

UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA
RED INALÁMBRICA EN EL COLEGIO
INTERNACIONAL SEK-QUITO, CONSIDERANDO
ASPECTOS DE SEGURIDAD DENTRO DEL ÁREA
PERIMETRAL**

Realizado por:

JOSÉ LUIS VILLACÍS MENDOZA

Como requisito para la obtención del título de

**INGENIERO EN SISTEMAS Y
TELECOMUNICACIONES**

QUITO, MAYO 2009

DECLARACIÓN JURAMENTADA

Yo, José Luis Villacís Mendoza, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

.....
José Luis Villacís Mendoza

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado

**ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA RED INALÁMBRICA
EN EL COLEGIO INTERNACIONAL SEK-QUITO, CONSIDERANDO
ASPECTOS DE SEGURIDAD DENTRO DEL ÁREA PERIMETRAL**

Realizado por el alumno

JOSÉ LUIS VILLACÍS MENDOZA

Como requisito para la obtención del título de
INGENIERO EN SISTEMAS Y TELECOMUNICACIONES
ha sido dirigido por el profesor
MBA. EDISON ESTRELLA
quien considera que constituye un trabajo original de su autor.

.....
Ing. EDISON ESTRELLA MBA.

Los profesores informantes
Ing. Xavier Barragán MBA. y el
Ing. Mario Chafla MBA.
después de revisar el trabajo escrito presentado,
lo han calificado como apto para su defensa oral ante el tribunal examinador.

.....
Ing. Xavier Barragán MBA.

.....
Ing. Mario Chafla MBA.

Quito, MARZO de 2009

DEDICATORIA

Dedico este logro a mis padres, Arq. Luis Villacís y Fanny Mendoza, que con su ejemplo me inculcaron la perseverancia, para lograr los objetivos y metas que me proponga.

A mi novia por su amor y comprensión, apoyo y estímulo permanente, pero sobre todo, por haberme soportado en los momentos difíciles, cuando algún tema se complicaba y me hacía perder el buen humor, gracias por compartir conmigo y ayudarme a pagar el precio de este proyecto que, estoy seguro, bien vale la pena. Como siempre, le entrego mi amor y este trabajo.

AGRADECIMIENTO

A la Universidad Internacional SEK por abrirme sus puertas y permitirme ser parte de los alumnos y profesionales que forman.

Al personal docente por brindarme sus conocimientos y ayudarme en el desarrollo profesional.

Un especial agradecimiento al Ing. Edison Estrella MBA. por su apoyo y profesionalismo con que supo direccionar el trabajo y alinear acertadamente cada una de las observaciones con respetados criterios.

Por el apoyo constante y el trabajo incondicional de muchos, mis más preciados agradecimientos para todos los que a lo largo de la vida de una u otra forma estuvieron cerca motivando y alentando el esfuerzo.

RESUMEN EJECUTIVO

El Colegio Internacional SEK-QUITO impulsa nuevos y modernos proyectos de innovación educativa enmarcados en esta era tecnológica, donde la información se convierte en herramienta fundamental para la obtención y aplicación de nuevos conocimientos. Bajo esta perspectiva y consciente de que el avance hacia la “superautopista de la información” continuará a un ritmo cada vez más rápido, sus directivos apoyan la ejecución de nuevos y modernos sistemas informáticos que le permitan seguir paso a paso el avance de nuevas tecnologías con una tendencia de información globalizada, eliminando las barreras del tiempo y la distancia, y permitiendo a los estudiantes compartir información y trabajar en colaboración gracias al uso y a la aplicación de los servicios que presenta el uso de las redes.

Una de las tecnologías de mayor desarrollo tecnológico en la última década, es la tecnología inalámbrica, la cual facilita la posibilidad de acceder a una red de datos, desde cualquier punto de una determinada área geográfica. La evolución de las tecnologías inalámbricas nos ha llevado al desarrollo de las Redes Inalámbricas, permitiendo que el mundo de la voz y los datos se encuentren totalmente integrados. La integración de redes facilita la creación de nuevas aplicaciones que integran voz y datos.

Esta investigación aborda temas relacionados con la red de datos actual de la Institución ya que para integrar una nueva tecnología se debe saber cuáles son las falencias actuales y detectándolas, para que cuando algo nuevo sea desplegado no se tenga problemas.

La solución que se diseña y se implementa en el presente documento es una restructuración de la topología de red, esto se le hace con el afán de tener un mejor rendimiento y soportar nuevas adiciones a esta, sin que sea penalizada por las deficiencias o limitaciones que pueda tener.

La red inalámbrica que se ha diseñado se la planteado de tal manera en que sea totalmente funcional para los usuarios móviles y sea totalmente segura sin involucrar deficiencias en la red.

