, (*Signaling Gateway*). Un gateway tradicional, cumple con la función de ofrecer conectividad y traducción entre dos redes diferentes e incompatibles como lo son las de Conmutación de Paquetes y las de Conmutación de Circuitos. En esta función, el gateway realiza la conversión del flujo de datos, y además realiza también la conversión de la señalización, bidireccionalmente. Así, la conversión del contenido multimedio es realizada por el MG, el control de la señalización del lado IP es realizada por el MGC, y el control de la señalización del lado de la red de Conmutación de Circuitos es realizada por el SG.

MGCP introduce esta división en los roles con la intención de alivianar a la entidad encargada de transformar el audio para ambos lados terminales, de las tareas de señalización, concentrando en el MGC el procesamiento de la señalización.

CAPÍTULO III

SITUACION ACTUAL DEL SISTEMA DE COMUNICACIONES INTERNO

3.1. ADMINISTRACION ZONAL VALLE DE LOS CHILLOS

Las Administraciones Zonales son las unidades responsables de desarrollar dos ejes estratégicos básicos de la administración municipal: La Descentralización – Institucional y el Sistema de Gestión Participativa.

El primero de esos ejes posibilita una atención más directa, inmediata y permanente del Municipio a las zonas, sectores urbanos y parroquias rurales del Distrito; el segundo articula la intervención directa y activa de la ciudadanía en la gestión de gobierno local.

La Administración Zonal del Valle de los Chillos fue creada con Resolución No. 041 del 1ero de septiembre de 1997 , por lo que ejerce sus competencias en la zona suburbana de los Chillos, que comprende las parroquias de Guangopolo, Alangasí, La Merced, Conocoto, Amaguaña y Píntag.

La Institución ha definido específicamente sus funciones principales, que son las siguientes:

- Aprobación de planos
- Aprobación de subdivisiones
- Declaraciones de propiedad horizontal
- Compatibilidad de uso del suelo y zonificación
- Permisos de construcción

- Ejecución y control de obras
- Control de invasiones de la propiedad municipal
- Levantamiento de hipotecas y prohibición de enajenar
- Informes de regulación metropolitana.
- Permisos de trabajos varios y de cerramiento
- Atención a denuncias.
- Velar por el cumplimiento de las ordenanzas.
- Balnearios de El Tingo y Rumiloma.
- Control de medio ambiente.
- Control de espacios públicos.
- Control de edificaciones y urbanizaciones.
- Control de rotulación
- Promoción de salud
- Valoración y revalorización de la identidad cultural
- Fortalecimiento a programas de Desarrollo Humano
- Políticas de seguridad ciudadana
- Factibilidad de obras a nivel zonal
- Recepción de fondos de garantía
- Pago de impuestos prediales, patentes tasas.
- Actualización de la propiedad municipal
- Recepción de pagos de agua potable
- Mediadores entre Juntas Parroquiales y Administración
- Facilitadores de la participación comunitaria en procesos de desarrollo.
- Proveedores de información básica y general de las seis parroquias del Valle de los Chillos.
- Dialogo Social
- Mantenimiento y actualización catastral Control del cumplimiento de la ordenanza 100 vigente (aseo).

3.2 SITUACION ACTUAL : LOGISTICA E INFRAESTRUCTURA

Físicamente, el edificio administrativo de la Administración Zonal Valle de los Chillos del Municipio Metropolitano de Quito se encuentra ubicado en el Cantón Rumiñahui, en la parroquia de San Rafael.

Las instalaciones de la A.Z.V.CH; se hallan asentadas sobre un área de 500 m2, distribuidos en tres plantas donde se encuentran todos los departamentos que ofrecen servicios a la comunidad.

3.2.1. Infraestructura física

En general, el área construida de la A.Z.V.CH. se compone de un edificio de tres plantas. Toda la edificación abarca un área de 500 m2. En la figura 3.1.**,**se muestra la las instalaciones de la A.Z.V.CH.

Figura 3.1. Administración Zonal Valle de los Chillos

La construcción es una estructura de hormigón armado, con paredes de ladrillo. Cuenta con lozas de hormigón, excepto el último piso, que se halla techado con planchas de asbesto.

En cada planta se encuentra distribuidos los departamentos de esta institución, así de esta manera:

En la figura 3.2., se muestra la primera planta de la administración, la cual cuenta con una distribución asimétrica de oficinas.

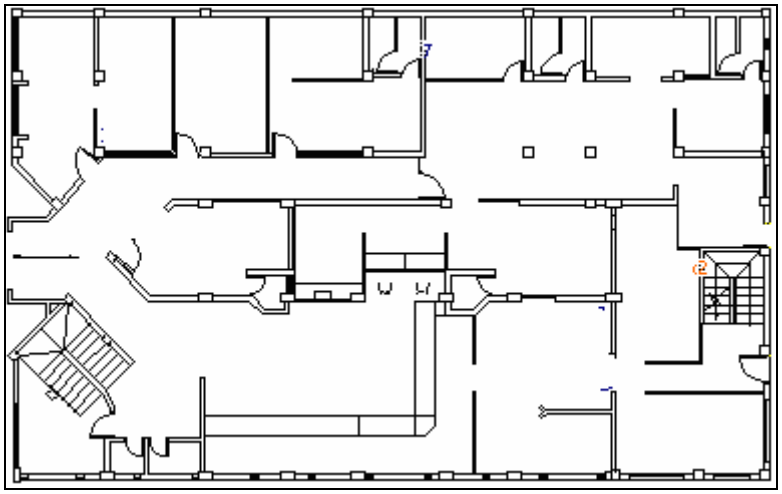


Figura 3.2. Planta baja de la A.Z.V.CH.

Las oficinas que se encuentran funcionando dentro de esta primera planta, se enlistan en la tabla 3.1.

Tabla 3.1. Dependencias en la primera planta

Primera Planta	
Dependencia	**Número**
Comisaría	1
Comisaría de Aseo	1
Control de la ciudad	1
Gestión Urbana	4
Avalúos y catastros	1
Fiscalización	1
Recaudaciones	1
Centro de documentación	1
Archivo	1

La segunda planta presenta una forma rectangular y tiene una distribución más compleja, con múltiples divisiones de paredes internas que en total crean casi 15 ambientes distintos.

En la figura 3.2. se presenta el plano de distribución correspondiente a la segunda planta del edificio.

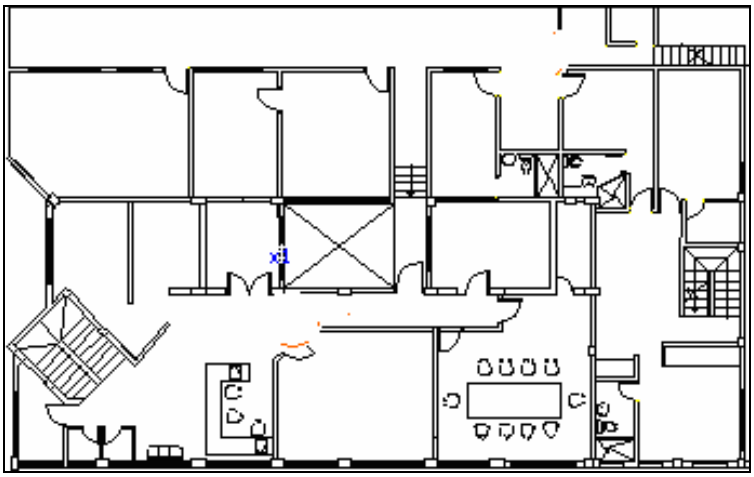


Figura 3.3. Segunda Planta de la A.Z.V.CH.

La distribución interna de los ambientes se resume en la tabla 3.2.

Tabla 3.2. Dependencias de la segunda planta.

Segunda Planta	
Dependencia	**Número**
Administración	1
Secretaria General	1
Asesoría Legal	2
Sala de Reuniones	1
Dialogo Social	1
Jefatura de Salud	1
Coordinación de Desarrollo	1
Obras Públicas	1
Centro de copiado	1
Bodega	1

La tercera planta una distribución más compleja, con múltiples divisiones de paredes internas, además existen varias divisiones modulares que en total crean casi 15 ambientes distintos.

La tercera planta cuenta con una distribución asimétrica de oficinas, mostrada en la figura 3.4.

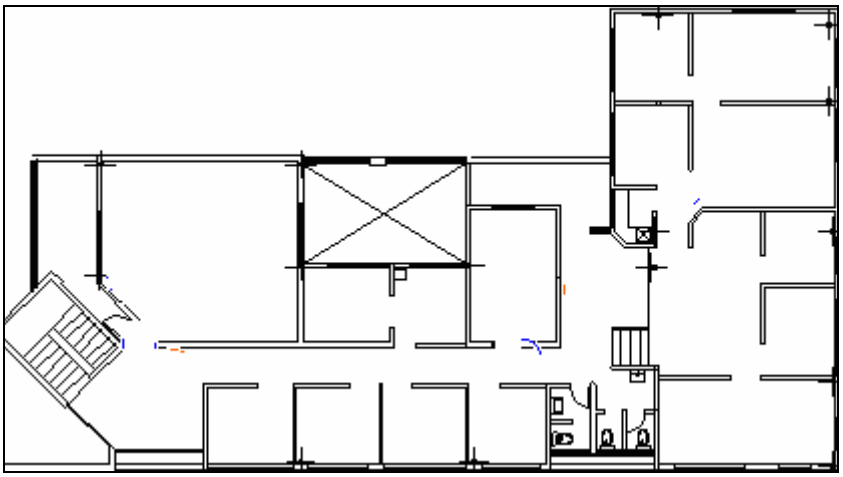


Figura 3.4. Tercera planta de la A.Z.V.CH.

Las oficinas que se encuentran funcionando dentro de esta tercera planta, se enlistan en la tabla 3.3.

Tabla 3.3. Dependencias de la tercera planta

Tercera Planta	
Dependencia	**Número**
Territorio	3
Recursos Humanos	1
Jefatura de Informática	1
Gestión Urbana	4
Fiscalización	2
Coordinación Administración y Servicios	1
Jefatura Financiera	1

3.2.2. Infraestructura tecnológica

Actualmente, la A.Z.C.CH. cuenta con una red de datos cableada que cubre ampliamente la demanda de los departamentos de la institución, es decir, permite realizar algunas aplicaciones como servicios de email, mensajería instantánea y transferencia de archivos, quedando totalmente desperdiciado el ancho de banda del cable UTP Cat5e con el que cuenta, e impidiendo contar con nuevas aplicaciones y servicios que incrementarían la productividad de la administración.

El requerimiento de esta institución es aprovechar el uso de un cableado estructurado para el mejor desempeño de las funciones y sobre todo estar a la vanguardia de la tecnología, por lo que el presente proyecto tiene la finalidad de analizar y estudiar la factibilidad de ofrecer servicios de voz, datos y video a toda la edificación de la A.Z.V.CH.

3.2.2.1 Equipos de Computación. La A.Z.V.CH. ha hecho progresivas adquisiciones de computadores para sus oficinas, así como equipos complementarios entre los que citamos UPS, impresoras, plotters.

Los equipos de computación están distribuidos en distintas oficinas en todo el edificio. Los más antiguos están designados a trabajo regular de las secretarias, mientras que los de mejores características son utilizados por los arquitectos, ingenieros, etc.

Al momento, el hardware existente en la A.Z.V.CH, se describe en la tabla 3.4.

Tabla 3.4. Listado de equipos de computación existentes

Hardware de la A.Z.V.CH	
Cantidad	**Descripción**
1	Servidor Genérico
90	PC desktop
9	Impresoras
1	Plotter

El servidor es de características robustas que opera actualmente para Internet y la Intranet. Los 90 computadores tipo desktop son de características muy distintas unos de otros, tanto en su hardware como software.

En la tabla 3.5. se ofrece un detalle de las especificaciones de ellos:

Tabla 3.5. Detalle de tipos de procesador de computadores tipo desktop

Procesador Pentium	Porcentaje
PIV	80%
P III	15%
P II - I	5%

3.3 PROYECTO DE MODERNIZACION

En las anteriores secciones queda reflejado el poco uso que le da a la infraestructura tecnológica de apoyo con la que cuenta la A.Z.V.CH. Sin embargo, no debe entenderse que la institución se ha despreocupado, sino que, de acuerdo a las necesidades que se presentan, esta en la obligación de dar una solución eficaz a cada una de ellas.

La distribución de las oficinas y el continuo cambio de estas, el mal gasto de las llamadas telefónicas internas, son algunas de la causas por la que la administración ha planteado realizar este proyecto de modernización de la A.Z.V.CH.

3.3.1 Necesidad Específica

Se pretende, primeramente contar con una red de datos inalámbrica en toda la edificación, ya que como se analizo en el capitulo 1, esta administración esta continuamente cambiando de lugar las oficinas y por tanto el numero de usuarios de red, además se instalan nuevos módulos o se los retira de acuerdo a la necesidad presente, por tanto, la instalación de una red inalámbrica es vital, ya que con esta se descarta cualquier

posibilidad de tener excesos o falta de puntos de red para conectar a los usuarios a la red interna.

Sobre esta red inalámbrica, se requiere saber la factibilidad de instalar una red de voz sobre IP, con el fina de abaratar los costos de comunicación telefónica interna, aunque se han tomado ciertas medidas hasta ahora para cumplir aquello, pero se pretende hacer uso al máximo del concepto de cableado estructurado, por lo que sobre la misma red de datos bien puede funcionar la red de voz sobre IP.

En resumen, la solución a la necesidad de mejoramiento de la eficiencia de la A.Z.V.CH. es la implantación de la Intranet en sus instalaciones, que tenga segmentos de conectividad inalámbricas capaz de brindar cobertura a el interior de la misma, de manera que todos los empleados cuenten con acceso a la red interna de la empresa.

El usuario que desee conectarse a la red necesitara entonces de un computador con un dispositivo de acceso a esta WirelessLAN, y como muchos de esos usuarios tienen PC desktops, se requiere también cotizar las tarjetas de red para todos los usuarios posibles de esta Intranet.

Aceptando como valida la solución propuesta, la A.Z.V.CH. ha determinado que al momento de estreno de la red y aplicaciones, esta serviría a por lo menos 90 computadores mas otros dispositivos como plotters, impresoras. Hablamos entonces, de una Intranet que soportara aproximadamente a 100 clientes.

CAPITULO IV

DISEÑO DE LA RED INALAMBRICA

La sección 3.3.1. Se refiere a la solución general consensuada para el problema de la A.Z.V.CH., solución consistente en la implantación de una nueva infraestructura de red de datos, que modernizará la entidad.

Habiéndose planteado tal solución, de manera general, es necesario ahora definir cómo llevar a cabo esas ideas, materializarlas y volverlas reales. Se ha mencionado que existe la tecnología que permitiría implantar el sistema imaginado, y efectivamente así es, pero las opciones son variadas y requieren análisis, debido a que se pretende contar con una Intranet funcionando bajo características muy especiales, por lo que los criterios de diseño deben ser sustentados de manera profesional, sin descuidar la imprescindible necesidad de optimización de los recursos utilizados en la red. A fin de cuentas ese es el objetivo de la ingeniería: conseguir el mayor beneficio con la menor inversión.

En función de lo anterior, el presente capítulo se centra en el diseño del sistema, a través de la selección de tecnología de entre las alternativas disponibles, y elaborar una propuesta adaptada exclusivamente a este caso particular. Se cumplirán los requerimientos planteados echando mano de herramientas interesantes y novedosas en proyectos de este tipo, que cambian el concepto de diseño de redes inalámbricas, utilizado hasta hoy en nuestro país. El resultado obtenido será más exacto y completo, a la vez que exigirá menos trabajo, lo que sin duda aumenta el beneficio a la A.Z.V.CH. En fin, se pretende hacer también un aporte en lo referente a métodos de diseño de WLANs, que incentive y perfeccione el desarrollo de nuevos proyectos en nuestro medio.

4.1. ANALISIS DE REQUERIMIENTOS

Es preciso definir con exactitud los requerimientos acerca de la red LAN que constituirá la Intranet para los departamentos de la A.Z.V.CH. Serán la base de las consideraciones de diseño.

4.1.1. Cobertura

El requerimiento de cobertura de la nueva red ha sido determinado por la propia administración. Según las actividades que se realizan en los departamentos, se han identificado los sitios que por su importancia sería ideal que estén cubiertos con el alcance de la red, y son todas las oficinas, modulares, que existen en las tres plantas del edificio de la administración.

La cobertura se refiere a que un usuario tenga acceso a los servicios de la red, desde cualquier punto comprendido en el interior de las zonas comprendidas.

El área considerada es difícil ya que presenta múltiples ambientes, cuyo número es elevado en relación con la superficie que ocupan. Anteriormente se detalló las zonas de cobertura en los planos del edificio.

4.1.2. Seguridad

Este tema es un requerimiento indispensable en todo el proceso de diseño, debido a que la información correspondiente a las labores institucionales de la administración ha sido catalogada como sensible y confidencial. Es obligatorio entonces poner en práctica las mejores medidas técnicas que permitan proteger esa información en todas las instancias, adicionalmente a los criterios de seguridad normales en el trabajo con redes de datos, debido a las vulnerabilidades que ellas conllevan. En general, los puntos a tomar en cuenta son: acceso a la Intranet, acceso a la información, protección contra amenazas propias de las redes de computadores, como son virus, spam, spoof, spyware, hacking, etc.

4.1.3. Escalabilidad.

La planificación para que una red soporte crecimiento de las condiciones iniciales de operación, es por hoy punto obligatorio de consideración al momento de dimensionar las capacidades que tendrá la red, en cuanto al número de usuarios, tráfico de datos, aplicaciones. La intranet deberá diseñarse para arrancar con 100 usuarios en condiciones que se tratarán más adelante, pero será necesario establecer un margen de crecimiento, más para aumento de tráfico que para aumento de usuarios, como consecuencia de nuevos usos que se le de a la red, así como nuevas aplicaciones tecnológicas que pudieran aparecer.

4.1.4. Calidad de servicio.

La percepción de calidad que el usuario tenga de la nueva infraestructura de apoyo depende de algunas características directamente relacionadas con el diseño. Pensemos en los usos que tendrá la red:

1. Servirá para compartir y transferir archivos e información regular, entre los usuarios de la red.

2. Brindará servicio de acceso a Internet.

3. Establecerá voz sobre IP para comunicar las dependencias internas del edificio.

Acerca de la opción de compartir y transferir archivos, documentos, audio, según el tamaño de tales archivos, pueden congestionar la red, si son demasiado grandes, o se utiliza mucho este servicio.

Por tanto, como se quiere provocar una percepción positiva, debe observarse en el diseño la implantación de una capacidad adecuada para el manejo del tráfico en general, y que los servicios de la Intranet sean rápidos y eficientes. Además de prácticos, serían satisfactorios desde el punto de vista de la comodidad del usuario. Recordemos que una de las principales percepciones de satisfacción de un usuario que navega por Internet es

precisamente la velocidad con la que lo hace, el corto tiempo para mostrar las páginas. Sucede el mismo con la transferencia de archivos.

En general, la calidad del servicio deberá observarse desde el punto de vista técnico, en cuanto a la disponibilidad, confiabilidad, seguridad, etc.

4.2. PLANIFICACIÓN DE LA WLAN

El tema de la planificación en un proyecto marca la diferencia entre la informalidad y el tratamiento profesional del mismo. Esta diferencia es muy notoria en el producto resultante, tanto en el desempeño técnico, como en el económico.

Planificar la red consiste en diseñarla de manera que cumpla con los requerimientos técnicos y económicos hechos para ella, esto es, obtener un producto óptimo. En el presente proyecto, los requerimientos específicos para la WLAN son:

1. Cumplir con la cobertura requerida, es decir que cubra todos los pisos del edificio de la administración.

2. Establecer una red inalámbrica dentro de esa cobertura, con tasas de transmisión en lo posible de la media hacia arriba de las contempladas en la norma 802.11g, de manera que se magnifique la calidad de servicio de la red.

3. Conformar la red con el número óptimo de Access Points.

4. Considerar los requerimientos generales establecidos para red LAN de la administración.

En la planificación de la red inalámbrica Wi-Fi obligatoriamente existirá, como en todo diseño, un componente propio del diseñador. Esto introduce un factor de

incertidumbre en el resultado, que puede ser minimizado si la planificación del diseño es basada en una predicción del desempeño de la red.

Los científicos e ingenieros han desarrollado métodos para predecir los resultados de una WLAN, cada vez con mayor exactitud. Estos resultados predichos pueden ser comparados con los requerimientos, para realizar modificaciones, correcciones o mejoras en el diseño, si fuera el caso.

En fin, la información obtenida a través de la predicción del desempeño de una WLAN, es la clave para el éxito en la planificación de la misma. Por supuesto, ese éxito consistirá en la implantación de un producto de óptima calidad.

A continuación inicio el tratamiento de las herramientas para la predicción del funcionamiento de la WLAN que se pretende implantar.

4.2.1 El modelo de predicción Dominant Path.

Para la planificación de redes inalámbricas (celulares o WLAN), en áreas urbanas y dentro de lugares cerrados o más conocidos como entornos "indoor"[1], existen algunos métodos para calcular su propagación y el área de cobertura, entre los cuales podemos mencionar a modelos empíricos (rayos directos), y modelos determinísticos de rayos ópticos (trazado de rayos).

En pos del mejoramiento de la predicción y el cálculo de la propagación de ondas, con una mejor exactitud y desempeño, en 1997 se constituyó en Alemania un grupo de científicos e investigadores autodenominados "Architects of the Wireless Evolution", que también emprendieron una gran iniciativa empresarial, AWE Communications. El institut fur Hochfrequenztechnik, la Universidad de Stuttgart y AWE Communications, proponen al IEEE, en Septiembre de 2004, un nuevo modelo de predicción de propagación de ondas llamado "Dominat Path Model" (DPM) o Modelo de Trayecto Dominante.

[1] Indoor: expresión usada para referirse a ambientes dentro de una edificación, ambientes cerrados.

Este nuevo modelo de predicción muestra los caminos o trayectos que prevalecen entre el transmisor y el receptor de ondas, estos parámetros están determinados y son usados para la predicción de las pérdidas que se producen durante el viaje entre el transmisor y receptor. Algunos de estos parámetros son por ejemplo: la distancia entre Tx y Rx, el número y tipo de interacciones, propiedades de los materiales que obstaculizan, línea de vista, etc.

Este método se ha desarrollado e implantado en una poderosa herramienta de software desarrollada por AWE Communications (Winprop), que permite simular en base a este modelo de predicción la cobertura de las redes inalámbricas, proporcionando información y herramientas para el diseño y planificación profesional de redes de comunicaciones.

4.2.2 La suite de software Winprop

AWE Communications utilizó sus investigaciones en el desarrollo de una herramienta que permitiera modelar redes de comunicaciones móviles, para realizar predicciones de su desempeño, bajo condiciones específicas. El software incorporó varios modelos de predicción, empíricos y determinísticos, para realizar cálculos de patrones de pérdidas y cobertura de redes de comunicaciones celulares, en ambientes o escenarios outdoor urbanos, ciudades enteras. La planificación de redes móviles empezó con las comunicaciones celulares, así que AWE creó este producto o herramienta para facilitar el diseño y planificación de estos sistemas, presentándolo por primera vez en el año 2000 con el nombre de “Winprop” y poniéndolo al servicio del público en general, como alternativa a herramientas equivalentes de otros fabricantes que también empezaban a figurar en el mercado.

El software fue perfeccionado continuamente desde entonces, adaptándolo a nuevas aplicaciones como la predicción en ambientes outdoor[2] de tipo rural, donde las condiciones son totalmente distintas a los escenarios urbanos. Y otra gran adaptación que se le hizo en el año 2001 fue para los escenarios “indoor”, interiores de edificios. A partir de este

[2] Outdoor: expresión usada para referirse a espacios abiertos, extensos.

avance, Winprop pudo ser utilizado para planificación de redes de comunicaciones tipo WLAN en escenarios indoor.

Los años de investigación y desarrollo por parte de los científicos de AWE rindieron sus frutos en Septiembre de 2004, cuando presentaron a la IEEE y comunidad científica en general su propio modelo de predicción de path loss (pérdidas de trayecto) y propagación de ondas de radio, para redes de comunicaciuones móviles, adaptado a condiciones prácticas. El modelo Dominant Path (DP) fue desarrollado y presentado con éxito como un nuevo sistema para estimar el desempeño de redes de comunicaciones móviles, en escenarios indoor, outdoor y urbanos.

La evolución de este software fue otra necesidad obligatoria para AWE, que necesitó tan solo 2 meses para incorporar el modelo DP a las otras opciones de modelos de predicción con que el programa había alcanzado cierta madurez y éxito, por lo que gozaba ya de la confianza de empresas de la talla de Siemens, Alcatel, Ericsson, France Telecom, Nokia, entre otras., que lo utilizaban que lo utilizaban para experimentos y planificación de redes celulares en varias ciudades alemanas y europeas. Algunos módulos, funcionalidades y modelos de Winprop, tales como el Intelligent Ray Tracing[3], fueron incorporados al software industrial de las multinacionales de telecomunicaciones. AWE desarrolló tales adaptaciones a paquetes como Aircom, NetAct de Nokia, Atoll de ALcatel, Tornado de Siemens, lo que explica que Winprop sea perfectamente compatible con ellos, para leer y modificar proyectos y resultados.

Actualmente, Winprop es una excepcional suite de software de interfaz gráfica, que incluye tres programas, cada uno de ellos con una función específica en el proceso de planificación de redes de comunicaciones móviles: Wallman, Aman, Priman. A continuación una explicación breve de cada uno:

1) *Wallman:* Wall Manager o administrador de paredes, programa diseñado para construir un modelo o plano tridimensional y realista del edificio, campus o ciudad

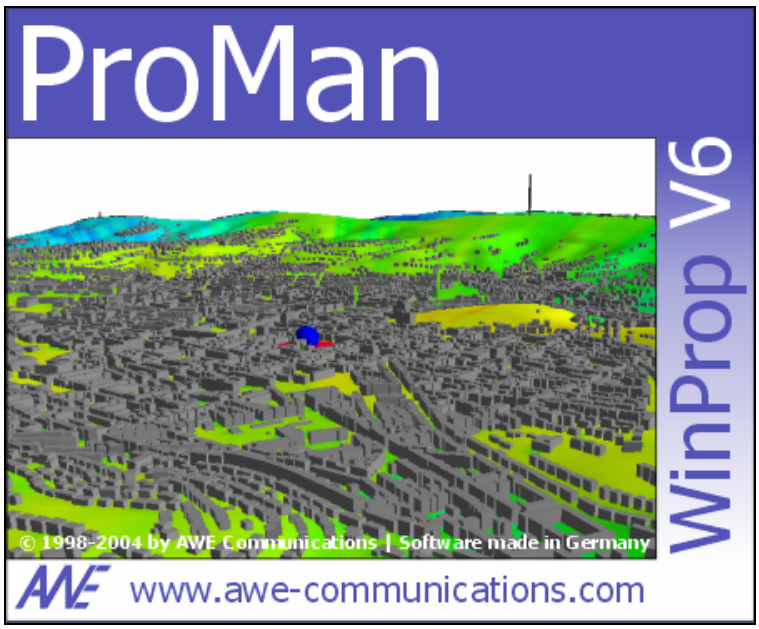
[3] Intelligent Ray tracing o IRT, modelo determinístico tridimensional de trazado de rayos para la predicción de propagación de ondas, presentado por AWE Communications en 1999, que le valió el premio Best Paper Award, en la conferencia PIMRC de la IEEE.

sobre la cual se planifica una red de comunicaciones. Su fortaleza está en permitir el desarrollo de modelos con detalles imprescindibles para predicciones de propagación de ondas, como por ejemplo dimensiones, formas tridimensionales, ubicación y composición de elementos tales como paredes, puertas, ventanas, escaleras, etc., con sus propias especificaciones de espesor, materiales, propiedades físicas, parámetros dieléctricos. AWE denomina al plano elaborado como "database", porque es la base de datos para el cálculo de la predicción realizado con los otros programas de la suite.

