

MIGRACIÓN HACIA LA PLATAFORMA DE INTERCONEXIÓN INALÁMBRICA
EN EL COLEGIO ANGLO AMERICANO

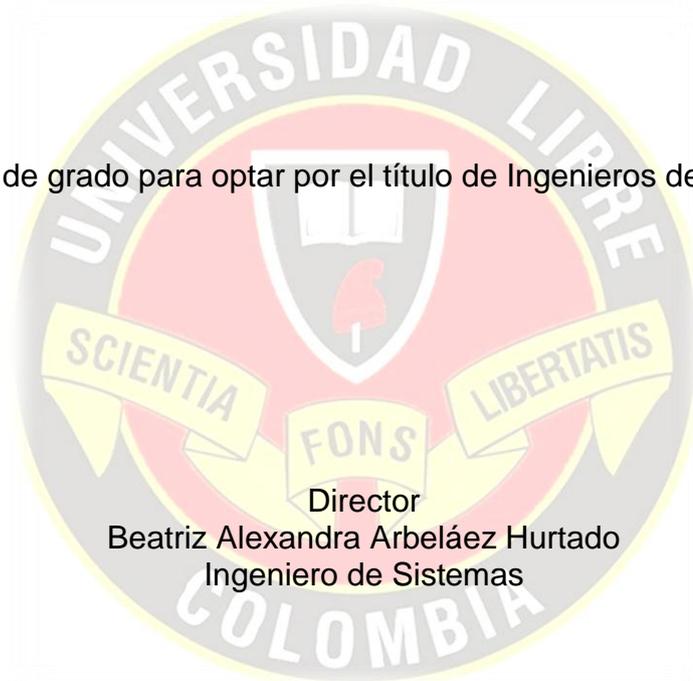


UNIVERSIDAD LIBRE
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
JULIO DE 2012

MIGRACIÓN HACIA LA PLATAFORMA DE INTERCONEXIÓN INALÁMBRICA
EN EL COLEGIO ANGLO AMERICANO

Javier Mauricio López Cárdenas 066051518
Andrés Mauricio Tangarife Medina 066051540

Trabajo de grado para optar por el título de Ingenieros de Sistemas



UNIVERSIDAD LIBRE
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
JULIO DE 2012

Nota de aceptación



Ing. Beatriz Alexandra Arbeláez
Tutora

Ing. Carlos Hernán Silva
Jurado 1

Ing. Eduardo Triana Moyano
Jurado 2

Bogotá D.C. 05 de Julio de 2012



La responsabilidad de los conceptos emitidos en este escrito es de los autores.

Son muchas las personas a las cuales quiero dedicar mis triunfos y en especial este logro tan grande que alcance después de años de esfuerzo, primero que todo doy gracias a Dios por darme la sabiduría, paciencia y fortaleza para afrontar este duro reto, gracias Mamá y Papá por enseñarme que los grandes hombres son capaces de sacar lo mejor de si para enfrentar cualquier desafío.

Agradezco a mis hermanos quienes con su voz de aliento me motivaron a seguir luchando tras los tropiezos que encontré en el camino, gracias Catalina Ramos por ser esa dama que siempre me brindo su amor, su comprensión y aquellos valiosos aportes que han sido fundamentales en mi vida, por último, infinitas gracias a mi tío Víctor Cárdenas quien ha luchado incansablemente por toda mi familia y en especial por verme formado como un profesional lleno grandes valores y principios morales.

Aquellas personas que no nombro pero que siempre han estado a mí lado agradezco todos y cada uno de sus valiosos consejos.

Esta etapa en mi vida que culminé representa un gran orgullo para mi, espero igualmente, ser motivo de orgullo para todos; los llevo en mi corazón.

JAVIER MAURICIO LÓPEZ C.

La tesis la dedico primero a dios por permitirme salir adelante con mi carrera pese a las dificultades. A toda mi familia, especialmente a mis padres quienes me apoyaron siempre.

A la coordinación administrativa del Colegio Anglo Americano por apoyar nuestro proyecto y por permitirnos realizar pruebas en sus instalaciones, de igual manera al Ingeniero Mario Insuasty por la colaboración y apoyo incondicional.

Un agradecimiento especial a los docentes de la facultad de Ingeniería de La Universidad por su esfuerzo y dedicación. Sus conocimientos, sus orientaciones, su manera de trabajar, su paciencia y su motivación han sido fundamentales en mi desarrollo académico. Ellos han inculcado en mí un sentido de seriedad, responsabilidad y rigor académico sin los cuales no podría haber tenido una formación completa como Ingeniero.

ANDRES MAURICIO TANGARIFE M.

AGRADECIMIENTOS

Expresamos nuestros más sinceros agradecimientos a:

- Viviana Sarmiento, coordinadora general del colegio Anglo Americano, quien depositó toda su confianza en nosotros y nos permitió realizar todas y cada una de las actividades programadas dentro de la institución, además nos permitió desarrollar nuestras habilidades como Ingenieros de la Universidad Libre.
- Al Ingeniero Mario Insuasty, jefe del departamento de informática y tecnología, por dedicarnos el tiempo necesario para explicarnos el funcionamiento regular del Colegio, los pro y los contras de la red LAN sobre la cual desarrollaríamos nuestro trabajo y sobre todo, por aportarnos su amplio conocimiento en cuanto a redes LAN se refiere.
- A la ingeniera Beatriz Alexandra Arbeláez, orientadora de nuestro proyecto de grado, quien basada en su experiencia y conocimientos, nos condujo por el camino hacia la elaboración y posterior conclusión del trabajo realizado para el colegio Anglo Americano.
- A la Universidad Libre De Colombia, recinto en el cual nos formamos como grandes profesionales capaces de enfrentar cualquier reto en la vida.

TABLA DE CONTENIDO

	RESUMEN	17
	INTRODUCCIÓN	18
1	MARCO REFERENCIAL DE DESARROLLO	19
1.1	DESCRIPCIÓN DEL PROBLEMA	19
1.2	FORMULACIÓN	21
1.3	OBJETIVOS	21
1.3.1	GENERAL	21
1.3.2	ESPECÍFICOS	22
1.4	DELIMITACIÓN	22
1.5	ANTECEDENTES	23
1.6	JUSTIFICACIÓN	23
1.7	ESPACIO DE DESARROLLO	24
	SITUACION ACTUAL DEL COLEGIO ANGLO	
1.7.1	AMERICANO	24
1.7.1.1	HISTORIA	24
1.7.1.2	PERFIL ANGLO AMERICANISTA	25
1.7.1.3	PRE-ESCOLAR	26
1.7.1.4	PRIMARIA	27
1.7.1.5	BACHILLERATO	28
1.7.1.6	CORPORACION SAN ISIDRO	29
2	MARCO TEÓRICO	31
2.1	REDES INALAMBRICAS	31
2.2	ESTANDAR IEEE 802.11	32
2.2.1	IEEE802.11B	33
2.2.1.1	CANALES 802.11B Y 802.11G	35
2.2.1.2	ANALISIS COSTO BENEFICIO	35
2.2.2	IEEE 802.11A	36
2.2.2.1	CANALES	37
2.2.2.2	ANALISIS COSTO BENEFICIO	37
2.2.3	IEEE 802.11G	38
2.2.3.1	ANALISIS COSTO BENEFICIO	39
2.3	OPERACIÓN BASICA DE WI-FI	39
2.4	VISION GENERAL DE PROTOCOLO WI-FI	40
2.5	SEGURIDAD DE LA RED INALAMBRICA	43

2.5.1	METODOS DE AUTENTICACION	44
2.5.1.1	FILTRADO DE DIRECCIONES MAC	45
2.5.1.2	SSID SERVICE SET IDENTIFIER	46
2.5.1.3	802.1X	46
2.5.1.4	WEP	49
2.5.1.4.1	LIMITACIONES	50
2.5.2	PROTOCOLO DE AUTENTICACION EXTENSIBLE EAP	51
2.5.3	METODOS DE ENCRIPACION DE DATOS	53
2.5.3.1	WI-FI PROTECTED ACCESS WPA	53
2.5.4	MEDIDAS DE SEGURIDAD ADICIONALES	55
2.5.4.1	RED PRIVADA VIRTUAL (VPN)	55
2.5.4.2	FIREWALLS	57
2.6	VOZ SOBRE IP	57
2.6.1	COMPONENTES DE VOZ SOBRE IP	58
2.6.2	PROTOCOLOS DE VOIP	59
2.6.2.1	PROTOCOLO H.323	60
2.6.2.2	PROTOCOLO SIP	61
2.6.2.3	PROTOCOLO IAX	62
2.6.2.4	PROTOCOLO MGCP	62
3	INGENIERÍA DEL PROYECTO	64
	SITUACION ACTUAL: LOGISTICA E INFRAESTRUCTURA	
3.1	DEL COLEGIO ANGLO AMERICANO	64
3.2	PROYECTO DE MODERNIZACION	65
3.2.1	NECESIDAD ESPECIFICA	66
3.3	DISEÑO DE LA RED INALAMBRICA	67
3.3.1	ANALISIS DE REQUERIMIENTOS	68
3.3.1.1	COBERTURA	68
3.3.1.2	SEGURIDAD	68
3.3.1.3	ESCALABILIDAD	69
3.3.1.4	CALIDAD DE SERVICIO	69
3.3.2	PLANIFICACION DE LA WLAN	70
3.3.2.1	EL MODELO DE PREDICCION DOMINANT PATH	71
3.3.2.2	LA SUITE DE SOFTWARE WINPROP	72
	DETERMINACION DE NUMERO Y UBICACIÓN DE	
3.3.3	ACCESS POINTS	75
3.3.3.1	CREACION DE LA BASE DE DATOS	77
3.3.3.2	UBICACIÓN DE LOS ACCESS POINTS	78
3.3.3.3	ACCESS POINTS	78
3.3.3.3.1	ADAPTADORES DE RED WIRELESS LAN	79
3.3.4	ARQUITECTURA DE LA RED ETHERNET	79
3.3.4.1	DIMENSIONAMIENTO DE LA INTRANET	79
3.3.4.1.1	VOZ SOBRE UNA RED INALAMBRICA	81

3.3.4.1.1.1	CALIDAD DEL SERVICIO (QOS)	82
3.3.4.1.1.1.1	WMM	82
3.3.4.1.1.2	CONTROL DE ADMISION DE LLAMADAS	85
3.3.4.1.1.3	EVALUACION EXPERIMENTAL	86
3.3.4.1.1.4	SOLUCION PARA VOIP	95
3.3.4.1.1.4.1	SERVIDOR ASTERISK	96
3.3.4.2	BACKBONE DE LA RED LAN	99
3.3.4.3	BASES TECNICAS DE EQUIPOS DE RED LAN	100
3.3.4.3.1	SWITCH DE BACKBONE	100
3.3.4.3.2	ROUTER DE BACKBONE	100
3.3.4.3.3	TARJETAS DE RED NIC PARA SERVIDORES	100
3.3.4.3.4	SERVIDOR DE VOZ	100
3.3.4.3.5	TARJETAS ANALOGAS	101
3.3.5	FUNCIONAMIENTO GENERAL DE LA RED MIXTA VOZ Y DATOS	101
3.4	ANALISIS ECONOMICO	103
3.4.1	SELECCIÓN DE EQUIPOS Y MATERIALES PARA LA INTRANET DEL COLEGIO SEGÚN ANALISIS DE RELACION COSTO-BENEFICIO	103
3.4.1.1	DISPOSITIVOS DE RED	105
3.4.1.2	CABLEADO ESTRUCTURADO	107
3.4.1.3	SERVIDORES DE RED Y SOFTWARE	108
3.4.1.4	MANO DE OBRA	109
3.4.2	PRESUPUESTO FINAL	109
3.4.3	FINANCIACION DEL PROYECTO	111
4	CONCLUSIONES	112
5	RECOMENDACIONES	113
	BIBLIOGRAFÍA	114
	INFOGRAFÍA	115
	ANEXOS	116

LISTA DE TABLAS

TABLA 1	FAMILIA DEL ESTANDAR IEEE 802.11	33
TABLA 2	CARACTERISTICAS DEL ESTANDAR 802.11B	34
TABLA 3	CARACTERISTICAS DEL ESTANDAR 802.11A	36
TABLA 4	CARACTERISTICAS DEL ESTANDAR 802.11G	38
TABLA 5	PILA DE PROTOCOLOS RTP	60
TABLA 6	CATEGORIAS DE ACCESO DE WI-FI MULTIMEDIA	83
TABLA 7	CUADRO COMPARATIVO DE PUNTOS DE ACCESO (AP) CUADRO COMPARATIVO DE ADAPTADORES DE RED	106
TABLA 8	PCI (TARJETAS INALAMBRICAS) CUADRO COMPARATIVO DE SERVIDORES PARA	106
TABLA 9	COMUNICACIÓN DE VOZ	108
TABLA 10	PRESUPUESTO FINAL DEL PROYECTO	110
TABLA 11	FINANCIACION DEL PROYECTO	111

LISTA DE FIGURAS

FIGURA 1	PREESCOLAR	27
FIGURA 2	PRIMARIA	28
FIGURA 3	BACHILLERATO	29
FIGURA 4	RED INALAMBRICA	31
FIGURA 5	ESPECTRO DE FRECUENCIAS PARA EL ESTANDAR 802.11B	34
FIGURA 6	ESPECTRO DE FRECUENCIAS DEL ESTANDAR 802.11A	37
FIGURA 7	ESTRUCTURA TIPICA DE UNA RED WI-FI	41
FIGURA 8	ARQUITECTURA DE UN SISTEMA DE AUTENTICACION 802.1X	47
FIGURA 9	ESTRUCTURA DE UNA VPN PARA ACCESO INALAMBRICO	55
FIGURA 10	SERVIDOR DE PROCESAMIENTO DE LLAMADAS MODELO DE RED TCP/IP & OSI Y PROTOCOLOS	58
FIGURA 11	PRINCIPALES	60
FIGURA 12	INFRAESTRUCTURA FISICA	64
FIGURA 13	AREA COLEGIO ANGLO AMERICANO	64
FIGURA 14	RACK DEL COLEGIO ANGLO AMERICANO	77
FIGURA 15	UBICACIÓN ROUTERS COLEGIO ANGLO AMERICANO	78
FIGURA 16	THROUGHPUT DE UNA LLAMADA DE VOZ vs NUMERO DE ESTACIONES	87
FIGURA 17	IMPACTO DE TXOP SOBRE DOS ESTACIONES SATURADAS	88
FIGURA 18	IMPACTO DE TXOP SOBRE DOS ESTACIONES SATURADAS (2)	89
FIGURA 19	IMPACTO DE CWmin SOBRE DOS ESTACIONES SATURADAS	90
FIGURA 20	IMPACTO DE CWmin SOBRE DOS ESTACIONES SATURADAS (2)	90
FIGURA 21	IMPACTO DE AIFS SOBRE DOS ESTACIONES SATURADAS	91
FIGURA 22	IMPACTO DE AIFS SOBRE DOS ESTACIONES SATURADAS (2)	91
FIGURA 23	DELAY PROMEDIO PARA UNA LLAMADA DE VOZ CON ESTACIONES SATURADAS	93
FIGURA 24	CDF PARA EL DELAY DE UNA LLAMADA NO PRIORIZADA, CON AIFS=4, CON AIFS=6	94
FIGURA 25	PORCION DE TIEMPO QUE LA CAPA MAC ESTA OCUPADA	95
FIGURA 26	ESQUEMA DE FUNCIONAMIENTO DE ASTERISK	97
FIGURA 27	AJUSTE DE LOS PARAMETROS MAC DE 802.11N	101

LISTA DE ANEXOS

ANEXO A	DISTRIBUCION RED BACHILLERATO Y COMEDOR	117
ANEXO B	DISTRIBUCION RED BLOQUE PRIMARIA Y OFICINA 4	118
ANEXO C	DISTRIBUCION RED PRE-ESCOLAR	119
ANEXO D	DISTRIBUCION RED RACK SISTEMAS	120
ANEXO E	DISTRIBUCION RED SALAS 3 Y 4	121
ANEXO F	DISTRIBUCION RED SALAS 1 Y 2	122

GLOSARIO

Access Point: Punto de acceso a una Wireless LAN. Es la interface 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 / Collision 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, sabotaje, 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 Área Network. Red de datos de área local. Se caracteriza por tener relativamente pequeñas extensiones, pero muy altas velocidades de transmisión.

Service Pack 3 (SP3): Paquete de Servicios No. 3, 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 enviados a algún punto de la red.