La ejecución del presente trabajo de investigación apoyara al desarrollo de actividades y dará el impulso que necesitan los estudiantes, docentes y administrativos, colaborando de esta manera a la misión del Colegio Internacional SEK-QUITO que es la de proporcionar servicio educativo integral a los alumnos de los diferentes sectores de la ciudad de Quito, basados en la aplicación de las innovaciones curriculares, en el rescate de los valores éticos, morales, cívicos; optimizando los recursos que ofrece el medio y la sociedad, a fin de contribuir al desarrollo del sistema educativo Provincial y Nacional.

ABSTRACT

The International School SEK-QUITO promotes new educational innovation projects towards this new technological, when information, becomes a fundamental tool obtaining applying knowledge. Under this perspective and aware that “superhighway of in information” will continue at a faster speed, the directors support of new and modern informatics system that allow the follow-up of the new technology advances with a globalized tendency, eliminating the time and distance barriers, and enabling students to share information and work in cooperation thanks to the use and application of the services offered by the web.

One of the most developed technologies of the decade is the wireless technology, which facilitates the possibility to get to a data web, form any geographic point. The evolution of this technology has taken is to the development of the wireless web, permitting the noise and data worlds to come to getter.

The integration of webs allows the creation of new applications to integrate noise and data. This investigation topics connected to the data web of the institution, for in order to integrate a new technology one must know which arte the current errors and detect then for when a new one is displayed there won't the any problems. The wireless web has been designed in such a way that is totally functional for the mobil users and it's safe without involving web deficiencies.

The execution of the present work will support the development of activities and will give the impulse that students, teachers and administrative need, collaborating to the mission of The International School SEK-QUITO which is to give educational integral to the students of different parts of Quito, based on the application of innovated curriculum, severing ethic moral and civic values optimizing the resources that society and the environment offers, in order the contribute to the development of the provincial and national education system.

ÍNDICE DE CONTENIDO

DECLARACIÓN JURAMENTADA.....	i
DECLARATORIA	ii
DEDICATORIA	iii
AGRADECIMIENTO	iv
RESUMEN EJECUTIVO	v
ABSTRACT	vii
ÍNDICE DE CONTENIDO.....	x
ÍNDICE DE TABLAS	xvii
ÍNDICE DE FIGURAS	xviii
ÍNDICE DE ANEXOS.....	xix
NOMENCLATURA.....	xv

Capítulo 1	1
1. INTRODUCCIÓN	1
1.1 ANTECEDENTES	1
1.2 DETERMINACIÓN DEL PROBLEMA	2
1.3 JUSTIFICACIÓN.....	3
1.4 SOLUCIÓN DEL PROBLEMA	4
1.5 OBJETIVOS.....	8
1.5.1 Objetivo General.....	8
1.5.2 Objetivos Específicos	8
1.6 ALCANCE	8
1.7 MARCO TEÓRICO	9
1.7.1 Redes.....	9
1.7.1.1 Concepto de una Red.....	9
1.7.1.2 Topología de las Redes.....	9
1.7.1.3 Tipos de Redes	12
1.7.1.4 Protocolos de Comunicación.....	13
1.7.1.5 Equipos de Comunicación	14
1.7.1.6 Tecnología de las Redes	15
1.7.1.7 Estándares de la IEEE	17

Capítulo 2	19
2 REDES WLAN	19
2.1 Redes Inalámbricas.....	19
2.1.1 Redes Híbridas (LAN cableadas y MAN inalámbricas).....	22
2.1.2 Tipos de Redes Inalámbricas	22
2.2 Redes Inalámbricas de Área Personal	23
2.2.1 Grupos de Trabajo	25
2.3 Redes Inalámbricas de Área Local	26
2.3.1 Grupos de Trabajo	28
2.3.2 Ubicación de las WLAN dentro de las tecnologías inalámbricas	31
2.4 Redes Inalámbricas de Área Metropolitana.....	32
2.5 Redes Inalámbricas Globales.....	33
2.6 Ondas electromagnéticas	35
2.6.1 Espectro Radioeléctrico	37
2.6.2 El Uso del Espacio, del Tiempo y del Espectro en Redes de RF.....	39
2.6.3 Comportamiento de RF.....	39
2.7 Propagación de la onda.....	40
2.7.1 Refracción.....	40
2.7.2 Reflexión.....	42
2.7.3 Difracción	43
2.7.4 Absorción.....	44
2.8 Técnicas de modulación	45
2.8.1 Técnicas de modulación Básica.....	45
2.8.2 Técnicas de Modulación WLAN	46
2.9 Técnicas de transmisión WLAN.....	47
2.9.1 Spread Sprectrum.....	47
2.9.1.1 DSSS	48
2.9.1.2 FHSS	48
2.9.1.3 Ventajas y Desventajas de Spread Spectrum.....	49
2.9.2 OFDM.....	49
2.9.2.1 Características de la modulación OFDM.....	50
2.10 Cómo funciona Wi-Fi	50
2.10.1 Modelo OSI para redes inalámbricas.....	51
2.10.2 Capas IEEE802.....	52
2.10.3 Capa Física	52
2.10.3.1 Elementos de la Capa física.....	54
2.10.4 MAC.....	55
2.10.4.1 Funciones principales de la Capa MAC	56