2) *Aman:* Antenna Manager a administrador de antenas, es otro programa opcional que incluye el paquete, y sirve para elaborar patrones de radiación de antenas diseñadas por el usuario. Los patrones elaborados con Aman se importan desde otro programa para calcular predicciones utilizando antenas de diseño propio, o bien antenas sectoriales.

3) *Proman:* Propagation Manager o administrador de propagación. Es el complemento de los dos programas anteriores y probablemente el más útil, porque utiliza las database y patrones de antenas elaborados con los otros programas del paquete, para elaborar lo que AWE llama Network Project, que consiste en ubicar equipos de comunicaciones, como radio bases celulares o Access >Points, dentro de la database creada anteriormente, para virtualmente construir una red de comunicaciones debidamente valorada, compilar el programa y que éste elabore los archivos con los resultados de la predicción. Priman permite establecer todas las características reales que una red involucra, tales como sistema de comunicaciones (GSM, CDMA, WiFi), potencias de transmisión, frecuencia de ondas, tipos de modulación, ganancia de antenas. Luego es posible seleccionar el modelo de predicción a ser utilizado: empíricos como el Okumura-Hata o el COST 231; determinísticos como el IRT o el nuevo modelo DP. Con todos los parámetros de cálculo definidos, se compila el network Project creado, tras lo cual se crean los archivos de resultados, que son gráficos de la database marcados con colores que indican potencias recibidas, tasas de transmisión, análisis probabilísticos, etc.

Para este proyecto de diseño de una WLAN, AWE Communications otorgó una licencia para fines educativos por un periodo de 30 días para usar los módulos Wallman y Proman de la suite de Winprop en la planificación de la WLAN de la administración.



4.3. DETERMINACIÓN DE NUMERO Y UBICACIÓN DE ACCESS POINTS

Esta es la tarea más importante en el diseño de una WLAN. Los Access Points son los equipos transmisores y receptores de las ondas electromagnéticas que establecen la cobertura de la red inalámbrica, por lo que su número y ubicación óptimos tienen influencia decisiva en la calidad de la red, tanto en el desempeño técnico, como en su costo de inversión.

Para determinar estos dos parámetros básicos, se utilizaran las herramientas de AWE, el modelo de predicción Dominant Path DP y su herramienta de cálculo. El método de diseño consistirá en simular la WLAN de la A.Z.V.CH. Con posibles ubicaciones de los AP. De esta manera se obtendrán predicciones del desempeño de cada alternativa probada, y será factible establecer comparaciones entre los resultados de las diferentes combinaciones de número y ubicación de los AP. El análisis y comparación de los resultados de las simulaciones mostraran la mejor alternativa, así como sugerirán probables cambios o ajustes a la solución que mejores resultados arroje.

Lo anterior es un método de aprovechamiento de las facilidades que brinda Winprop para realizar modelamiento y simulación de redes de comunicaciones móviles, y estudiar su desempeño con gran confiabilidad, mientras que ahorra inmensa cantidad de tiempo, porque evita realizar mediciones de campo para cada nueva combinación de número y ubicación de AP. También es más práctico y exacto que realizar predicciones matemáticas de cobertura y propagación, utilizando cualquiera de los modelos empíricos disponibles. Hay que recordar que esta poderosa herramienta puede predecir esos datos en base a un modelo nuevo y superior que es el DP. Y ejecutar una predicción determinística como el Trazado de Rayos, sin una herramienta de software, es una tarea muy compleja, y por que no decir imposible.

Finalmente, antes de empezar, es indispensable establecer tres condiciones iniciales eminentemente técnicas, obligatorias, para crear las simulaciones e interpretar los resultados:

1) *Tasas de transmisión esperadas:* se busca conceder a los usuarios una conexión con las tasas mas altas de la norma IEEE 802.11g, esto es 36, 48 y 54 Mbps.

2) *Factor de diseño:* aunque el modelo de predicción DP y las simulaciones ofrezcan un buen grado de confiabilidad en los resultados obtenidos, no descuido considerar factores indeterminados que introduzcan errores e incertidumbre en las predicciones. Tales factores pueden ser muy variados, desde fallas en la elaboración de la database o errores acerca de las propiedades de los materiales de los edificios, hasta imprecisiones en las características de los equipos que integran la red, pasando por interferencias y factores externos difíciles de establecer, como el mobiliario y cruce de personas por los rayos. Por tanto es indispensable considerar un factor de diseño que empeore intencionalmente las condiciones de resultantes de la simulación. Técnicamente la conexión dependerá de la potencia recibida en los puntos de interés de cobertura, y se la considerara valida en 3 dB por debajo de la potencia recibida que indique Proman. Ahora bien, esos 3 dB equivalen a bajar un nivel mas la mínima tasa de transmisión aceptable, que en el ítem anterior fue fijada en 36 Mbps. Por tanto, considerando este factor de diseño, la nueva tasa de transmisión mínima aceptable queda fijada en 24 Mbps.

3) *Mínima potencia de señal recibida:* las tarjetas inalámbricas de usuario tienen estandarizados algunos parámetros técnicos tales como la potencia de transmisión, que es de 15 dBm, y la sensibilidad, especialmente importante para captar la señal de los AP. Esta sensibilidad se refiere a la capacidad de detección del nivel de potencia recibida por la tarjeta desde los AP, para establecer con ellos una conexión a cierta velocidad de transmisión. Si las tasas mínimas aceptables quedaron establecidas en 54, 48, 36 y 24 Mbps, a ellas les corresponde una sensibilidad en el receptor de -68, -69,-75 y -79 dBm respectivamente, dato técnico de los principales fabricantes. En conclusión, se pretende que el mínimo nivel de potencia recibida de los AP, en las zonas de cobertura sea de -79 dBm, a fin de garantizar una conexión al menos de 24 Mbps.

4.3.1. Creación de la Base de Datos

La unidad de trabajo para la predicción de propagación es la "database". El programa Wallman permite establecer los materiales que componen los edificios a modelar, con sus propiedades físicas y eléctricas, para crear un modelo matemático que simula la estructura de los edificios, en 2 o 3 dimensiones, con su real distribución de paredes, columnas, techos, lozas, ventanas puertas, etc. Es dentro de este modelo bidimensional que se simulara luego la propagación de ondas de una red de comunicaciones.

En las tablas 4.1, 4.2, 4.3. y 4.4., se muestran los materiales que componen el edificio de la A.Z.V.CH. Las propiedades físicas, tales como espesor, altura, composición han sido establecidas en la exploración de las instalaciones. Las propiedades eléctricas para los elementos encontrados en la database fueron proporcionados por AWE.

Tabla 4.1. Propiedades físicas y eléctricas de las paredes de la database.

Paredes (f = 2440 MHz)	
Propiedades Físicas	*Descripción*
Material	Ladrillo
Espesor	20 cm
Altura	3 m

Propiedades Eléctricas	*Cantidad*
Perdidas de transmisión	11.22 dB
Perdidas de reflexión	9.51 dB
Perdidas de difracción	24 dB
Permitividad relativa	4
Permeabilidad relativa	1
Conductividad	0.064 S/m

Tabla 4.2. Propiedades físicas y eléctricas de las puertas de la database.

Puertas (f = 2440 MHz)	
Propiedades Físicas	*Descripción*
Material	Madera
Espesor	5 cm.
Altura	2.10 m
Propiedades Eléctricas	*Cantidad*
Perdidas de transmisión	3.5 dB
Perdidas de reflexión	16.5 dB
Perdidas de difracción	28 dB
Permitividad relativa	1.7
Permeabilidad relativa	1
Conductividad	0.057 S/m

Tabla 4.3. Propiedades físicas y eléctricas de vidrio de la databas.

Vidrio, ventanas (f = 2440 MHz)	
Propiedades Físicas	*Descripción*
Material	Vidrio
Espesor	1 cm.
Altura	Variable
Propiedades Eléctricas	*Cantidad*
Perdidas de transmisión	1.8 dB

Perdidas de reflexión	7.53 dB
Perdidas de difracción	23 dB
Permitividad relativa	6
Permeabilidad relativa	1
Conductividad	0.006 S/m

Tabla 4.4. Propiedades físicas y eléctricas de pisos, columnas y techos de la databas.

Pisos, columnas, techo (f = 2440 MHz)	
Propiedades Físicas	*Descripción*
Material	Concreto
Espesor	20 cm.
Altura	Variable
Propiedades Eléctricas	*Cantidad*
Perdidas de transmisión	13.5 dB
Perdidas de reflexión	7.51 dB
Perdidas de difracción	23 dB
Permitividad relativa	6
Permeabilidad relativa	1
Conductividad	0.093 S/m

Cabe indicar que la A.Z.V.CH. facilitó los planos de la edificación, lo que resultó mas conveniente y práctico, ya que solamente se cambio los valores de las propiedades físicas y eléctricas en Wallman, y se tuvo lista la base de datos para realizar los cálculos de propagación.

4.3.2. Ubicación de los Access Points

Una vez conocida la infraestructura de la administración, como primera opción estaría la de usar uno o dos AP con antenas omnidireccionales en todo el edificio, pero debido a la gran cantidad de paredes y ambientes resulta muy inconveniente realizar esta combinación.

Los fabricantes ofrecen AP con potencias de transmisión de 15, 17, 18 o 20 dBm, según la marca y tipo. En general, uno de línea empresarial transmite a 17 dBm, pudiéndose agregar varias antenas, de 2, 5, 10 hasta 14 Dib. Para conformar un transmisor con potencia efectiva radiada deseada.

4.3.2.1. Primera Planta. Para la primera planta se hicieron varias pruebas. Para evitar gastos mayores, para las simulaciones se utilizo Access Points de línea empresarial con una potencia de 17 dBm más una antena adicional con una ganancia de 2 dBi., lo que en total da 19 dBm de potencia radiada. Se hicieron pruebas con antenas más potentes y costosas, pero el resultado era el mismo, por lo que se decidió por no utilizar antenas adicionales a las que se tiene cuando se compra el AP.

La primera prueba que se hizo fue con un AP ubicado a la entrada de esta planta. Los resultados de la simulación con estas condiciones se muestran en la figura 4.1.

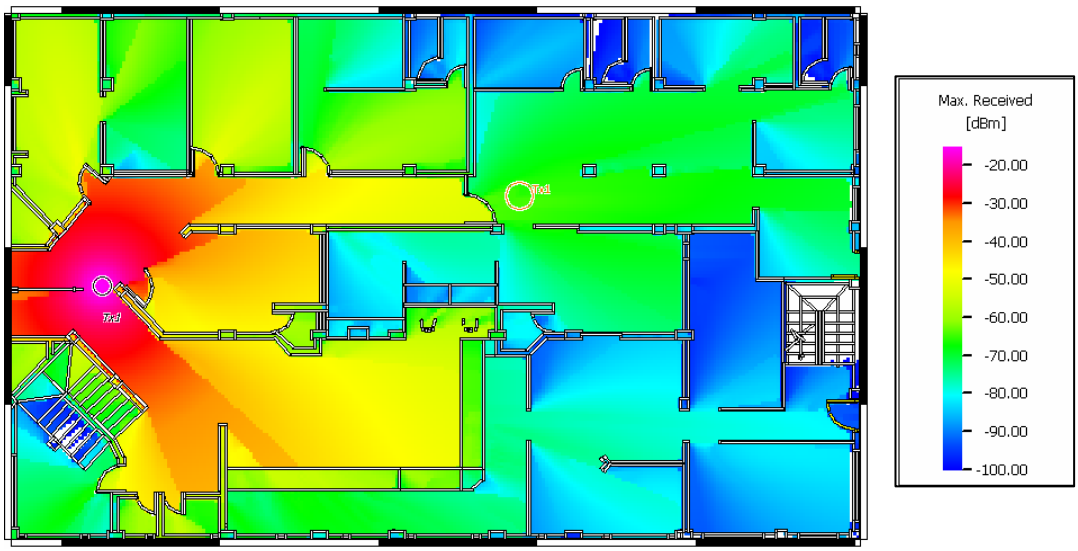


Figura 4.1. Potencia recibida en la primera planta con un Tx de 19 dBm.

La escala de colores indica que un 70% del área total de la planta es irradiada con una potencia de hasta -79 dBm, y existen áreas en las que se recibe potencias inferiores a la mínima aceptable. Esto se debe principalmente a la gran concentración de paredes y ambientes.

En la siguiente prueba, se simulo igualmente con un AP ubicado en otro lugar de la planta.

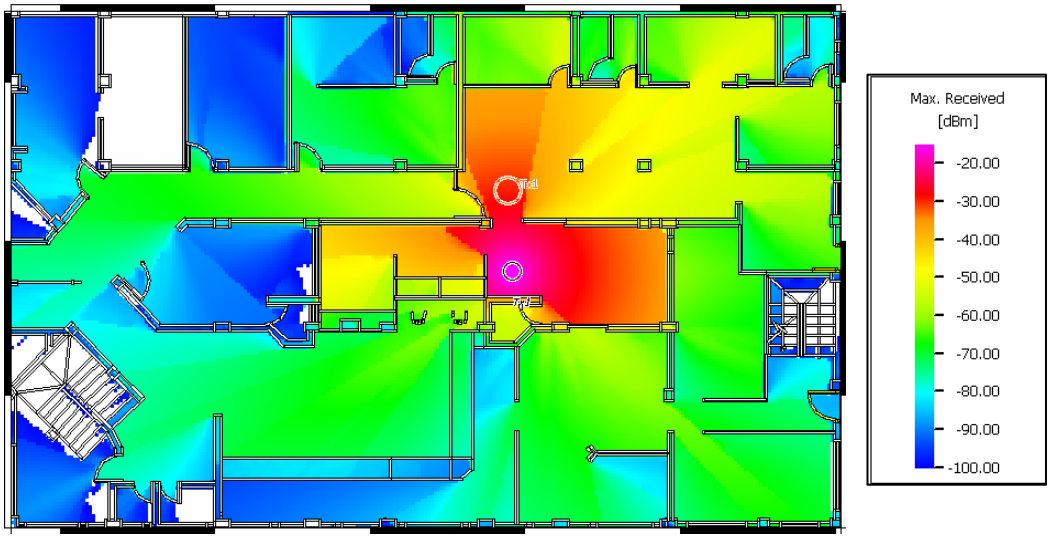


Figura 4.2. Potencia recibida en la primera planta con un Tx de 19 dBm ubicado en otro sitio.

Como se observa en la figura 4.2. se tiene el mismo comportamiento. No importa donde se ubique el AP, siempre quedara un área sin cobertura. Queda claro que debe colocarse un número mayor de estos equipos.

Se decidió entonces, colocar dos AP en los lugares anteriormente mostrados, y se tuvo los resultados mostrados en la figura 4.3.

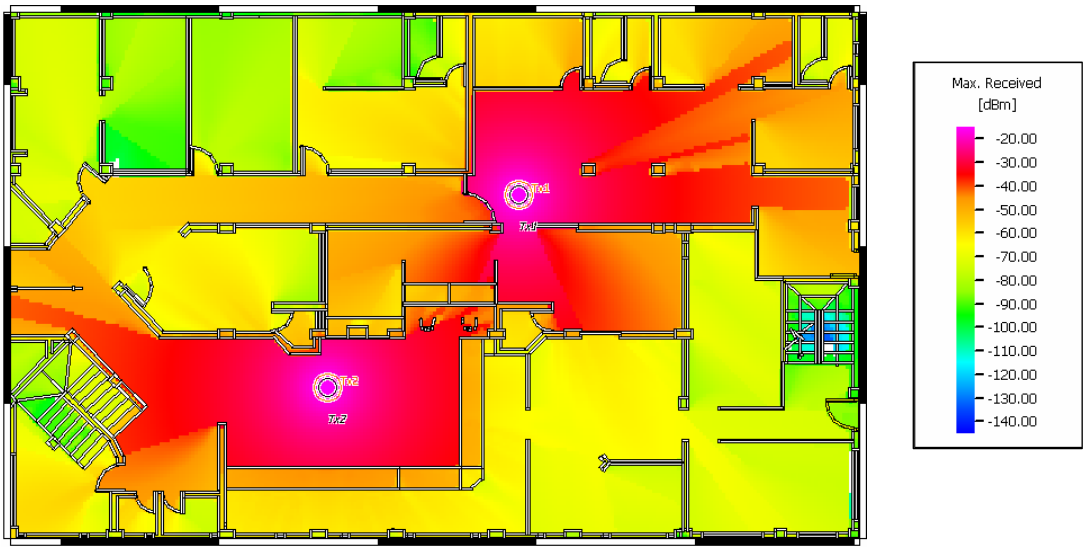


Figura 4.3. Potencia recibida en la primera planta con dos Tx de 19 dBm

Se obtuvo un muy buen resultado. La cobertura cubre en 100% la primera planta con una potencia de hasta -70 dBm, muy superior al límite establecido anteriormente. En realidad, el conformar la red de este modo, con varios AP concentrados en el piso creando celdas de cobertura más pequeñas pero con mejor tasa de transmisión, es una muy buena solución, pero que conlleva dificultades técnicas y económicas derivadas de una combinación de número y ubicación de AP de este tipo.

La dificultad técnica que se presenta, es que al tener varias celdas de cobertura creadas por varios AP's, puede existir un problema de organización de celdas. Hay que recordar que la norma selecciona para la red WLAN es 802.11g, que tiene solamente 3 canales sin traslapamiento. Por tanto, se decidió conformar la red de la siguiente manera:

- ✓ Por cada piso van a existir dos AP's; uno de los dos estará configurado de modo master y el otro de modo Bridge (slave), los dos funcionando en el canal 1 para el primer piso. De igual manera, para el segundo piso, existirá la misma configuración, pero en el canal 6. y en el ultimo piso, se repite el mismo paso, pero en el canal 11. De esta manera se resuelve el problema técnico, ya que no existirá la llamada interferencia co-canal debido a que no se repite ningún canal de los 3 disponibles.

- ✓ Además, cada piso tendrá su SSID propio, con lo cual, los computadores que están en el primer piso solo podrán asociarse a los AP's del primer piso y no a los de los otros pisos. De igual mera para los siguientes pisos.

En cuanto a las dificultades económicas, se piensa que el colocar dos AP's por piso, 6 en total, no es un fuerte gasto, ya que es una buena inversión que tendrá resultados satisfactorios en las comunicaciones de la administración.

Ahora bien, para el primer piso se tiene una tasa de transmisión máx. De 54 Mbps, como se muestra en la figura 4.4.

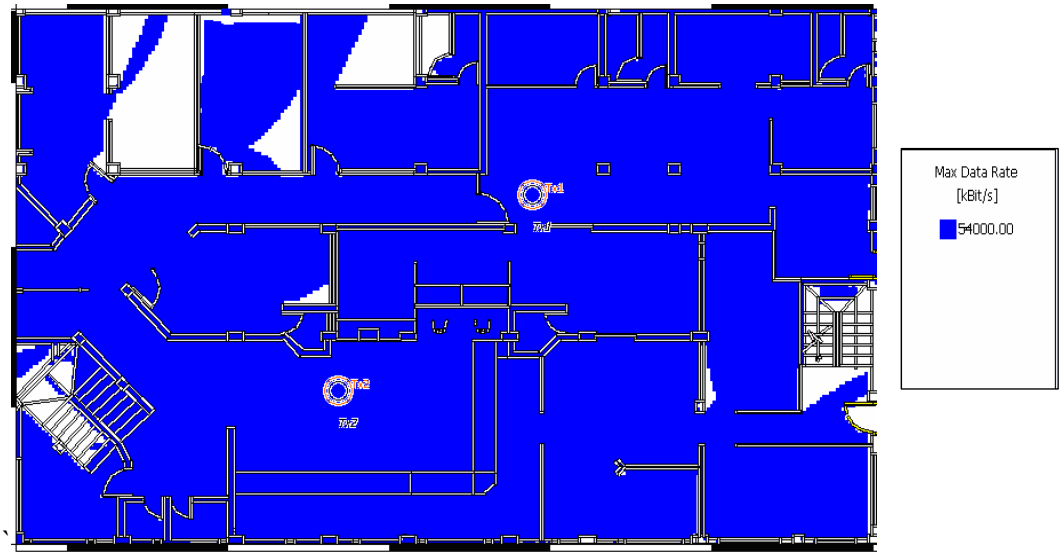


Figura 4.4. Tasa máx... De datos recibida en la primera planta con dos Tx de 19 dBm

4.3.2.2. Segunda Planta. De igual manera que en el primer piso, se hicieron varias pruebas, con un AP, luego con dos; concluyendo que la mejor opción es la que contiene dos AP's funcionando de la manera ya expuesta anteriormente.

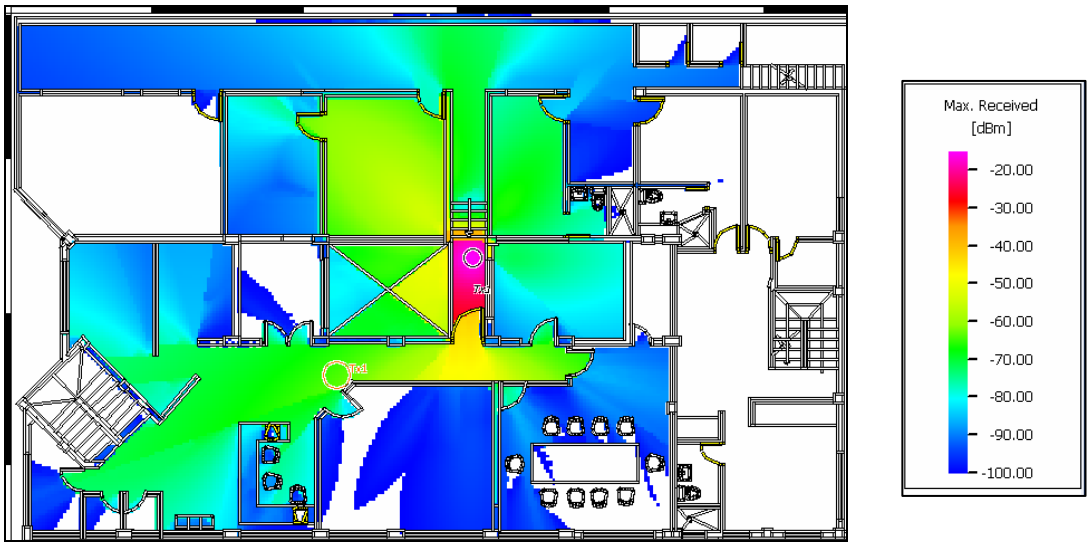


Figura 4.5. Potencia recibida en la segunda planta con un Tx de 19 dBm

Como se observa en el figura 4.5., la potencia no cubre ni el 40% de la planta. Se probó con otras antenas de hasta 31 dBm, pero el resultado es el mismo, ya que existe una alta concentración de paredes, que impiden que la señal se propague por todo el área

disponible. Lo que propone que se debe usar más de un AP de menor potencia para cubrir toda la planta.

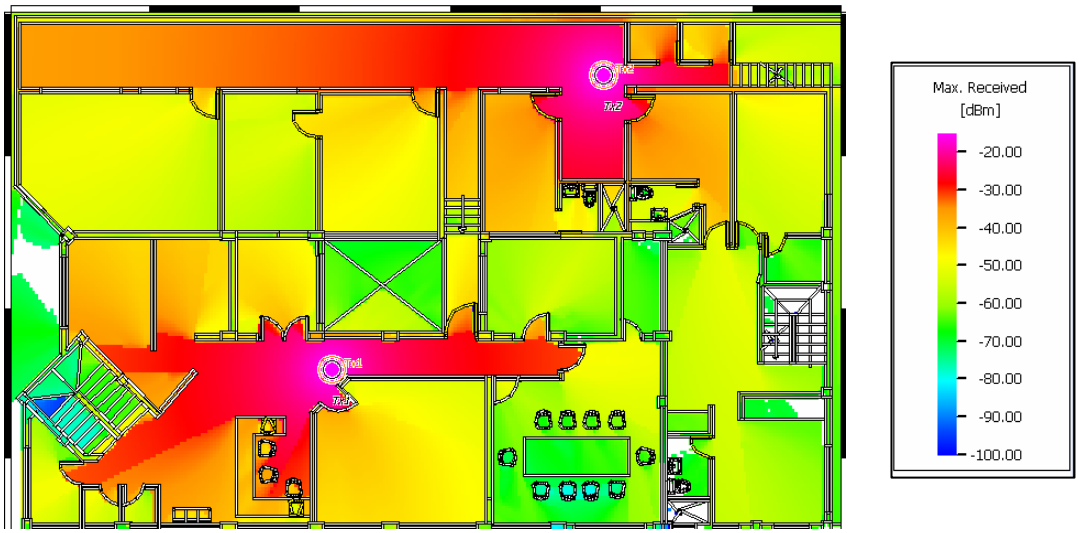


Figura 4.6. Potencia recibida en la segunda planta con dos Tx de 19 dBm

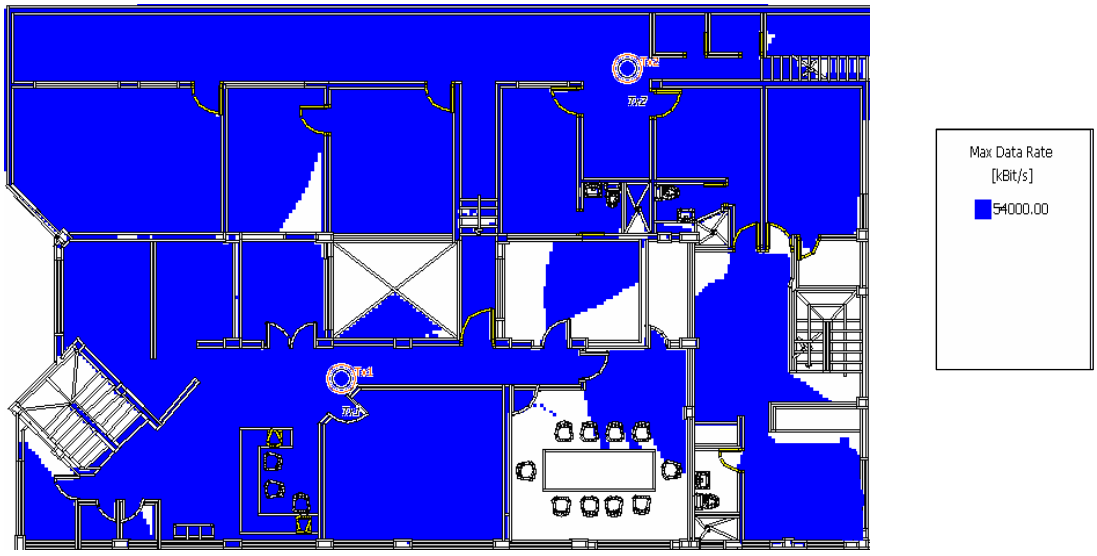


Figura 4.7. Tasa máx.. De datos recibida en la segunda planta con dos Tx de 19 dBm

Gracias a Proman, se puede saber de antemano la máxima tasa de transmisión esperada en la planta, que en este caso, es de 54 Mbps en el 98% de esta.

4.3.2.3. Tercera Planta. Siguiendo con la misma forma, se coloco dos AP's para cubrir el área. Como resultado se tuvo una muy buena cobertura en toda la planta, llegando

con una buena tasa de transmisión a todos las oficinas de este piso. Los resultados se muestran en la figura 4.8.