Wireless LAN: 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 interoperabilidad.

RESUMEN

La red con la que cuenta el colegio Anglo Americano permite que las diferentes dependencias compartan información (archivos), recursos (impresoras), y servicios (internet) entre si, por ello, en este proyecto se presentan los resultados obtenidos de una investigación realizada para poder mejorar la eficiencia y eficacia del funcionamiento de la red de dicha institución, así mismo identificar los pro y los contra que posee la estructura actual aplicando normas ISO , estándares IEEE, implementación de protocolos OSI, análisis de trafico entre otros. La ejecución de dicho estudio se realizara en las instalaciones del colegio y estará fundamentado en temas como redes LAN y WAN, arquitectura de computadores, sistemas operativos, telecomunicaciones, redes móviles, desde el punto de vista ingenieril, equipos especializados nuevos y algunos ya en uso .

Adicionalmente se describen las herramientas que se van a utilizar para dar solución al problema planteado inicialmente, damos a conocer de manera detallada las redes LAN y WAN, su estructura, funcionamiento y conceptos básicos. Finalmente se elabora una propuesta adaptada exclusivamente al problema planteado.

ABSTRACT

The network that American Anglo School has allows different departments to share information (files), resources (printers) and services (internet). This Project presented as result of improvement investigation and efficiency and institution systems operation effectiveness, qualities and defect for current structure applying ISO, IEEE implementation of OSI protocols, traffic analysis and more. The study implementation is conducted in the school premises and will be base on issues such as LAN and WAN network, architecture, operating system, telecommunication mobile network as engineering view and specialized new equipment and already some in used.

Also recibes tools that will be use to solve the inically posted problem, we present detail of LAN and WAN structure, function and base concepts. Finally, proposal is adapted to this individual problema.

INTRODUCCIÓN

En el colegio Anglo Americano actualmente se cuenta con una red LAN la cual sirve de apoyo a las diversas dependencias, ya que por medio de ella estudiantes, docentes y directivos acceden a servicios como archivos, bases de datos, backup, website etc., por ello se pretende hacer un estudio a fondo del estado actual de dicha red con el fin realizar las modificaciones necesarias para optimizar su funcionamiento; entendiéndose por modificaciones al diseño de planos, cambio de los equipos y reestructuración de la misma.

Este proyecto se presenta como una solución al problema de comunicación y a la necesidad de tener un sistema eficaz, eficiente y completo que satisfaga todas las necesidades a nivel de comunicación. Por ello, nuestra investigación estará encaminada hacia las redes inalámbricas (WI-FI) y VoIP, esto con el fin de proponer la implementación de tecnologías de este tipo las cuales impulsen al colegio Anglo Americano al desarrollo e incursión de nuevos y mejores tipos de sistemas informáticos.

1. MARCO REFERENCIAL DE DESARROLLO

1.1 DESCRIPCIÓN DEL PROBLEMA

El Colegio Anglo Americano inicia sus actividades como institución educativa el 9 de febrero de 1965 en la Carrera 14 # 72-85 con las secciones de preescolar, primaria y primer curso de básica secundaria, congregando un número de aproximado de 60 estudiantes. A raíz de su rápido crecimiento la institución se vio en la necesidad de trasladar sus instalaciones a la Calle 170 # 8-80 puesto que empezaron a necesitar amplias aulas, aula virtual de matemáticas, música y danzas, bibliotecas, laboratorios de INGLÉS, FÍSICA, QUÍMICA, CIENCIAS, apropiadas áreas administrativas y sobre todo nuevas y mejores salas de cómputo.

A medida que el Colegio fue creciendo se hizo indispensable la utilización de tecnologías de información para poder llevar a cabo el control de los procesos internos de la institución, dicho crecimiento los llevo a crear redes LAN si ningún tipo de control ni estandarización.

La institución cuenta con una comunidad virtual en la cual se pueden consultar boletines, informes disciplinarios, circulares, responder encuestas, revisar cronogramas de evaluaciones de los estudiantes y se mantiene una constante comunicación entre docentes, padres de familia y personal administrativo, debido a esto el departamento de sistemas del colegio tiene como responsabilidad garantizar el funcionamiento interno de la red ya que los docentes alimentan la base de datos para los diferentes módulos ya sea de interna como de los padres de familia. Actualmente podemos identificar tres tipos de problemas en la red que clasificaremos de la siguiente manera:

- **Problemas de Software:** Problemas de Aplicación, protocolos incompatibles direcciones IP en conflicto, tablas de enrutamiento mal configuradas.
- **Problemas de Hardware:** tarjetas de red y switch en mal estado, Routers mal configurados.
- **Problemas físicos:** Conectores en mal estado, cables rotos, oxidación de contactos.

Tomando como referente el planteamiento anteriormente citado, se podría decir que la problemática principal radica en la ineficiencia e inestabilidad de la red con la que cuenta actualmente el Colegio Anglo Americano, ya que en los últimos dos años se han presentado problemas en el funcionamiento.

La posible solución a la problemática pretende dar respuesta al siguiente interrogante:

¿Cómo podemos estandarizar la Red LAN actual con la que cuenta el Colegio en sus instalaciones para prevenir posibles pérdidas en la información?

Este gran interrogante permite plantear una serie de pequeños interrogantes como:

- ¿La red actual cuenta con planos o algún tipo de documentación que sirva de apoyo al momento de un percance?
- ¿La distribución de la red dentro de las instalaciones del Colegio esta debidamente fundamentada por los diversos estándares internacionales en cuanto a redes se refiere?
- ¿Existe un modelo artificial de la red en algún tipo de software simulador de redes?
- ¿El Colegio cuenta con los recursos y el equipo necesario para trabajar en un proyecto de esta magnitud?
- ¿Es posible implementar nuevamente la red en el colegio?

De esta manera se desea proponer la implementación de 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 usaran 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 determinaran las plataformas de software para la operación de la Intranet, así como sus sistemas informáticos aplicados.

Se utilizara el software WinProp lo que permitira 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.

1.2 FORMULACION

¿Incide Diseño e implementación de la red mixta del colegio Anglo Americano con el uso del estándar 802.11n?

1.3 OBJETIVOS

1.3.1 GENERAL

- Implementar una red inalámbrica mixta para el sistema de comunicaciones del colegio Anglo Americano, con tecnología de punta y bajo costo operacional que sirva de apoyo a las comunicaciones de voz y datos, mejorando el tipo de servicios ofrecidos.

1.3.2 ESPECIFICOS

- Corregir errores en el diseño, proceso y mantenimiento de la red existente
- Implementar una red inalámbrica mixta
- Aplicar nuevas tecnologías para mejorar el uso de las comunicaciones en el colegio Anglo Americano
- Brindar nuevos servicios para la toda la comunidad educativa del Colegio Anglo Americano

1.4 DELIMITACIÓN

El proyecto avanzara siempre y cuando en Colegio Anglo Americano proporcione los recursos necesarios para la implementación del mismo, es decir, la investigación no se compromete a proporcionar ningún tipo de dispositivo que llegara a requerirse.

El proyecto, al nombrar dentro de sus objetivos específicos la Implementación, no hace referencia al montaje de la Red como tal, es decir, a la elaboración de toda la infraestructura; esto hace referencia básicamente a la administración de los procesos que se realicen durante el trabajo y la posterior puesta en marcha a cargo de los investigadores.

Por otra parte, los investigadores se comprometen a hacer un estudio bien documentado en cuanto vigilancia IP se refiere, dejando claro los beneficios que esto traería para el Colegio, ya que es una institución en vías de desarrollo; en ningún momento la investigación realizara el montaje de dicho sistema de video vigilancia en caso que la institución adopte la idea.

Por ultimo, la investigación no se compromete a prestar ningún tipo de soporte posterior a la fecha de culminación del proyecto.

1.5 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 Inalámbricas.

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 & negro y después a color).

1.6 JUSTIFICACIÓN

En vista de los posibles inconvenientes que pueda llegar a tener el Colegio Anglo Americano se procederá a desarrollar un proyecto el cual tiene como finalidad implementar una red inalámbrica mixta voz y datos para mejorar la eficiencia y eficacia de funcionamiento de red. Los pros y los contras que posee la estructura actual, teniendo en cuenta aspectos puntuales en el diseño de

redes como lo son: normas ISO, estándares IEEE, implementación de protocolos OSI, análisis de tráfico entre otros.

Considerando la magnitud del problema se ha diseñado un plan de trabajo el cual tiene como finalidad hacer que los procesos y comunicaciones tanto internos como externos del Colegio tengan un buen funcionamiento, esto con la posibilidad de contar con algún tipo de soporte que garantice que una persona capacitada puede entender la infraestructura de la red propuesta.

Las diferentes estaciones que tendrá el trabajo están fundamentadas en temas como: redes LAN y WLAN, arquitectura de computadores, sistemas operativos, telecomunicaciones, redes móviles, desde el punto de vista ingenieril, equipos especializados nuevos y algunos de segunda como Router, Switch, Rack, servidores, PC, conversores de fibra óptica, cajas receptoras de fibra óptica, Patch panel, cable UTP categoría 6, conectores RJ 45, desde el punto de vista técnico.

La culminación del proyecto encaminara mas a la institución a seguir vinculándose con nuevas tecnologías y porque no, seguir siendo líder y pionero en educación de la mano de las tecnologías de información.

1.7 ESPACIO DE DESARROLLO

1.7.1 SITUACIÓN ACTUAL DEL COLEGIO ANGLO AMERICANO

1.7.1.1 HISTORIA

El Colegio Anglo Americano inició sus actividades el 9 de febrero de 1965 en la Carrera 14 N° 72-85 con las secciones de preescolar, primaria y primer curso de básica secundarias, congregando un número aproximado de 60 estudiantes. En 1966 se abrieron los cursos de segundo y tercero de básica secundaria; en 1967 el curso cuarto y en 1968 el quinto de bachillerato. Desde 1973 funciona en las instalaciones de la calle 170 N° 8-80, acordes a las necesidades de la

Institución: amplias aulas, salas de cómputo, aula virtual de matemáticas, música y danzas, bibliotecas, laboratorios de INGLÉS, FÍSICA, QUÍMICA, CIENCIAS, dos campos de fútbol con medidas reglamentarias, canchas de baloncesto y voleibol, extensas zonas verdes y apropiadas áreas administrativas.

En 1969 egresó la primera promoción integrada por 21 bachilleres. Hasta la fecha han salido de su claustro 41 promociones para un número aproximado de 3.500 egresados con muy alto nivel de conocimientos en el idioma Inglés, calificados hoy como excelentes profesionales y motivo de orgullo para la Institución.

Desde sus inicios, el Colegio Anglo Americano se ha trazado como norte trabajar en busca de la excelencia educativa, dando un máximo de importancia a la formación de valores y al nivel académico con especial énfasis en el idioma Inglés.

Recomendamos remitirse a la sección de departamentos para recibir información sobre cada una de las asignaturas incluyendo inglés.

En el año de 1997, la Secretaría de Educación del Distrito otorgó a nuestra Institución una meritoria distinción: **el premio al mejor Proyecto Educativo Institucional.**

1.7.1.2 PERFIL ANGLO AMERICANISTA

El proyecto pedagógico está orientado a la formación de un modelo de ciudadano ejemplar, de acuerdo con el perfil anglo americanista que es el siguiente **"seguro de sí mismo, respetuoso, afectivo, consciente de la importancia de estudiar por el profundo deseo de aprender, con la firme aspiración de ser un persona culta y un profesional con éxito. Ser responsable, honesto y leal. Ser sensible a los problemas y necesidades de las personas más desprotegidas".**

El colegio brinda un ambiente propicio para fortalecer la autoestima de los estudiantes, dando especial atención a quienes presentan dificultades en este aspecto.

Los directivos y docentes realizan reflexiones constantes con los estudiantes con el propósito de recordarles que la honestidad es un principio que se fundamenta en la rectitud al obrar y hablar. A través del dialogo se les recuerda la importancia del respeto a sí mismo, a sus familiares y a los miembros de la comunidad educativa. De la misma manera se trabaja con gran empeño en enseñarles a transmitir afectividad y en inculcarles la necesidad de **estudiar por el profundo deseo de aprender**. Consideramos esencial en el desarrollo del ser humano el asumir los deberes con responsabilidad.

Para el colegio es fundamental que sus estudiantes interioricen que es un deber social el compartir y ayudar a los demás, en especial a aquellas más desprotegidas.

1.7.1.3 PRE-ESCOLAR

El Colegio Anglo Americano tiene especial interés por su sección de preescolar, donde inician prácticamente la totalidad de bachilleres que egresan de la Institución, pues es la cuna de la gran familia Anglo-Americanista. Los niños aprenden a amar su Colegio junto con sus profesores y profesoras, profesionales idóneos enamorados de su carrera cuyo excelente desempeño les permite proyectar su vocación de manera natural y formarse según el perfil Institucional.

Quienes visitan esta sección del Colegio se llevan una agradable impresión de su planta física dotada de hermosas zonas verdes con jardines, parques, aulas amplias, luminosas, decoradas con gran esmero para que los niños se sientan acogidos como en su propio hogar. La Institución cuenta con diversos materiales y recursos como la casa de muñecas, las aulas especializadas de danzas, música, lectura, inglés e informática. Cada docente orienta su trabajo implementando en su metodología cantos, rondas, juegos, cuentos y otras

actividades de tipo lúdico que hacen sus clases especiales y facilitan el aprendizaje significativo, logrando así sentar bases firmes en su proceso de educación. La figura 1 ilustra una de las aulas de informática de pre-escolar.

Figura 1 Pre-escolar



Fuente: <http://www.angloamericanobogota.edu.co/preescolar.html>

1.7.1.4 PRIMARIA

Preocupados por el desarrollo integral de los estudiantes, nuestro objetivo principal es la formación de personas con una base sólida en valores, capaces de enfrentar el acelerado avance del mundo actual. La Sección Primaria cuenta con un cuerpo de docentes especializados en cada una de las asignaturas que se imparten y brindan los medios y herramientas necesarias para potenciar el desarrollo de habilidades, procesos de pensamiento e inteligencias múltiples. En su labor diaria dan constantemente el máximo de importancia a la formación en valores. Los estudiantes reciben clases de inglés intensivo incluyendo el área de ciencias. Tienen actividades extraescolares los días miércoles de 3:30 a 5:00 p.m. y los días sábados en escuelas deportivas y artísticas. Adicionalmente se brinda estudio dirigido a los estudiantes que necesitan ayuda de sus profesores para superar sus dificultades en las diferentes asignaturas.

Conscientes de que hoy en día es indispensable forjar en los estudiantes una cultura en el conocimiento de Tecnología de la Informática y las Comunicaciones, el colegio les permite desde temprana edad desarrollar destrezas y habilidades en estas áreas, a través de la elaboración de diferentes proyectos. La figura 2 hace alusión a estudiantes adquiriendo conocimientos informáticos.

Figura 2 Primaria



Fuente: <http://www.angloamericanobogota.edu.co/informatica.html>

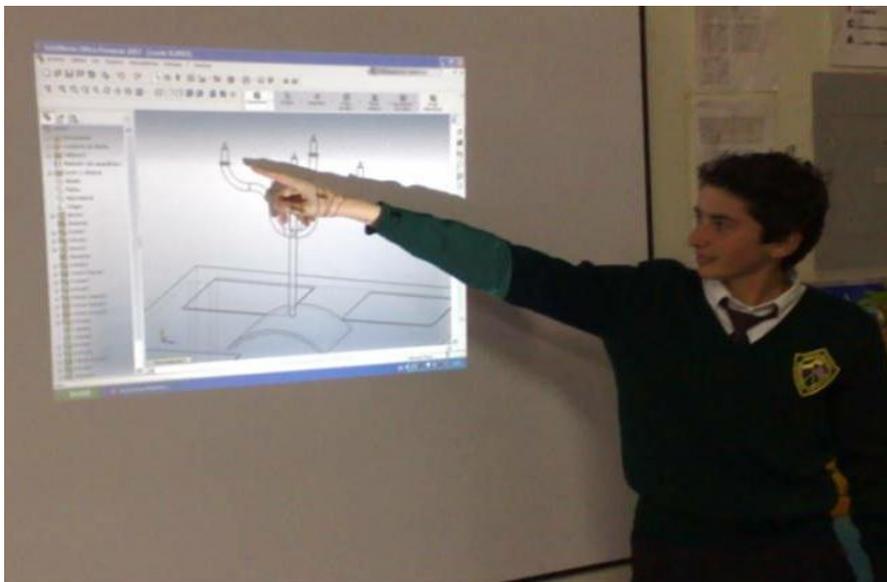
1.7.1.5 BACHILLERATO

En esta sección la mayoría de los estudiantes que iniciaron su proceso en preescolar culminan su vida de colegio, siendo fundamental la generación de espacios para compartir sus experiencias y descubrir los intereses que marcarán su vida futura.