2.11	Estructura Wi-Fi.....	59
2.11.1	Distintas direcciones IP.....	59
2.11.2	DHCP.....	60
2.11.3	NAT.....	61
2.11.4	DMZ.....	63
2.12	Aplicaciones de Redes Inalámbrica.....	65
2.12.1	Aplicaciones Indoor.....	65
2.12.2	Aplicaciones Outdoor.....	65
2.12.2.1	Enlaces Punto a Punto.....	66
2.12.2.2	Enlaces Punto a Multipunto.....	66
2.12.2.3	Servicio de Internet Inalámbrico.....	66
Capítulo 3.....		67
3	SEGURIDAD PARA REDES INALÁMBRICAS.....	67
3.1	Principios de seguridad.....	67
3.1.1	Vulnerabilidades de una WLAN.....	70
3.1.2	Amenazas WLAN.....	71
3.1.3	Ataques contra las WLAN.....	72
3.1.4	Debilidades de las Wi-Fi.....	73
3.2	Mecanismos de Seguridad en las Redes Inalámbrica.....	73
3.2.1	Filtrado de direcciones MAC.....	74
3.2.2	WEP.....	75
3.2.3	Autenticación.....	76
3.2.3.1	OSA.....	76
3.2.3.2	SKA.....	77
3.2.3.3	CNAC.....	78
3.2.3.4	ACL.....	78
3.2.4	802.1x.....	78
3.2.5	WAP.....	79
3.2.5.1	Comparación Modelos OSI, TCP/IP y WAP.....	80
3.3	Medidas de Protección.....	81
Capítulo 4.....		83
4	ANÁLISIS DE LA RED EN EL COLEGIO INTERNACIONAL SEK-QUITO.....	83
4.1	Análisis de la infraestructura Colegio Internacional SEK-QUITO.....	83
4.1.1	Infraestructura LAN.....	83
4.1.1.1	Mapa de la Red.....	85
4.1.1.2	Medios LAN.....	87
4.1.2	Comprobación de la red LAN.....	90
4.1.3	Rendimiento de la red LAN.....	90

4.2	Inspección y descripción de la infraestructura.....	91
4.2.1	Inspección de la infraestructura	92
4.2.2	Inspección de equipos activos existentes.....	93
4.3	Documentación de análisis e inspecciones de la red LAN.....	94
4.3.1	Equipos existentes.....	94
4.3.2	Direcciones IP.....	94
4.3.3	Máscara de Subred.....	97
4.3.4	Dirección Proxy.....	97
4.4	Requerimientos del Colegio Internacional SEK-QUITO.....	104
4.5	Informe de la red del Colegio Internacional SEK-QUITO.....	105
Capítulo 5	107
5	DISEÑO WLAN COLEGIO INTERNACIONAL SEK-QUITO	107
5.1	Principios del Diseño (PDIOO).....	107
5.2	Estudio del diseño WLAN Colegio Internacional SEK-QUITO.....	109
5.2.1	Matriz (Equipos-Solución)	110
5.2.2	Requisitos de Diseño	114
5.2.2.1	Objetivo Financiero.....	115
5.2.2.2	Objetivo Técnico	115
5.3	Situación Actual de la Red	115
5.3.1	Servicios de Red que dispone el Colegio Internacional SEK-QUITO	116
5.3.2	Densidad de Usuarios	117
5.3.3	Número de Puntos de Red y Host.....	117
5.3.4	Requerimientos de los usuarios	117
5.3.5	Escalabilidad de la Red Actual	118
5.3.6	Disponibilidad de la Red Actual.....	118
5.3.7	Calidad.....	119
5.3.8	Seguridad	120
5.3.8.1	Seguridad Lógica.....	121
5.3.8.2	Seguridad Física	122
5.3.9	Topología Física	122
5.3.9.1	Dimensionamiento de las Instalaciones.....	122
5.3.9.2	Distribución.....	122
5.3.9.3	Materiales que componen el área de trabajo de las instalaciones.....	124
5.3.9.4	Esquema de Distribución física.....	125
5.3.10	Topología Lógica.....	125
5.3.10.1	Esquema de Red Actual.....	125
5.3.11	Red inalámbrica.....	127
5.4	Propuesta WLAN Colegio Internacional SEK-QUITO	127