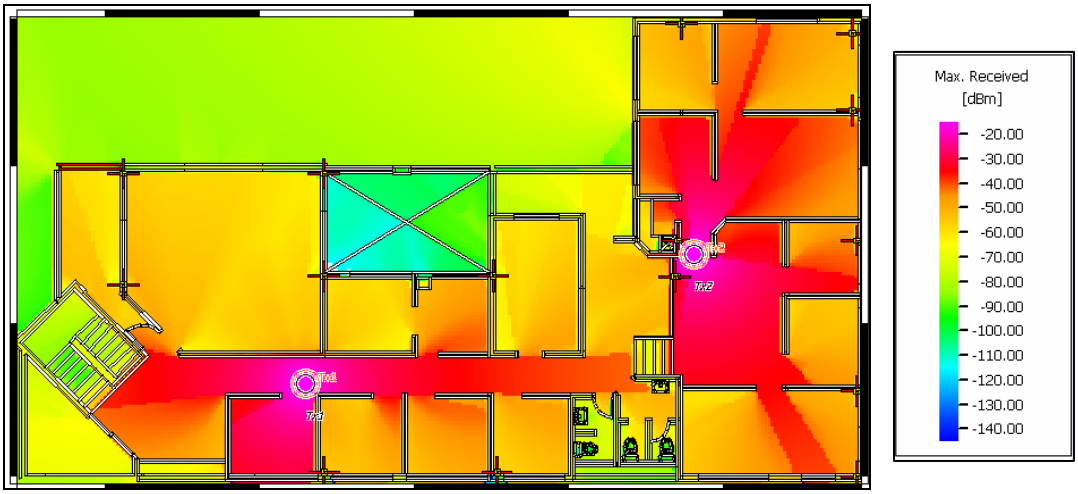


Figura 4.8. Potencia recibida en la tercera planta con dos Tx de 19 dBm

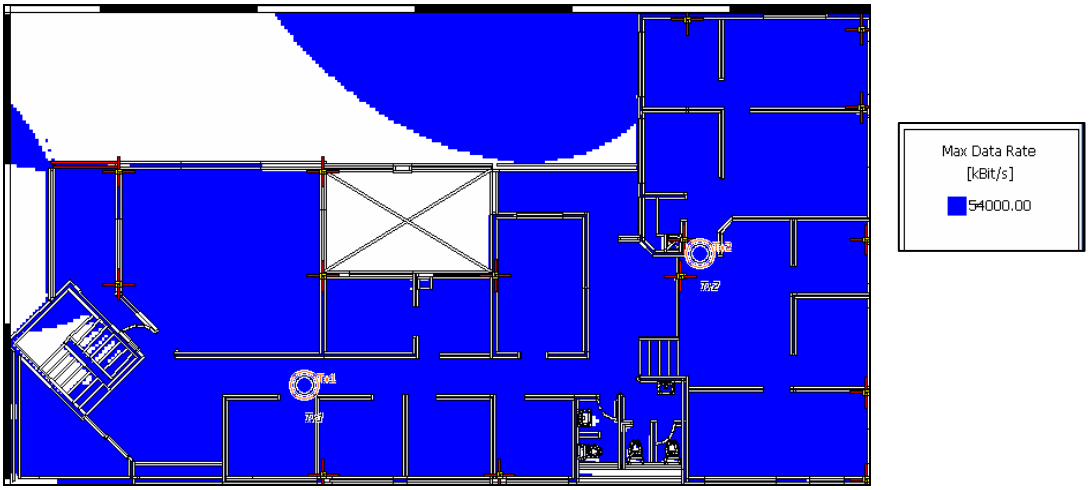


Figura 4.9. Tasa max. de transmisión en la tercera planta con dos Tx de 19 dBm

4.3.3. Bases técnicas de los dispositivos WLAN

Se ha establecido el diseño de la red inalámbrica para la A.Z.V.CH. En concordancia con el diseño, se indicaran ahora las características y especificaciones mínimas que deberán tener los equipos que conformaran esta red, en lo que se refiere a la capa 1 del modelo OSI. Estos datos constituyen las bases técnicas con las que deberán seleccionarse los AP y las tarjetas de red.

4.3.3.1. Access Points.

1. Deben ostentar la certificación Wi-Fi.
2. Operación bajo el estándar IEEE 802.11g
3. Potencia mínima de transmisión de 17 dBm, o 50 mW.
4. Sensibilidad mínima de -70 dBm para conexión a 4 Mbps.
5. 6 AP con antenas omnidireccionales de 2 Dib. de ganancia.
6. Deben soportar la función de roaming y bridge.
7. Deben tener priorización de tráfico, así como también la modificación de los parámetros MAC.

4.3.3.2. Adaptadores de red Wireless LAN

1. Deben ostentar la certificación Wi-Fi.
2. Operación bajo el estándar IEEE 802.11g
3. Potencia mínima de transmisión de 15 dBm. O 32 mW.
4. Sensibilidades mínimas de:
    - -70 dBm para conexión a 54 Mbps.
    - -72 dBm para conexión a 48 Mbps.
    - -75 dBm para conexión a 36 Mbps.
    - -79 dBm para conexión a 24 Mbps.

4.4. ARQUITECTURA DE LA RED ETHERNET

La red inalámbrica ha quedado totalmente diseñada, a través del establecimiento del número y ubicación exacta de los AP que la conforman. Esta información permite continuar el proyecto con el diseño minucioso de la red LAN cableada, que constituye el llamado Sistema de Distribución de los AP. Muchas decisiones están pendientes, acerca de la red cableada, por lo que su determinación y especificación corresponde a la ejecución de la verdadera Arquitectura de red, en función del uso que se dará a la misma.

4.4.1. Dimensionamiento de la Intranet

El diseño de la red LAN de tipo Ethernet debe realizarse de manera que considere el requerimiento de escalabilidad, tratado en la sección 4.1.3 de este capítulo.

Desde el punto de vista del número de usuarios, la red debe soportar a por lo menos 100 usuarios en este momento, y se tiene previsto que el incremento en el número de usuarios no llegue a ser mayor de un 10%, con lo que la red soportaría hipotéticamente a 110 usuarios simultáneamente, en el peor de los casos. Como esos usuarios accederán a la Intranet a través de los AP, es importante considerar la capacidad de estos dispositivos. En el mercado existen AP que soportan desde 48 hasta 248 usuarios simultáneamente. Tomando en cuenta que son 6 los AP que integran la WLAN, la capacidad teórica de esta seria al menos de 248 usuarios, por lo que la red cumple y ampliamente sobrepasa la posibilidad de crecimiento en el número de usuarios.

Desde el punto de vista del tráfico, la Intranet en la A.Z.V.CH., funcionará para brindar servicio de Internet, transporte de archivos entre usuarios, y para telefonía entre departamentos.

En lo que se refiere al tráfico de Internet, se sabe que cuando se navega por la red produce una carga de 12Kbps por usuario. Ahora si tenemos los 110 usuarios potenciales usando Internet simultáneamente, se tendrá la siguiente carga:

$$\boxed{12000 \times 110 = 132000bps}$$

Es decir, el trafico por navegar en Internet será de 1.32 Mbps aproximadamente, que es perfectamente soportado por el ancho de banda disponible.

Ahora bien, en cuanto a la transferencia de archivos, mucho va a depender del tamaño de ellos. En general, la transmisión de archivos, documentos, MP3 y demás información, producen una carga mucho mas alta que la de Internet, por tanto, es importante disponer de una adecuada capacidad y velocidad de transmisión de datos, de manera que no se afecte la calidad de servicio.

En lo que se refiere a la telefonía IP, el tráfico generado es muy sensible a los delays (retrasos), más cuando se lo hace en una red inalámbrica. La carga que produce no es significativa, gracias a los codecs (codificadores de voz) que comprimen la voz y utilizan muy poco ancho de banda. Así, para la norma G.729 que usa una compresión de voz de 8Kbps[4] si los 110 usuarios usaran sus softphones al mismo tiempo, se tendrían la siguiente carga en la red:

$$\boxed{8000 \times 110 \times 2 = 1760000 bps}$$

El ancho de banda utilizado por VoIP será de aproximadamente 2Mbps. En términos de ancho de banda, no habrá ningún problema, ya que nuestra red dispone de 100 Mbps, lo que satisface ampliamente las necesidades. Ahora bien, la telefonía IP sobre una WLAN tiene cierta dificultad, en lo que se refiere a la técnica de acceso al medio, lo que conlleva a analizar que tan factible es implantar telefonía IP sobre la red inalámbrica diseñada.

4.4.1.1. Voz sobre una red inalámbrica. Combinar voz con tráfico de datos introduce algunos desafíos a la red debido a los requerimientos de la comunicación de voz. La voz es una aplicación en tiempo real que requiere baja latencia y "entrega segura" dentro de la red. En redes de voz y datos, los mecanismos de calidad de servicio (QoS) son necesarios para conseguir una buena calidad de voz.

Proveer conectividad inalámbrica para aplicaciones de datos es más sencillo y comprobable, mientras que para aplicaciones de voz es más complejo y requiere mayor planificación y consideraciones.

El estándar original de acceso al medio de la IEEE 802.11 entrega una Función de Coordinación Distribuida (Distribuied Coordination Function) para transmitir sobre el medio que es el aire, entre suscriptores y Access points. El estándar utiliza una técnica conocida como Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), para "escuchar antes de enviar" información sobre el aire. Como se sabe, cuando existen muchos usuarios finales dentro de la misma área de cobertura, el ancho de banda se ve

[4] Tasa de compresión especificada por el estándar del codec G.729A.

afectado. Cuando dos o mas usuarios intentan transmitir al mismo tiempo, una colisión ocurre. Para evitar estas colisiones, cada suscriptor debe esperar un periodo de duración randómica, conocido como intervalo randomico Backoff. El backoff es un contador que es reducido solo cuando el medio esta desocupado. Los dispositivos suscriptores deben escuchar y ver si el medio esta libre para intentar transmitir de nuevo. Si una colisión ocurre el backoff es incrementado en los puntos finales. Como resultado, muchas colisiones pueden producir retardos y pérdidas de paquetes soportando algunas aplicaciones y usuarios, lo cual incide en la calidad de audio y la cancelación de llamadas.

4.4.1.1.1. Calidad de Servicio (QoS). Los flujos de voz y datos tienen diferentes requerimientos de red. La mayoría de las aplicaciones pueden soportar perdidas de paquetes, porque el protocolo TCP puede retransmitir los paquetes perdidos para asegurar una entrega segura. Las retransmisiones introducen retardos, los cuales son perceptibles en comunicaciones de tiempo real, como la voz, rompiendo el flujo de una conversación de voz y haciendo difícil que las personas puedan entender lo que escuchan. Sin embargo, las comunicaciones de voz sobre IP (Internet Protocol) pueden lograrse con mínimos retardos, mínima perdida de paquetes y mínimo jitter (variaciones en los retrasos). Los mecanismos de calidad de servicio son necesarios para conseguir estos niveles de servicio en ambientes 802.11.

La IEEE ha ratificado un estándar de Calidad de Servicio conocido como 802.11e para promover la interoperatibilidad entre marcas, permitiendo a los usuarios la capacidad de seleccionar entre alguna de ellas.

Wi-Fi Multimedia (WMM) soportara dos modos de operación conocidos como Enhanced Distributed Coordination Function (EDCF), llamado comúnmente como WMM, y Hybrid Coordination Function (HCF), conocido como WMM Scheduled Access, que todavía esta en desarrollo.

4.4.1.1.1.1. WMM. Este estándar permite distinguir entre diferentes aplicaciones contenidas para un mismo ancho de banda, y trata la entrega de cada aplicación a la vez, basado en ciertas características de tráfico.

Define cuatro categorías de acceso: voz, video, best effort y background. Estas cuatro categorías son descritas en la Tabla 4.5.

Tabla 4.5. Categorías de Acceso de Wi-Fi Multimedia

Categoría	Descripción
Voz	Categoría de prioridad más alta, diseñada para permitir múltiples Llamadas IP. Provee a los paquetes de voz baja latencia para alta calidad en las comunicaciones.
Video	Permite que el video sea transportado con prioridad sobre aplicaciones de datos, pero un poco abajo de las comunicaciones de voz.
Best Effort	Diseñada para transportar trafico de aplicaciones que carecen de capacidades de QoS. Trafico promedio de un usuario, como navegar en Internet, porque es menos sensitivo a la latencia, pero grandes retardos pueden llegar a ser inaceptables.
Background	Categoría de más baja prioridad, diseñada para trafico que no es sensitivo al retardo. Por ejemplo, descargar archivos o imprimir trabajos.

Cada aplicación viaja a través del aire a su destino que puede ser un dispositivo suscriptor o AP habilitados con WMM, y es primeramente clasificado dentro de las cuatro categorías y movidas dentro de una cola de envió apropiada. Si un suscriptor esta soportando varias aplicaciones, y si todas intenta transmitir al mismo tiempo, ocurrirá una colisión internas entre ellas. Cuando esto sucede la lógica de cola debe resolver la colisión internamente. La lógica interna de la cola es ilustrada en la figura 4.10.

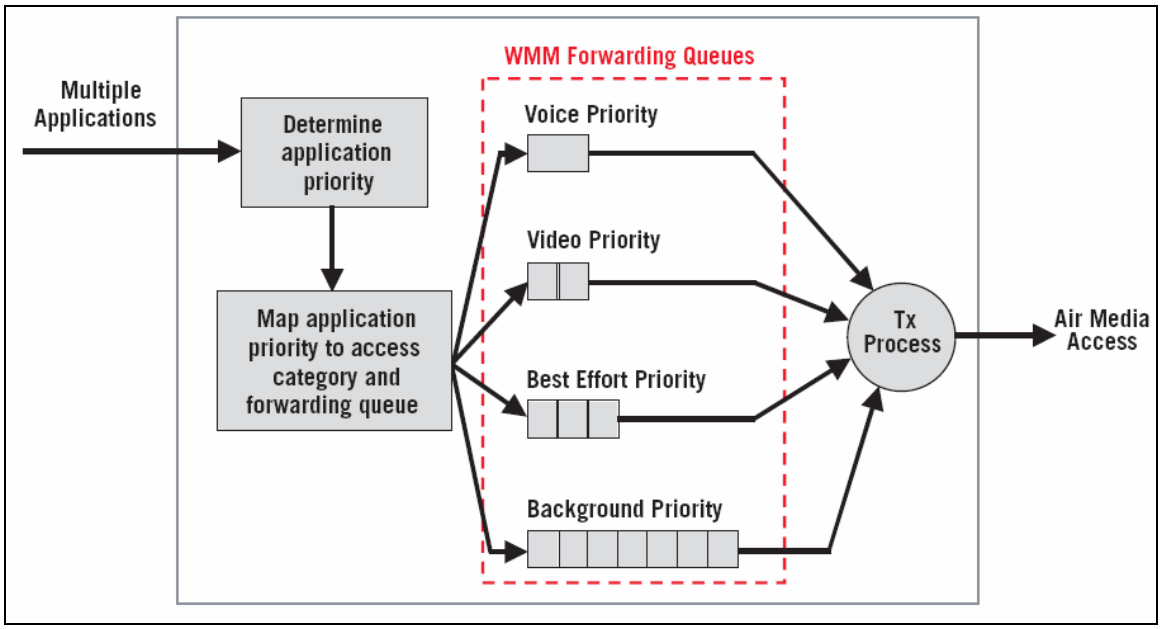


Figura 4.10. Lógica interna de cola en WMM

Una vez que un suscriptor o un AP tienen la oportunidad de transmitir, los datos son selectivamente transmitidos usando un set único de parámetros de acceso al medio, de acuerdo a la categoría de acceso de las aplicaciones. Los diferentes niveles de servicio son proporcionados por la diferencia de AIFS (arbitration inter frame space), CW (contention window size) y TXOP (transmit opportunity) de cada categoria de acceso.

1. **AIFS (arbitration inter frame space) :** especifica el intervalo de tiempo entre las negociaciones de medio desocupado y empezar el acceso al medio. Cada categoría es asignada con un valor diferente de AIFS. El trafico con categoría de acceso alta recibe un valor bajo de AIFS, y viceversa. El resultado es un favorable TXOP para el tráfico de más alta prioridad.

2. **CW (contention window size)** : es una función de la categoría de acceso. Las categorías con la más alta prioridad tienen un rango corto de CW a seleccionar. Esto corresponde a menos slots de backoff atravesados por transmisión, en promedio.

3. **TXOP (transmit opportunity)** : el limite de TXOP especifica la duración que un suscriptor puede transmitir para una categoría de acceso dada. Puede ser usada para

dar acceso largo para tráfico de alta prioridad, que a los de media y baja prioridad a los que se les da un corto acceso.

Cuando se detecta que el medio inalámbrico esta desocupado por un periodo AIFS, cada estación inicializa un contador en un numero randomico seleccionado uniformemente sobre el parámetro CW. El tiempo es particionado y el contador es disminuido en uno durante cada partición en que el medio es observado como desocupado. Una característica importante es que la cuenta descendente se mantiene cuando el medio llega a estar ocupado y continua después de que el medio esta libre por un periodo AIFS. Una vez que el contador llega a cero, la estación intenta transmitir y puede hacerlo por una duración de tiempo máximo TXOP. Si más de una estación intenta transmitir simultáneamente, ocurre una colisión. Las estaciones que chocan doblan su CW, al valor máximo permitido, CWmax, seleccionan un nuevo contador backoff uniformemente y el proceso se repite. Después de una transmisión exitosa, CW es reseteado a su mínimo valor, CWmin, y una nueva cuenta descendente empieza sin tomar en cuenta la presencia de un paquete en la capa MAC. Si el paquete llega a la MAC después de que la cuenta esta completada, la estación censa el medio. Si el medio esta desocupado, la estación intenta transmitir inmediatamente; y si esta ocupado, otro contador es escogido desde un intervalo mínimo.

4.4.1.1.2. Control de Admisión de Llamadas. Existen otros inconvenientes que pueden afectar adversamente la calidad de voz, esto ocurre cuando algunos usuarios con la misma alta prioridad luchan por el mismo ancho de banda de un Access point. Esto se conoce como *sobre suscripción.* La sobre suscripción de ancho de banda ocurre cuando N+1 usuarios intentan transmitir voz, o datos, o los dos al mismo tiempo, pero solo existe ancho de banda para soportar N usuarios. Esto introduce colisiones excesivas y perdidas de paquetes, lo cual puede degradar la calidad de audio para todas las transmisiones de voz asociadas con la sobrecarga del AP.

Un control de admisión de llamadas debe ser usado para restringir nuevas llamadas una vez que el límite de usuarios o de ancho de banda ha sido alcanzado. En redes convergentes, datos y voz, esto requiere que todos los dispositivos, incluyendo laptops.

PC's, compartan un mecanismo de QoS común, que pueda habilitar o negar a usuarios de voz o datos de acuerdo a las políticas predefinidas.

4.4.1.1.3. Evaluación Experimental. Para verificar que este tipo de red funcione, es necesario hacer ciertas evaluaciones en los parámetros descritos anteriormente. En este caso, no es posible hacerlo en la práctica, ya que como se trata de un estudio de ingeniería no se dispone de los equipos en estos momentos. De todas maneras se va ayudar de una evaluación experimental[5] hecha por los propios fabricantes, lo cual hacen para mostrar a sus clientes los beneficios de sus equipos en este tipo de redes.

El nuevo protocolo MAC 802.11e extiende el mecanismo del estándar 802.11 CSMA/CA permitiendo el ajuste de los parámetros MAC que fueron previamente manipulados. Antes ha habido muchos estudios abstractos sobre este protocolo, ya que no existía el hardware para comprobarlo. Ahora, el hardware esta disponible lo cual permite investigar la operación de 802.11 EDCA (WMM) en un ambiente real de prueba.

Como se lo dijo anteriormente, el tráfico de datos tiene un impacto adverso en la calidad de servicio de una llamada de voz en una WLAN. La figura 4.11. muestra la medida de throughput de una llamada de voz de 64 Kbps versus el numero de estaciones en la red. Se nota claramente que a medida que aumenta el número de estaciones el throughput disminuye.

[5] "Experimiental Evaluation of 802.11e EDCA for Enhanced Voice over WLAN Performance", por Ian Dangerfield, David Malone, Douglas Leith,

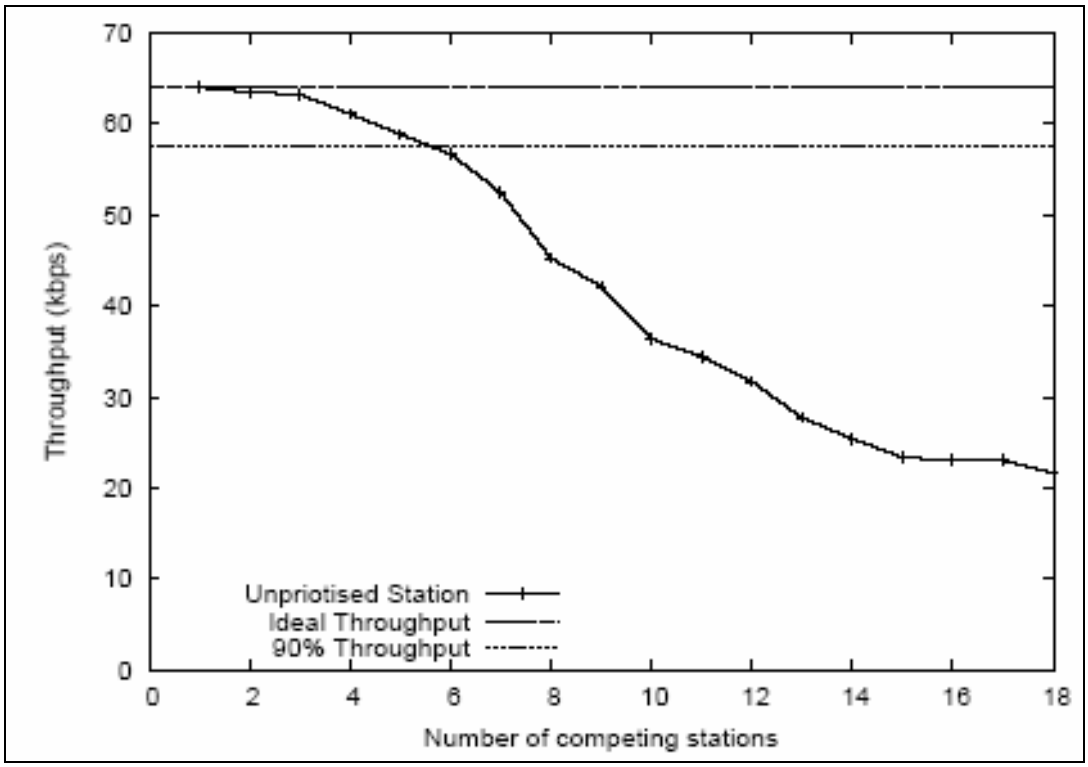


Figura 4.11. Throughput de una llamada de voz vs numero de estaciones

Solo son necesarias 5 estaciones que envíen datos para inducir a una disminución de la tasa de bit de una llamada de voz que exceda el 10% de disminución de throughput, lo cual en la practica produce una disminución en la calidad de voz y hasta la perdida de comunicación entre estaciones.

El estudio en el que se basa, esta enfocado en hacer una medición experimental del desempeño de la solución propuesta por el estándar 802.11e. Se presenta una técnica práctica para medir el retraso entre las capas MAC del estándar 802.11 y se combina esta técnica con la sintonización de los parámetros de la misma capa descritos anteriormente, para demostrar que la voz sobre una WLAN puede ser protegida del tráfico de datos.

Se variara los parámetros AIFS, Cwmin y TXOP en esta evaluación. AIFS es ajustable en unidades de medida de slot. Cwmin es sintonizada en potencias de 2, y TXOP es una medida de tiempo, especificada en microsegundos.

Entonces, se empieza haciendo una variación en TXOP de dos estaciones de una WLAN 802.11b. Las dos estaciones están saturadas, es decir, siempre tienen un paquete

para enviar, por tanto el backoff asociado estará presente en las mediciones. Una estación tiene su TXOP modificado de tal manera que solo puede transmitir un paquete en cada oportunidad de transmisión. Se varió el TXOP de la otra estación, el figura 4.12. muestra el throughput conseguido por ambas estaciones y el throughput total del sistema.

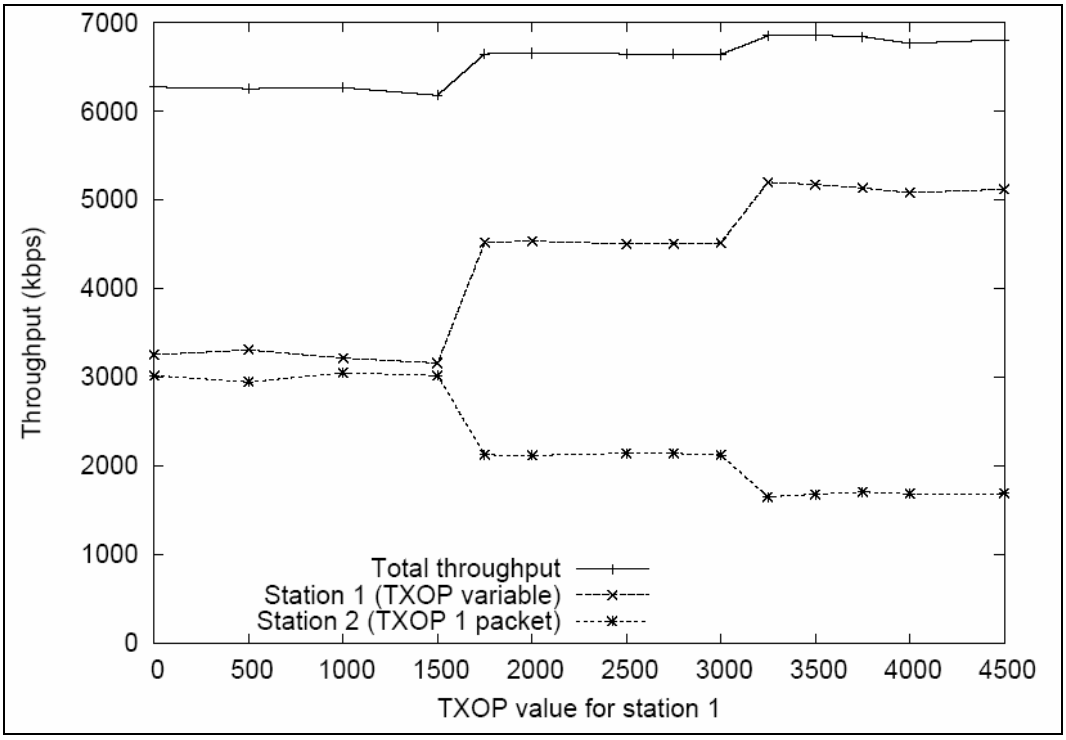


Figura 4.12. Impacto de TXOP sobre dos estaciones saturadas.

Nótese que el throughput total del sistema se incrementa conforme se incrementa TXOP, debido a que la contención esta amortizada para muchos paquetes.

La figura 4.13. muestra el retraso promedio medido para la estación que tiene el TXOP variable, y el producto del retraso medido por el throughput medido. Para las estaciones saturadas, este producto debe ser la medida del paquete. Como se esperaba, se observa que el delay promedio de las estaciones saturadas disminuye, mientras que el producto throughput-delay se mantiene aproximadamente constante en 1470 bytes.