En esta etapa se forman jóvenes capaces de afrontar los retos universitarios. Para ello los estudiantes encuentran la oportunidad de expresar sus opiniones, ser creativos y solucionar las problemáticas propias de la adolescencia, dentro de un ambiente de exigencia no sólo académica sino de vivencia de las normas, que permiten un desarrollo de la persona acorde con el mundo actual. Teniendo en cuenta sus habilidades y aptitudes pueden participar de los énfasis en ciencias de la salud, humanidades, ingeniería y administración, que les permite conocer y tomar decisiones apropiadas en cuanto a su carrera

futura. LA figura 3 muestra a un bachiller haciendo uso de una de las herramientas tecnológicas que ofrece el colegio.

Figura 3 Bachillerato



Fuente: <http://www.angloamericanobogota.edu.co/informatica.html>

1.7.1.6 CORPORACION SAN ISIDRO

La Corporación San Isidro es una entidad sin ánimo de lucro que administra los ingresos del Colegio Anglo Americano y por acuerdo con la sociedad propietaria de la institución, destina la totalidad de sus excedentes en la construcción de viviendas para familias de extrema pobreza. Para la realización de cada uno de los proyectos ha sido necesario recibir algunas donaciones y otras ayudas financieras, por ejemplo: la firma constructora CONCONCRETO hizo el trabajo de administración delegada sin cobrar honorarios, en la compra de los materiales, los proveedores más importantes nos han hecho grandes descuentos, el arquitecto y otros profesionales han trabajado con honorarios muy bajos.

El Consejo Superior presidido por su Representante Legal Dr. Hugo Alirio Moreno es el gestor de los proyectos. Hasta la fecha Julio 30 de 2010 la Corporación San Isidro ha construido 2041 apartamentos. En el

tercer proyecto construyó un colegio para los hijos de los beneficiarios y dos salones para talleres de capacitación.

Procedimiento para la selección de familias beneficiarias – postulaciones y ventas:

La Corporación San Isidro selecciona familias de extrema pobreza, en su mayoría habitantes de tugurios o de inquilinatos donde tres o cuatro familias con varios niños comparten el baño y la cocina. Les entrega un apartamento de 45 m² con acabados y totalmente terminado, para que lo habiten en calidad de arrendatarios durante un mínimo de cuatro años, pagando una mensualidad de aprox. \$ 90.000, valor que pagarían por una pieza de inquilinato. El objetivo es observar el comportamiento de la familia durante este período para reconfirmar que merece el beneficio de que se les escriture el apartamento. En caso de queja se les da la oportunidad de mejorar, firmando un acta de compromiso y al no cumplirla no se les renueva el contrato y se inicia un proceso de restitución del inmueble para venderlo a personas fuera del programa. Las familias que pierden el derecho a la renovación del contrato de arrendamiento y a comprar el apartamento en condición de beneficiarios, han manifestado su inconformidad con actividades de protesta denunciando información que no corresponde a la realidad. Son personas que han dado motivo de queja por algunas de las siguientes causales:

Consumo de drogas, actividades de delincuencia, exceso en el consumo de licor, hijos de residentes que pertenecen a pandillas que se dedican a actividades al margen de la ley, irrespeto con representantes de la Corporación o con otros residentes del conjunto, incumplimiento en el pago del canon de arrendamiento o hipoteca.

Transcurridos los cuatro años, hace directamente el trámite para que las familias reciban el subsidio del Estado. Para poder tramitar el subsidio, los beneficiarios afiliados a cajas de compensación deben tener una cuenta de ahorro programado con el 10 % del valor del apartamento. No lo exigen a personas con trabajo independiente.

2 MARCO TEORICO

2.1 REDES INALAMBRICAS

Una red inalámbrica es 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.

En la figura 4, 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 Wi-Fi (802.11), que es un conjunto de reglas que proveen seguridad, confiabilidad y rapidez de conectividad inalámbrica. Más adelante se detallara su funcionamiento.

Figura4 Red inalámbrica



Fuente: http://susy-lopz.blogspot.com/2011_06_01_archive.html

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 publicó 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 EE.UU, pero sí 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 Seleccion" (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 1 se presenta un resumen de toda la familia del estándar

Tabla 1 Familia del estándar IEEE 802.11

FAMILIA DEL ESTÁNDAR IEEE 802.11		
ESTANDAR	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.

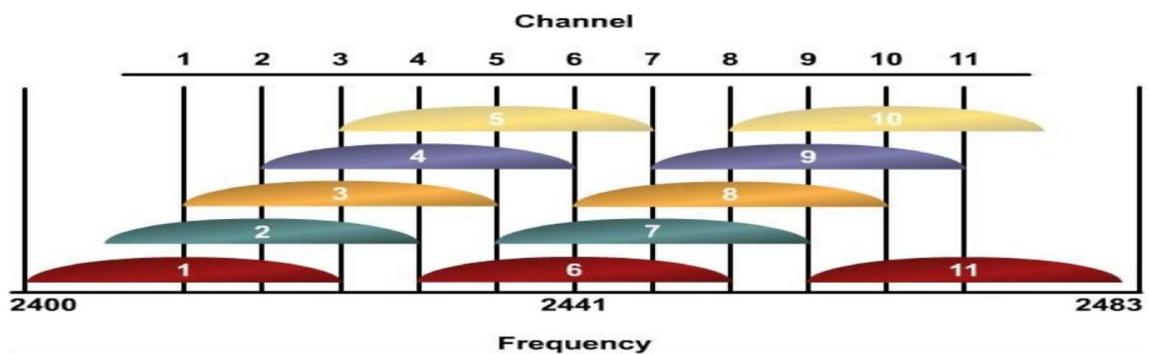
Este estándar define el Carrier Sense Multiple Access with Collision Avoidance (CSMA / CA) como protocolo de acceso al medio. Un gran porcentaje de la capacidad de canal disponible ha sido sacrificado (debido al uso de CSMA/CA) para incrementar la seguridad en las transmisiones de datos bajo condiciones diversas y adversas del ambiente. En la tabla 2 se presentan las características principales de este estándar.

Tabla 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)

El estándar 802.11b y el 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 5.

Figura 5 Espectro de frecuencias para estándar 802.11b



Fuente: <http://cesarcabrera.info/1disenno.pdf>

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.

2.2.1.1 CANALES 802.11b Y 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 puede 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.

A continuación, en la tabla 3 se presenta las características principales de este estándar.

Tabla 3 Características del estándar 802.11a

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

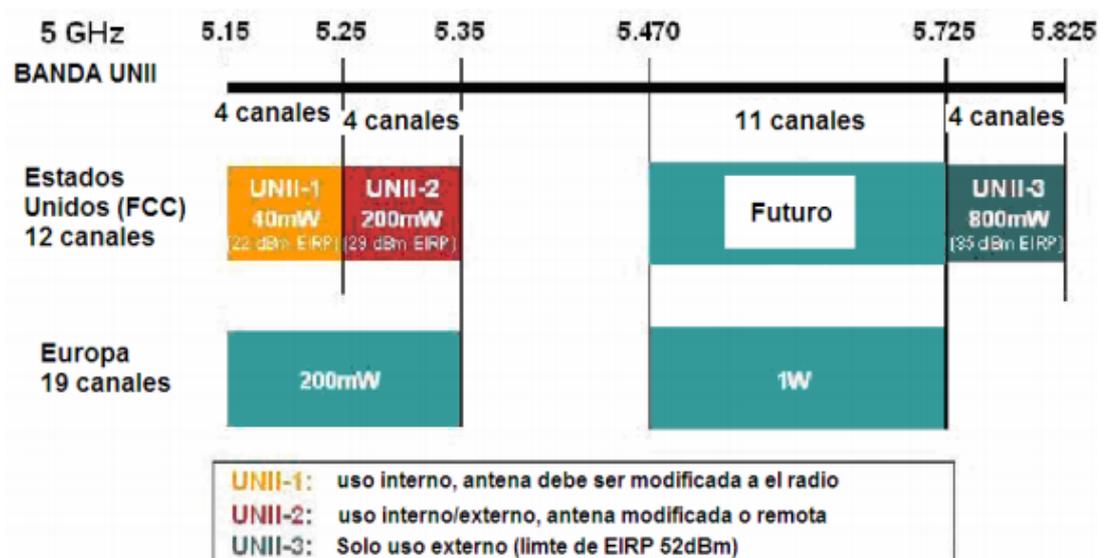
La tasa de datos es reducida a 48, 36, 24, 18, 12, 9 y 6 Mbps si se requiere. Dentro de los doce canales, ocho son dedicados para enlaces interiores y cuatro para enlaces punto a punto.

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 6 se indica una gráfica, en la cual se observa la distribución de los canales para el estándar 802.11a.

Figura 6 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 canales 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 4 se indican las características del estándar 802.11g.

Tabla 4. Características de estándar 802.11g

Frecuencia de operación	2.4 GHz ISM
Tasa de transferencia (teórica)	54 Mbps
Tasa de transferencia (Tx de lx)	20 - 30 Mbps (promedio)
Mecanismo	OFDM (Orthogonal Frequency Division Multiplexing)
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 ésta finaliza su modo de operación de infraestructura, puede desasociarse y desautenticarse 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).

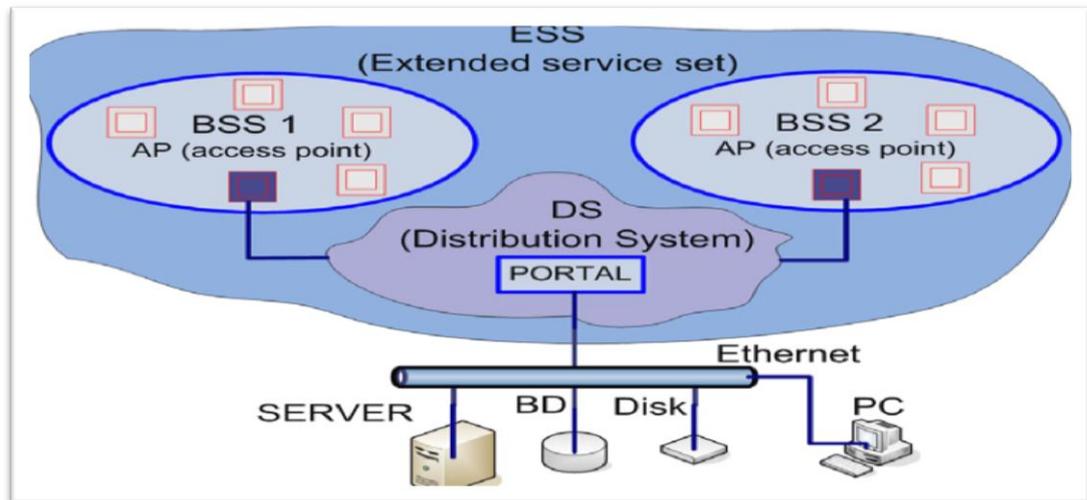
Alternativamente, una infraestructura BSS puede ser parte de una red extensa, a esto se lo llama Extended Service Set (ESS). Un ESS es el conjunto de una o más infraestructuras BSS conectadas vía distribución sistema, cuya naturaleza no esta especificada por el estándar, pudiendo ser una red cableada 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. Además, 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 7 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 7 Estructura Típica de una red Wi-Fi.



Fuente: <http://flylib.com/books/en/2.317.1.37/1/>

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 utiliza 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 además 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 demodulación 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: 3/4, 2/3 o 1/2, 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 está 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

Se han expuesto los grandes beneficios que la WLAN 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 sea 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.

2.5.1 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

2.5.1.1 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.

2.5.1.2 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.

2.5.1.3 802.1x

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:

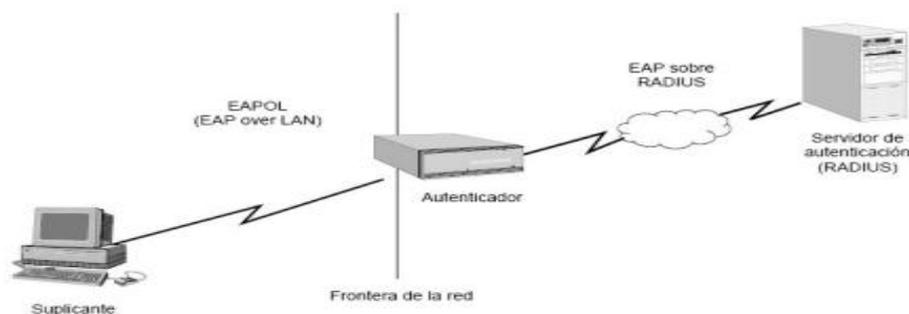
- El equipo del cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In 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.

En la figura 8 se muestra un ejemplo de un sistema de autenticación basado en el protocolo 802.1x.

Figura 8 Arquitectura de un sistema de autenticación 802.1x



Fuente: <http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf>

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 alámbrado) 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 RADIUS Access-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 renvía 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.

2.5.1.4 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 WEPCrack8 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.

2.5.1.4.1 LIMITACIONES

WEP protege el tráfico inalámbrico combinando la clave secreta WEP con un número de 24 bits generado aleatoriamente 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 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 ENCRIPCIÓN 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.

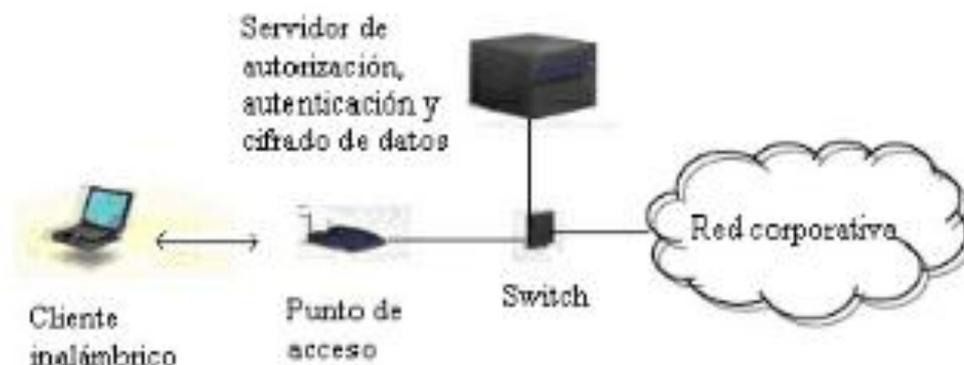
2.5.4 MEDIDAS DE SEGURIDAD ADICIONALES

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. LA figura 9 muestra un esquema de conexión de una VPN.

Figura 9 Estructura de una VPN para acceso inalámbrico



Fuente: <http://es.scribd.com/doc/73274511/47/Figura-5-3-Estructura-de-una-VPN-para-acceso-inalambrico-seguro>

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 interoperabilidad. 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 interoperabilidad 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.

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 está ocupado durante el tiempo que el paquete está 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.

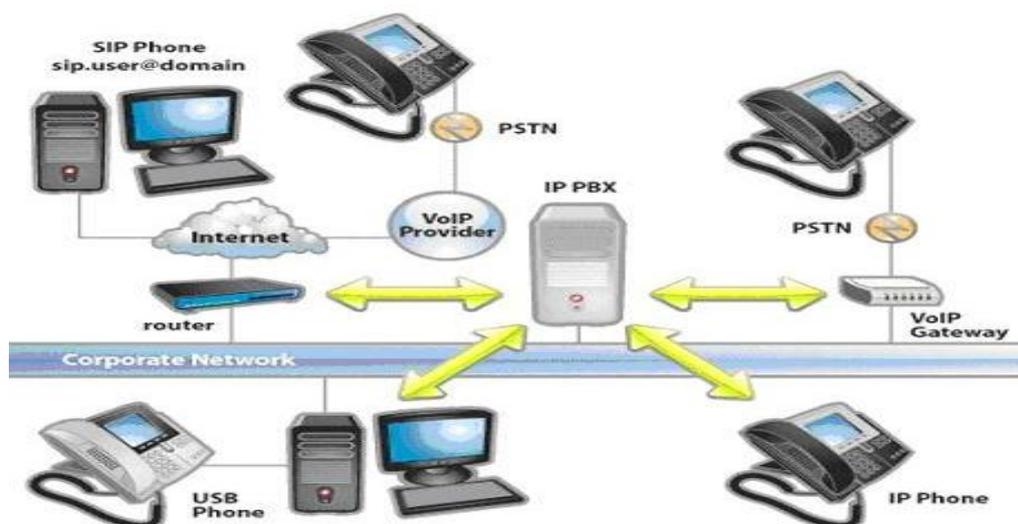
En el mundo IP, la voz es otra aplicación de datos funcionando sobre una red IP. En un ambiente mixto, los PBX llegan a ser el equivalente a un súper servidor que está en la red y es accesado por clientes remotos en cualquier lugar de la red sobre cualquier tipo de líneas de transmisión.