5.4.1	Ubicación de puntos de acceso	133
5.4.2	Mapas de Cobertura	137
5.4.2.1	Cobertura Horizontal	141
5.4.2.2	Direccionamiento IP para equipos inalámbricos	143
5.4.2.3	Seguridad	143
5.4.2.4	Resumen de segmento inalámbrico	143
5.5	Administración WLAN Colegio Internacional SEK-QUITO	144
5.5.1	Elementos involucrados en la Administración de Red	145
5.5.2	Operaciones de la Administración de Red	146
5.5.3	Funciones de Administración definidas por OSI y aplicadas en la red del Colegio Internacional SEK-QUITO	147
Capítulo 6		148
6	IMPLEMENTACIÓN DE WLAN COLEGIO INTERNACIONAL SEK-QUITO..	148
6.1	Implementación WLAN Colegio Internacional SEK-QUITO	148
6.1.1	Configuración de los puntos de acceso	150
6.1.1.1	Propiedades configurables en el punto de acceso	160
6.1.1.2	Selección del canal	167
6.1.1.3	Conexión con la red LAN	169
6.1.1.4	Comprobar el funcionamiento	170
6.1.2	Configuración de los ordenadores	172
6.1.2.1	Gestión de la Red	175
6.1.2.2	Medir Velocidad	176
6.2	Conexión a Internet	177
6.2.1	Acceso a Internet	178
6.2.1.1	Ancho de Banda	178
6.2.2	Acceso de Banda Ancha	179
6.2.3	Conexión de Wi-Fi con Internet	180
6.2.3.1	Instalación conexión entre Wi-Fi e Internet	181
6.2.3.2	Configuración del punto de acceso	181
6.2.4	Pruebas y Monitoreo WLAN Colegio Internacional SEK-QUITO	182
6.2.4.1	Comprobar el acceso a Internet	188
Capítulo 7		190
7	DEFINICIÓN DE POLÍTICAS Y ESTÁNDARES DE SEGURIDADES EN LA WLAN COLEGIO INTERNACIONAL SEK-QUITO.....	190
7.1	Creación de Estándares de Seguridad	190
7.2	Implementación de las política y estándares de para la WLAN Colegio Internacional SEK-QUITO	195
7.2.1	Pruebas y Monitoreo WLAN Colegio Internacional SEK-QUITO	198

Capítulo 8	201
8 CONCLUSIONES Y RECOMENDACIONES	201
8.1 CONCLUSIONES.....	201
8.2 RECOMENDACIONES	203
ANEXOS	205
BIBLIOGRAFÍA	223

ÍNDICE DE TABLAS

Tabla 1.1 Grupos de Trabajo del comité de normalización IEEE 802	18
Tabla 2.1 Bandas ISM	20
Tabla 2.2 Tipos de redes inalámbricas	23
Tabla 2.3 Grupo de Trabajo 802.15	25
Tabla 2.4 Grupo de Trabajo 802.11	29
Tabla 2.5 Espectro Radioeléctrico	38
Tabla 2.6 Relación de los protocolos de red local	51
Tabla 4.1 Mapa de Red	86
Tabla 4.2 Resumen General del Flujo de Información del Colegio SEK-QUITO	91
Tabla 4.3 Clientes registrados – Máquinas de red	97
Tabla 4.4 Máscara de Subred	97
Tabla 4.5 Personas Promedio	102
Tabla 4.6 Alumnos de Primaria con disponibilidad de equipos inalámbricos	102
Tabla 4.7 Alumnos de Secundaria con disponibilidad de equipos inalámbricos	103
Tabla 4.8 Docentes con disponibilidad de equipos inalámbricos	103
Tabla 4.9 Alumnos de primaria con disponibilidad de equipos inalámbricos	103
Tabla 5.1 Puntos de Datos y Hosts Habilitados	117
Tabla 5.2 Datos de disponibilidad de red actual	119
Tabla 5.3 Parámetros de throughput	119
Tabla 5.4 IP's Fijas – Área Administrativa	126
Tabla 5.5 IP's Fijas – Impresoras en Red	127
Tabla 5.6 Asignación de canales para cada bloque	130
Tabla 5.7 Descripción de los Equipos	136
Tabla 5.8 Ubicación de los Equipos	136
Tabla 5.9 Medición cobertura horizontal Bloque I, II y Administración	142
Tabla 5.9 Medición cobertura horizontal Bloque III	142
Tabla 5.10 Medición cobertura horizontal Bloque IV	142
Tabla 5.11 Medición cobertura horizontal BIBLIOTECA	142
Tabla 5.12 Medición cobertura horizontal Bloque IV (PASILLO)	142
Tabla 5.13 Direcciones IP para equipos inalámbricos	143
Tabla 5.14 Resumen de segmento inalámbrica	143
Tabla 6.1 Estándares 802.11, números de canales y capacidad	149
Tabla 6.2 Descripción de los botones de comando	167
Tabla 6.3 Canales y bandas de frecuencia de rede 802.11g,b	168
Tabla 6.4 Cuadro comparativo de obstrucciones de propagación	170
Tabla 6.5 Obstrucción de señales de materiales	171