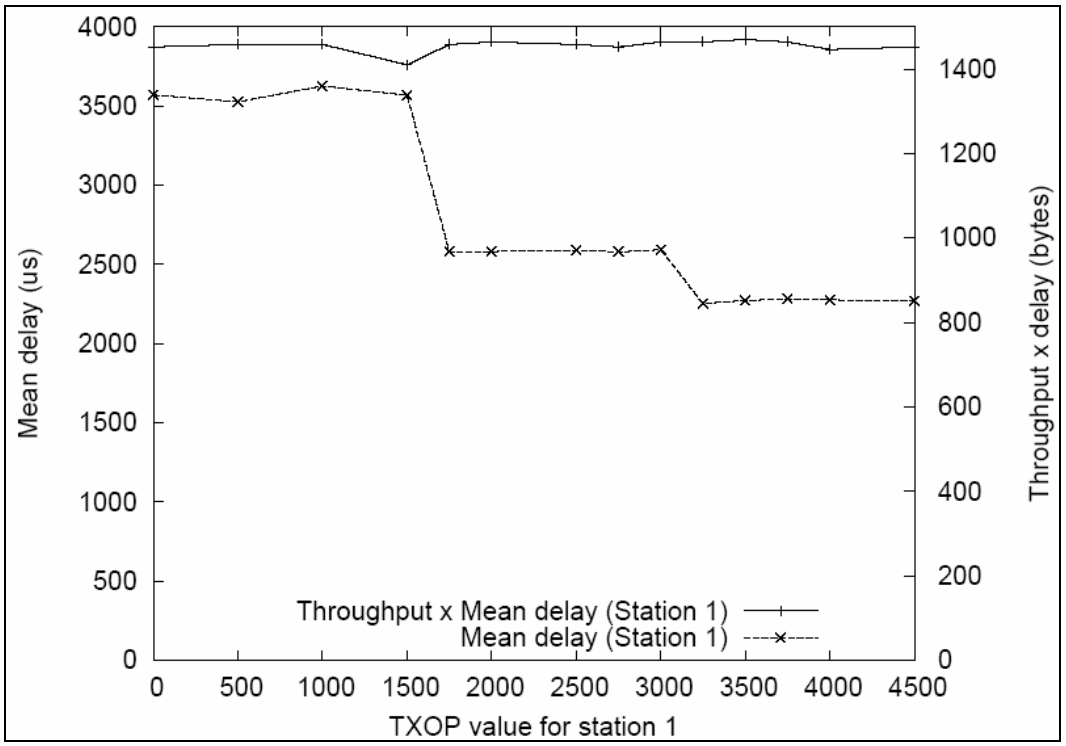


Figura 4.13. Impacto de TXOP sobre dos estaciones saturadas (2).

La siguiente prueba que se hizo, fue mantener el Cwmin para una estación, mientras se vario el mismo parámetro de la otra estación (en potencias de 2).

En las figuras 4.14 y 4.15, se observa que al duplicar CWmin, el efecto es que existe una duplicación de cuantos slots la estación debe contar en promedio, resultando en un doblete del delay promedio. El throughput esta aproximadamente en proporción al valor de Cwmin.

Además se nota que, el throughput total cae cuando se incrementa este parámetro. Esto es porque el Cwmin óptimo para dos estaciones saturadas es pequeño, mucho menos que 15.

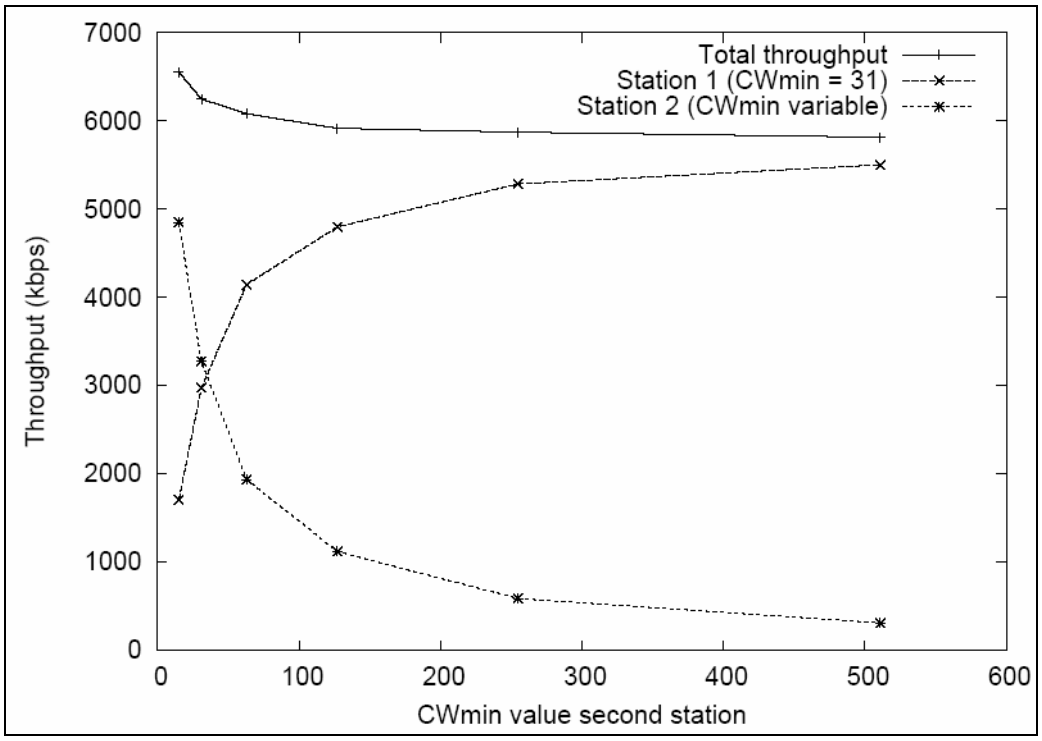


Figura 4.14. Impacto de CWmin sobre dos estaciones saturadas

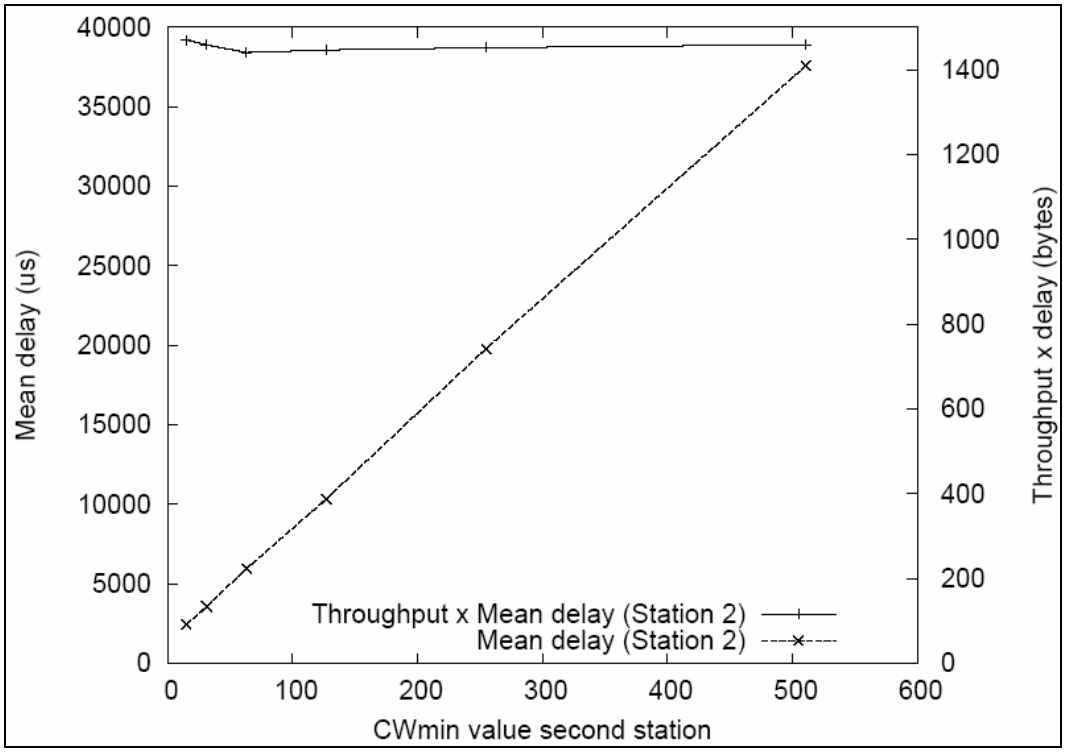


Figura 4.15. Impacto de CWmin sobre dos estaciones saturadas (2)

El siguiente ensayo que se hizo fue con el tercer parámetro, es decir con AIFS. Las s figuras 4.16 y 4.17, muestran como este parámetro cambia el throughput y el delay.

Es esperado que el efecto que tendrá AIFS sea dependiente de la carga, y se ve que para dos estaciones, este parámetro tiene un menor impacto que modificar Cwmin, en términos de separación de throughput y delay. También, esto causa una pequeña disminución en el throughput total de sistema, debido a que una estación debe esperar más tiempo para acceder al medio.

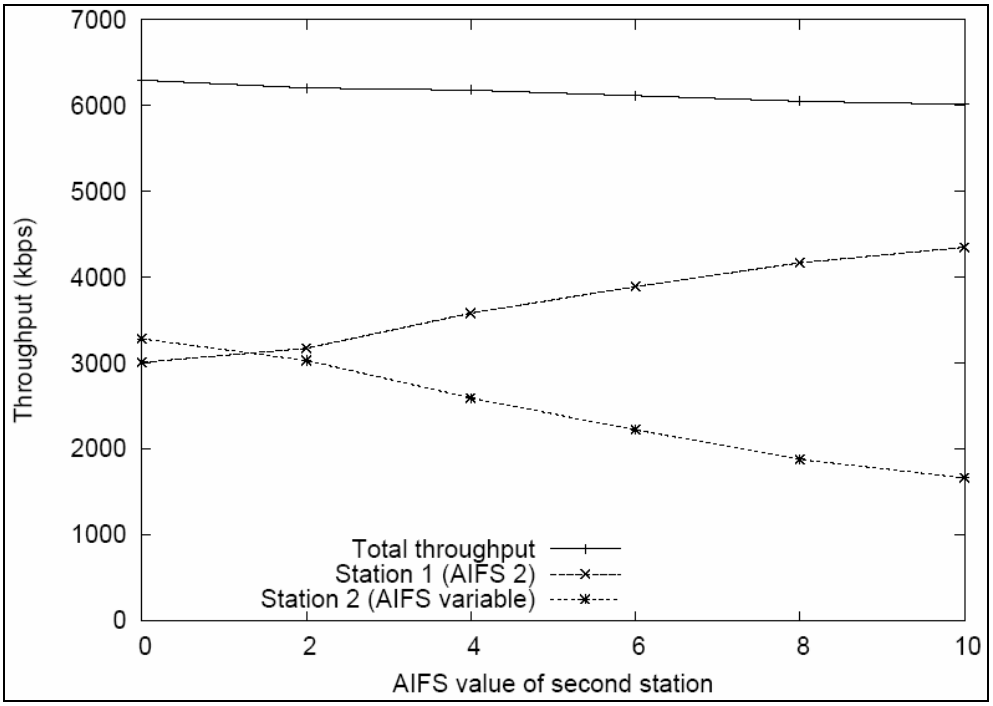


Figura 4.16. Impacto de AIFS sobre dos estaciones saturadas

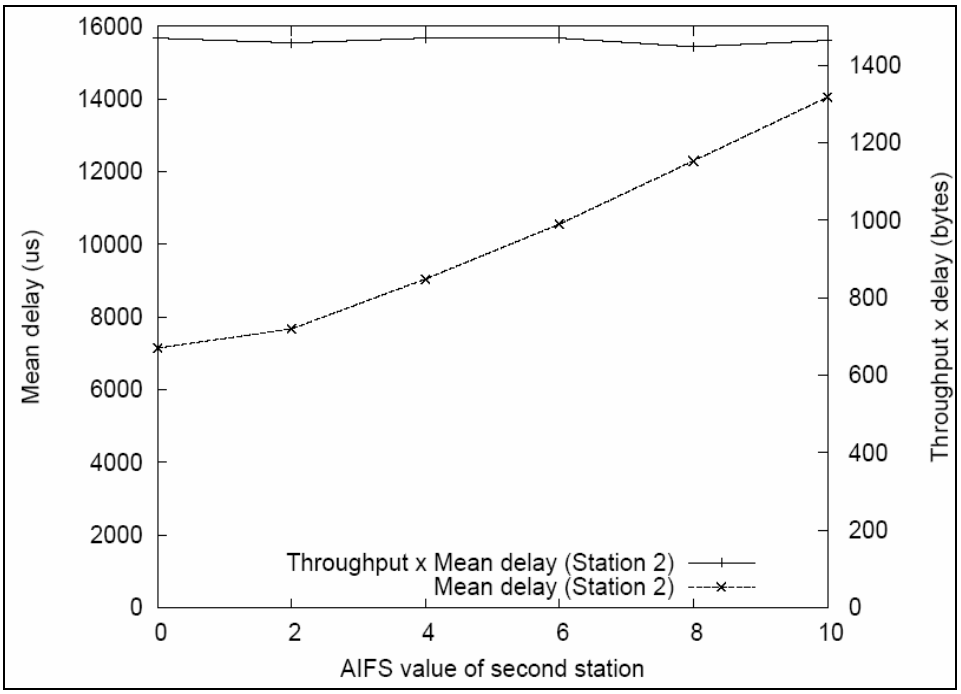


Figura 4.17. Impacto de AIFS sobre dos estaciones saturadas (2)

El objetivo se centra en priorizar la voz sobre los datos. Una vez estudiados los efectos que producen los parámetros MAC al modificarlos, ahora es posible encontrar un camino para alcanzar el objetivo.

El esquema que utiliza este estudio para priorizar la voz es simple: se incrementa el valor de AIFS usado por las otras estaciones[6]. Incrementando el valor de AIFS resulta en un incremento del delay después de cada transmisión en la red antes de que la estación pueda continuar decrementando sus contadores. Por tanto el efecto notable, es que AIFS es más fuerte conforme la carga aumenta, se espera entonces que, cuando la carga aumente, una modificación del valor de AIFS sea suficiente para conseguir el objetivo de calidad de servicio para la voz.

Se considera una muestra de voz de 64 kbps transmitidos cada 10 ms. Cada paquete tiene una carga de 80 bytes. La llamada de voz comparte la red con un número de estaciones que están saturadas, transmitiendo paquetes de 1470 bytes cuando la MAC lo

[6] Seria preferible reducir este valor en vez de aumentarlo, sin embargo esto esta fuera del alcance del estándar, ya que puede interferir con el manejo de transmisión de tramas y ACKs.

permita. Cada experimento de lo hizo durante 20 minutos para un numero pequeño de estaciones, y durante 30 minutos para mas estaciones. Esto se lo hizo porque, cuando no esta priorizada la voz, el throughput cae rápidamente, por tanto se tuvo que hacer el experimento durante un buen tiempo para transmitir suficientes paquetes para acumular retrasos estáticos exactos.

La figura 4.18. muestra que a medida que aumenta el número de estaciones, el delay se incrementa significativamente. Además se observa, que en contraste con el caso de sin priorizacion, al modificar los valores de AIFS en 4 y 6 respectivamente, el throghput se estabiliza.

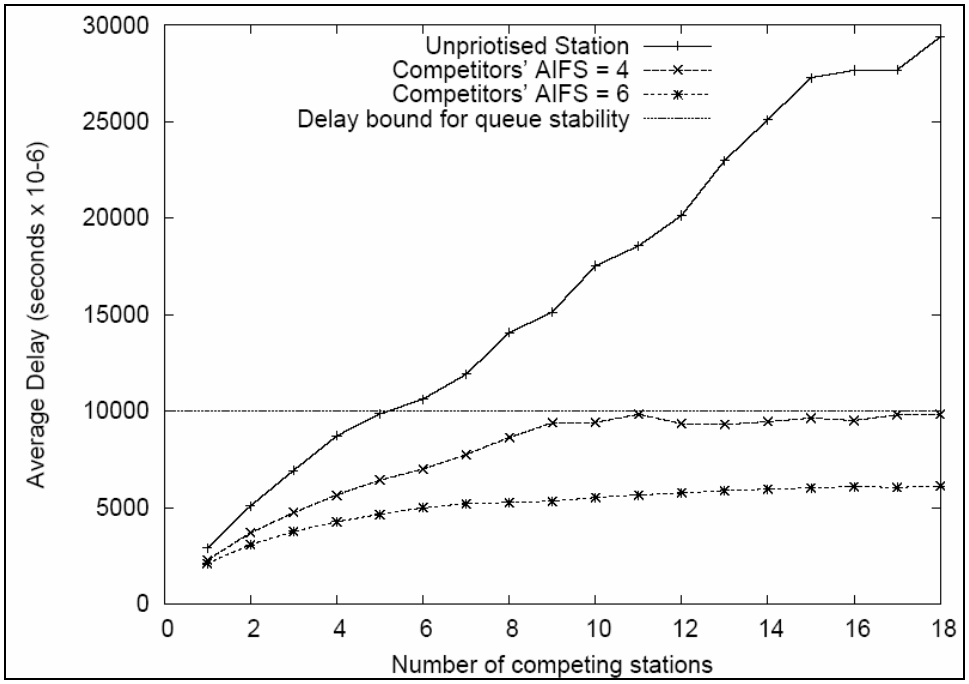


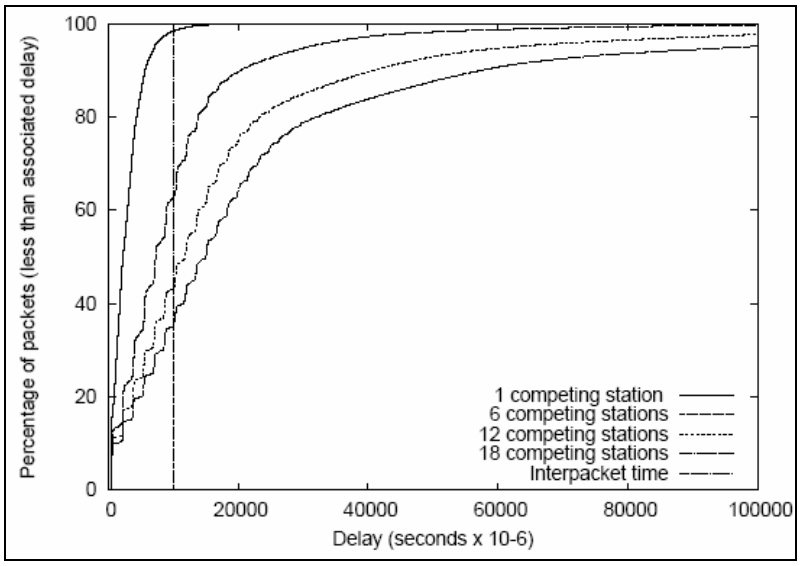
Figura 4.18. Delay promedio para una llamada de voz con estaciones saturadas.

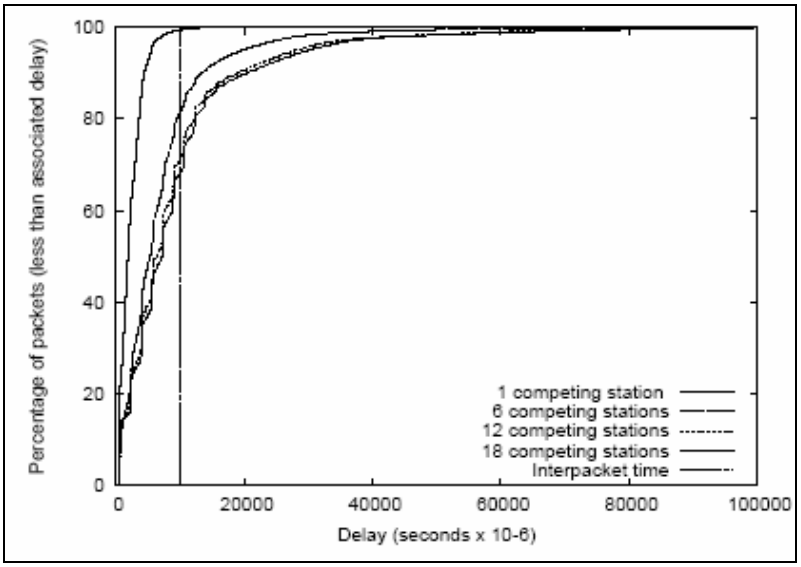
Esto confirma que un valor modificado de AIFS, será suficiente para priorizar una llamada de voz contra un número grande de estaciones.

Un AIFS con valor de 4, puede ser usado para mantener el delay promedio justo por debajo del Inter Packet Time, el cual es requerido para que la cola sea estable; y mantiene el throughput en un 90%.

Un AIFS de 6, mantiene el delay promedio muy por debajo del Inter Packet Time y consigue un throughput total.

Sin embargo, no solo el delay promedio es importante. La figura 4.19 muestra como los tiempos de transmisión son distribuidos cuando la llamada de voz no esta priorizada, priorizada con AIFS de 4 y de6.





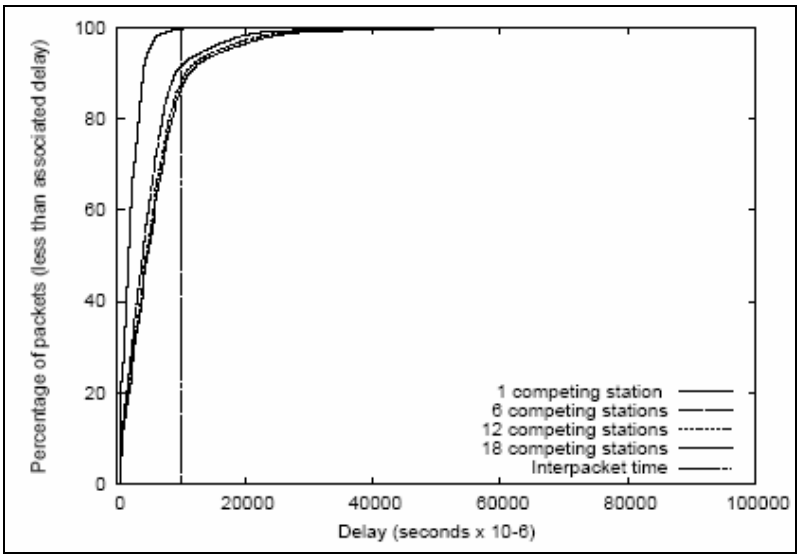


Figura 4.19. CDF para el delay de una llamada no priorizada, con AIFS=4, con AIFS=6.

Estos gráficos muestran una curva regular correspondiente al número de paquetes transmitidos antes de que cada paquete de voz sea exitosamente transmitido.

En el caso de la llamada no priorizada, se observa que con 12 estaciones simultaneas, menos de la mitad de los paquetes de voz pueden ser despejados antes que los otros paquetes lleguen. Para los casos priorizados, se observa que la distribución del retraso varía menos al considerar un gran número de estaciones. Casi el 70% de los paquetes pueden ser despejados antes que los otros lleguen, cuando AIFS es 4; y en un 90% cuando AIFS es 6.

Se dijo anteriormente que, la medida del paquete estaba dada por el producto de throughput por el delay promedio, en estaciones saturadas. En la figura 4.20, se muestra este producto, dimensionado para que la medida del paquete sea 1. Esto representa la porción de tiempo que la capa MAC que maneja la llamada de voz tiene un paquete para transmitir.

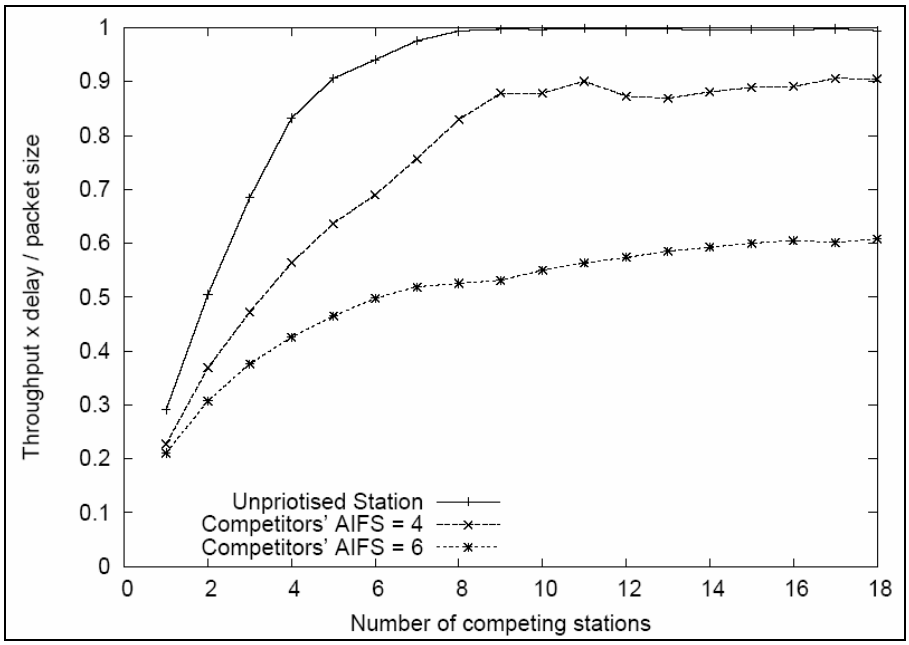


Figura 4.20. Porción de tiempo que la capa MAC esta ocupada

Como se observa, la modificación de los valores de AIFS, previene que la capa MAC llegue a estar saturada.

4.4.1.1.4. Solución para VoIP. Una vez analizados los parámetros MAC, ahora se puede determinar con certeza que la red mixta, voz y datos, va funcionar de una manera confiable y segura, modificando estos de acuerdo a las necesidades de la red.

En el mercado existen pocas marcas comerciales que ofrecen AP con la capacidad de modificar los parámetros MAC del estándar 802.11e. Se tiene que buscar estos AP para conseguir el funcionamiento deseado de la red. Además, se va a utilizar un servidor de voz, llamado Asterisk, para el manejo de las llamadas tanto internas como externas de esta institución.

Como se dijo anteriormente, se va utilizar softphones en cada usuario de la red para realizar las llamadas de voz. Esto reducirá los costos, ya que la alternativa de usar la red telefónica y adaptarla para usar VoIP resulta demasiado cara; inclusive comprar teléfonos de escritorio o móviles que soporte esta tecnología acarrea una gran inversión.

4.4.1.1.4.1. Servidor Asterisk. Es una completa solución de comunicaciones "open source" que utiliza la red LAN, Internet y la Red Telefónica Pública, ofreciendo además un sin número de aplicaciones que permiten tomar ventaja de la convergencia entre comunicaciones de voz, datos, y la Telefonía IP.

Es un sistema de comunicaciones inteligentes basado en software libre. Convergen aplicaciones de voz, datos y video. Hay que resaltar que Asterisk es un software, exclusivamente software, y que actúa como un soft-switch, es decir una PBX – IP.

Se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una PSTN.

Soporta y traduce distintos protocolos de VoIP como SIP, MGCP y H.323. Se ejecuta en PC estándar (arquitectura x86_32, x86_64) bajo GNU/Linux. Además, soporta todas las funcionalidades de las PBX tradicionales y muchas más!

Asterisk es capaz de trabajar con prácticamente todos los estándares de telefonía tradicional: Líneas analógicas FXS, FXO, o líneas digitales: E1, T1, ISDN.

El esquema conceptual de funcionamiento se detalla en la figura 4.21.