2.6.1 COMPONENTES DE VOZ SOBRE IP

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

- **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 tráfico 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 (tráfico 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. La figura 10 muestra una central PBX para VoIP.

Figura 10 Servidor de procesamiento de llamadas



Fuente: <http://e-estrategia.blogspot.com>

- **Teléfonos IP:** utilizan el protocolo TCP/IP para comunicarse con la red IP. Debe tener una dirección IP de la red en la que está instalado. Típicamente, estos teléfonos usan DHCP, protocolo para asignamiento dinámico de direcciones IP a dispositivos en una red.
- **Gateway 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. A continuación en la tabla 5 mostramos la pila de protocolos RTP.

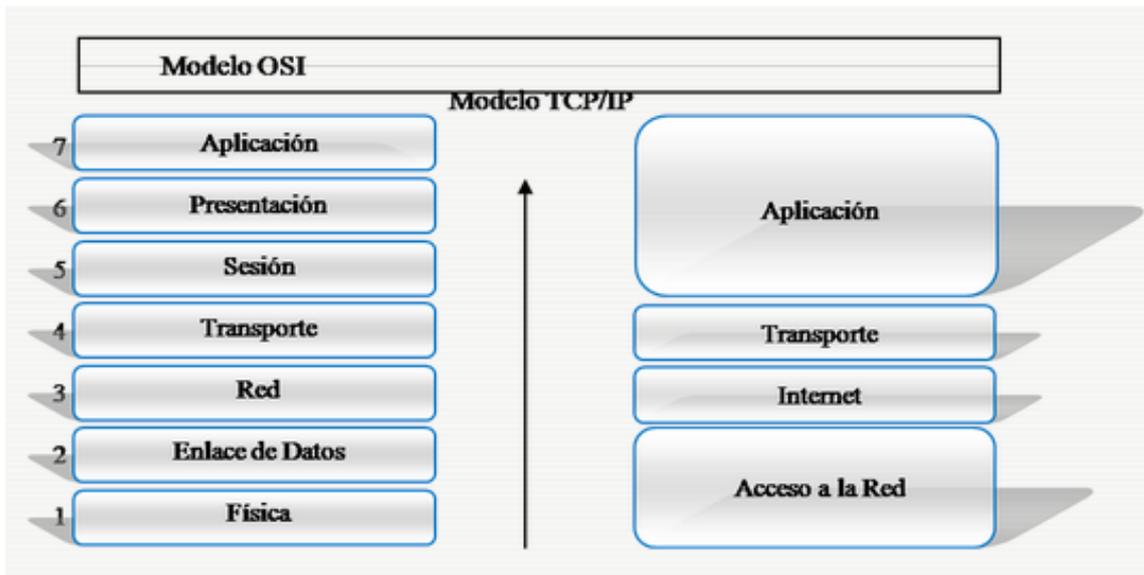
Tabla 5 Pila de protocolos RTP

MUESTREO DE VOZ
CODEC
RTP
UDP
IP

Fuente: <http://www.aslan.es/boletin/boletin30/acterna.shtml>

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). La figura 11 ilustra la tabla del modelo OSI y TCP y sus protocolos principales.

Figura 11 Modelo de red TCP/IP & OSI y protocolos principales



Fuente: <http://www.ciscoredes.com/tutoriales/60-modelo-osi-y-tpc-ip.html>

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 protocolos 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 multimedia 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.

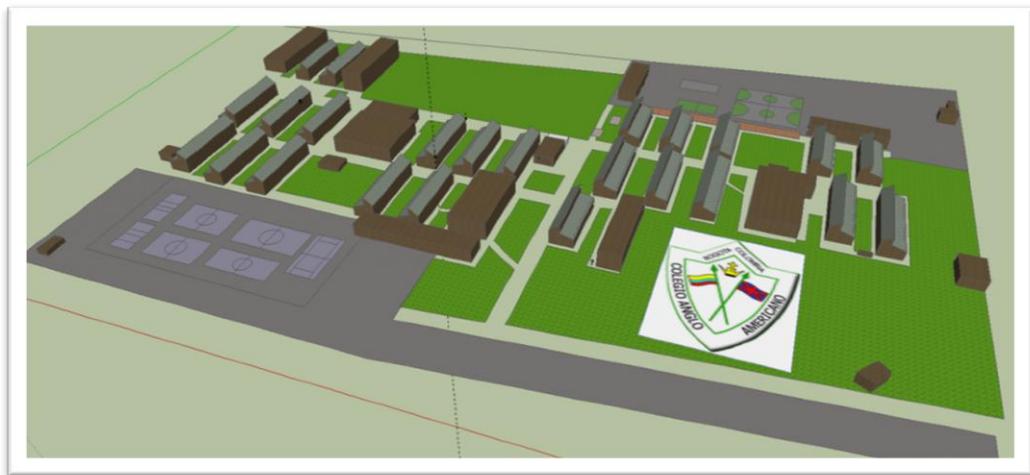
MGCP introduce esta división en los roles con la intención de aliviar a la entidad encargada de transformar el audio para ambos lados terminales, de las tareas de señalización, concentrando en el MGC el procesamiento de la señalización.

3. INGENIERÍA DEL PROYECTO

3.1 SITUACION ACTUAL: LOGISTICA E INFRAESTRUCTURA DEL COLEGIO ANGLO AMERICANO

El plano que se presenta en la figura 12 hace referencia a la infraestructura total del colegio con todas sus dependencias que en este caso, hacen parte de la infraestructura de la WLAN a implementar.

Figura 12 Infraestructura física



Fuente: Diseño realizado por los estudiantes en el programa GOOGLE SKETCHUP
Posteriormente en la figura 13 se analiza el área total del colegio gracias a una foto tomada por satélite mediante Google Earth.

Figura 13 Área del colegio Anglo Americano



Fuente: Imagen capturada desde GOOGLE EARTH

Infraestructura tecnológica

Actualmente el colegio Anglo Americano 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 Cat6 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 del colegio Anglo Americano

Equipos de Computación.

El colegio Anglo Americano 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 secretarías, mientras que los de mejores características son utilizados por los arquitectos, ingenieros, etc.

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

3.2 PROYECTO DE MODERNIZACION

En las anteriores secciones se muestra la infraestructura tecnológica con la que cuenta el Colegio Anglo Americano. Sin embargo, no debe entenderse que la institución se ha despreocupado, sino que, de acuerdo a las necesidades que se presentan, está en la obligación de dar una solución eficaz a cada una de ellas.

La distribución de las diferentes áreas del colegio y el continuo cambio de estas, el mal gasto de las llamadas telefónicas internas, son algunas de las causas por la que la administración ha planteado realizar este proyecto de modernización de la infraestructura tecnológica del colegio Anglo Americano

3.2.1 NECESIDAD ESPECÍFICA

Se pretende, primeramente contar con una red de datos inalámbrica en toda la edificación, ya que como se analizó en el capítulo 1, las áreas del colegio están en continuo cambio y modernización por tanto el número de usuarios de red, además se instalan nuevos módulos o se retiran 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 internamente.

Sobre esta red inalámbrica, se requiere saber la factibilidad de instalar una red de voz sobre IP, con el finalidad de reducir 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 del Colegio Anglo Americano 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 del colegio.

El usuario que desee conectarse a la red necesitara entonces de un computador con un dispositivo de acceso a esta Wireless LAN, 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 válida la solución propuesta, el colegio Anglo Americano ha determinado que al momento de estreno de la red y aplicaciones, esta serviría

a por lo menos 200 computadores más otros dispositivos que se añadan a esta. Hablamos entonces, de una Intranet que soportara aproximadamente a 250 clientes.

3.3 DISEÑO DE LA RED INALÁMBRICA

La sección 3.2.1. Se refiere a la solución general consensuada para el problema del colegio, esta 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 numeral 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 al colegio Anglo Americano. 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.

3.3.1 ANALISIS DE REQUERIMIENTOS

Es preciso definir con exactitud los requerimientos acerca de la red LAN que constituirá la Intranet para las diferentes áreas del Colegio Anglo Americano. Serán la base de las consideraciones de diseño.

3.3.1.1 COBERTURA

El requerimiento de cobertura de la nueva red ha sido determinado por la propia administración. Según las actividades que se realizan en las áreas, se han identificado los sitios que por su importancia sería ideal que estén cubiertos con el alcance de la red.

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 instalaciones.

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.

3.3.1.2 SEGURIDAD

Este tema es un requerimiento indispensable en todo el proceso de diseño, debido a que la información correspondiente a las labores institucionales del Colegio Anglo Americano 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.

3.3.1.3 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 180 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 dé a la red, así como nuevas aplicaciones tecnológicas que pudieran aparecer.

3.3.1.4 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 áreas 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.

3.3.2 PLANIFICACIÓN DE LA WLAN

El tema de la planificación en un proyecto que 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 todas las áreas del Colegio Anglo Americano.
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 802.11n, 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 iniciamos el tratamiento de las herramientas para la predicción del funcionamiento de la WLAN que se pretende implantar.

3.3.2.1 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 für 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.

Este método se ha desarrollado e implantado en una poderosa herramienta de software desarrollada por AWE Communications (Winprop), que permite

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.

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.

3.3.2.2 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”¹ 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 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 comunicaciones móviles, adaptado a condiciones prácticas. El modelo

¹ Outdoor: expresión usada para referirse a espacios abiertos, extensos.

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 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 Tracing³, 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, Proman. A continuación una explicación breve de cada uno:

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

- **Aman:** Antena 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.
- **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. Proman 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, se pretende que AWE Communications otorgue 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.

3.3.3 DETERMINACIÓN DE NÚMERO 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 utilizarán 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 del colegio ANGLO AMERICANO 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 mostrarán 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 qué no decir imposible.

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

- **Tasas de transmisión esperadas:** se busca conceder a los usuarios una conexión con las tasas más altas de la norma IEEE 802.11g. esto es 36, 48, 54 Mbps.
- **Factor de diseño:** aunque el modelo de predicción DP y las simulaciones ofrezcan un buen grado de confiabilidad en los resultados obtenidos, no se descuida 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 más 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.
- **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.

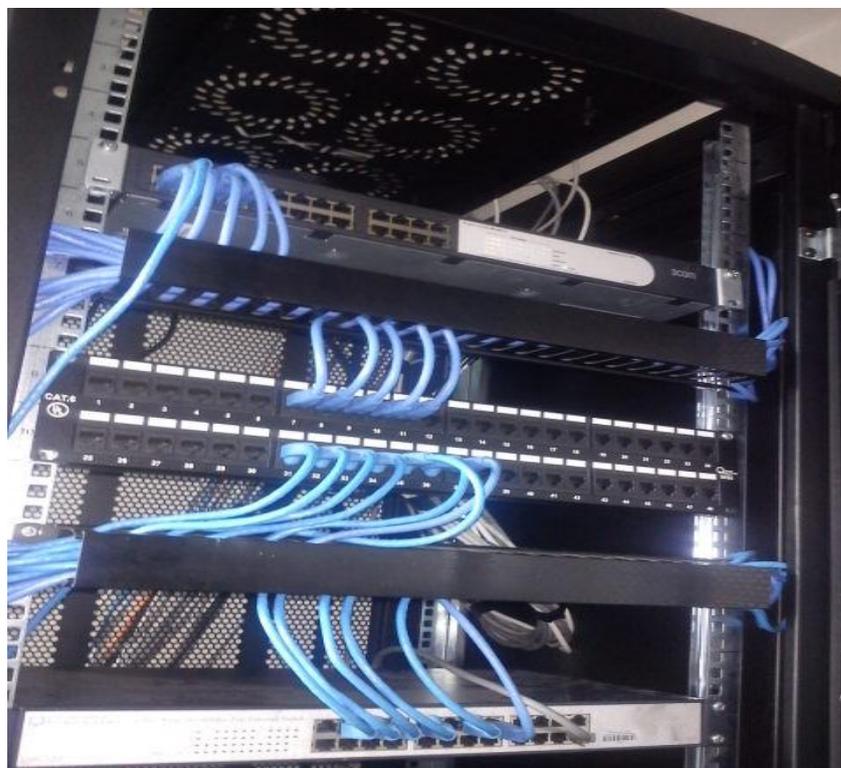
3.3.3.1 CREACIÓN DE LA BASE DE DATOS

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.

Tablas de materiales del salón de rack

Cabe indicar que el colegio ANGLO AMERICANO facilitara los planos de la edificación, lo que resultara más conveniente y práctico, ya que solamente se cambiaran los valores de las propiedades físicas y eléctricas en Wallman, y se tendrá la base de datos para realizar los cálculos de propagación. En la figura 14 se presenta el Rack donde se encuentra el servidor con la base de datos.

Figura 14 Rack Colegio Anglo Americano



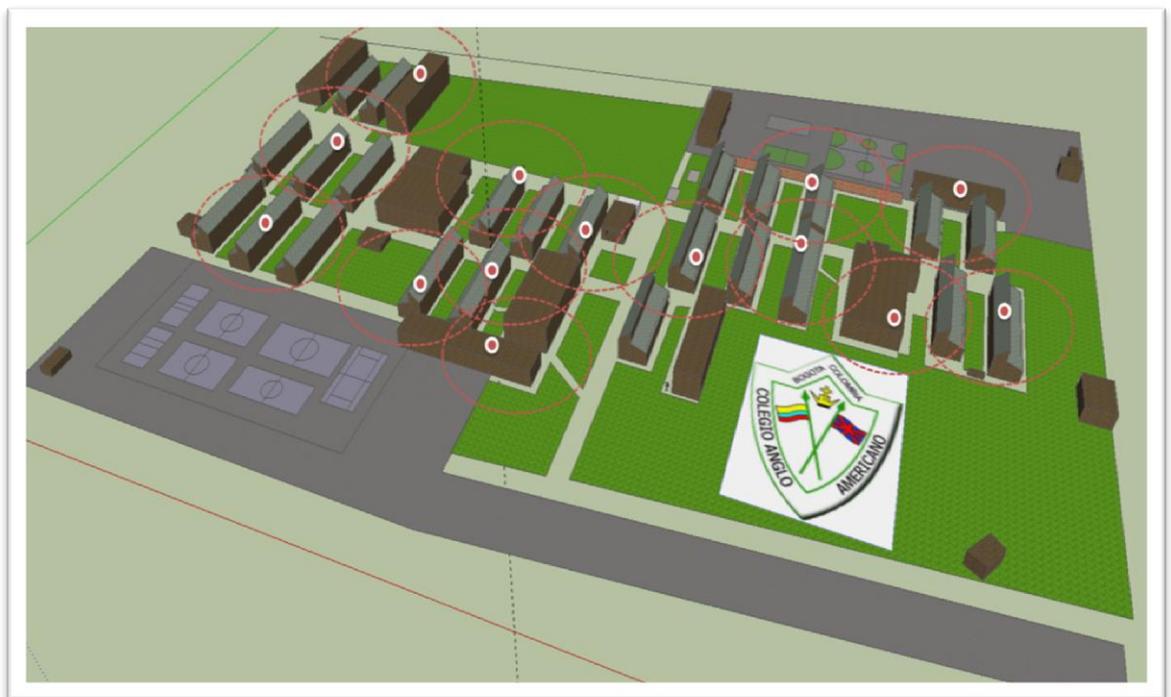
Fuente: Imagen capturada del Rack principal del Colegio Anglo Americano

3.3.3.2 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. En la figura 15 se presenta una distribución empírica de los Access Point.

Figura 15 Ubicación Router



Fuente: Diseño realizado por los estudiantes de la U. Libre

3.3.3.3 ACCESS POINTS

- Deben ostentar la certificación Wi-Fi.
- Operación bajo el estándar IEEE 802.11g
- Potencia mínima de transmisión de 17 dBm, o 50 mW.