ÍNDICE DE FIGURAS

Figura 1.1 Topología de Red Inalámbrica Propuesta	7
Figura 1.2 Topología de Bus	10
Figura 1.3 Topología de Anillo	11
Figura 1.4 Topología en Estrella	12
Figura 1.5 Tipos de Redes	13
Figura 1.6 Modelo OSI.....	14
Figura 2.1 Disponibilidad del Espectro	19
Figura 2.2 Tecnologías Inalámbricas.....	22
Figura 2.3 Posicionamiento Estándares Wireless.....	34
Figura 2.4 Espectro Electromagnético	37
Figura 2.5 Refracción	41
Figura 2.6 Representación de la Refracción con la Densidad	42
Figura 2.7 Reflexión.....	42
Figura 2.8 Representación de la Reflexión.....	43
Figura 2.9 Principio De Huygens	44
Figura 2.10 Representación de la Difracción	44
Figura 2.11 Absorción Atmosférica	45
Figura 2.12 Funcionamiento DHCP	61
Figura 2.13 Arquitectura DMZ.....	64
Figura 3.1 Acceso no autorizado a una red Wireless	68
Figura 3.2 Arquitectura de un sistema de autenticación 802.1x.....	79
Figura 3.3 Modelos OSI, TCP/IP y WAP	80
Figura 4.1 Esquema de Cableado Estructurado.....	87
Figura 4.2 Cable UTP.....	88
Figura 4.3 PLUG	88
Figura 4.4 JACK.....	88
Figura 4.5 Fibra Óptica.....	89
Figura 4.6 Medios LAN Colegio Internacional SEK-QUITO.....	89
Figura 4.7 Ubicación del Colegio Internacional SEK-QUITO	92
Figura 4.8 Bloques y Espacios Abiertos del Colegio Internacional SEK-QUITO	93
Figura 4.9 Direcciones IP y Máscara de Subred	96
Figura 4.10 Conexión a través de Proxy	98
Figura 4.11 Tracert www.google.com.....	99
Figura 4.12 Resultados de la prueba piloto	101
Figura 5.1 Ciclo de Vida de una Red	107
Figura 5.2 Tareas del Diseño de la Red.....	109