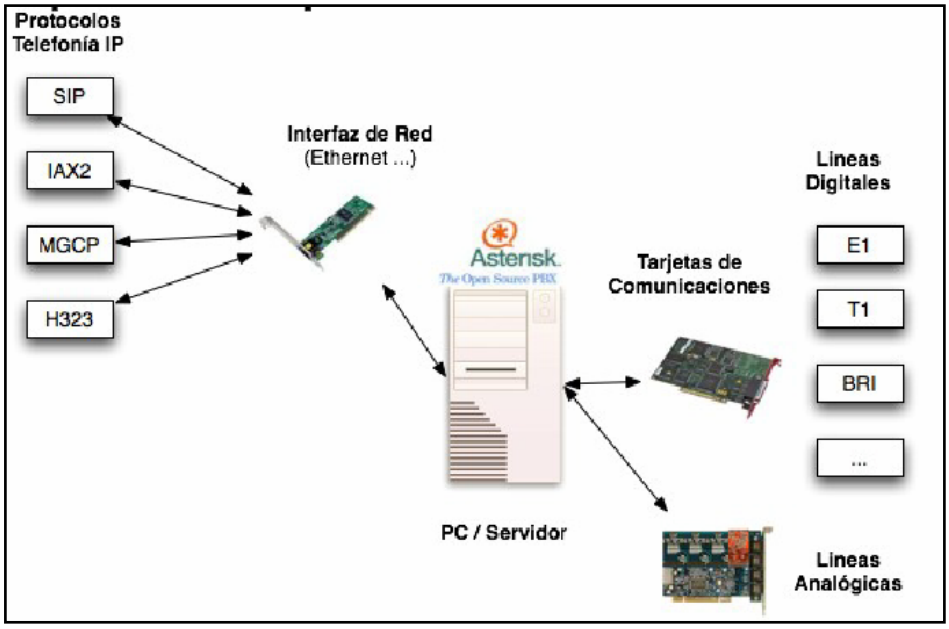


Figura 4.21. Esquema de funcionamiento de Asterisk

Algunas de las facilidades que ofrece este servidor son las siguientes:

- Transferencia
- Transferencia Atendida
- Llamada en espera
- Caller ID
- Bloqueo de Caller ID
- Timbres distintivos
- Música en espera
- Salas de Conferencia (10 simultáneos)
- Call Back (recogida de llamada)
- Call Group
- Buzón de Voz personal.
- Colas de llamada
- Colas con prioridad.
- Registro de llamadas en Base de Datos.
- Buzón de Voz por Mail.
- Pickup de llamadas.
- Desvío si ocupado.
- Desvío si no responde.
- Música en transferencia.
- Búsqueda en Bases de Datos.

Existen además funciones avanzadas, que hacen de Asterisk un verdadero servidor de comunicaciones:

- **IVR**: Interactive Voice Response, gestión de llamadas con menús interactivos.
- **LCR**: Least Cost Routing, encaminamiento de llamadas por el proveedor VoIP más económico.
- **AGI**: Asterisk Gateway Interface, integración con todo tipo de aplicaciones externas.
- **AMI**: Asterisk Management Interface, gestión y control remoto de Asterisk.

- Configuración en base de datos: usuarios, extensiones, proveedores ...
- Tablero de control de monitoreo en Tiempo Real.
- Grabación de llamadas total o bajo demanda.
- Marcación Predictiva, Progresiva y Selectiva.

Se sabe que un software de tales prestaciones y realizando funciones tan importantes, necesita que el servidor sea de características robustas. Principalmente, Asterisk requiere Procesador Intel, 1Gb de RAM. Según Digium: Equipo Dual Intel Xeon 1.8 Ghz 1 Gb RAM soporta 60 llamadas concurrentes codificando con el codec G.729.

Los principales beneficios que se obtienen al utilizar esta tecnología son los siguientes:

- Plan de marcado inteligente.
- Monitor de llamadas entrantes y salientes online.
- Una sola red IP, para todas las llamadas internas y nacionales.
- Ahorro en más del 40% en las planillas telefónicas.
- Usuarios internos móviles a cualquier parte del mundo.
- Software compatible con todos los equipos Voip SIP.

4.4.2. Backbone de la red LAN

Esta claro que la conexión de los dos AP de cada planta ha de ser hacia un concentrador tipo switch que soporte QoS, ubicado en el respectivo cuarto de comunicaciones. Como las distancias son cortas, el enlace será a través de cable UTP CAT5e, el más común de las redes LAN Ethernet.

Todo el tráfico de datos y voz captado por los AP de los terminales de usuarios encausado hacia el switch del edificio, conformando las estrellas de la topología seleccionada para esta red.

El sistema de distribución de AP debe tener capacidad para soportar un nivel de tráfico mayor al soportado por las conexiones Fast Ethernet o 100 BaseT, a 100 Mbps. Este

sistema de distribución constituye el backbone o troncal de la red LAN, que canalizará todos los paquetes provenientes del switch, hacia el servidor de datos y al servidor de voz, que también "enfrentaran" todo el sistema hacia el Internet.

Será necesario un soporte de pared o de piso, pequeño, donde se instalara el switch. En este soporte deberá organizarse todo el cableado, utilizando patch panels, face plates, match coros, jacks, etiquetas, etc.

La protección de todo el cableado deberá realizarse principalmente con canaleta decorativa, como en las oficinas, donde la estética es importante.

Determinados ya todos los elementos, parámetros y componentes de la red LAN y de la WLAN, queda terminado el diseño físico de la Intranet para la A.Z.V.CH.

En la figura 4.22. se ofrece un esquema general de la intranet completa, con detalle de la red LAN, la WLAN, así como algunos usuarios.

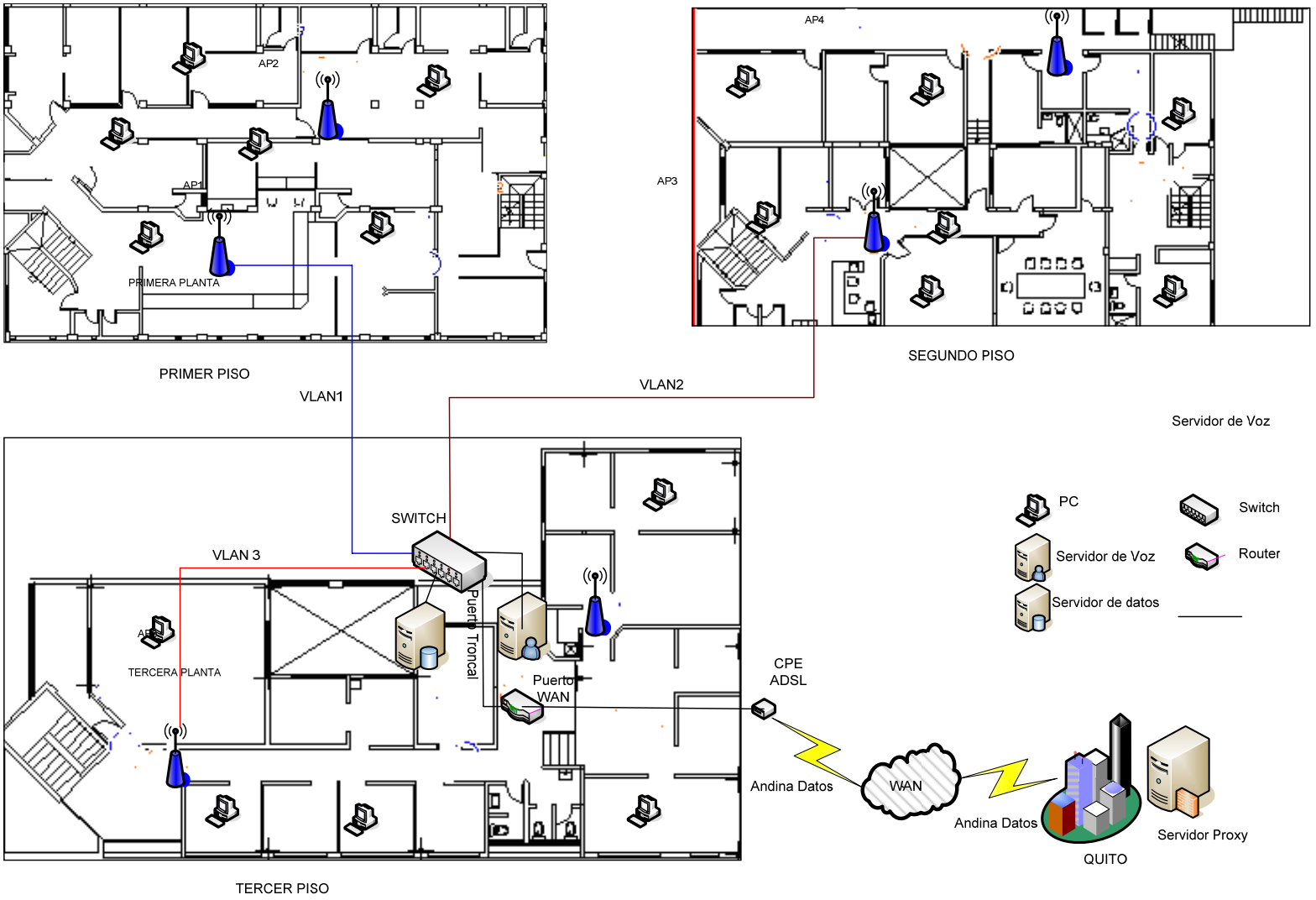


Figura 4.22. Esquema General de la Intranet

4.4.3. Bases técnicas de equipos de red LAN

4.4.3.1. Switch de Backbone

1. Un switch capa 2, tipo Giga Ethernet 10/100/1000 BaseT, mínimo 8 puertos, que soporte el estándar 802.11e (QoS). Además que permita la configuración de VLANs.

4.4.3.2. Router de Backbone

1. Router 4 puertos LAN/DMZ switch: 10/100 Mbps Ethernet , Puerto WAN: 10/100 Mbps Ethernet, que soporte VLAN, firewall

4.4.3.3. Tarjetas de red NIC para servidores

1. Tarjeta de red 32/64 bits, tipo Giga Ethernet 10/100/1000 BAseT

4.4.3.4. Servidor de Voz

1. Equipo Dual Intel Xeon 1.8 Ghz 1 Gb RAM, sugerido por Digium.

4.4.3.5. Tarjetas Análogas

1. Tarjeta análoga compatible con Asterisk, mínimo 4 puertos FXO

4.5. FUNCIONAMIENTO GENERAL DE LA RED MIXTA VOZ Y DATOS.

En la figura 4.22. se tiene el esquema de red total para la A.Z.V.CH. Este permitirá la comunicación tanto de datos como de voz a través de la misma. A continuación, voy a dar una breve descripción del funcionamiento y configuración que deben tener cada uno de los elementos que componen esta red mixta.

En primer lugar, como se dijo en secciones anteriores, los AP a utilizar deben soportar el estándar 802.11e. Este, permite priorizar el tráfico en una red mixta como la del estudio. Además de soportar este estándar, al momento de configuración, debe permitir la modificación de los parámetros MAC, como se vio anteriormente, de manera que se pueda tener una red eficiente, y que pueda transportar voz y datos sobre la red

inalámbrica, sin perder calidad de voz en las llamadas. Un ejemplo de configuración de estos parámetros se muestra en la figura 4.23.

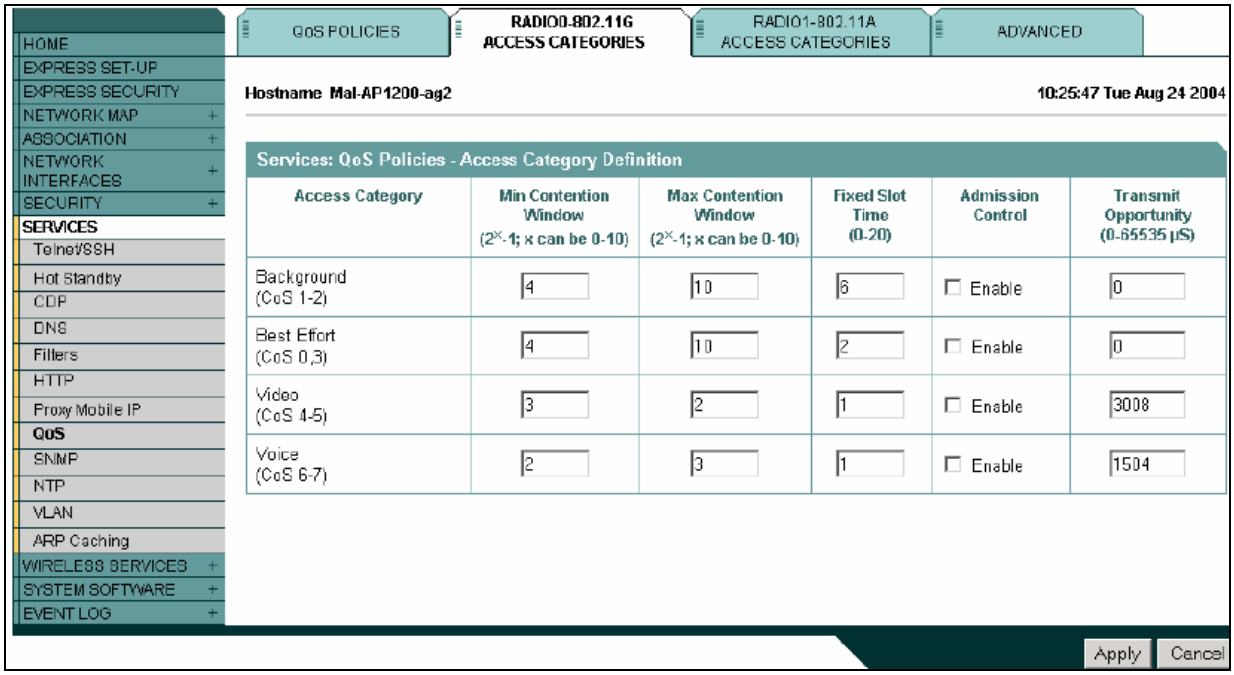


Figura 4.23. Ajuste de los parámetros MAC de 802.11e

Esto permite tener control sobre la manera en que los paquetes, tanto de voz como de datos, acceden al medio inalámbrico. La configuración final dependerá mucho de los requerimientos de la red y es necesario instalar la red y de esa manera ir haciendo pruebas hasta encontrar el funcionamiento correcto. Claro, se puede basar en el estudio realizado anteriormente, y partir desde ahí, para encontrar la configuración optima.

Cabe indicar que como hay dos AP por cada piso, uno de ellos va actuar como master, mientras que el otro lo hará en forma de bridge, permitiéndonos utilizar solo una de las tres frecuencias no traslapadas del estándar 802.11g para un piso. Esta configuración nos permite salvar un problema como es la interferencia co-canal que se da frecuentemente cuando se utiliza el estándar 802.11g. Obvio, toda esta configuración se lo hará a través de la interfase Web del AP.

El siguiente paso es segmentar la red. Los cables UTP que salen de los AP van hacia un switch administrable, lo que permite la disminución del tamaño del dominio de colisión, ya que cada AP master tendrá un puerto asignado en el switch. Adicionalmente, usando la característica de que el switch es administrable, se crearan

VLANs por cada piso, para limitar el dominio de broadcast, y de esta manera tener la ventaja de una red segura y flexible. Para esto, se habilitaran subredes, a partir de la IP dada por la Dirección Metropolitana de Informática, haciendo una subred por cada piso, entonces se tendrán tres subredes, las cuales a la vez, serán una VLAN cada una. Además, en el switch irán conectados tanto el servidor de datos como el servidor de voz (Asterisk).

A través del puerto trunk del switch se conecta mediante cable UTP al router, el cual nos va a permitir la distribución de Internet en todo el edificio, como también, el envío y la recepción de datos entre las diferentes VLANs de la red, gracias a que el router conmuta paquetes entre ellas. Para esto, se debe configurar el router adecuadamente, para que el funcionamiento de la red sea el deseado.

En cuanto al servidor de voz, se usara el software Asterisk, el cual es una IP PBX, que permitirá la comunicación interna como externa de la administración. Adicionalmente, se instalara y configurara los drivers necesarios para el uso de SJ softphones, en todas las PCs de la red.

Gracias a la versatilidad de Asterisk, se puede crear las extensiones necesarias en el edificio, solamente programándolas y asignándolas las direcciones IP de cada computador. Un gateway de voz estará conectado al servidor, y a este llegaran las 8 líneas telefónicas disponibles de la administración. De igual manera, se puede programar los puertos por los que se quiere realizar una llamada hacia el exterior, además de otras facilidades que ofrece este software.

4.6. FUNCIONAMIENTO LÓGICO DE LA RED

Como se dijo en capítulos anteriores, la red estará basada en VLANs para cada piso para limitar el dominio de broadcast y hacer más eficiente la comunicación de la red completa de la A.Z.V.CH.

Hay que tomar en cuenta que la A.Z.V.CH. tiene un reglamento de asignación de direcciones IP para todas las administraciones Zonales del Municipio de Quito dado por

la Dirección Metropolitana de Informática. En el caso de la A.Z.V.CH., el rango de direcciones que puede utilizar para establecer su sistema de comunicaciones es de 172.20.7.0.hasta 172.20.7.254.

Algunos de los ítems del reglamento se detallan a continuación:

- Las direcciones IP de la 1 a la 9 de cada subred serán utilizadas para los servidores.
- La dirección IP 10 es reservada y sirve como puerta de enlace definida en el Switch principal.
- La dirección IP 172.20.24.93 es reservada y sirve como puerta de enlace de las terminales del sistema 390.
- Las direcciones IP de la 11 hasta la 99 serán distribuidas entre los computadores que no tienen acceso al sistema 390.
- Las direcciones IP de la 100 hasta la 254 serán distribuidas entre los computadores que tienen acceso al sistema 390.
- Si dispone de servidores con Windows NT Server 4.0 o superior **no** se deben configurar el servidor DHCP para asignación de direcciones IP en forma dinámica.

En base a este reglamento, ahora se procede a realizar un diagrama lógico de la red mostrado en la figura 4.24.

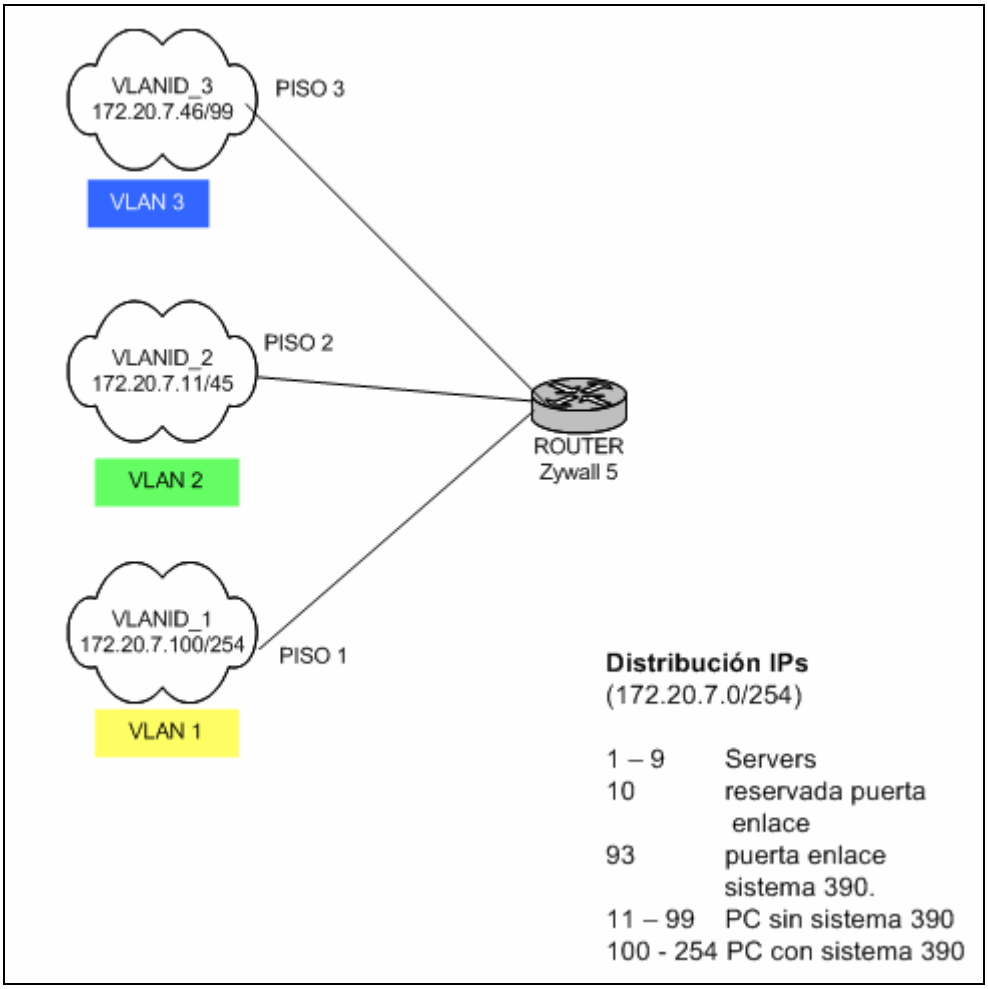


Figura 4.24. Diagrama Lógico de red

Para el primer piso, en donde existen computadores que tienen acceso al sistema 390, se creara la VLAN_1, y utilizara el rango de direcciones IP de la 172.20.7.100 hasta la 172.20.7.254. Existen alrededor de 30 computadoras en este piso, y queda abierta la posibilidad de incrementar más usuarios.

Para el segundo y tercer piso, los computadores de las diferentes oficinas no tienen acceso al sistema 390 por lo que el rango de direcciones en el que trabajaran sera de 172.20.7.11 hasta la 172.20.7.99. Ahora bien, existen alrededor de 60 computadores entre los dos pisos, por lo que el rango queda satisfecho para este caso.

La VLAN_2 entonces quedara conformada por aproximadamente por 30 direcciones de este rango. Quedara a disposición de la dirección de Informática asignar las direcciones a cada computador que pertenezcan a esta VLAN.

De igual manera, la VLAN_3 utilizara direcciones de este rango, y la dirección de informática será la encargada de asignar las IP pertinentes.

Tanto para el servidor de datos como el servidor de voz, los encargados de la dirección de informática podrán escogerlas dentro del rango 172.20.7.1/9.

CAPÍTULO V

ANÁLISIS ECONÓMICO

5.1. SELECCIÓN DE EQUIPOS Y MATERIALES PARA LA INTRANET DE LA A.Z.V.CH. , SEGÚN ANÁLISIS DE RELACIÓN COSTO – BENEFICIO

En los capítulos anteriores ha quedado plenamente definido el diseño total de la Intranet de la Administración Zonal Valle de los Chillos del Municipio de Quito, desde el punto de vista técnico. Se han establecido las bases técnicas de los equipos y componentes de la red, según las características y especificaciones que el diseño en su conjunto exige.

Con seguridad existen en el mercado varias alternativas de productos, de distintos fabricantes, que cumplen con las bases técnicas elaboradas. De haber, entonces, varias marcas de productos y equipos que servirían para implantar la Intranet, se vuelve indispensable establecer las políticas y criterios que permitan seleccionar los equipos y materiales a ser adquiridos. En otras palabras, hay consideraciones especiales que deben tomarse en cuenta para realizar el análisis comparativo entre las opciones que ofrece el mercado, consideraciones que permitirán ajustar este análisis a la situación particular de la A.Z.V.CH.

La primera consideración a ser observada es el hecho de que la A.Z.V.CH. es una entidad pública. Por ello la institución está sujeta al reglamento de contratación vigente, el que establece que para adquisiciones de un monto superior a USD $ 5000, la operación deberá ser llevada a un Concurso de Ofertas, en el que participarían personas naturales o jurídicas, empresas proveedoras de tecnología. Este método de adquisición de los equipos y materiales, así como su instalación, es entonces obligatorio para el caso de este proyecto, por lo que el objetivo de este capítulo se centra en la determinación de un monto total de

inversión, bajo condiciones estrictamente reales, que servirá como referencia para comparar con las ofertas presentadas por las empresas participantes en el mencionado concurso, para la adjudicación del contrato de adquisición de equipos e implantación de la Intranet.

Una segunda consideración: la A.Z.V.CH., como la mayoría de instituciones públicas, tiene recursos económicos limitados, aunque es una entidad que se financia principalmente de la autogestión. Es fundamental, para el éxito de este proyecto, partir de la premisa de que la administración destinara un presupuesto para la implantación de la Intranet muy poco flexible.

Aunque técnicamente siempre habrá varias alternativas para desarrollar un proyecto, y aunque existan equipos de distintas marcas que simultáneamente cumplan las especificaciones requeridas, la recomendación técnica se inclina por utilizar materiales y equipos de marcas reconocidas y de prestigio, para que aumente el grado de confiabilidad. Sin embargo, la mayoría de veces, esas marcas no son las más económicas.

En el proyecto de implantación de la Intranet, la situación no puede ser más apegada a la realidad de nuestro país: quien diseña y espera instalar la nueva infraestructura se enfrenta al desafío de conseguir técnicamente una Intranet funcional, confiable, eficaz y cumplidora de los resultados que se esperan de ella, con un presupuesto referencial. Esa es la realidad de la vida profesional. El valor total de dinero que la A.Z.V.CH. deba invertir en la adquisición y montaje de esta tecnología tendrá que aproximarse lo más posible a ese presupuesto referencial, porque de ello dependerá la viabilidad del proyecto en su totalidad. Expresado de otra manera, en caso de que el presente proyecto cueste más de lo esperado, no sería factible, sencillamente no se desarrollaría. El reto es: no permitir que éste sea otro proyecto más que se quedó en los estudios, en los papeles.

Estas importantes aclaraciones previas tendrán mucha influencia en las decisiones a tomarse para la selección de equipos y materiales, y también explican algunos de los criterios de diseño previamente utilizados.

Las políticas de selección de equipos, materiales y proveedores en general, están anotadas a continuación:

- Todos los equipos a ser adquiridos deberán cumplir a cabalidad las bases técnicas establecidas en el diseño de la Intranet.

- Dichos equipos deberán acreditar un año de garantía como mínimo, que será soportada por una marca con representación en el país, a fin de asegurar futuro mantenimiento, reposición, servicio técnico, etc.

- El proveedor seleccionado deberá ofrecer una solución total, es decir que tendrá que ofrecer el hardware en su totalidad, así como será responsable de la instalación y puesta en marcha de la Intranet. Esta condición presenta varias ventajas: facilidad de contratación, gestión y coordinación al ser un solo proveedor; mejor precio final que hacerlo con distintas empresas, etc.

- Obviamente se dará preferencia a las opciones de menor precio, a fin de apegarse al presupuesto mencionado, siempre y cuando esas opciones cumplan con todas las condiciones previamente establecidas.

5.1.1. Dispositivos de red

El hardware para la Intranet consiste en los dispositivos de red para el backbone, tales como switches y tarjetas de red o NIC's (Network Interface Card); y, dispositivos para Wireless LAN o red inalámbrica, tales como puntos de acceso (Access Points) y tarjetas inalámbricas o WNIC (Wireless NIC).

Por facilidades acerca de la garantía, compatibilidad, así como por unificar el proveedor, se prefiere que estos equipos sean del mismo fabricante. A continuación se muestra un cuadro comparativo de estos equipos, en cuatro marcas muy difundidas en el Ecuador, y que se encuentran debidamente representadas en nuestro país, por varias empresas. Los precios que se muestran a continuación varían constantemente según condiciones de mercado, aunque la tendencia generalmente es a la baja, luego de pocos

meses de que los modelos especificados logran un alto nivel de presencia en el mercado. Es importante aclarar que se necesita solamente 1 switch de capa 2, y un router. Por ser dispositivos de bajo costo, se los excluirá de los cuadros comparativos, para que su selección dependa de los equipos para Wireless LAN, que son muchos y representan el rubro más significativo del valor total:

Tabla. 5.1. Cuadro comparativo de Puntos de Acceso (AP).