- Sensibilidad mínima de -70 dBm para conexión a 4 Mbps.
- AP con antenas omnidireccionales de 2 Dib. de ganancia.
- Deben soportar la función de roaming y bridge.
- Deben tener priorización de tráfico, así como también la modificación de los parámetros MAC.

3.3.3.3.1 ADAPTADORES DE RED WIRELESS LAN

- Deben ostentar la certificación Wi-Fi.
- Operación bajo el estándar IEEE 802.11n
- Potencia mínima de transmisión de 15 dBm. O 32 mW.
- 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.

3.3.4 ARQUITECTURA DE LA RED ETHERNET

La red inalámbrica ha de quedar 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.

3.3.4.1 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 3.3.1.3 de este capítulo.

Desde el punto de vista del número de usuarios, la red debe soportar a por lo menos 200 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 14 los AP que integran la WLAN, la capacidad teórica de esta sería al menos de 300 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 el colegio Anglo Americano funcionará para brindar servicio de Internet, transporte de archivos entre usuarios, y para telefonía entre áreas.

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 200 usuarios potenciales usando Internet simultáneamente, se tendrá la siguiente carga:

$$12000 \times 200 = 240000\text{bps}$$

Es decir, el tráfico por navegar en Internet será de 2.4 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 más 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 200 usuarios usaran sus softphones al mismo tiempo, se tendrían la siguiente carga en la red:

$$8000 \times 200 \times 2 = 320000\text{bps}$$

El ancho de banda utilizado por VoIP será de aproximadamente 4Mbps. 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 qué tan factible es implantar telefonía IP sobre la red inalámbrica diseñada.

3.3.4.1.1 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 (Distributed 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 afectado. Cuando dos o más usuarios intentan transmitir al mismo tiempo, una colisión ocurre. Para evitar estas colisiones, cada suscriptor debe esperar un periodo de duración aleatoria, conocido como intervalo aleatorio Backoff. El backoff es un contador que es reducido solo cuando el medio está desocupado. Los dispositivos suscriptores deben escuchar y ver si el medio está 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.

3.3.4.1.1.1 CALIDAD DE SERVICIO (QOS)

Los flujos de voz y datos tienen diferentes requerimientos de red. La mayoría de las aplicaciones pueden soportar pérdidas de paquetes, porque el protocolo TCP puede retransmitir los paquetes perdidos para asegurar una entrega positiva.

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 pérdida 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 interoperabilidad 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.

3.3.4.1.1.1.1 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 6.

Tabla 6 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 tráfico de aplicaciones que carecen de capacidades de QoS. Tráfico promedio de un usuario, como navegar en Internet, porque es menos sensible a la latencia, pero grandes retardos pueden llegar a ser inaceptables.
Background	Categoría de más baja prioridad, diseñada para tráfico que no es sensible al retardo. Por ejemplo, descargar archivos o imprimir trabajos.

Fuente:<http://recursostic.educacion.es/observatorio/web/es/component/content/article/961-monografico-redes-wifi?start=6>

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 tráfico de aplicaciones que carecen de capacidades de QoS. Tráfico promedio de un usuario, como navegar en Internet, porque es menos sensible a la latencia, pero grandes retardos pueden llegar a ser inaceptables.

Background: Categoría de más baja prioridad, diseñada para tráfico que no es sensible 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 envío apropiada. Si un suscriptor esta soportando varias aplicaciones, y si todas intentan transmitir al mismo tiempo, ocurrirá una colisión interna entre ellas. Cuando esto sucede la lógica de cola debe resolver la colisión internamente.

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 categoría de acceso.

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.

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.

TXOP (transmit opportunity)

El límite 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 está desocupado por un periodo AIFS, cada estación inicializa un contador en un número 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, CW_{max}, seleccionan un nuevo contador backoff uniformemente y el proceso se repite.

Después de una transmisión exitosa, CW es reseteado a su mínimo valor, CW_{min}, 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.

3.3.4.1.1.2 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.

3.3.4.1.1.3 EVALUACIÓN EXPERIMENTAL

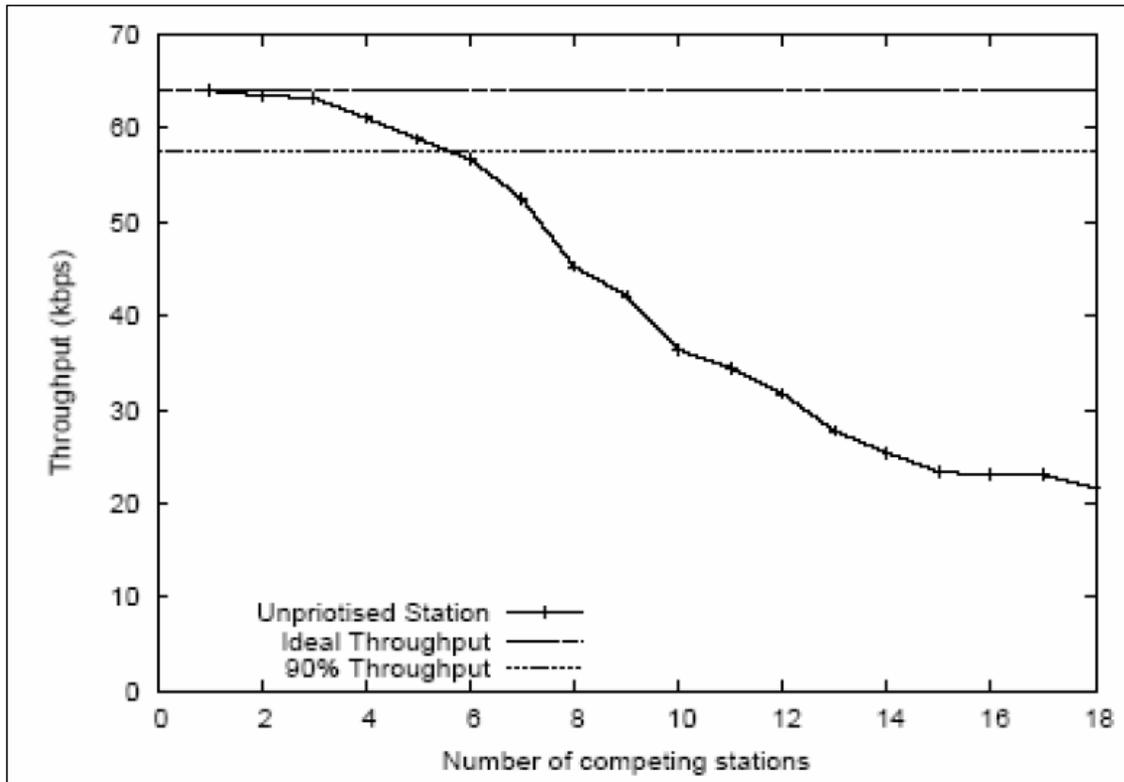
Para verificar que este tipo de red funcione, es necesario hacer ciertas evaluaciones en los parámetros descritos anteriormente. En este caso, no es posible hacerlo en la práctica, ya que como se trata de un estudio de ingeniería no se dispone de los equipos en estos momentos. De todas maneras se va ayudar de una evaluación experimental 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 16 muestra la medida de throughput¹ de una llamada de voz de 64 Kbps versus el número de estaciones en la red. Se nota claramente que a medida que aumenta el número de estaciones el throughput disminuye.

¹ Se llama throughput al volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos. Particularmente significativo en almacenamiento de información y sistemas de recuperación de información, en los cuales el rendimiento es medido en unidades como accesos por hora.

Figura 16 Throughput de una llamada de voz vs número de estaciones



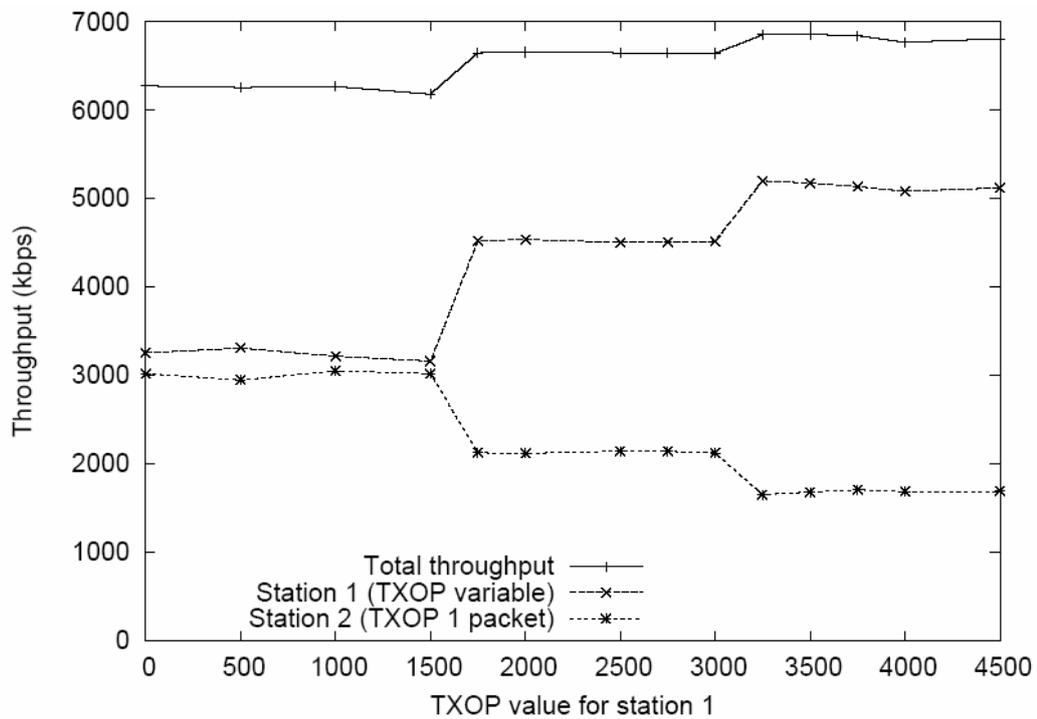
Solo son necesarias 5 estaciones que envíen datos para inducir a una disminución de la tasa de bit de una llamada de voz que exceda el 10% de disminución de throughput, lo cual en la práctica produce una disminución en la calidad de voz y hasta la pérdida de comunicación entre estaciones.

El estudio en el que se basa, está 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 back off 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 figura17 muestra el throughput conseguido por ambas estaciones y el throughput total del sistema.

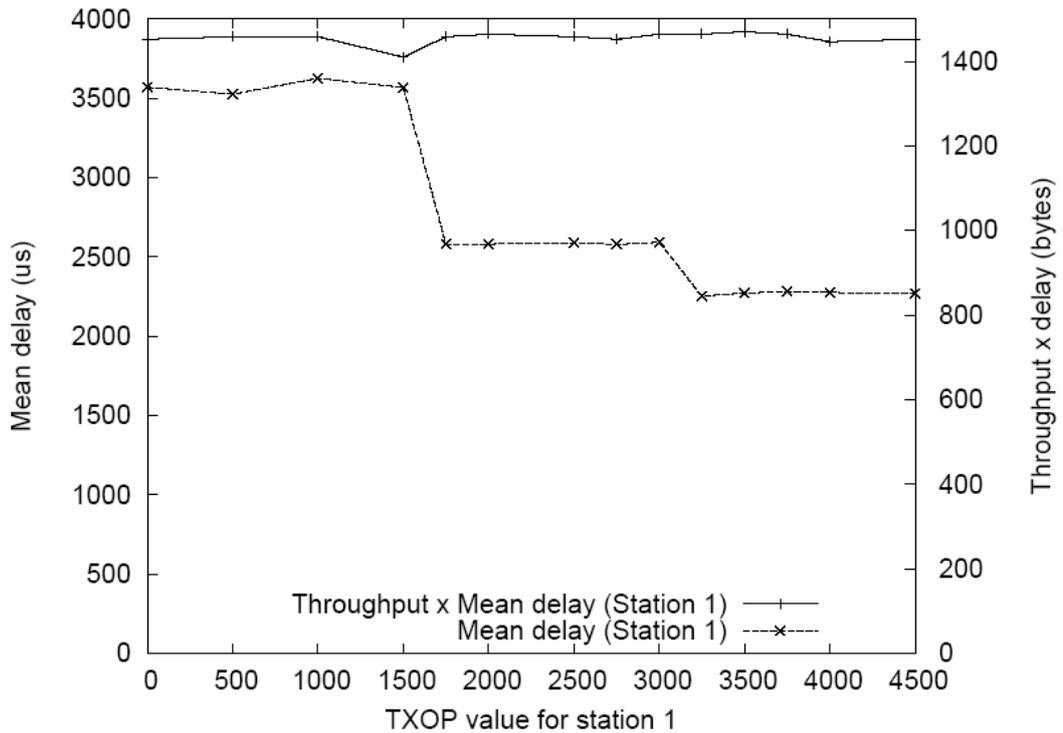
Figura 17 Impacto de TXOP sobre dos estaciones saturadas



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

La figura18 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 18 Impacto de TXOP sobre dos estaciones saturadas (2)



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

En las figuras 19 y 20, se observa que al duplicar CW_{min} , 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 Cw_{min} .

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

Figura 19 Impacto de CWmin sobre dos estaciones saturadas

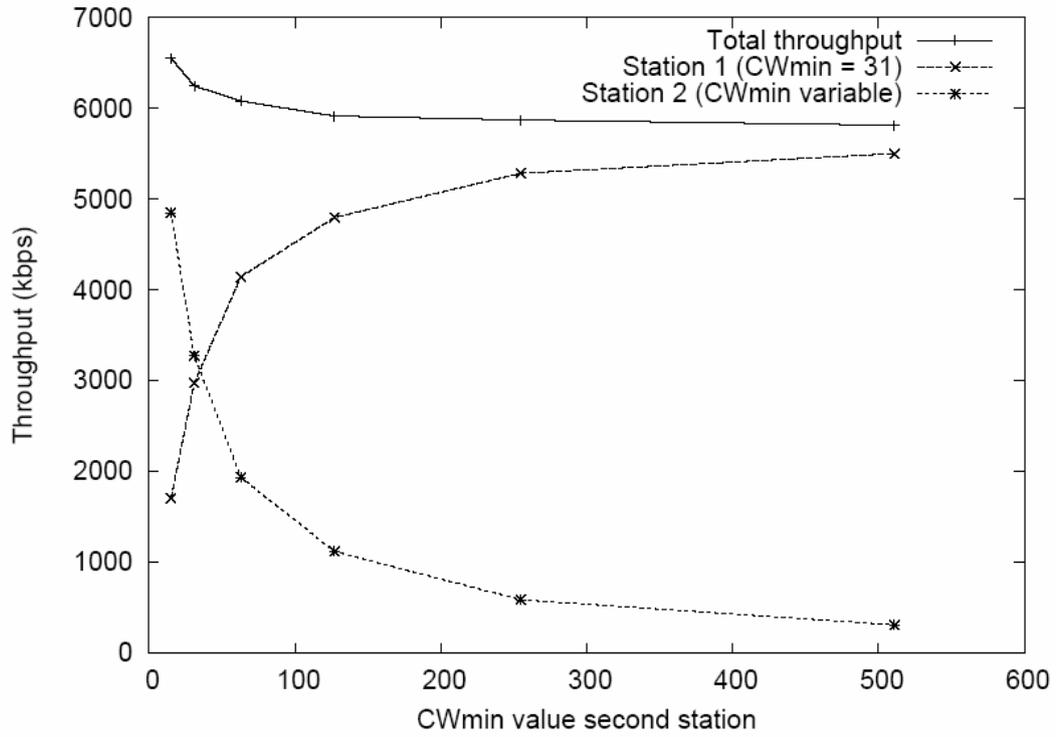
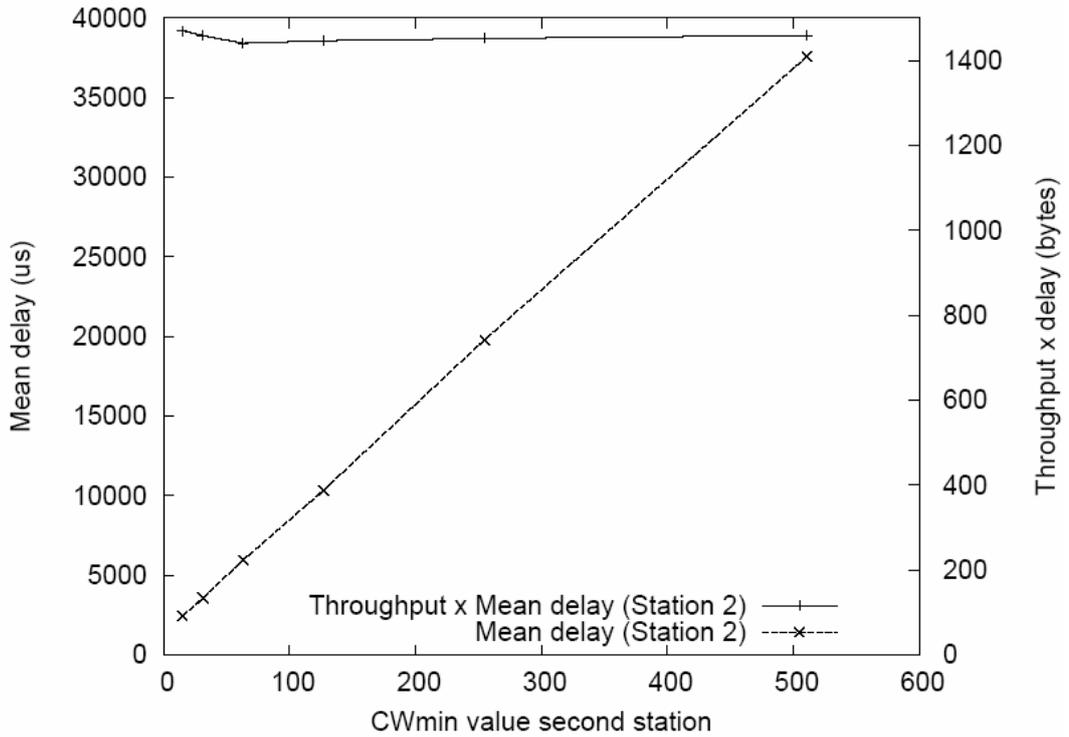


Figura 20 Impacto de CWmin sobre dos estaciones saturadas (2)



El siguiente ensayo que se hizo fue con el tercer parámetro, es decir con AIFS. Las figuras 21 y 22, muestran como este parámetro cambia el Throughput y el delay.