Figura 5.3 Diagrama de Puestos de trabajo	111
Figura 5.4 Servidores de la red del Colegio Internacional SEK-QUITO	113
Figura 5.5 Tamaño de Paquetes.....	120
Figura 5.6 Utilización de la Red.....	120
Figura 5.7 Esquema de Cableado Estructurado hacia los Puntos de Acceso	128
Figura 5.8 Puntos de acceso en cada bloque	129
Figura 5.9 Asignación de canales múltiples bloques.....	130
Figura 5.10 Bloque I (Administración y Preescolar).....	132
Figura 5.11 Bloque II y III (Primaria).....	132
Figura 5.12 Bloque IV (Secundaria)	132
Figura 5.13 Biblioteca y Áreas de recreación.....	133
Figura 5.14 Ubicación de los Equipos	137
Figura 5.15 Diseño físico WLAN propuesto para el Colegio Internacional SEK-QUITO	138
Figura 5.16 Software para el monitoreo del diseño de la red WLAN	140
Figura 5.17 Interfaz gráfica del software utilizado para mediciones	140
Figura 5.17 Interfaz gráfica del software utilizado para mediciones	141
Figura 6.1 Punto de Acceso Aironet 1310 de CISCO	152
Figura 6.2 Conectores Aironet 1310 de CISCO.....	153
Figura 6.3 Antena omnidireccional de 5,2 dBi de CISCO para techo.....	154
Figura 6.4 Ejemplo de patrón de radiación Azimut de la antena.....	154
Figura 6.5 Modelos de Ganancia de una Antena.....	156
Figura 6.6 Seguridad con las Líneas de Alta Tensión	156
Figura 6.7 Atenuación	157
Figura 6.8 Bloque I (Administración y Preescolar).....	158
Figura 6.9 Bloque II y III (Primaria y Secundaria)	158
Figura 6.10 Bloque IV (Secundaria)	159
Figura 6.11 Opciones de Conexión	159
Figura 6.12 Conexión al CISCO Aironet 1310	165
Figura 6.13 GUI del IOS	166
Figura 6.14 Topología de una Red en Infraestructura	169
Figura 6.15 Configuración de la tarjeta.....	173
Figura 6.16 WLAN del Colegio Internacional SEK-QUITO	182
Figura 6.17 Mapa de Cobertura Experimental Bloque I (Administración y Preescolar)	183
Figura 6.18 Mapa de Cobertura Experimental Bloque II y III (Primaria y Secundaria)	183
Figura 6.19 Mapa de Cobertura Experimental Bloque IV (Secundaria)	184
Figura 6.20 Medición a 6 metros en el Bloque I, II y Administración.....	185
Figura 6.21 Medición a 9 metros en el Bloque I, II y Administración.....	185
Figura 6.22 Medición a 6 metros en el Bloque III.....	186
Figura 6.23 Medición a 9 metros en el Bloque III.....	186
Figura 6.24 Medición a 6 metros en el Bloque IV	186
Figura 6.25 Medición a 9 metros en el Bloque IV	187
Figura 6.26 Medición a 3 metros en Biblioteca.....	187
Figura 6.27 Medición a 6 metros en Biblioteca.....	187
Figura 6.28 Medición a 3 metros en el Bloque IV (Pasillo).....	188

Figura 6.29 Medición a 6 metros en el Bloque IV (Pasillo).....	188
Figura 7.1 Rueda de Seguridad en una WLAN	192
Figura 7.2 Websense Policy Server	194
Figura 7.3 Websense	195
Figura 7.4 Opción Seguridad.....	197
Figura 7.5 Autenticación Punto de Acceso	198
Figura 7.6 Contraseña.....	199

ÍNDICE DE ANEXOS

Anexo A ESQUEMA DE LA DISTRIBUCIÓN DEL CABLEADO DE LA RED	205
Anexo B ESQUEMA DE CONEXIÓN FÍSICA DEL COLEGIO SEK-QUITO	208
Anexo C DISEÑO WLAN PROPUESTO PARA EL COLEGIO	210
Anexo D DATASHEET 3COM 4800G	212
Anexo E DATASHEET SUPERSTACK 3226.....	216
Anexo F TABLA DE ÁREAS DE LA CURVA	220

NOMENCLATURA

AES	Advanced Encryption Standard
ASK	Amplitude Shift Keying
BPSK	Binary Phase Shift Keying
CA	<i>Corriente Alterna</i>
CCA	Clear Channel Assesment
CCK	Complementary Code Keying
COFDM	Coded OFDM
CRC	Cyclic Redundancy Check
CEPT	Conference of European Post and Telecommunications
CDPD	Cellular Digital Packet Data
CDMA	Code Division Multiple Access
CONATEL	Consejo Nacional de Telecomunicaciones
CSMA/CD	Carrier Sense Multiple Access / Collision Avoidance
DSSS	Direct Sequency Spread Spectrum
DHCP	Dynamic Host Configuration Protocol
DMT	Discreet Multitone Modulation
DECT	Digital Enhanced Cordless Telecommunications
DMZ	Demilitarized Zone
DNS	Domain Naming System
DQDB	Distributed Queue Dual Bus
DQPSK	Differential Quadrature Phase Shift Keying
DBPSK	Differential Binary Phase Shift Keying
EAP	Extensible Authentication Protocol,
ETSI	Instituto de Estándares de Telecomunicaciones Europeo
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
FCC	Comisión Federal de Comunicaciones
FPLMTS	Future Public Land Mobile Telecommunications System
GSM	Global System for Mobile Communications
HEC	Header Error Control
IEEE	Institute of Electrical and Electronics Engineers
IMT2000	International Mobile Communications
IP	Internet Protocol
IOS	Internetwork Operating System
ISS	Internet Information Server
ISM	Industrial Scientific Medical