Cuadro comparativo de Access Points				
Marca : *Modelo:*	**CISCO Aironet 1100**	**3COM Enterprise 7250**	**D-LINK DWL 2200/7100**	**Zyxel ZyAir G-3000H**
¿Cumple bases Técnicas?	SÍ	NO	NO	NO
Garantía	1 AÑO	1 AÑO	1 AÑO	1 AÑO
Representación En el país	SÍ	SÍ	SÍ	SÍ
Precio USD $	400	370	165	262

Cabe indicar, que el AP necesario para la Intranet, debe tener la opción de modificar los parámetros MAC, siendo el único que permite esta opción, el AP Cisco Aironet 1100 Series. Por tanto, en el caso de los AP, no habrá duda en utilizar los de marca Cisco para la instalación de la red.

Tabla. 5. 2. Cuadro comparativo de Adaptadores de Red PCI (Tarjetas Inalámbricas).

Cuadro comparativo de Adaptadores de Red PCI Wireless				
Marca : *Modelo:*	**CISCO Aironet PCI-G**	**3COM OfficeConnect 802.11g PCI**	**D-LINK DWL G-520**	**Zyxel ZyAir G-300**

¿Cumple bases Técnicas?	SÍ	NO	NO	NO
Garantía	1 AÑO	1 AÑO	1 AÑO	1 AÑO
Representación En el país	SÍ	SÍ	SÍ	SÍ
Precio USD $	278.99	59	55.05	115.00

Tabla. 5.3. Cuadro comparativo de Adaptadores de Red USB compactos

Cuadro comparativo de Adaptadores de Red USB Wiíreless				
Marca : *Modelo:*	**CISCO Aironet USB-G**	**3COM OfficeConnect 802.11g USB**	**D-Link DWL G-122**	**Zyxel ZyAir G-200**
¿Cumple bases Técnicas?	SÍ	NO	NO	NO
Garantía	1 AÑO	1 AÑO	1 AÑO	1 AÑO
Representación en el país	SI	SÍ	SÍ	SÍ
Precio USD $	299.00	79.00	41.99	110.00

Después de analizar los cuadros comparativos de las tablas 5.2 y 5.3. de los principales componentes de la Intranet, en cuanto al hardware, es posible observar que se han elaborado con cuatro marcas de gran difusión en el Ecuador, donde no todas ellas cumplen las bases técnicas de diseño.

Las marcas CISCO, 3COM, D-LINK y ZYXEL en términos generales cumplen las políticas y condiciones planteadas para la selección, con sus líneas intermedias de

productos Wireless, dedicados al mercado "Medium Office" o Enterprise (empresarial). Pero, solo una cumple con los requisitos extras planteados en este estudio, es decir, soporta el estándar 802.11e, esta es CISCO. Existe otro dispositivo que satisface los requerimientos de la marca ASIARF, que además resulta muy económico para mis pretensiones.

No se puede ocultar que la marca CISCO es una de las más reconocidas en todo el mundo, es un referente, pero la diferencia en precio con otros fabricantes es decisiva para el caso de la A.Z.V.CH., donde hay un presupuesto para tomar en cuenta.

En conclusión, según todos los puntos de vista considerados en el presente análisis, se ha creado una relación costo – beneficio, mejor representada para el caso de este proyecto por los equipos de Wireless LAN de marca ASIARF, por lo que se convierten en la selección para la Intranet, con los modelos analizados.

En lo que se refiere al Switch y al router serán de la marca Zyxel, teniendo estos, también la característica de calidad de servicio QoS.

5.1.2. Cableado estructurado

El backbone de la Intranet, así como la instalación y montaje de los equipos se ha diseñado con criterios de cableado estructurado. Este rubro involucra la instalación de puntos de red, instalaciones eléctricas, etc.

Todas estas instalaciones ya existen en la administración actual. Cabe recordar que al momento poseen una red cableada que ha sido diseñada bajo estándares de cableado estructurado. Por tanto, no se va a considerar en el presente análisis económico.

Será solo necesario hacer uso de las instalaciones actuales para el montaje de los AP en los lugares determinados anteriormente, tanto los puntos de red como puntos eléctricos.

5.1.3. Servidores de Red y Software

De acuerdo al diseño propuesto, la red incluye dos servidores, uno de datos y otro para voz. En cuanto se refiere al servidor de datos, se utilizara el mismo que esta en estos momentos, por lo que no entra en el análisis económico.

De otro lado, para el servidor de voz se requiere un equipo robusto, que soporte llamadas y aplicaciones complejas simultáneas, además de recodificaciones. Es difícil determinar con exactitud los requerimientos necesarios del sistema, pero es recomendable proveerse de un buen hardware con el fin de evitar inconvenientes.

La marca americana Digium, patrocinadora de Asterisk, recomienda utilizar un equipo Dual Intel Xeon 1.8 Ghz 1 Gb RAM que soporta 60 llamadas concurrentes codificando con el codec G.729. De aquí, que en la propuesta económica se va buscar equipos de semejantes características.

A continuación, la tabla 5.4. se muestra los servidores que podrían ser usados para la red:

Tabla 5.4. Cuadro Comparativo de Servidores para comunicación de voz

Descripción	Precio
Intel Xeon (3.00 GHz), 1 GB, 80 GB	1579
Intel Core 2 Duo (1.86 GHz), 1 GB DDR II SDRAM, 250 GB Standard	1499
IBM eServer xSeries 226 8488 - Tower 1 x Xeon 3 GHz - RAM 1 GB	1027.71

A pesar de que Asterisk corre bajo plataforma Linux, es necesario comprar el software desarrollado por Digium, Asterisk Business Edition, el cual provee todas las funciones críticas y características para pequeñas y medianas empresas para comunicaciones de voz, es decir es el IP PBX, que contiene todas las características mencionadas en capítulos anteriores. La tabla 5.5. muestra el código de producto y su precio, dados directamente por Digium.

Tabla 5.5. Precio de Asterisk Business Edition

Descripción	Código de producto	Precio
Asterisk Business Edition Single License	BUSEDB1PACK	995.00

Ahora bien, una vez escogido el servidor y el software de Asterisk, se requiere conocer el costo por el uso del codec G.729, que utilizará cada uno de los usuarios de la red para la comunicación de voz. G.729 requiere una licencia por cada canal usado. Esta licencia es comprada a Digium.

Tabla 5.6. Licencia para codec G.729

Descripción	Código de producto	P. Unitario	P.Total
Asterisk G.729 License	G729CODE	10.00	900.00

Para conectar la red de voz interna de la administración con la red publica telefónica, es necesario disponer de tarjetas análogas compatibles con Asterisk, que permitan la interconexión de las dos redes. Buscando la compatibilidad de hardware y software, se comprara también estas tarjetas a Digium. A continuación, en detalle en la tabla 5.7.

Descripción	Código de producto	P. Unitario	P.Total
Tarjeta de interfaz análoga	Wildcard TDM400P	400.00	800.00

Tabla 5.7. Tarjetas análogas

5.1.4. Mano de Obra

Para poder valorar en términos reales y con exactitud la mano de obra necesaria para implantar la Intranet, es necesario tomar en consideración las condiciones actuales de estos servicios en el mercado ecuatoriano.

La primera distinción que debe hacerse es que en el proyecto se requieren dos tipos de mano de obra, la general a nivel de obreros, y la especializada, a nivel de técnicos o mejor ingenieros.

Como se dijo anteriormente, la mano de obra a nivel de obreros va ser muy relativa, ya que se utilizara las instalaciones actuales de la administración.

Sobre la mano de obra general, el detalle de precios se muestra a continuación en la tabla 5.8.

Tabla. 5.8. Detalle de precios de mano de obra especializada.

Precios de mano de obra especializada			
CANTIDAD	**DESCRIPCIÓN**	**P.U.**	**P.T.**
6	Certificación de punto de datos CAT5E	30	180.00
50	Hora técnica, configuración de servidor de voz, Asterisk, codecs	120	6000.00
4	Hora técnica, instalación y configuración de Access Points	20.00	80.00
20	Hora técnica, configuración de 90 computadores con tarjetas inalámbricas	20.00	400.00
	TOTAL USD $		**6,660**

Haciendo una estimación de tiempo para el desarrollo de estas actividades, resultan alrededor de 6 a 8 días laborables, de un ingeniero.

El valor total de mano de obra será la suma de la general y la especializada, y su monto asciende a USD $ .6660.00

5.2. PRESUPUESTO FINAL

En las secciones anteriores se han obtenido los costos de cada rubro componente del proyecto de implantación de la Intranet de la A.Z.V.CH. A continuación se juntarán esos

componentes para calcular la cantidad a la que asciende el monto total. El valor final obtenido corresponde a una estimación del presupuesto de inversión para adquirir la nueva infraestructura, se detalla en la tabla 5.9.

Tabla. 5.9. Determinación del Monto Total de Inversión estimado para la Intranet de A.Z.V.CH.

Presupuesto Final del Proyecto			
CANTIDAD	**DESCRIPCIÓN**	**P.U.**	**P.T.**
6	Access Point Cisco Aironet 1100 Series	400.00	2400.00
90	Wireless Network Adapter	35	3150.00
2	Tarjeta de interfaz análoga	400.00	800.00
90	Softphones Cubix	10	900.00
1	Servidor de Voz (software)	995.00	995.00
90	Licencia de codec G.729	90.00	900.00
1	Servidor para comunicaciones de voz (hardware)	1500.00	1500.00
1	Mano de Obra		6660.00
	TOTAL USD $		**17,305.00**

Nótese que los equipos de red son recibidos luego de 45 días de adjudicado el proyecto. Ese tiempo corresponde al proceso de importación de tales equipos, que son traídos desde USA, debido a que los proveedores en el Ecuador no tienen disponibilidad inmediata de todos los modelos seleccionados, mientras que los equipos que sí se cuentan en stock, no existen en las cantidades requeridas.

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- Al finalizar el presente trabajo es posible afirmar que se ha analizado, diseñado y desarrollado una moderna y funcional infraestructura de comunicaciones en la Administración Zonal Valle de los Chillos del Municipio Metropolitano de Quito.

- El estándar IEEE 802.11g es el preferido por estos días para implantar redes tipo WirelessLAN, con tecnología WI-FI. Ha desplazado ya al conocido 802.11b, aunque convivirán por un buen tiempo todavía. Si observamos la tendencia mundial, notaremos que el 802.11g tampoco durará mucho tiempo, porque la evolución e innovación en tecnologías inalámbricas mantiene un progreso vertiginoso. La misma banda ISM en 2.4 GHz puede ser reemplazada en mediano plazo por nuevos estándares sostenidos por los grandes fabricantes y desarrolladores de tecnología, que le han dado preferencia a bandas por los 5 GHz. Tal es el caso del nuevo estándar 802.11n para WirelessLAN, donde se aumenta aún más la velocidad de transmisión, se mejora el alcance con tecnologías como MIMO, y el desarrollo en 5 GHz es impulsado por gigantes como Intel, Sony, Toshiba, Cisco, entre otros.

- La tecnología de redes inalámbricas WI-FI se encuentra ampliamente difundida en el mundo, ha obtenido madurez y sigue en evolución y crecimiento. Las promesas que WI-FI hacía hace pocos años, son ahora realidades. Como ejemplo, el presente proyecto aprovecha los beneficios únicos de esta tecnología para solucionar necesidades específicas como la distribución de la red, imposible de atender de otra manera. Con seguridad, cada día serán mayores las utilidades y nuevas aplicaciones que se den a las WirelessLAN, lo que impulsará aún más su desarrollo y

proliferación. La evolución de WI-FI es otro hecho concreto: hace pocos años se la vislumbró como otro agente de convergencia de tecnologías, y así está sucediendo, pero WI-FI se encamina de una manera más ambiciosa hacia una nueva tecnología totalmente revolucionaria: WI-MAX. Se trata de redes de comunicaciones equivalentes a las WirelessLAN, pero de área metropolitana, con una cobertura comparable a las redes celulares, aunque con un ancho de banda y velocidades de transmisión muy superiores. WI-MAX sigue en desarrollo pero ya está presente, y sus primeros productos están en el mercado, mostrando nuevas aplicaciones y posibilidades impensables aún.

- El modelo de predicción de propagación de ondas Dominant Path (DP) o de trayectorias dominantes, es el más reciente, efectivo y exacto de los modelos disponibles. Su desempeño superior se debe a que aprovecha las mejores ventajas de sus equivalentes, tanto empíricos como determinísticos (por lo que se le ha considerado un modelo mixto, híbrido o intermedio), e incorpora otros beneficios adicionales, como la menor complejidad de cálculo, menor tiempo de cómputo, y sobre todo el hecho de que es tolerante a un grado de inexactitud en el modelo matemático del edificio, campus, ciudad o terreno donde se estudia la propagación de ondas. Ese grado de tolerancia permite al modelo DP seguir manteniéndose exacto en una predicción, a pesar de los errores e imprecisiones normales en la elaboración de un modelo matemático o Database. La precisión y exactitud del modelo DP han sido comprobadas a través de múltiples campañas de medición ejecutadas por importantes instituciones, con el objetivo de comparar sus predicciones con información obtenida experimentalmente.

- Una desventaja del modelo de predicción DP frente a los empíricos es que se basa en estructuras de redes neuronales para la determinación de las trayectorias dominantes, por lo que su cálculo manual se ve ampliamente dificultado, obligando prácticamente a su utilización mediante herramientas de software (WinProp en el caso del presente proyecto). Por tanto, si se desea realizar un estudio de propagación de ondas utilizando el modelo de predicción DP, será necesario desarrollar el software que permita su aplicación, o bien se deberá adquirir o conseguir software previamente desarrollado para ese modelo y que esté disponible

en el mercado. Lo anterior involucrará una licencia, un permiso y probablemente un costo.

- La suite de software WinProp y su modelo de predicción DP son herramientas modernas, novedosas, efectivas y sobre todo prácticas, que permiten ejecutar una verdadera planificación y diseño de redes inalámbricas de comunicaciones, sean celulares, WI-FI y WirelessLAN en general. El desarrollo y culminación del presente proyecto suponen un aporte a las telecomunicaciones en nuestra Patria, mediante la información y facilitación permanentes de tales herramientas, de manera que su aplicación estimule el verdadero análisis, planificación y diseño profesional de infraestructuras de comunicaciones inalámbricas, tan en boga en estos tiempos, y que signifique también un avance de nuestro medio hacia la Ingeniería del primer mundo.

- La solución integral al problema de distribución de red implicó la ejecución de un proyecto que incorpore tecnología de apoyo, tanto en Telecomunicaciones como en Sistemas e Informática. Estas dos ramas han demostrado más que nunca ser absolutamente complementarias, por lo que los profesionales de una especialidad debemos necesariamente incursionar en la otra, de manera que se enriquezca nuestro criterio técnico y visión global acerca de un proyecto.

- La convergencia de redes mixtas de voz y datos sobre redes inalámbricas tiene muchos parámetros a tomar en cuenta. Ya que la voz es una aplicación en tiempo real es necesario mecanismos que permitan que los paquetes de voz estén por encima de los paquetes de datos, en prioridad. Esto se consigue mediante el estándar de calidad de servicio QoS planteado por la IEEE.

- El presupuesto necesario para instalar toda la infraestructura de comunicaciones es relativamente alto. Esto se debe a que la tecnología a emplear es novedosa, mas en lo que se refiere a la voz, pero tiene su ventaja. La inversión es grande pero en un futuro permitirá recuperar dicha inversión, ya que ahorrara costos en las llamadas telefónicas hechas por la administración.

- La Intranet diseñada para la A.Z.V.CH. constituye una verdadera solución que beneficia a la entidad, y fue ejecutada con un presupuesto medio alto. La conclusión que se despliega de ese hecho es que, en el ejercicio de la profesión en Telecomunicaciones y probablemente en otras donde existe la responsabilidad de desarrollar e implantar proyectos, no debe descuidarse más la observación de un parámetro fundamental: el dinero. Aunque el ingeniero ejecute siempre cualquier trabajo tomando en cuenta el concepto de optimización, en muchas situaciones reales esto no será suficiente, debido al factor financiero. Es necesario entonces apelar al ingenio, a la creatividad y la experiencia para desarrollar la capacidad de resolver problemas y adaptarse a las situaciones, de manera que un proyecto no falle en su factibilidad porque sencillamente no se ajustó a las condiciones económicas. Quien recurre al ingeniero, porque tiene una necesidad, espera soluciones.

- Usando la flexibilidad de este nuevo estándar 802.11e, se demuestra en el estudio realizado que ciertos valores del parámetro AIFS pueden ser usados para proteger una llamada contra un gran numero de estaciones, manteniendo throughput, con retardos dentro del rango que la calidad de voz es aceptable.

- Un número limitado de conexiones de voz puede ser soportado por una VoWLAN debido a la sobrecarga del medio y a la ineficiencia del protocolo MAC. Mediante el análisis hecho en este estudio, es posible conseguir una buena calidad de voz y además mantener un tráfico de datos normal, modificando los parámetros de la capa MAC.

- Todos los equipos utilizados deben soportar calidad de servicio QoS, en cualquier estándar, claro que permita operatibilidad entre ellos. Es muy necesario esta característica, ya que de esta depende que la red pueda funcionar correctamente.

- El análisis financiero del proyecto arrojó resultados que hacen de la VoWLAN una tecnología implementable, y sería mas rentable si se tomara en cuenta que se tendrán significativos ahorros en las cuentas de teléfono.

- Los altos costos del proyecto son justificables debido a su carácter novedoso, pero como todo, mientras mas se vaya implementando esta tecnología en el mundo, los costos tenderán siempre a la baja.

6.2. RECOMENDACIONES

- Para los computadores y terminales en general que pertenecen a la Intranet, se recomienda ampliamente mantenerlos actualizados en cuanto a las versiones de su sistema operativo. Como todos esos equipos utilizan Windows, deberían actualizarse a la última versión que es el Service Packet 2 (Windows SP2). En ese paquete de servicios se incorporan las herramientas necesarias para el reconocimiento de la encriptación usada por WPA y el estándar de seguridad 802.1X. Con todos los usuarios de la red usando Windows SP2, será posible activar un mayor nivel de seguridad en la WirelessLAN, reemplazando el actual sistema WEP por el citado WPA. Los Access Points y los adaptadores de acceso inalámbrico a la red con que ya cuenta la A.Z.V.CH. soportan ambos niveles de seguridad.

- Todos los equipos WI-FI que se instalen en la WirelessLAN de la A.Z.V.CH. deben poseer drivers y firmware original de fábrica, es decir el que viene preinstalado en el equipo, en su empaque original. Todo software, a todo nivel presenta algún grado de errores, y su fabricante suele corregirlos luego de un corto tiempo. Las marcas fabricantes de los equipos seleccionados, ponen a disposición de sus clientes en todo el mundo las actualizaciones mejoradas y corregidas de sus drivers y firmware, que pueden ser descargadas desde el sitio web de la empresa. Por tanto, se recomienda a los responsables del mantenimiento de la Intranet revisar en pocos meses el sitio web de las empresas para obtener esas actualizaciones y mejorar el desempeño de los equipos. Las descargas son gratuitas, como valor agregado de la marca a sus clientes.

- Es necesario evaluar en la práctica el funcionamiento de la voz IP sobre una red inalámbrica. Se puede basar inicialmente en este estudio, pero dependerá mucho de las condiciones que vayan apareciendo ya en la puesta en marcha de la red. Claro, este trabajo servirá como punto de partida para conseguir los requerimientos deseados.

- Todo proveedor de los equipos a utilizar en la VoWLAN deberán realizar mantenimiento una vez al año. Esto generalmente abarca en sus cotizaciones, pero si no es así, se debe exigir este requisito.

- Es imprescindible capacitar al personal para el buen uso de la tecnología inalámbrica, tanto para la transmisión de datos como para la comunicación de voz.

- De la misma manera, es muy recomendable capacitar a personal en lo que se refiere al manejo del servidor de voz, ya que como se observo en el análisis económico, la configuración de este es muy costosa, y es preferible tener en la misma compañía a personal que pueda manejarlo para solucionar problemas que pudieran aparecer.

REFERENCIAS BIBLIOGRÁFICAS

IEEE Wireless Communications, Volumen 11 No. 2, Edición ISSN 1536-1284/ IEEE 2004, Editorial Scanning the Literature Songwu Lu, UCLA, USA, Michele Zorzi Editor–in-Chief, Universita Degli Sudi di Ferrara, Italy, New York-USA Abril de 2004, PG 32-39.

IEEE Wireless Communications, Volumen 11 No. 3, Edición ISSN 1536-1284/ IEEE 2004, Editorial Scanning the Literature Songwu Lu, UCLA, USA, Michele Zorzi Editor–in-Chief, Universita Degli Sudi di Ferrara, Italy, New York-USA Junio de 2004, PG 16-23, 72-79.

IEEE Wireless Communications, Volumen 11 No. 4, Edición ISSN 1536-1284/ IEEE 2004, Editorial Scanning the Literature Songwu Lu, UCLA, USA, Michele Zorzi Editor–in-Chief, Universita di Padova, Italy, New York-USA Agosto de 2004, PG 6-14, 66-75.

IEEE Wireless Communications, Volumen 11 No. 6, Edición ISSN 1536-1284/ IEEE 2004, Editorial Scanning the Literature Songwu Lu, UCLA, USA, Michele Zorzi Editor–in-Chief, Universita di Padova, Italy, New York-USA Diciembre de 2004, PG 38-43.

IEEE Wireless Communications, Volumen 12 No. 1, Edición ISSN 1536-1284/ IEEE 2005, Editorial Scanning the Literature Songwu Lu, UCLA, USA, Michele Zorzi Editor–in-Chief, Universita di Padova, Italy, New York-USA febrero de 2005, PG 12-36.

DOMINANT PATHS FOR THE FIELD STRNGTH PREDICTION, G. Wölfle, FM. Landstorfer, Institut für Hochfrequenztechnik, University of Stuttgard, Stuttgard-Germany. woelfle@ihf.uni-stuttgard.de

Dominant Path Prediction Model for Indoor and Urban Scenarios, Gerd Wölfle 1), René Wahl 1), Pascal Wildbolz 1), Philipp Wertz 2)1), AWE Communications GmbH, Otto-Lilienthal-Str. 36, 71034 Boeblingen, Germany, www.awe-communications.com 2) Institut für Hochfrequenztechnik, University of Stuttgart, Pfaffenwaldring 47, 70569 Stuttgart, Germany.

Propagation Model Development & Comparisons, Paul M. McKenna e-mail pmckenna@its.bldrdoc.gov.

Estándares IEEE 802.11, http://www.ieee.org,

Dominant Paths, http://www.ihf.uni-stuttgart.de,

SHORT GUIDE FOR WINPROP INDOOR MODULES, Stefan Burger AWE Communications, *e-mail: stefan.burger@awe-communications.com.*, http://www.awe-communications.com.

CCNA1, CCNA4, http://cisco.netacad.net,.

Servidor Asterisk, http://www.asteriskguru.com,.

Precios de componentes de voz sobre IP, http://www.digium.com,.

ANEXO 1

AWE DOMINANT PATH PREDICTION MODEL FOR INDOOR AND URBAN SCENARIOS

Dominant Path Prediction Model for Indoor and Urban Scenarios

Gerd Wölfle [1], René Wahl [1], Pascal Wildbolz [1], Philipp Wertz [2]

[1] AWE Communications GmbH, Otto-Lilienthal-Str. 36, 71034 Boeblingen, Germany, www.awe-communications.com [2] Institut für Hochfrequenztechnik, University of Stuttgart, Pfaffenwaldring 47, 70569 Stuttgart, Germany

***Abstract*— Currently, for the planning of wireless networks (cellular or WLAN) in urban and indoor scenarios either empirical (direct ray) or ray-optical (ray tracing) propagation models are used. In this paper both approaches are compared to one another and to measurements in different urban city centres and in different (multi-floor) buildings. Additionally a new concept - which is called dominant path model - is presented in this paper. This new concept does not focus only on the direct ray (like empirical models) and it does not consider hundreds of rays for a single pixel (like ray tracing), but it focuses on the dominant path(s) between transmitter and receiver. The parameters of these dominant paths are determined (e.g. path length, number and type of interactions, material properties of objects along the path, …) and are used for the prediction of the path loss between transmitter and receiver. Thus the computational effort is far below ray tracing and in the range of empirical models. But the accuracy of the new model in very complex environments (where multiple interactions occur) is even higher than the accuracy of ray tracing models (because of their limitations in the number of interactions considered). This very high accuracy is shown with the comparison to measurements in different cities and buildings.**

Keywords—wave propagation, urban, indoor, ray tracing, dominant paths, measurements

I. Introduction

The planning of wireless communication networks in urban or indoor scenarios must be based on accurate propagation models for the prediction of the path loss between fixed base station antennas and mobile terminals. Many different approaches have been investigated during the last years to obtain accurate and fast propagation models. Today either statistical/empirical models or ray-optical models are used. For the ray-optical models significant accelerations are available leading to computation times in the range of empirical models [1].

Today vector databases of cities or buildings are available and can be used without any restrictions. These databases provide a high accuracy – but errors in the material definitions or in the coordinates lead to significant errors if ray-optical propagation models are used (see figure 4). So there is a demand for models which are fast and consider multiple interactions (e.g. diffractions) – but which are not relying on each detail of the vector database. In this paper such an approach is presented and compared to empirical and rayoptical propagation models as well as measurements.

II. Dominant Path Model

A. Current status

Figures 1 and 2 show the problem of empirical propagation models. They are based on the direct ray between transmitter and receiver. In indoor and in urban scenarios this ray is not always dominant and very often this path is highly attenuated.

Focusing a model on this path must lead to errors in all scenarios

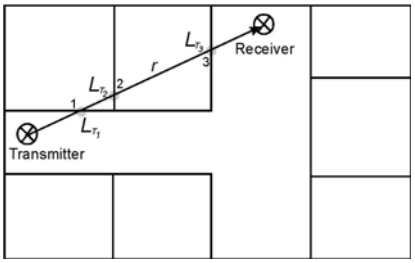


Figure 1.Empirical propagation models in indoor scenarios

where this path is contributing only a very small part to the total received signal power.

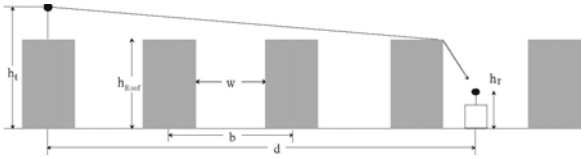


Figure 2. Empirical propagation models in urban scenarios

In figure 3 the principle of ray-optical propagation models is shown. Many hundreds of rays are computed for each receiver location. The contributions of each ray are superposed to obtain the received power. In most cases only 2 or 3 rays are contributing more than 95% of the energy, i.e. by focusing on these dominant rays the accuracy would be sufficient.

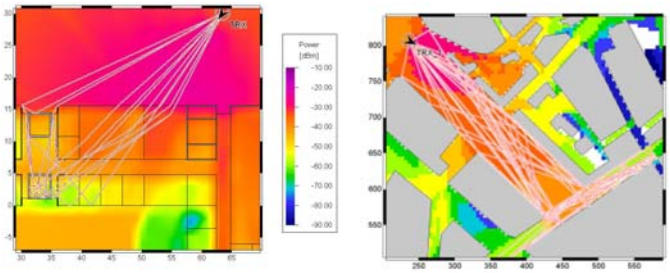


Figure 3. Ray-optical propagation models in indoor (left) and urban (right) scenarios

A second disadvantage of ray-optical models is shown in figure 4. Small inaccuracies in the databases lead to totally different prediction results. As angular criteria are evaluated during the ray-optical prediction, the orientation of walls is extremely important. Unfortunately databases with this very high accuracy incl. a very detailed description of the material properties are not available.