Figura 21 Impacto de AIFS sobre dos estaciones saturadas

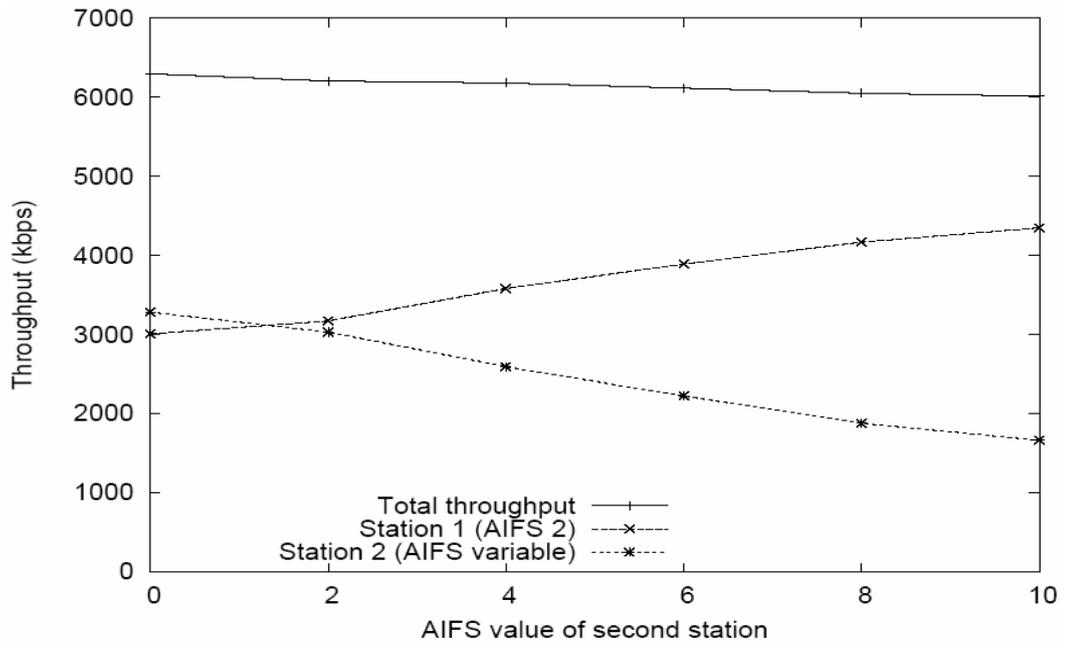
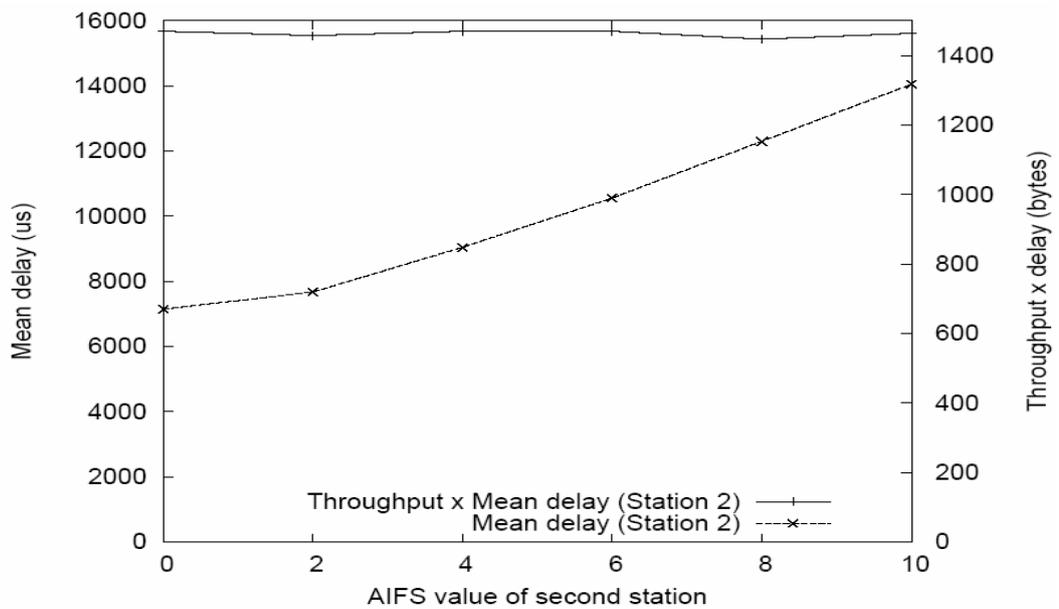


Figura 22 Impacto de AIFS sobre dos estaciones saturadas (2)



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 C_{wmin} , 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.

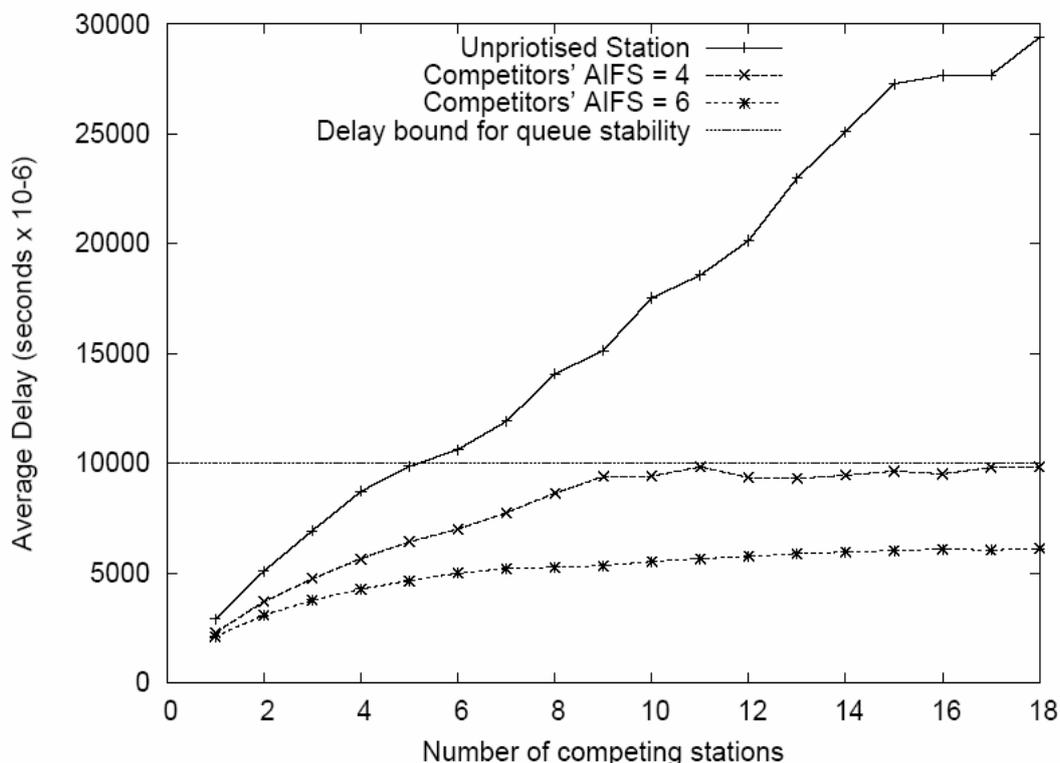
El objetivo se centra en priorizar la voz sobre los datos. Una vez estudiados los efectos que producen los parámetros MAC al modificarlos, ahora es posible encontrar un camino para alcanzar el objetivo.

El esquema que utiliza este estudio para priorizar la voz es simple: se incrementa el valor de AIFS usado por las otras estaciones. 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 permita. Cada experimento de lo hizo durante 20 minutos para un número pequeño de estaciones, y durante 30 minutos para más 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 28 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 priorización, al modificar los valores de AIFS en 4 y 6 respectivamente, el throughput se estabiliza.

Figura 28 Delay promedio para una llamada de voz con estaciones saturadas

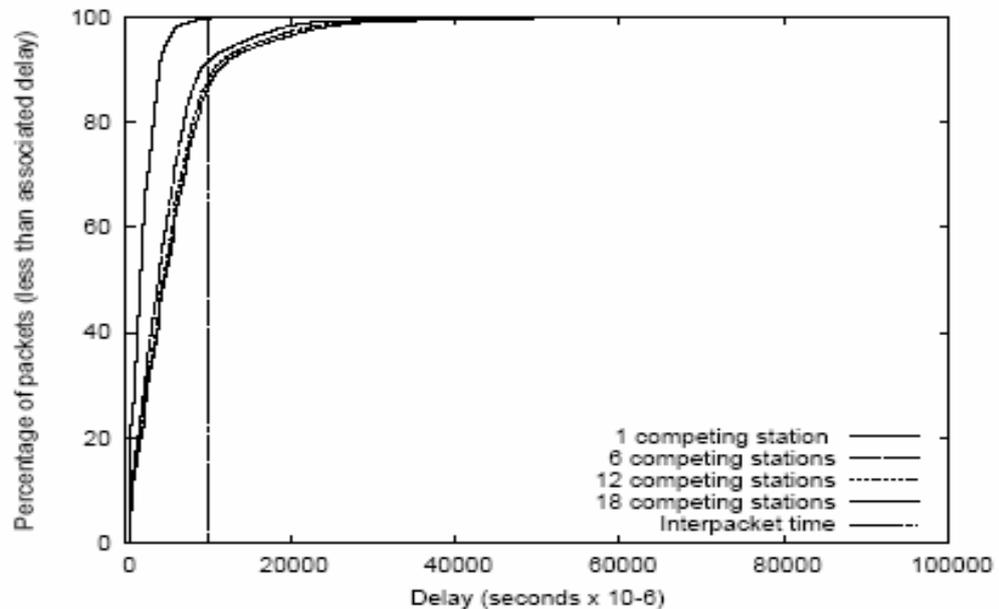


Esto confirma que un valor modificado de AIFS, será suficiente para priorizar una llamada de voz contra un número grande de estaciones.

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 24 muestra como los tiempos de transmisión son distribuidos cuando la llamada de voz no esta priorizada, priorizada con AIFS de 4 y de 6.

Figura 24 CDF para el delay de una llamada no priorizada, con AIFS=4, con AIFS=6

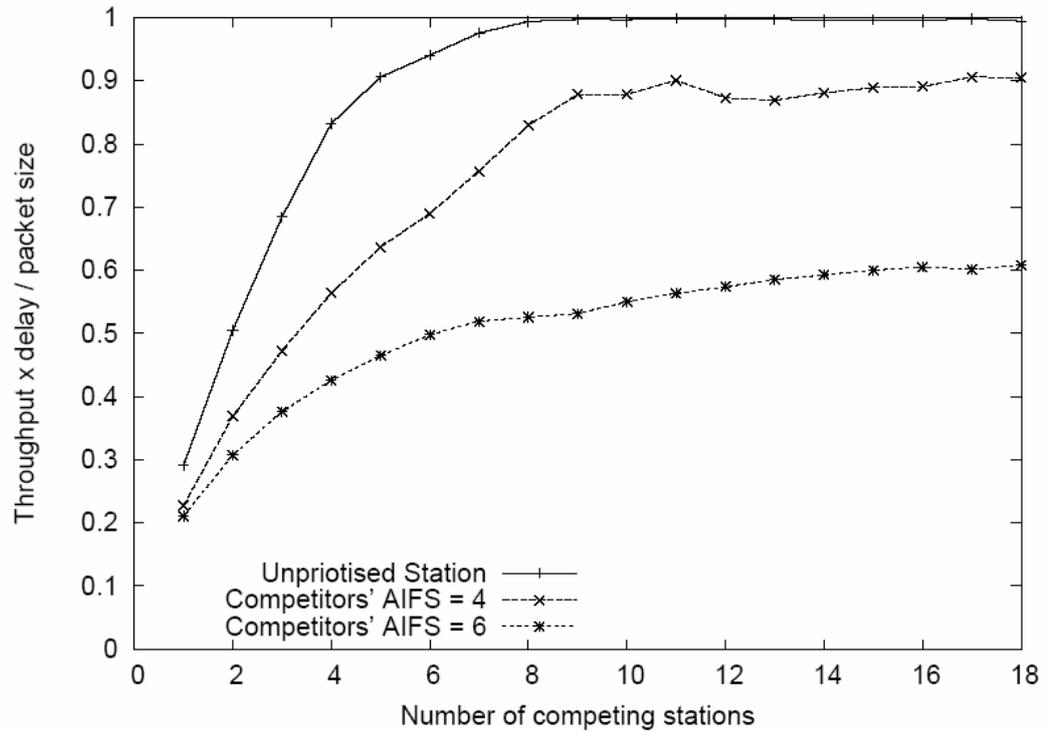


Estos gráficos muestran una curva regular correspondiente al número de paquetes transmitidos antes de que cada paquete de voz sea exitosamente transmitido.

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 25, 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 25 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.

3.3.4.1.1.4 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.

3.3.4.1.1.4.1 SERVIDOR ASTERISK

Es una completa solución de comunicaciones “open source” que utiliza la red LAN, Internet y la Red Telefónica Pública, ofreciendo además un sinnúmero de aplicaciones que permiten tomar ventaja de la convergencia entre comunicaciones de voz, datos, y la Telefonía IP.

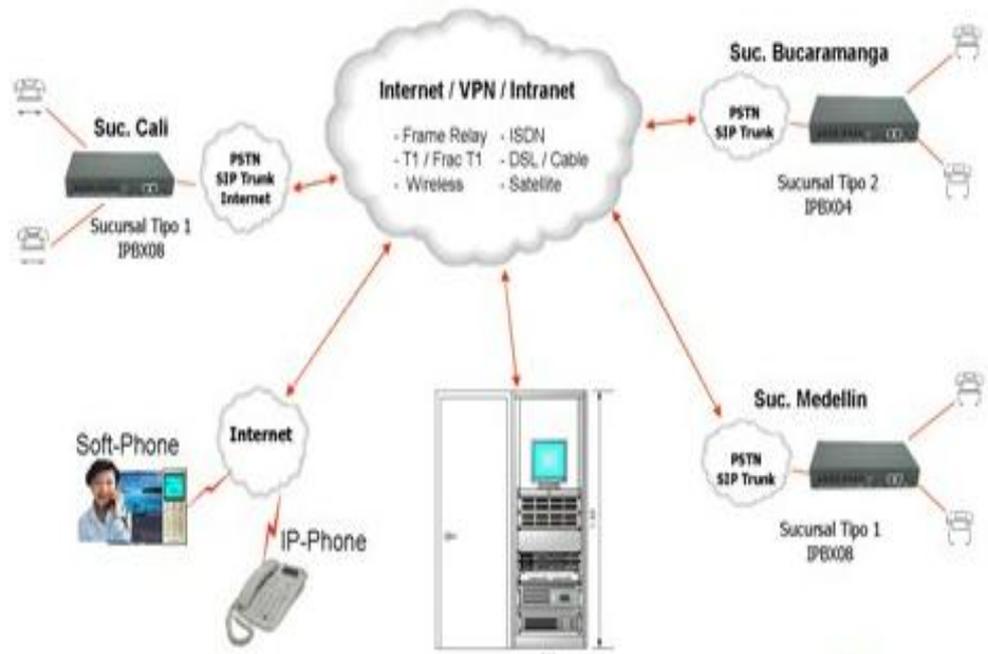
Es un sistema de comunicaciones inteligentes basado en software libre. Convergen aplicaciones de voz, datos y video. Hay que resaltar que Asterisk es un software, exclusivamente software, y que actúa como un soft-switch, es decir una PBX – IP.