LAN	Local Area Network
LLC	Logical Link Control
LMDS	Local Multipoint Distribution Service
MAN	Metropolitan Area Network
MAC	Medium Access Control
MMDS	Microwave Multipoint Distribution Service
NAT	Network Address Translation
NOS	Network Operating System
OSI	Open System Interconnection
OFDM	Orthogonal Frequency Digital Multiplexing
OEM	Ondas electromagnéticas
PAT	Port Address Translation
PAN	Personal Area Network
PEAP	Protected Extensible Authentication Protocol
PSK	Phase Shift Keying
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
PHY	Physical Layer
QPSK	Quadrature Phase Shift Keying
QAM	Quadrature Amplitude Modulation
RF	Propagación de la radiofrecuencia
SNMP	Simple Network Management Protocol
SWAP	Share Wireless Access Protocol
SSID	Service Set Identifier
S/R	Signal to noise ratio
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TD SCDMA	Time Division Synchronous Code Division Multiple Access}
TLS	Transport Layer Security
TTLS	Tunneled TLS
UIT	Unión Internacional de Telecomunicaciones
UMTS	Universal Mobile Telecommunications System
VSWR	Voltaje de Onda Estacionaria
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WMAN	Wireless Metropolitan Area Network
WDSL	Wireless DSL
WWAN	Wireless Wide Area Network
WCDMA	Wideband CDMA

Capítulo 1

1. INTRODUCCIÓN

Este capítulo muestra las ideas generales para encontrar una solución viable a los problemas de la red informática del Colegio Internacional SEK-QUITO, tomando como solución preliminar, el uso de Redes Inalámbricas. A continuación se detalla las partes del plan del proyecto de análisis, diseño e implementación de una Red Inalámbrica en el Colegio Internacional SEK-QUITO.

1.1 ANTECEDENTES

El Colegio Internacional SEK-QUITO, es uno de las catorce Centros Educativos Internacionales que conjuntamente con las tres universidades conforman la Institución Internacional SEK que se encuentra ubicada en tres continentes.

Inició su servicio educativo a la comunidad ecuatoriana a partir de 1984, con una sólida visión innovadora la cual forma entes críticos, reflexivos con un gran dominio cognitivo y una formación en valores y actitudes, contando con una infraestructura acorde con las exigencias de vanguardia, aulas debidamente equipadas, un extenso comedor, innovador polideportivo, piscina cubierta, áreas recreacionales y canchas deportivas.

Bajo el carácter de plantel experimental el Colegio Internacional SEK-QUITO ejecuta innovadores proyectos educativos acordes con las exigencias tecnológicas y sociales, entre los cuales figuran, el Bachillerato Nacional y el programa internacional que abarca el MYP (Programa de Años Intermedios) y el Diploma bilingüe de la Organización de Bachillerato Internacional de Ginebra, tratamiento académico de ciertas áreas de estudio en este idioma, capacitación permanente del personal docente, entre otros.

Dado el constante crecimiento de la población estudiantil, al momento cuenta en sus aulas con 1400 alumnos, en sus tres niveles de formación: pre-escolar, primario y secundaria. Este último cuenta con Bachillerato Nacional e Internacional, lo que obligan

a la Institución a incrementar sus instalaciones, laboratorios y talleres acordes a los últimos adelantos tecnológicos.

1.2 DETERMINACIÓN DEL PROBLEMA

Las empresas privadas y públicas no solo centran su atención en los recursos que son tangibles, sino que en la actualidad las empresas dependen de la comunicación para desarrollar su actividad y para transmitir valor, por lo que dan mayor prioridad a la información y a la tecnología, puntos claves para el desarrollo y productividad de una sociedad.

La comunicación oportuna, precisa y segura es de vital importancia a la hora de tomar decisiones o realizar planificaciones; es por eso que en el sector de las comunicaciones se buscan alternativas que brinden conectividad y calidad en todo momento.

Con el avance tecnológico de las redes de datos y en especial las redes inalámbricas tienen que ser capaces de soportar cualquier tipo de servicio; ya que actualmente se habla de la convergencia de servicios. Se puede digitalizar texto, música, imagen y video, que luego viaja por los canales de comunicación; dichos flujos de información no solo tienen que cumplir con normas de seguridad; sino que tienen que ser de calidad, lo que hace que las empresas tecnológicas, busquen mecanismos para gestionar y administrar las redes.

Una de las tecnologías de mayor desarrollo tecnológico en la última década, es la tecnología inalámbrica, la cual facilita la posibilidad de acceder a una red de datos, desde cualquier punto de una determinada área geográfica, campus universitario, edificios empresariales, edificios escolares, sin la necesidad de una conexión física, a usuarios que por sus características de uso requieren moverse dentro de las áreas especificadas.

En redes cableadas, el uso de tecnologías inalámbricas es complementario, cubriendo en ciertos casos limitaciones de crecimiento de la red, que por razones técnicas y

económicas imposibilita el seguir incrementado puntos adicionales en la red física, que es el caso para el cual se va a desarrollar el presente proyecto.