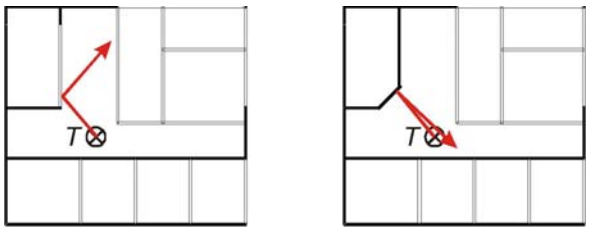


Figure 4. Accuracy of building databases

B. Requirements for a new model

After analyzing the status of the model currently available, the requirements for a new model can be defined:

- Model should not dot depend on each micro-detail in the vector database (see figure 4).
- Focusing on the dominant paths (see figure 5) and not computing hundreds of irrelevant paths
- Simple calibration possible with reference data (e.g. measurements)

With these requirements the dominant path model was defined.

C. *The dominant path model*

The dominant path model can be subdivided into two steps:

- Determination of the dominant paths (geometry)
- Prediction of the path loss along the paths

Determining the dominant paths is not a very simple task. For indoor scenarios the algorithm is published in [4] and [8]. The same principle can also be used for urban scenarios. Figure 5 shows an example for dominant paths in indoor scenarios.

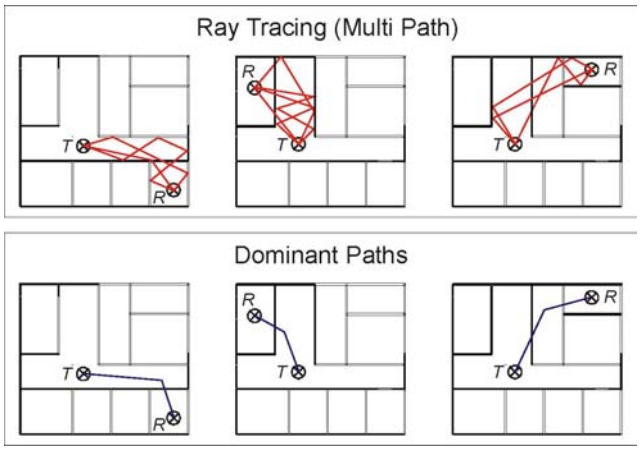


Figure 5. Dominant paths in indoor scenarios

By adjusting the weights described in [8], different paths can be obtained (small number of interactions or short paths or small number of transmissions…….). Obviously more than one path can be computed for each pixel if several runs with different weighting factors are computed and the contributions of the paths are superposed. In this paper the single path approach is used, i.e. only one path is determined per pixel. This reduces the computation time as each new set of weighting factors leads to a new computation of the paths, i.e. 5 different sets lead to a 5 times longer computation time compared to the single path approach.

It should also be mentioned that the path search algorithm works either in 2D or in 3D. If in urban scenarios the model is combined (superposed) with the COST 231 Walfisch-Ikegami Model (for multiple diffractions in over-rooftop propagation) the dominant path model can compute in 2D (horizontal plane) to save computation time. In multi floor indoor environments the model can work in rigorous 3D.

The prediction of the path loss along the path is done with the following equation:

$$L = n * (1 - 0.5 * \alpha) * 20 * \log(d) + \sum_{i=1}^{n} \left(w_i * \frac{\varphi_i}{180°} * L_D \right)$$

L is the path loss in dB after a path length of d (in meters). α is the waveguiding factor (see below). And L_D is the loss in dB due to an interaction, i.e. changing the direction of propagation. The angle between the former direction and the new direction of propagation is φ_i. Thus the loss increases linear with the angle, normalized to 180°. If no change of direction, the loss is 0 dB and if 90° the loss is $0.5*L_D$. Obviously more complicated

dependency on the angle could be implemented – but it is difficult later if L_D must be determined with linear regression from measurements. Then a linear dependency is much better.

The factor w_i can be used to reduce the weight of higher interactions. For example, w_2 could be 0.95 and w_3 0.9. This would emphasize the first interactions compared to the latter. And this is reasonable because later the wave is very diffuse and so multiple options for interactions occur and the loss is not so high.

The waveguiding factor α is described in [9]. The reflection loss of the walls along the path as well as their distance to the path influence the value. The smaller the reflection loss and the closer the wall to the path, the higher the waveguiding factor. As described in [9], the factor is limited to the range between 0 (no waveguiding, free space) and 1.0 (full waveguiding with small reflection loss). The difference between max. and min waveguiding would result in 50% of the path loss exponent *n*. Figure 6 shows an example for the waveguiding factor in indoor scenarios. For urban scenarios the waveguiding factor is determined in a similar way.

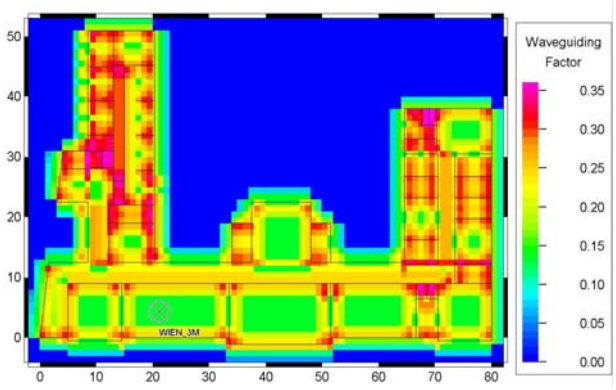


Figure 6. Waveguiding factor in indoor scenarios

The model could be improved with more details to increase the accuracy. But if an automatic calibration (e.g. linear regression) of the parameters (n, L_D, w_i) should be possible, the dependency should not be too complicated – otherwise the automatic calibration will not be possible.

III. Indoor Propagation

A. General

For indoor environments the Dominant Path Model is extended with some features: In contrast to urban scenarios, the indoor prediction considers not only the total number of interactions, but also the individual angle of each interaction (0 to 90 degrees) for the determination of the attenuation caused by the interactions. Thus, it is possible to separate between small and large changes of the direction of propagation, which results in smoother transitions between adjacent pixels. Additionally the 'waveguiding'-factor (as described in section II.C) is included, which improves the accuracy especially in long corridors. The exponent n for the path loss is set to fit the indoor requirements (i.e. this factor is higher than the value in the urban case).

To demonstrate the performance of the Dominant Path Model in indoor environments, measurement campaigns in different types of buildings were used. New office buildings like the University of Stuttgart [6], older office buildings like the University of Vienna [4],[5] as well as buildings with multiple floors like the Instituto de Telecomunicações in Lisbon [7] were used for the comparison. The results concerning accuracy and performance were compared to the other prediction models "Intelligent Ray Tracing" (IRT) and "Multi Wall" (MW).

B. Modern office building

One measurement campaign was conducted in a modern office building at the University of Stuttgart, which is mainly built of concrete and glass. The database of the building contains 108 planar objects with more than 130 subdivisions (windows, doors…).

The campaign includes 20 different transmitter locations and many measurement routes for each location. Two of the transmitter locations are presented in this paper. The comparison of all other measurement routes and

transmitter locations can be found in [3]. The results of the prediction for transmitter site 10 with different prediction models are presented in figures 7 to. 9 The path loss measurements obtained in this building were performed with a CW signal. The carrier frequency was 1800 MHz and the transmitter output power was 20 dBm.

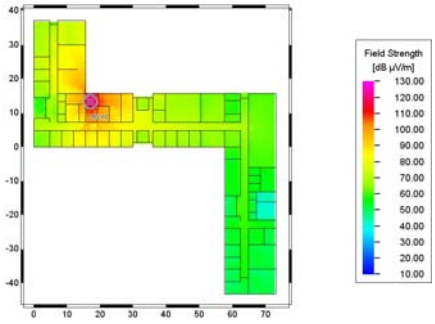


Figure 7. Prediction for site 10 with Dominant Path Model Figure 8. Prediction for site 10 with ray tracing (IRT) with 5 diffractions and 4 reflections in multiple combinations

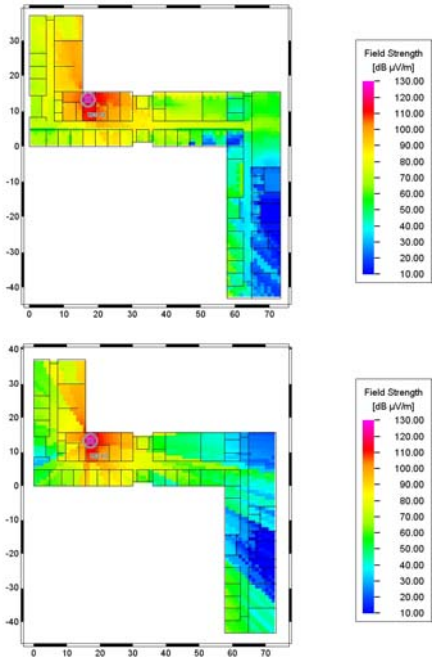


Figure 9. Prediction for site 10 with Multi-Wall Model

The results of the prediction with the Dominant Path Model are more realistic compared to the results of the other two models. Especially after multiple diffractions and large distances, the fieldstrength of the ray tracing and the Multi-Wall Model are too pessimistic. This can be explained with the fact, that the ray tracing considers 5 diffractions and 4 reflections in contrast to the Dominant Path Model, which has no limit for the number of interactions. The accuracy of the Multi-Wall Model is even worse, which is obviously a consequence of the fact that it considers only the direct ray and does not consider reflections and diffractions.

Figures 10 and 11 show the difference between prediction and measurement for transmitter sites 10 and 15. The standard deviation for site 10 is approx. 3.9 dB. The difference between prediction and measurement for site 15 leads to a higher but still acceptable standard deviation (5.3 dB). The computation time for the Dominant Path Model is very short for this building and therefore the model can be used for network planning purposes.

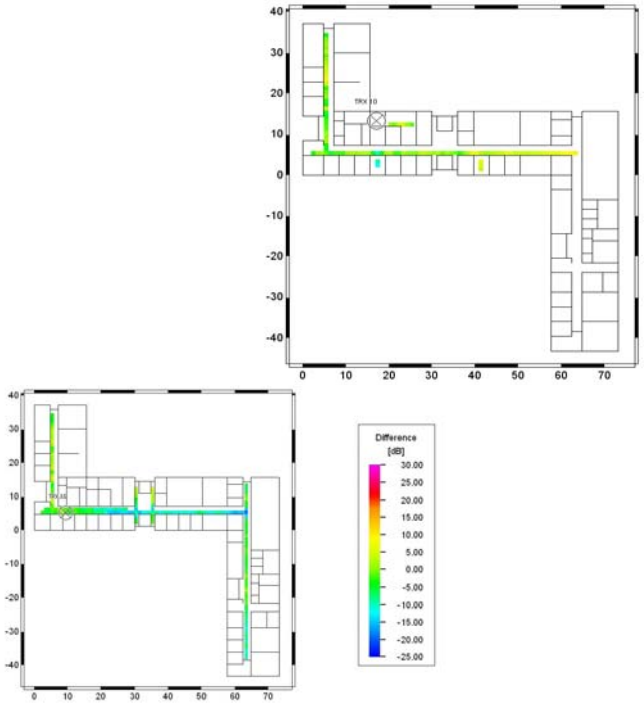


Figure 11. Difference between prediction and measurement for Dominant Path Model, Site 15

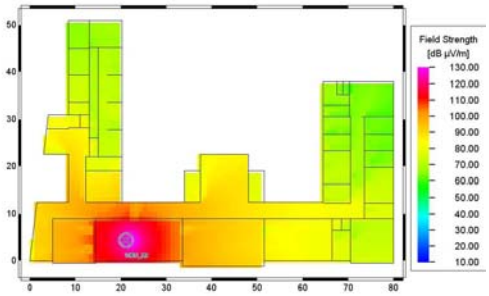


Figure 12. Prediction for Dominant Path Model, Site 3

Table I shows the difference between prediction and measurements. The computation times can be found in table II.

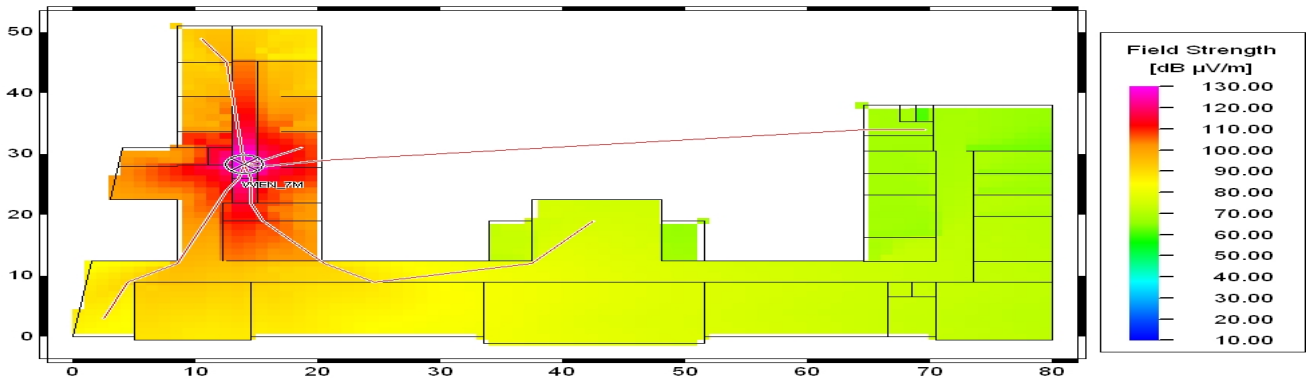


TABLE I. COMPARISON TO MEASUREMENTS **Site**	**Difference (Predictions – Measurements) in dB**					
	IRT		**Dominant Path**		**Multi Wall**	
	Mean	***Std.***	***Mean***	***Std.***	***Mean***	***Std.***

	value	*Dev.*	*value*	*Dev.*	*value*	*Dev.*
TRX 10	5.21	5.29	1.07	3.97	-3.56	7.79
TRX 15	1.64	3.90	-5.84	5.29	-10.00	15.04

Site	**Computation times in seconds**		
	IRT	**Dominant Path**	**Multi Wall**
TRX 10	20 s	< 1 s	< 1 s
TRX 15	2880 s	< 1 s	< 1 s

TABLE III. COMPARISON TO MEASUREMENTS

B. Old office building

Figures 12 and 13 show the predictions for two transmitter locations in a building of the Institute for Radio Frequency

Site	**Difference (Predictions – Measurements) in dB**					
	IRT		**Dominant Path**		**Multi Wall**	
	Mean value	***Std. Dev.***	***Mean value***	***Std. Dev.***	***Mean value***	***Std. Dev.***
TRX 3	9.94	7.31	-1.09	6.23	3.07	8.17
TRX 7	3.23	6.32	-3.96	5.74	0.19	5.90

TABLE IV. COMPUTATION TIMES (AMD ATHLON 2800+)

Technology at the University of Vienna [4], [5]. This building
is mainly built of brick and wood – so it represents the older office buildings. The database of the building contains 107 planar objects.

The carrier frequency for the measurements was 1800 MHz. A detailed description of the measurement equipment and campaign can be found in [4].

In figure 13 some propagation paths are presented. For each receiver location only one set of weighting factors for the determination of the paths is used. Each diffraction and each transmission causes an additional attenuation along the propagation path. The computation is made in 2D as everything (transmitter, receiver) is located on the same floor.

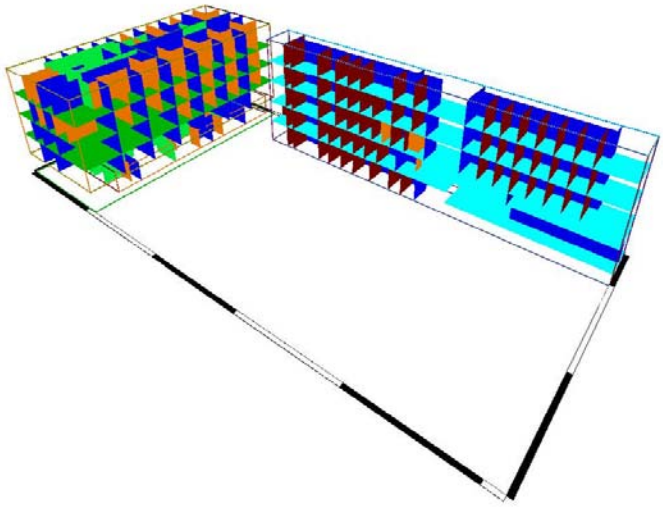
The comparison between the prediction models can be found in the tables III and IV. The results of the Dominant Path Model are good and in particular the computation time is very short in contrast to the IRT Model.

Site	Computation times in seconds		
	IRT	Dominant Path	Multi Wall
TRX 3	131 s	< 1 s	< 1 s
TRX 7	55 s	< 1 s	< 1 s

C. Multi-floor building

The considered multi-floor building is the office building of the Instituto de Telecomunicações (Instituto Superior Técnico, IST) and it is mainly built of concrete and glass – so it represents a typical modern office building. The multi floor building database of this building contains 355 planar objects.

In this scenario the transmitting antenna is located on the top of the building [7]. Measurements and predictions were made in two adjacent buildings, see figures 15 and 16. A three dimensional view of this scenario is given in figure 14.



The carrier frequency for this measurement was 950 MHz. As in this scenario the mobile station and the base station antenna are located on different floors (height of antenna: 19.5m, height of prediction: 7.8m, 4th floor), the 3D extension of the Dominant Path Model was used for the computation. When using the 3D Dominant Path Model, not only one prediction plane in the height of the receiver is used for the computation, but several layers between transmitter and receiver are used in order to improve the result. The differences between predictions and measurements are presented in table
V. The computation times are given in to table VI. All measurements together with a detailed description of the equipment can be found in [7].

If the transmitter is located outside a building the Dominant Path Model uses two different path loss exponents *n*. For the outdoor pixels, the coefficient 2.0 (ideal free space) is used.

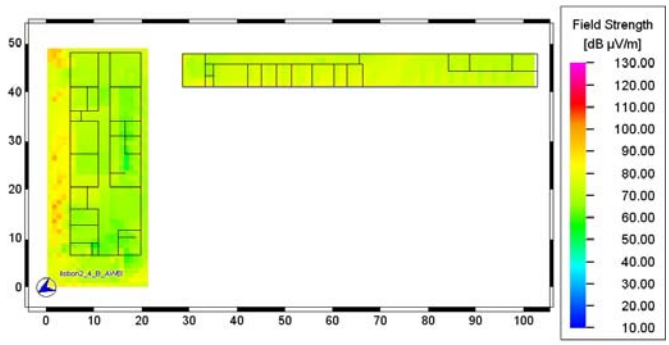
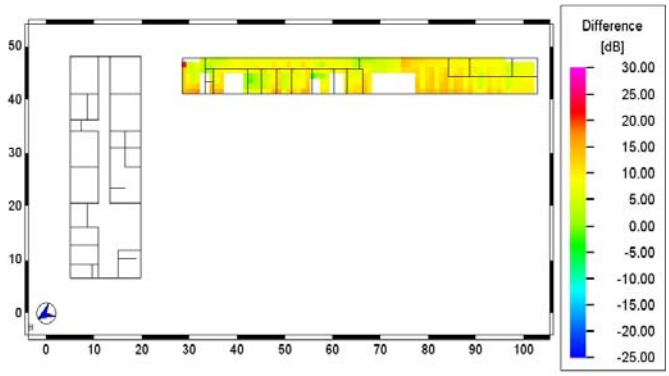


Figure 15. Prediction for Dominant Path Model (3D mode), Site 2_4_B



The tables V and VI show the differences to measurements for the compared prediction models and the computation times of the different models.

TABLE V. COMPARISON TO MEASUREMENTS **Site**	**Difference (Predictions – Measurements) in dB**					
	IRT		**Dominant Path**		**Multi Wall**	
	Mean value	***Std. Dev.***	***Mean value***	***Std. Dev.***	***Mean value***	***Std. Dev.***
2_4_B	1.32	4.37	8.71	3.17	-26.48	14.48

After the path entered the indoor area, the coefficient *n* is set to the value used for all indoor pixels (generally slightly higher than 2.0). This indoor coefficient includes the influence of furniture and other objects not included in the database.

TABLE VI. COMPUTATION TIMES (AMD ATHLON 2800+)

The result of the Dominant Path Model for this scenario is

Site	**Computation times in seconds**		
	IRT	**Dominant Path**	**Multi Wall**

2_4_B	5 s	31 s	1 s

quite good, but the computation time is longer than for IRT. This is due to the fact that the 3D mode was used for computation, in order to improve the accuracy of thr results (only 3.17 dB std. dev.).

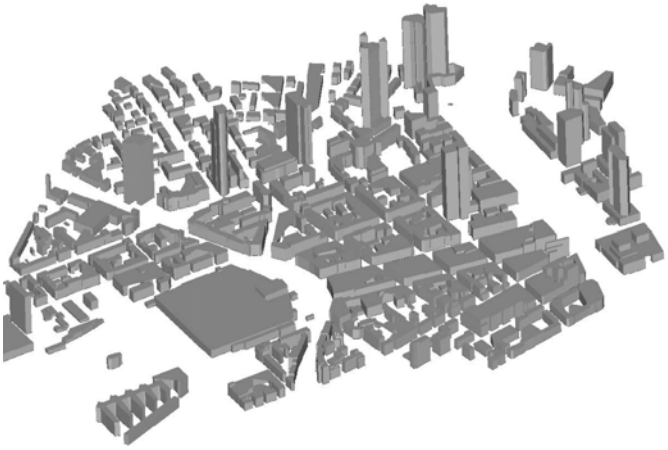
IV. URBAN PROPAGATION

A. General

The application of the Dominant Path approach to urban scenarios leads to some simplifications:

- Transmissions do not need do be considered
- The geometry of the considered building objects is less complex (polygonal cylinders)

As already stated in section II.A, the available building databases have a limited accuracy. For wave propagation modelling in urban scenarios, the databases usually only have
2.5 D information, i.e. for each building a polygonal cylinder and the height are defined (see figure 17). Therefore, the shape of the roof can not be considered in the modelling approach, which can have an impact especially if over-rooftop propagation is dominant.



This may be the case in scenarios with antenna locations above the mean building height. In this case the Dominant Path Model offers advantages as it is less sensitive to the inaccuracies that are caused by the simplification of the diffractions at the roofs.

Especially in scenarios where the transmitter is located below the mean building height, waveguiding effects become dominant for the propagation.

This is impressively demonstrated in figure 18. For a transmitter located below rooftop level (antenna height 15 meters), the results of the COST 231 Walfisch/Ikegami model (COST), the Ray Tracing Model (IRT) and the Dominant Path Model (DPM) model are shown.

The COST 231 model is too pessimistic in most parts of the scenario as there is a building obstructing the direct ray near the transmitter. The dominant effects of diffractions at this building and reflections that lead to waveguiding effects in street canyons are not modelled.

These effects are very well modelled by the IRT model, however far away from the transmitter, especially in the southern part of the image, the results are again too pessimistic as the number of interactions (max. 6) used for the computation limits the accuracy of the model, as obviously the rays that were found are not the ones which carry the main part of the power.

The Dominant Path Model result does not show these disadvantages. The whole scenario shows comprehensive results. Waveguiding effects are also visible in the Dominant Path Model.

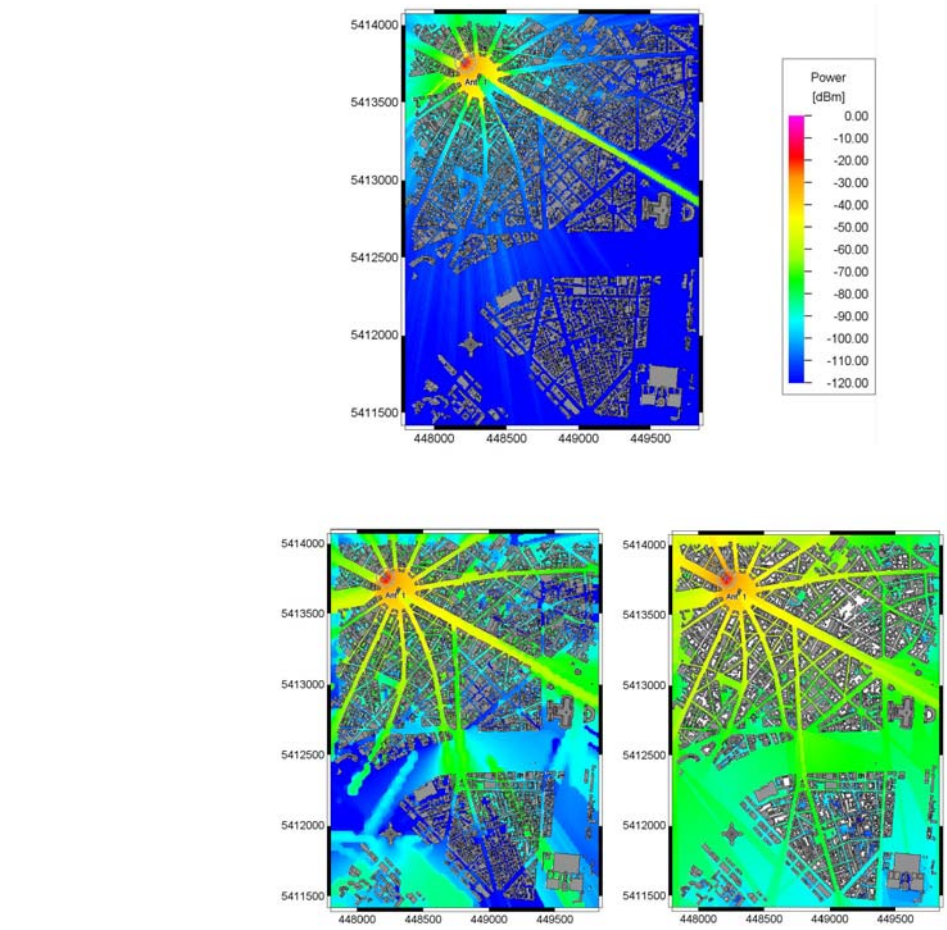
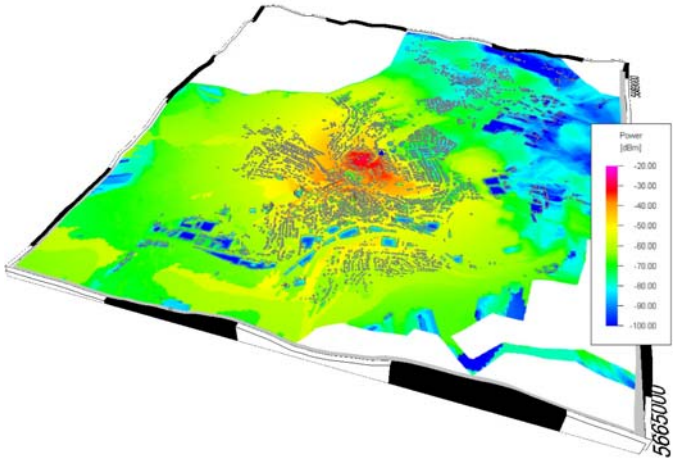


Figure 18. Prediction of received power with a transmitter below rooftop level: COST 231 W/I model (upper image), IRT model (lower left) and Dominant Path model (lower right)

In general, the topography of urban scenarios must also be taken into account, as it may influence the visibility of interactions points that are computed.

Figure 19 shows a prediction of a small city that is surrounded by hilly terrain using the IRT model. The area in the upper right part shows lower received power values due to the shadowing effect of the terrain. If the topography would not be considered a too optimistic prediction in this area would occur.



Both the Intelligent Ray Tracing model and the Dominant Path model allow the consideration of the topography.

B. Example I: COST 231 Benchmark in Munich

Several urban microcell prediction models have been developed and reviewed in COST 231. To verify and compare these models in a semi-blind test, vector-building data of downtown Munich (Germany) and three different measurement routes have been supplied by the German GSM network operator Mannesmann Mobilfunk GmbH (now Vodafone GmbH).