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 26.

Figura 26 Esquema de funcionamiento de Asterisk



Fuente: http://www.teletiemendasweb.com/product.php?id_product=22

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.

3.3.4.2 BACKBONE DE LA RED LAN

Está claro que la conexión de los dos AP (Access Point) de cada planta ha de ser hacia un concentrador tipo switch que soporte QoS (Quality of Service), ubicado en el respectivo cuarto de comunicaciones. Como las distancias son cortas, el enlace será a través de cable UTP CAT 5e, 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 cores, jacks, etiquetas, etc.

El cableado está protegido 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 el Colegio Anglo Americano.

3.3.4.3 BASES TÉCNICAS DE EQUIPOS DE RED LAN

3.3.4.3.1 SWITCH DE BACKBONE

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.

3.3.4.3.2 ROUTER DE BACKBONE

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

3.3.4.3.3 TARJETAS DE RED NIC PARA SERVIDORES

Tarjeta de red 32/64 bits, tipo Giga Ethernet 10/100/1000 BaseT

3.3.4.3.4 SERVIDOR DE VOZ

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

3.3.4.3.5 TARJETAS ANÁLOGAS

Tarjeta analógica compatible con Asterisk, mínimo 4 puertos FXO

3.3.5 FUNCIONAMIENTO GENERAL DE LA RED MIXTA VOZ Y DATOS

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 27.

Figura 27 Ajuste de los parámetros MAC de 802.11e

The screenshot shows the TP-LINK 300M Wireless N Gigabit Router web interface. The top header is green with the TP-LINK logo and the model number TL-WR1043N / TL-WR1043ND. The left sidebar contains a navigation menu with options: Status, Quick Setup, QSS, Network, Wireless, DHCP, Network Sharing, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control (highlighted), Control Settings, Rules List, IP & MAC Binding, Dynamic DNS, and System Tools. The main content area is titled 'Bandwidth Control Rule Settings' and contains the following fields and controls:

- Enable:
- IP Range: -
- Port Range: -
- Protocol: ALL (dropdown menu)
- Min Bandwidth(Kbps):
- Max Bandwidth(Kbps):
- Egress Bandwidth:
- Ingress Bandwidth:

At the bottom of the form are 'Save' and 'Back' buttons. To the right of the form is a 'Bandwidth Control Rules Setting Help' section with the following text:

This page is for the bandwidth configure of the Bandwidth Control rules.

- **Enable** Enable or disable the rule.
- **IP Range** - Interior PC address range. If both are blank (or 0.0.0.0), the domain is noneffective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank (or 0), the domain is noneffective.
- **Protocol** - Transport layer protocol, here there are all, TCP, UDP.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port, default number is 0.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port, default number is 0.

Fuente: Imagen capturada del Router Colegio Anglo Americano

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 óptima.

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.

3.4 ANÁLISIS ECONÓMICO

3.4.1 SELECCIÓN DE EQUIPOS Y MATERIALES PARA LA INTRANET DEL COLEGIO ANGLO AMERICANO, SEGÚN ANÁLISIS DE RELACIÓN COSTO BENEFICIO

En los capítulos anteriores ha quedado plenamente definido el diseño total de la Intranet del colegio Anglo Americano, 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 del Anglo Americano.

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.

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 esperado. Esa es la realidad de la vida profesional. El valor total de dinero que el Anglo Americano deba invertir en la adquisición y montaje de esta tecnología tendrá que aproximarse lo más posible a un presupuesto cómodo, 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.

3.4.1.1 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 Colombia, 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 ya existen un previo montaje de sistema de comunicación, además tenemos dispositivos que no describiremos 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, la tabla 7 muestra las diferencias entre 4 tipos de AP.

Tabla 7 Cuadro comparativo de Puntos de Acceso (AP)

MARCA	Cisco	3bumen	Encoré	D link
MODELO	Aironet 100	Rompe muros 300 MBPS	Wireless D 150	Wireless N 300
¿CUMPLE BASES TÉCNICAS?	SI	SI	SI	Si
PRECIO	450.000	320.000	280.000	250.000

Fuente: Cuadro diseñado por los estudiantes de la U. Libre

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 3bumen rompe muros. Por tanto, en el caso de los AP, no habrá duda en utilizar los de marca 3bumen para la instalación de la red.

Tabla 8 Cuadro comparativo de Adaptadores de Red PCI (Tarjetas Inalámbricas)

MARCA	Cisco	3bumen	Encoré	D link
MODELO	Cisco Aironet Pci-g	Tarjeta inalámbrica 3bumen	Tarjeta encoré inalamb pci 150 1xn42	Tarjeta Dlink inalámbrica usb
¿CUMPLE BASES TÉCNICAS?	SI	SI	SI	Si
PRECIO	450.000	320.000	280.000	250.000

Fuente: Cuadro diseñado por los estudiantes de la U. Libre

Las marcas CISCO, 3bumen, Encore y Dlink 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 802.11n, esta es 3bumen.

No se puede ocultar que la marca 3bumen esta empezando a tener reconocidas en todo el mundo, es un referente, pero la diferencia en precio con otros fabricantes es decisiva para el caso del Anglo Americano donde hay un presupuesto para tomar en cuenta para viabilidad del proyecto.

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 3bumen, 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 3bumen teniendo estos, también la característica de calidad de servicio QoS.

3.4.1.2 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.

3.4.1.3 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 está 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 códec G.729. De aquí, que en la propuesta económica se va buscar equipos de semejantes características.

A continuación, la tabla 9 se muestra los servidores que podrían ser usados para la red

Tabla 9 Cuadro Comparativo de Servidores para comunicación de voz

DESCRIPCIÓN	PRECIO
Intel Xeon (3.00 GHz), 1 GB, 80 GB	\$ 1.800.000
Intel Core 2 Duo (1.86 GHz), 1 GB DDR II SDRAM, 250 GB Standard	\$ 1.600.000
IBM eServer x Series 226 8488 - Tower 1 x Xeon 3 GHz - RAM 1 GB	\$ 1.500.000

Fuente: Cuadro diseñado por los estudiantes de la U. Libre

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.

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.

Para conectar la red de voz interna de la administración con la red pública 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 comprará también estas tarjetas a Digium.

3.4.1.4 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.

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 utilizará las instalaciones actuales del Colegio Anglo Americano.

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

3.4.2 PRESUPUESTO FINAL

En las secciones anteriores se han obtenido los costos de cada rubro componente del proyecto de implantación de la Intranet del Colegio Anglo Americano 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 10.

Tabla 10 Presupuesto final del proyecto

ITEMS	\$/HORA	No. HORAS	TOTAL	FUENTE FINANCIADORA
Talento Humano				
Proponente	10.000	900	9.000.000	PROPONENTE
Proponente	10.000	900	9.000.000	PROPONENTE
Director	35.000	40	1.400.000	COLEGIO
Asesor	30.000	15	450.000	UNIVERSIDAD
Total Talento Humano			19.850.000	
Gastos Maquinaria y Equipo				
Equipos			15.000.000	COLEGIO
Otros			1.250.000	COLEGIO
Total Maquinaria y Equipo			16.250.000	
Fungibles				
Medios magnéticos			60.000	PROPONENTES
Fotocopias			30.000	PROPONENTES
Internet			300.000	COLEGIO
Libros			120.000	COLEGIO
Papel			80.000	PROPONENTES
Tonner			300.000	PROPONENTES
Total Fungibles			890.000	
Otros Gastos				
Transporte (2)			900.000	PROPONENTES
Otros			150.000	PROPONENTES
Total otros gastos			1.050.000	
TOTAL ANTES DE IMPREVISTOS			38.040.000	
Imprevistos 2-6% (3.5%)			1.331.400	PROPONENTES
COSTO TOTAL DEL PROYECTO (ΣGASTOS)			39.371.400	

Fuente: Cuadro diseñado por los estudiantes de la U. Libre

3.4.3 FINANCIACIÓN DEL PROYECTO

El costo total del Proyecto será responsabilidad de las Fuentes Financiadoras y se compartirá así como lo muestra la figura 11.

Tabla 11 Financiación del proyecto

FUENTE	COSTO A CARGO	[%]
Proponentes	23.622.840	60%
Universidad Libre	2.598.512	6.6%
Colegio	13.150.048	33.4%
Costo Total Proyecto	39.371.400	100%

Fuente: Cuadro diseñado por los estudiantes de la U. Libre

4. CONCLUSIONES

- Después de haber cumplido a cabalidad el trabajo de campo en las instalaciones del colegio Anglo Americano, es posible afirmar que se pudo analizar en su totalidad la red LAN dando solución a los problemas que presentaba tanto físicos como de transmisión, pues se rediseño la red existente aplicando mejoras en cableado y equipos, de igual manera se implementaron los estándares mínimos de calidad; se puede decir que la red es ahora una moderna y funcional infraestructura de comunicaciones.
- La tecnología WI-FI en nuestros días se encuentra en constante evolución y crecimiento, razón por la cual se presento una propuesta de migración de la red LAN hacia una plataforma WLAN, mostrando los beneficios que se pueden obtener al momento de implementarla con el fin de solucionar los problemas específicos de distribución que presenta el colegio. Para ello es necesario conocer los estándares a implementar, en nuestro caso nos basamos en el estándar 802.11n, pues maneja una velocidad de transmisión mayor que los demás (10 veces) y resulta compatible con todas las revisiones del 802.11.
- De la mano de esta investigación mostramos que existen herramientas con las cuales se puede realizar la planificación y el diseño casi profesional de infraestructuras de comunicaciones inalámbricas. La suite del software WinProp y su modelo de predicción DP (Dominant Path) son ejemplos de algunas de ellas, estas resultan ser efectivas y sobre todo prácticas ya que permiten ejecutar una verdadera planificación en cuanto a redes WLAN se refiere.

5. RECOMENDACIONES

- Los equipos y terminales en general que van a pertenecer a la Intranet, deben contar mínimo con el sistema operativo Windows XP service Pack 3 desde este sistema operativo en adelante se incorporan las herramientas necesarias para el reconocimiento de la encriptación usada por WPA y el estándar de seguridad 802.1X; Así se puede iniciar el cambio del sistema actual WEP por WPA.
- Todos los equipos WI-FI que se instalen en la Wireless LAN del colegio deben poseer drivers y firmware suministrado por el fabricante para así obtener fácilmente soporte técnico en caso de necesitarlo.
- 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.

BIBLIOGRAFÍA

- BARCELO ORDINAS, Josep M; INIGO GRIERA, Jordi; ABELLA, Jaume. Estructura de redes de computadores. Editorial UOC. Barcelona (España) 2008. Internet:
http://books.google.es/books?id=QAxAJEBgUWYC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- HUIDOBRO, José Manuel. Redes de área local. Editorial Paraninfo. Madrid (España) 2006. Internet:
http://books.google.com.co/books?id=tioFpJdQJhsC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. NTC 1486. Sexta actualización. Bogotá: El Instituto, 2006, p.1
- MAGAÑA LIZARRONDO, Eduardo. Comunicaciones y redes de computadores. Editorial Pearson Prentice Hall. Madrid (España) 2006. Internet:
<https://sites.google.com/site/rubenloredoamaro/biblioteca/tele/comunicacion-es-y-redes-de-computadores-problemas-y-ejercicios-resueltos-escrito-por-eduardo-magana-lizarrondo>
- RIERA GARCIA, Juan B; ALABAU MUÑOZ, Antonio. Teleinformática y redes de computadores. Editorial Marcombo. Barcelona (España) 1992. Internet:
http://books.google.com.co/books?id=KKU7uTBmMNAC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- TANENBAUM, Andrew S. Redes de computadores. Editorial Pearson Educación. México 2003. Internet:
<http://www.mediafire.com/?psexw7b6rn58dpr>

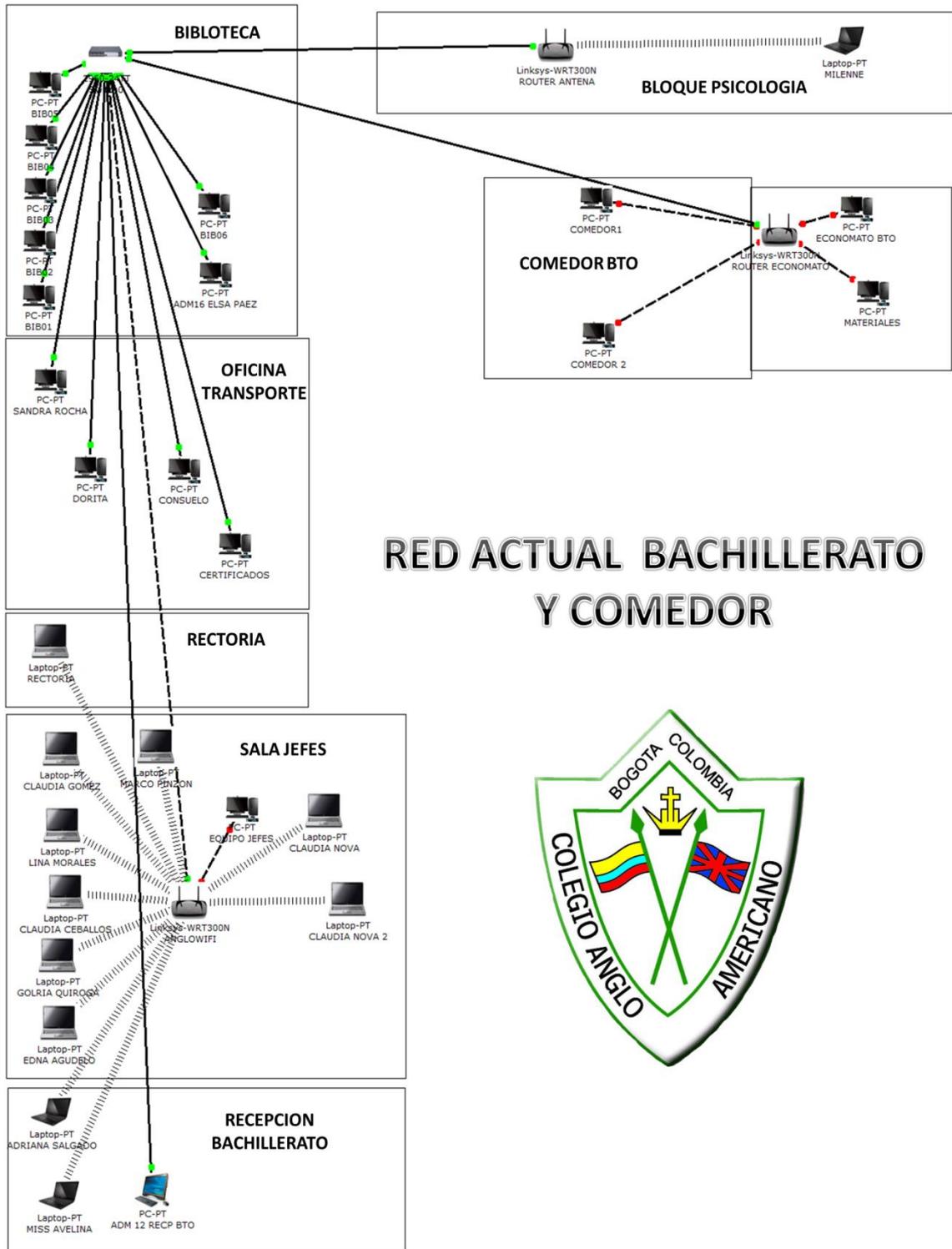
INFOGRAFÍA

- <http://www.edutecne.utn.edu.ar/wlan_frt/fis_ondas_rad_IEEE802-11b.pdf>
- <<http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf>>
- <<http://es.scribd.com/doc/23647929/Redes-Inalambricas>>
- <<http://wirelessinfo-r-us.blogspot.com/2007/11/basic-service-set-bss-vs-extended.html>>
- <<http://wirelessinfo-r-us.blogspot.com/2007/11/basic-service-set-bss-vs-extended.html>>
- <<http://es.scribd.com/doc/73274511/47/Figura-5-3-Estructura-de-una-VPN-para-acceso-inalambrico-seguro>>
- <<http://www.slideshare.net/gppoloc/protocolos-y-modelo-osi>>
- <<http://redalyc.uaemex.mx/redalyc/html/784/78460103/78460103.html>>
- <<http://www.aplicacionesempresariales.com/implementando-qos-en-las-redes.htm>>
- <http://www.uc3m.es/portal/page/portal/biblioteca/aprende_usar/como_citar_bibliografia>
- <<http://www.x-net.es/tecnologia/wireless.pdf>>
- <<http://www.anexom.es/tecnologia/mi-conexion/ventajas-del-estandar-wi-fi-80211n/>>
- <<http://tpredes.galeon.com/redes.pdf>>