Table VII shows some details of the scenario, figure 20 shows the topography including the building heights as well as a 3D view of the scenario.

TABLE VII. SCENARIO DESCRIPTION FOR DOWNTOWN MUNICH

Scenario	*Area*	2.5 x 3.5 km = 8,75 km2
	Number of Buildings	2087
Transmitter	*Location*	(1281.36|1381.27|13.00)
	Frequency	947 MHz
	Antenna Type	Omni

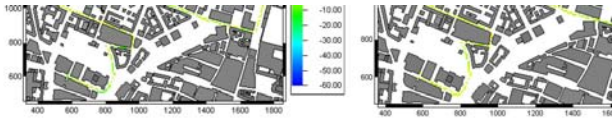


Figure 22. Difference of prediction and measurements (route 1): Ray Tracing (IRT) (left), Dominant Path Model (DPM) (right)

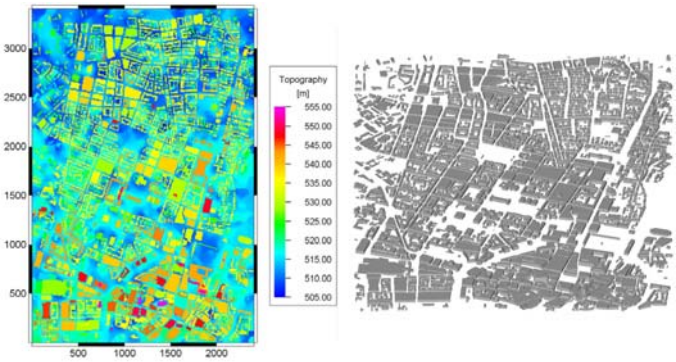


Figure 20. Downtown Munich scenario: Topography incl. building heights (left) and 3D view of buildings (right)

Figure 21 shows the prediction results of a ray tracing propagation model (here IRT [1], [3]) and the Dominant Path Model. Unlike in section A, the maximum number of interactions (6) was sufficient for this scenario. Therefore, only slight differences are visible, but the statistical evaluation (see below) allows the discussion of the differences.

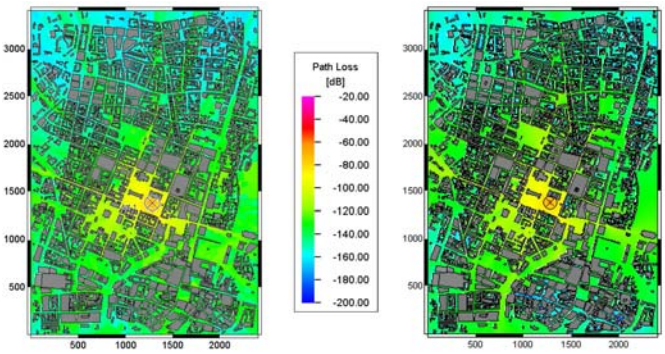


Figure 21. Prediction results: Ray Tracing (IRT) model (left), Dominant Path Model (DPM) (right)

The results were compared to all 3 available measurement routes. As an example, figure 22 shows the difference of the predictions and the measurements for measurement route 1.

Table VIII shows the results of a statistical evaluation for all 3 measurement routes. Although the Dominant Path model does not reach the accuracy of the Ray Tracing model, the results are very good especially in view of the computation times (see below).

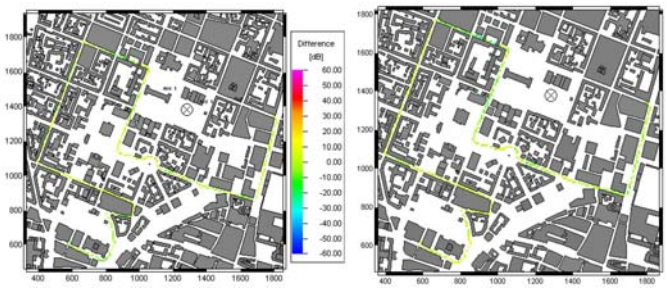


TABLE VIII. COMPARISON TO MEASUREMENTS

Route	**Difference (Predictions – Measurements)**			
	IRT		**Dominant Path**	
	Mean value	***Std. Dev.***	***Mean value***	***Std. Dev.***
0	-0.3	7.7	3.2	8.5
1	0.3	5.5	-0.2	5.6
2	-0.4	7.4	0.25	8.0

Table IX shows the prediction times for the Munich scenario. There is not much difference in the prediction times; the Dominant Path model is even slightly faster at a comparable accuracy.

However, there is one important point to mention: For predictions with the IRT model, a complex preprocessing [1] of the building data has to be done. Although this preprocessing has to be done only once per scenario independent of the number of transmitters and their position, it may be a constraint especially in very large scenarios.

TABLE IX. COMPARISON OF COMPUTATION TIMES

Transmitter	**Computation times [min:sec]** (using a standard PC with an a CPU AMD Athlon XP 2000+™ and 512 MB of RAM)	
	Intelligent Ray Tracing	**Dominant Path Model**

	Preprocess.	*Prediction*	*Preprocess.*	*Prediction*
1	117:30	0:28	0:05	0:26

C. Example II: Helsinki

The scenario, measurement, and all related topics are described in [1] and are therefore not repeated again in this document.

Table X shows some details of the scenario, figure 23 shows the topography including the building heights as well as a 3D view of the scenario. The map data was provided by FM-Kartta, Oy [11].

TABLE X. DESCRIPTION OF THE HELSINKI SCENARIO [1]

Scenario	*Area*	1.3 x 1.5 km = 1,95 km2
	Number of Buildings	228
Transmitter 1	*Location*	(5968.35|5011.39|4.00)
	Frequency	900 MHz
	Antenna Type	Omni
Transmitter 2	*Location*	(5724.95|4467.59|4.00)
	Frequency	900 MHz
	Antenna Type	Omni

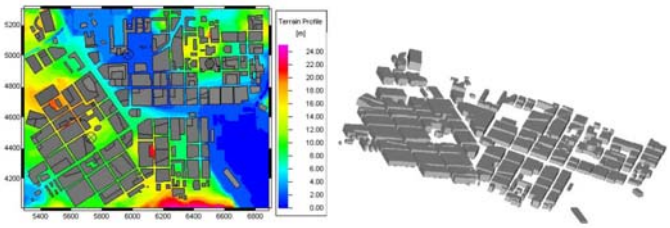


Figure 23. Helsinki scenario: Topography incl. building heights (left) and 3D view of buildings (right). Data provided by FM-Kartta [11].

Figure 24 shows the prediction results of both propagation models for transmitter 1. Like in section B, the maximum number of interactions (6) was sufficient for this scenario. Again, differences can mainly be seen in the statistical evaluation (see below).

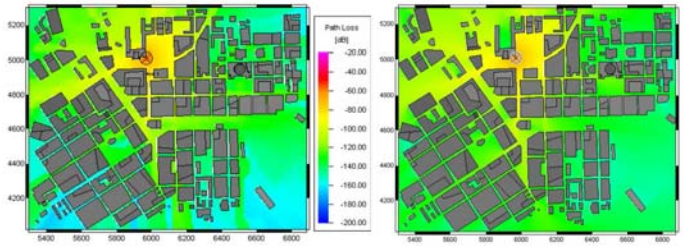


Figure 24. Prediction results for transmitter 1: IRT model (left), Dominant Path model (right)

The results for both transmitters were compared to the corresponding measurement routes. The accuracy obtained was acceptable with both models. Further discussion of the prediction results together with an analysis and description of the measurement routes is available in [1].

Table XI shows the results of a statistical evaluation for both transmitter positions. The results are comparable to the ones for the Munich scenarios (see section B), thus the dominant path model delivers good results at short computation times (see below).

TABLE XI. COMPARISON TO MEASUREMENTS

Transmitter	Difference (Predictions – Measurements)			
	IRT		Dominant Path	
	Mean value	*Std. Dev.*	*Mean value*	*Std. Dev.*
1	-0.4	7.1	2.3	8.0
2	0.7	6.7	0.45	6.8

Table IX shows the prediction times for the Helsinki scenario. There is no significant difference in the prediction times.

Concerning the required complex preprocessing of the building data see section B.

TABLE XII. COMPARISON OF COMPUTATION TIMES

Transmitter	**Computation times [min:sec]** (using a standard PC with an a CPU AMD Athlon XP 2000+™ and 512 MB of RAM)			
	Intelligent Ray Tracing		Dominant Path Model	
	Preprocess.	*Prediction*	*Preprocess.*	*Prediction*
1	03:55	0:04	0:01	0:03
2		0:03		0:03

D. Summar (Urban Models)

As both discussed scenarios are rather small, the limitations of the (Intelligent) Ray Tracing in terms of the number of interactions did not have an adverse effect on the results.

However, it is expected that in larger scenarios the results of the Dominant Path Model will be much more accurate especially for longer distances from the transmitter (depending on the building structure).

Together with the fact that an additional preprocessing is needed for the Intelligent Ray Tracing, the Dominant Path Model should be given preference for the analysis of large urban scenarios.

V. CONCLUSIONS

A new approach for propagation modelling in indoor and urban scenarios based on vector datbaabases is presented in this paper. The approach is based on the fact that not all rays between tranmsitter and receiver contribute a similar part of the energy. Some path are dominant and by determining only these dominant paths, the computation time is reduced without influencing the accuracy.

The new indoor and urban propagation models are compared to measurements performed in indoor and urban environments. In comparison to results of ray tracing predictions it is shown that the new propagation models reach the accuracy of ray tracing models or even exceed it. The computation times are in the range of empirical models and therefore very short. No preprocessing of the building data is needed.

As the models compute the dominant ray paths, also wideband properties of the channels (channel impulse response, delay spread) could be computed with statistical channel models. This will be the object of further studies together with the validation of the urban model in extremly hilly terrain (e.g. Hong Kong). .

REFERENCES

[1] R. Hoppe, P. Wertz, F. M. Landstorfer, and G. Wölfle: *Advanced rayoptical wave propagation modelling for urban and indoor scenarios including wideband properties*, European Transactions on Telecommunications 2003; 14:61-69.

[2] C. Carciofi, A. Cortina, C. Passerini, and S. Salvietti: *Fast field prediction techniques for indoor communication systems*, 2nd European Personal and Mobile Communications Conference (EPMCC), Bonn (Germany), pp. 37 – 42, Nov. 1997.

[3] AWE Communications, Germany, Software tool WinProp for the planning of mobile communication networks (incl. demo-version), www.awe-communications.com, March 2003.

[4] R. Gahleitner: *Radio Wave Propagation in and into Urban Buildings*, PhD Thesis, Technical University of Vienna, 1994.

[5] G. Woelfle, F.M. Landstorfer, R. Gahleitner, E. Bonek: *Extensions to the field strength prediction technique based on dominant paths between transmitter and receiver in indoor wireless communications*,. 2nd European Personal and Mobile Communications Conference (EPMCC) 1997, Bonn, Germany, pp. 29-36, Sept 1997.

[6] G. Woelfle, P. Wertz, F.M. Landstorfer: *Performance, Accuracy, and Generalization Capability of Indoor Propagation Models in Different Types of Buildings,* 10th IEEE Internat. Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) 1999, Sept. 1999, Osaka, Japan F5-2

[7] G. C. Angelo, I. Neto, L. M. Correia: *Health and Penetration Issues in Buildings with GSM Base Station Antennas on Top*,. 48th IEEE Vehicular Technology Conference (VTC) 1998, Ottawa, Ontario, Canada, May 1998

[8] G. Wölfle and F.M. Landstorfer: *Dominant Paths for the Field Strength Prediction,* 48th IEEE Vehicular Technology Conference (VTC) 1998, Ottawa, Ontario, Canada, May 1998, pp 552-556

[9] G. Wölfle and F.M. Landstorfer: *Field strength prediction with dominant paths and neural networks for indoor mobile communications* MIOP 1997, 22.-24. April 1997, Sindelfingen, Germany, pp. 216-220, Apr. 1997.

[10] T. Rautiainen, G. Wölfle, and R. Hoppe: *Verifying Path Loss and Delay Spread Predictions of a 3D Ray Tracing Propagation Model in Urban Environments,* 56th IEEE Vehicular Technology Conference (VTC) 2002 - Fall, Vancouver (British Columbia, Canada), Sept. 2002

[11] www.fm-kartta.com

ANEXO 2

HOJAS TECNICAS DE EQUIPOS

AP CISCO AIRONET 1100

ADAPTADOR INALAMBRICO CLIENTE USB - ASIARF

P/N: AWUG2407

WLAN USB Adapter

for IEEE802.11b/g
Auto Switch External Antenna Connector
AP and Client Modes
Support Point to Multi-point Base Station Support
Sony PSP X link
Support WMM TM (WiFi Multi Media)
Embeded Software Bridge

Product Specifications	
Standards Compliance	IEEE802.11b/g (Wireless)
Chipset	ZyDAS1211
Operation Mode	Ad hoc, Infrastructure (Access Points is needed)
Modulation Method	IEEE 802.11b: CCK, DQPSK, DBPSK IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM
RF Spreading Method	IEEE 802.11b : DSSS (Direct Sequence Spread Spectrum) IEEE 802.11g : OFDM (Orthogonal Frequency Division Multiplexing)
Operation Mode	Ad HOC Infrastructure (Access Point is needed)
Frequency Band	N. America / FCC : 2.412 ~ 2.462 GHz (11 channels) Europe CE / ETSI : 2.412 ~ 2.472 GHz (13 channels) Japan : 2.412 ~ 2.484 GHz (14 channels)

	France : 2.457 ~ 2.472 GHz (4 channels) Spain : 2.457 ~ 2.462 GHz (2 channels)
Transmission Rates	1 ~ 54 Mbps, with auto fallback
Transmitter Characteristics	17 dBm @11b, 14 dbm @11g
Receiver Characteristics	Sensitivity: at 11 Mbps: < –85 dBm @8% FER at 54 Mbps: < –68 dBm @8% FER
Security	64-bit or 128-bit WEP (Wired Equivalent Privacy) /WPA TKIP (Temporal Key Integrity Protocol)
I/O interface	USB 2.0
LED	Green LED Indicador
Antenna	On borrad Chip Antenna
Environmental Requirements	Operating Temperature:0° to 55° C Storage Temperature: -20° to 70°C Humidity: 5% to 90%, non-condensing
Dimensions	58 x 23 x 9 mm
Weight	9.6g
Power Consumption	Transmit: <320mV, Receive: <210Mv
Regulartory Approval	FCC;CE
Software Support	Windows-based Wireless Management System. Windows 98, Me, NT 4.0 (SP4 or above), 2000, XP, Linux, MAC
Transmission Range	100 to 300 meters (depend on surrounding)

Cisco Aironet 1100 Series Access Point

The Cisco® Aironet® 1100 Series Access Point provides a high-speed, secure, affordable, and easy-to-use wireless LAN solution that combines the freedom and flexibility of wireless networking with the features and services required in enterprise networks (Figure 1). The Cisco Aironet 1100 Series uses radio and network management features for simplified deployment, along with integrated diversity dipole antennas that provide robust and predictable WLAN coverage for offices and similar RF environments. The access point offers flexibility and investment protection for wireless networks.

The Cisco Aironet 1100 Series supports a single 802.11g radio. Users can enjoy up to 54 Mbps data rates while maintaining full backward compatibility with legacy 802.11b devices. Administrators can configure the access point to support both 802.11g and legacy 802.11b clients for investment protection, or for higher performance, the access point can be configured to support only 802.11g clients. The Cisco Aironet 1100 Series also features an innovative mounting system for easy installation and reliable coverage in a variety of locations and orientations. The Cisco Aironet 1100 Series is a component of the Cisco Unified Wireless Network, a comprehensive solution that delivers an integrated,
end-to-end wired and wireless network. Using the radio and network management features of the Cisco Unified Wireless Network for simplified deployment, the Cisco Aironet 1100 Series extends the security, scalability, reliability, ease of deployment, and manageability available in wired networks to the wireless LAN.

The Cisco Aironet 1100 Series is available in two versions: unified or autonomous. Unified access points operate with the Lightweight Access Point Protocol (LWAPP) and work in conjunction with Cisco wireless LAN controllers and the Cisco Wireless Control System (WCS). When configured with LWAPP, the Cisco Aironet 1100 Series can automatically detect the best-available Cisco wireless LAN controller and download appropriate policies and configuration information with no manual intervention. Autonomous access points are based on Cisco IOS® Software and may optionally operate with the CiscoWorks Wireless LAN Solution Engine (WLSE). Autonomous access points, along with the CiscoWorks WLSE, deliver a core set of features and may be field-upgraded to take advantage of the full benefits of the Cisco Unified Wireless Network as requirements evolve.

ENTERPRISE-CLASS SECURITY SOLUTION

The Cisco Aironet 1100 Series is part of the award-winning Cisco Wireless Security Suite, which supports 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA and numerous Extensible Authentication Protocol (EAP) types. WPA and WPA2 are the Wi-Fi Alliance certifications for interoperable, standards-based WLAN security. These certifications support IEEE 802.1X for user-based authentication, Temporal Key Integrity Protocol (TKIP) for WPA encryption, and the Advanced Encryption Standard (AES) for WPA2 encryption. These certifications help to ensure interoperability between Wi-Fi-certified WLAN devices from different manufacturers.

The hardware-accelerated AES encryption of Cisco Aironet 1100 Series Access Points supports enterprise-class, government-grade secure encryption over the WLAN without compromising performance. IEEE 802.1X authentication helps to ensure that only authorized users are allowed on the network. Backward compatibility for WPA client devices running TKIP, the RC4 encryption algorithm, is also supported.

SIMPLIFIED DEPLOYMENT FOR RAPID CONNECTIVITY

The Cisco Aironet 1100 Series defines enterprise office deployment capability. Designed in an attractive, durable plastic enclosure, with integrated diversity dipole antennas, the Cisco Aironet 1100 Series can be quickly deployed with a reliable, omnidirectional coverage pattern. Supported in various mounting orientations and locations, it can be easily moved throughout the work area as needs change (Figure 2). A standard, surfacemounting bracket supports installation on office walls and ceilings for elevated placement. UL 2043 certification for the plenum rating requirements set by local fire codes supports installation in environmental air spaces such as areas above suspended ceilings. The design protects against tampering and theft using single- or master-keyed padlocks. The Cisco Aironet 1100 Series can also be brought into the cubicle space with a cubicle wallmounting bracket or device stand. The device stand positions the access point on any horizontal surface, such as a desktop or shelf. Theft is deterred in these installations using the security slot with standard security cables. Support for either local or inline Power over Ethernet further simplifies installation. The Cisco Aironet 1100 Series is Wi-Fi certified to ensure interoperability with other IEEE 802.11g and IEEE 802.11b devices.

KEY FEATURES AND BENEFITS

The Cisco Aironet 1100 Series merges enterprise features, manageability, security, and availability into a scalable, easy-to-deploy, and cost-effective WLAN solution. Tables 1 and 2 highlight key features and product specifications for the Cisco Aironet 1100 Series.

Feature Benefit

2.4 GHz 802.11g Radio, Configurable up to 100 mW

2.4 GHz WLAN solution that delivers data rates of up to 54 Mbps with backwards compatibility to legacy 802.11b equipment.

Management Frame Protection • Provides strong cryptographic authentication of WLAN management frames and provides detection capabilities against publicly available Intrusion

Detection System (IDS) tools. Management frame protection is effective against known attacks, as well as any future attacks that rely on the unprotected nature of the WLAN management frames.

Hardware-Assisted AES Encryption Provides high security without performance degradation.

Quality of Service (QoS) • Prioritizes traffic for different application requirements.
• Improves user experience of voice and video.

Feature Benefit

Wi-Fi Multimedia (WMM) • Subset of the IEEE 802.11e QoS draft standard, supporting QoS prioritized media access through the Enhanced Distributed Channel Access (EDCA) method.

• Improves the user experience for audio, video, and voice applications over a Wi-Fi wireless connection.

Multiple Basic Service Set Identifier
(MBSSID)
Supports up to 8 BSSIDS for configuration flexibility when segmenting traffic.

Flexible Mounting Orientations Supports installation for a wide range of locations, including walls, ceilings, desktops, and cubicle partitions.

Anti-Theft Security Slot and Security Hasp
• Supports standard security cables or padlocks (not included).
• Locks can be single- or master-keyed for simplified inventory management.

Integrated Diversity Dipole Antennas • Has compact antenna profile.

• Provides spherical coverage pattern that is optimized for any orientation.

• Improves reliability in high-multipath environments such as offices.

Auto-Channel Selection Determines and selects least congested channel.

Supports Inline Power over Ethernet

• Eliminates need for local AC power.

• Reduces cable clutter.

• Enables deployment in remote locations.

Item Specification

Part Number • 802.11g: AIR-AP1121G-x-K9 (Cisco IOS® Software)

• 802.11g: AIR-LAP1121G-x-K9 (Cisco Unified Wireless Network Software).

Note: The Cisco Aironet 1100 Series may be ordered with Cisco IOS Software to operate as an autonomous AP or with Cisco Unified Wireless Network Software using the LWAPP. When operating as a lightweight access point, a WLAN controller is required.

Regulatory domains: (X=regulatory domain)

• A=FCC

• E=ETSI

• J=TELEC (Japan)

Customers are responsible for verifying approval for use in their country. Please visit http://www.cisco.com/go/aironet/compliance to verify approval and to identify the regulatory domain that corresponds to a particular country. Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.

Software • Cisco IOS Software Release 12.3(8)JA or later (autonomous).

• Cisco IOS Software Release 12.3(11)JX or later (Lightweight Mode).

• Cisco Unified Wireless Network Software Release 4.0 or later.

Data Rates Supported 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps

Network Standard IEEE 802.11b or IEEE 802.11g

Uplink Autosensing 802.3 10/100BaseT Ethernet

Item Specification

Frequency Band 802.11g:

• 2.412 to 2.462 GHz (FCC)

• 2.412 to 2.472 GHz (ETSI)

• 2.412 to 2.484 GHz CCK: (TELEC)

• 2.412 to 2.472 GHz Orthogonal Frequency Division Multiplexing (OFDM): (TELEC)

Network Architecture Type Infrastructure, star topology

Wireless Medium • 802.11g: OFDM

• 802.11b and 802.11g: Direct sequence spread spectrum (DSSS)

Media Access Protocol Carrier sense multiple access with collision avoidance (CSMA/CA)

Modulation OFDM:

• BPSK @ 6 and 9 Mbps

• QPSK @ 12 and 18 Mbps

• 16-QAM @ 24 and 36 Mbps

• 64-QAM @ 48 and 54 Mbps

DSS:

• DBPSK @ 1 Mbps

• DQPSK @ 2 Mbps

• CCK @ 5.5 and 11 Mbps

Operating Channels 802.11g ETSI: 13; Americas: 11; TELEC (Japan): CCK-14, OFDM-13

Nonoverlapping Channels Three

Receive Sensitivity 802.11b:

• 1 Mbps: -94 dBm

• 2 Mbps: -91 dBm

• 5.5 Mbps: -89 dBm

• 11 Mbps: -85 dBm

802.11g:

• 1 Mbps: -95 dBm

• 2 Mbps: -91 dBm

• 5.5 Mbps: -89 dBm

• 6 Mbps: -90 dBm

• 9 Mbps: -84 dBm

• 11 Mbps: -88 dBm

• 12 Mbps: -82 dBm

• 18 Mbps: -80 dBm

• 24 Mbps: -77 dBm

• 36 Mbps: -73 dBm

• 48 Mbps: -72 dBm

• 54 Mbps: -72 dBm

Item Specification

Available Transmit Power Settings 802.11g:

• CCK:

– 100 mW (20 dBm)

– 50 mW (17 dBm)

– 30 mW (15 dBm)

– 20 mW (13 dBm)

– 10 mW (10 dBm)

– 5 mW (7 dBm)

– 1 mW (0 dBm)

• OFDM:

– 30 mW (15 dBm)

– 20 mW (13 dBm)

– 10 mW (10 dBm)

– 5 mW (7 dBm)

– 1 mW (0 dBm)

Maximum power setting will vary according to individual country regulations.

Range Indoors: Distance across open office environment

• 90 ft (27 m) @ 54 Mbps

• 95 ft (29 m) @ 48 Mbps

• 100 ft (30 m) @ 36 Mbps

• 140 ft (42 m) @ 24 Mbps

• 180 ft (54 m) @ 18 Mbps

• 210 ft (64 m) @ 12 Mbps

• 220 ft (67 m) @ 11 Mbps

• 250 ft (76 m) @ 9 Mbps

• 300 ft (91 m) @ 6 Mbps

• 310 ft (94 m) @ 5.5 Mbps

• 350 ft (107 m) @ 2 Mbps

• 410 ft (125 m) @ 1 Mbps

Outdoors:

• 110 ft (34 m) @ 54 Mbps

• 200 ft (60 m) @ 48 Mbps

• 225 ft (69 m) @ 36 Mbps

• 325 ft (100 m) @ 24 Mbps

• 400 ft (122 m) @ 18 Mbps

• 475 ft (145 m) @ 12 Mbps

Item Specification

• 490 ft (150 m) @ 11 Mbps

• 550 ft (168 m) @ 9 Mbps

• 650 ft (198 m) @ 6 Mbps

• 660 ft (201 m) @ 5.5 Mbps

• 690 ft (210 m) @ 2 Mbps

• 700 ft (213 m) @ 1Mbps

Ranges and actual throughput vary based upon numerous environmental factors, so individual performance may differ.

Compliance Standards

• Safety:

– UL 1950

– CSA 22.2 No. 950-95

– IEC 60950

– EN 60950

• Radio approvals:

– FCC Part 15.247

– RSS-210 (Canada)

– EN 300.328 (Europe)

– ARIB-STD 33 (Japan)

– ARIB-STD 66 (Japan)

– AS/NZS 4268:2003 (Australia and New Zealand)

• EMI and susceptibility (Class B)

– FCC Part 15.107 and 15.109

– ICES-003 (Canada)

– VCCI (Japan)

– EN 301.489-1 and -17 (Europe)

• Security

– 802.11i, WPA2, WPA

– 802.1x

– AES, TKIP

• Other

– IEEE 802.11b and IEEE 802.11g

– FCC Bulletin OET-65C

– RSS-102

SNMP Compliance MIB I and MIB II

Antenna Integrated 2.2 dBi diversity dipole antennas

Item Specification

Security Authentication

Security Standards

• WPA

• WPA2 (802.11i)

• Cisco TKIP

• Cisco message integrity check (MIC)

• IEEE 802.11 Wired Equivalent Privacy (WEP) keys of 40 bits and 128 bits

802.1X EAP Types:

• EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)

• Protected EAP-Generic Token Card (PEAP-GTC)

• PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAP),

• EAP-Transport Layer Security (EAP-TLS)

• EAP-Tunneled TLS (EAP-TTLS)

• EAP-Subscriber Identity Module (EAP-SIM)

• Cisco LEAP

Encryption:

• AES-CCMP encryption (WPA2)

• TKIP (WPA)

• Cisco TKIP

• WPA TKIP

• IEEE 802.11 WEP keys of 40 bits and 128 bits

Status LEDs Three indicators on the top panel report association status, operation, error/warning, firmware upgrade,

and configuration, network/modem, and radio status.

Dimensions 4.1 in. (10.4 cm) wide; 8.1 in. (20.5 cm) high; 1.5 in. (3.8 cm) deep

Weight 10.5 oz. (297 g)

Environmental • 32–104° F (0-40° C)

• 10–90% humidity (noncondensing)

System Memory • 16 MB RAM

• 8 MB FLASH

Input Power Requirements • 100–240 VAC 50-0Hz (power supply)

• 33–57 VDC (device)

Power Draw 4.9 watts, RMS

Warranty One year

Wi-Fi Certification