ANEXOS

ANEXO A	DISTRIBUCION RED BACHILLERATO Y COMEDOR
ANEXO B	DISTRIBUCION RED BLOQUE PRIMARIA Y OFICINA 4
ANEXO C	DISTRIBUCION RED PRE-ESCOLAR
ANEXO D	DISTRIBUCION RED RACK SISTEMAS
ANEXO E	DISTRIBUCION RED SALAS 3 Y 4
ANEXO F	DISTRIBUCION RED SALAS 1 Y 2
ANEXO G	MANUAL WINPROP

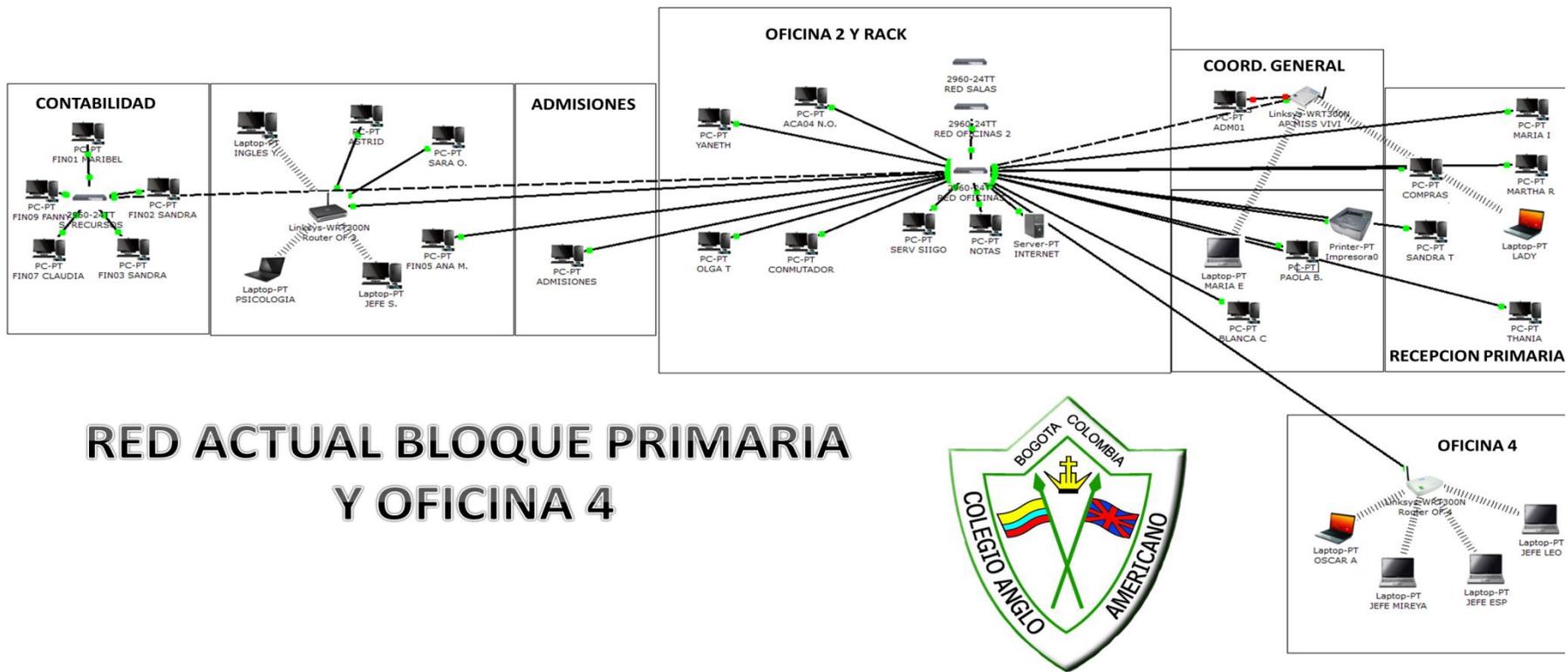
ANEXO A DISTRIBUCIÓN RED BACHILLERATO Y COMEDOR



RED ACTUAL BACHILLERATO Y COMEDOR



ANEXO B DISTRIBUCIÓN RED BLOQUE PRIMARIA Y OFICINA 4

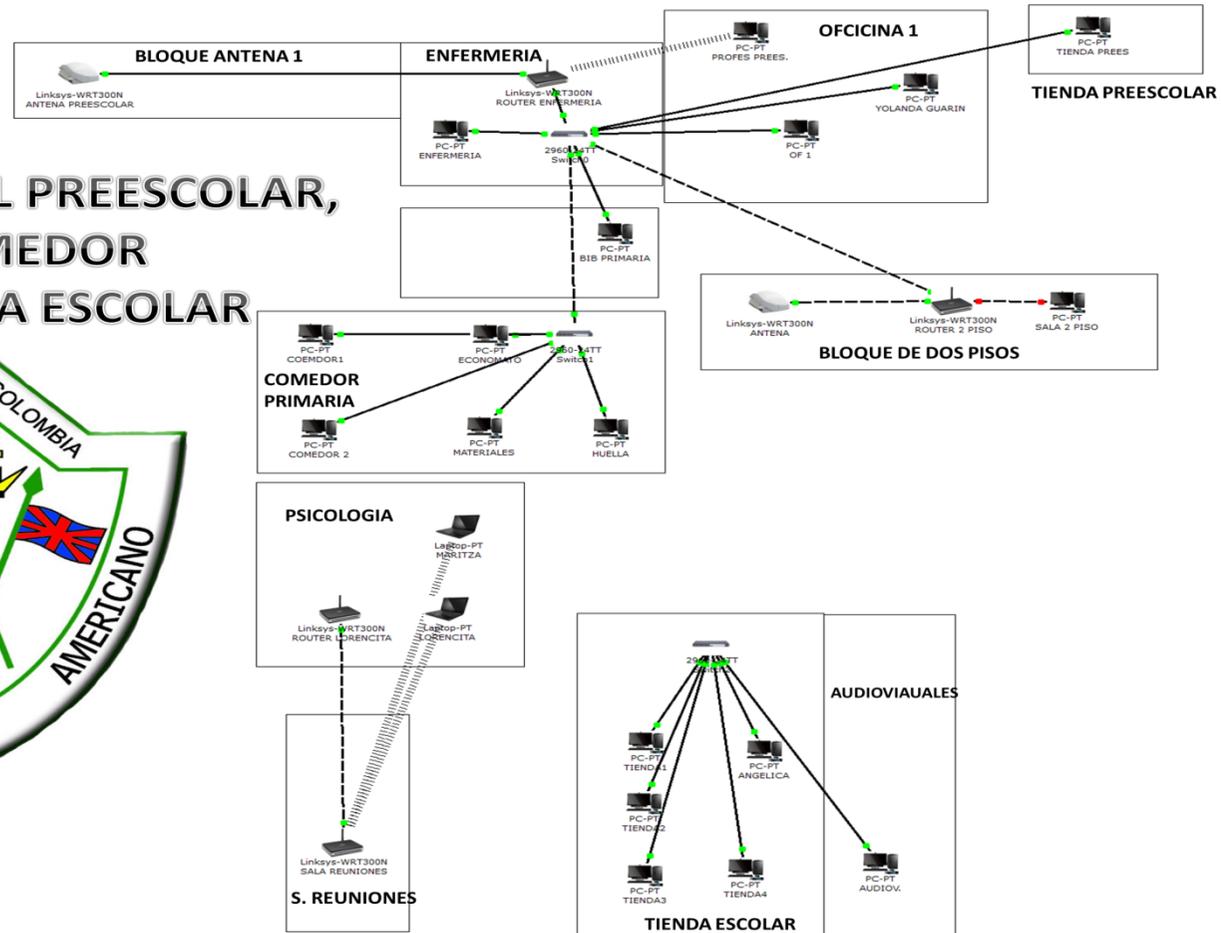


RED ACTUAL BLOQUE PRIMARIA Y OFICINA 4

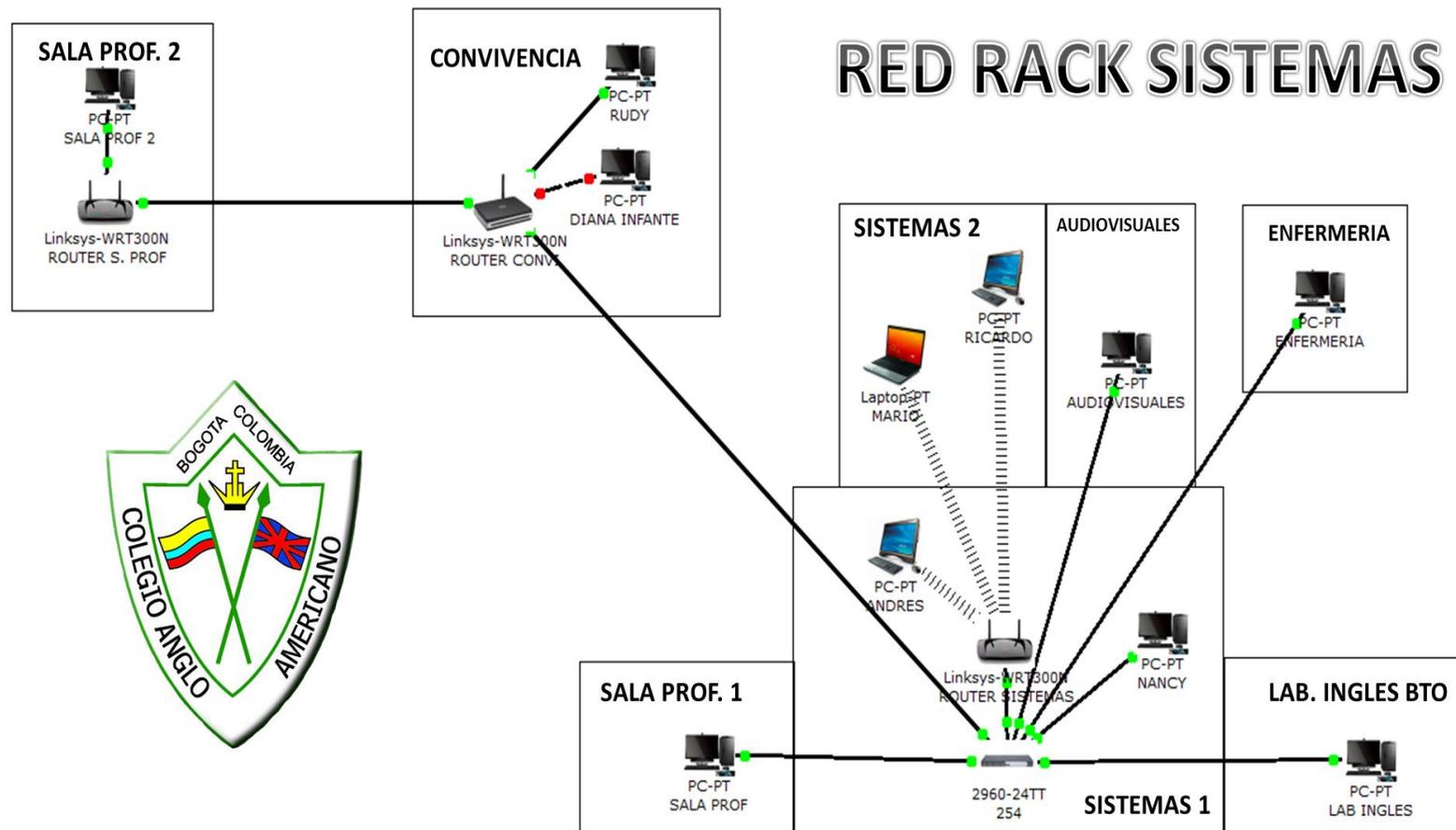


ANEXO C DISTRIBUCIÓN RED PRE-ESCOLAR

RED ACTUAL PREESCOLAR,
COMEDOR
Y TIENDA ESCOLAR



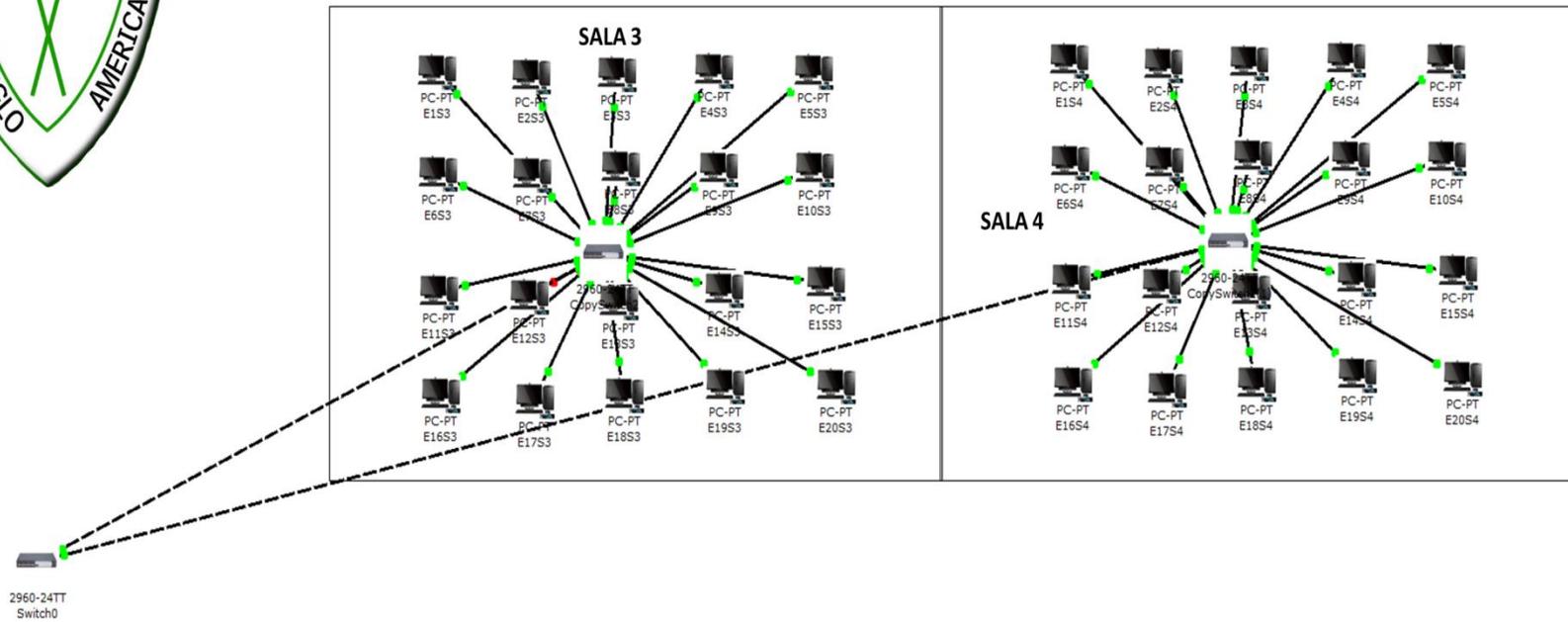
ANEXO D DISTRIBUCIÓN RED RACK SISTEMAS



ANEXO E DISTRIBUCIÓN RED SALAS 3 Y 4



RED SALAS SISTEMAS BACHILLERATO



ANEXO F DISTRIBUCIÓN RED SALAS 1 Y 2



RED SALAS DE SISTEMAS PRIMARIA