El Colegio Internacional SEK-QUITO al momento funciona en el sector norte de Quito con dirección C/ Carmen Olmo Mancebo y Guayacanes, la infraestructura física que soporta la red institucional fue proyectada con una cantidad de puntos que actualmente se torna insuficiente para atender el volumen creciente de usuarios que solicitan acceso a la red. La creación, remodelación o mudanzas de direcciones, oficinas o aulas, en los distintos departamentos ha exigido la extensión de la red a tal nivel que actualmente nos vemos imposibilitados de poder agregar nuevos puntos de acceso, lo que se explica por el número de puertos que ofrecen los switches que se encuentran en diferentes puntos del establecimiento.

Aparte de la demanda de puntos de red que se genera por los distintos departamentos, se debe sumar las solicitudes de acceso que realizan los administradores, personal docente y estudiantes que poseen equipos personales portátiles, limitándose el acceso a la red del colegio en áreas en la que se podría considerar espacios de tranquilidad.

Un caso crítico lo constituye la sección de primaria-secundaria, donde se encuentra la biblioteca, y donde se han implementado 50 equipos portátiles para el uso de profesores y estudiantes desde la cual nos es imposible ofrecer acceso a la red por las razones ya expuestas.

1.3 JUSTIFICACIÓN

La era tecnológica en la actualidad, ha hecho que en diferentes proyectos de innovación empresarial-educativa, la información se convierte en herramienta fundamental para la obtención y aplicación de nuevos conocimientos, obligando al Colegio Internacional SEK-QUITO a tener nuevos y modernos sistemas de acceso a la red interna del establecimiento, y que se permitan seguir paso a paso el avance de nuevas tecnologías con una tendencia de información globalizada, eliminando las barreras del tiempo y la

distancia y permitiendo al personal administrativo, docente y alumnado, a compartir información y trabajar en colaboración gracias al uso y a la aplicación del Internet.

Frente a la problemática que se ha descrito, el Departamento de Sistemas del Colegio Internacional SEK-QUITO, se ha visto en la necesidad de diseñar los lineamientos generales de una solución que atienda la demanda actual y a mediano plazo del acceso a la red. Por lo que la ejecución del presente proyecto tendrá que someterse a las evaluaciones básicas, para que estas tengan la aprobación y visto bueno, convirtiéndose en viabilidades que se deben dar al mismo tiempo para alcanzar la factibilidad del proyecto, para que con el desarrollo del presente proyecto buscar definir la calidad de acceso, además de las ventajas, tipos de servicio, escalabilidad que brinda la utilización de infraestructuras inalámbricas, así como las limitaciones que pueden tener los equipos a la hora de incorporar nuevas modificaciones, y principalmente, con los cambios a realizar, no se atente contra la arquitectura de la infraestructura ya consolidada que soporta los recursos de comunicación que a su vez apoyan las distintas actividades académicas y administrativas propias de nuestra Institución

La ejecución del presente trabajo de investigación apoyarán al desarrollo de actividades y dará el impulso que necesitan los estudiantes para profundizar y obtener nuevos conocimientos, colaborando de esta manera a la misión de la Institución que es la de proporcionar servicio educativo integral a los alumnos que asisten de los diferentes sectores de la capital del país, basados en la aplicación de las innovaciones curriculares, en el rescate de los valores éticos, morales, cívicos; optimizando los recursos que ofrece el medio y la sociedad, a fin de contribuir al desarrollo del sistema educativo Provincial y Nacional.

1.4 SOLUCIÓN DEL PROBLEMA

Una vez conocidas las dificultades que en la actualidad el Colegio Internacional SEK-QUITO se encuentra atravesando, y tras analizar todos los requerimientos y características que el proyecto debe contener, se presenta una propuesta técnica que incluye el análisis del sitio y las configuraciones de los equipos para la comunicación.

El análisis del sitio se realizará una exploración de todas las áreas en las cuales los usuarios tienen la necesidad de un punto de acceso, este análisis se lo efectuara en busca de la mejor ubicación de los puntos de accesos para que así no se vea comprometido el desempeño de ese segmento de la red.

Una vez revisados los inconvenientes de los docentes y alumnos, se han planteado posibles alternativas que podrían implementarse, las cuales incluyen el acceso de los usuarios a través de puntos de acceso en cada área en las cuales sea necesario permitiendo esto la conexión con la red actual.

Se evaluaron dos alternativas:

- a) Extensión del cableado actual.
- b) Extensión de los servicios a través de medios inalámbricos.

En ambos casos se lograría la extensión de la red institucional; sin embargo, proponemos la adopción de la segunda alternativa, apoyados en las siguientes razones:

- **Costos.-**

La primera opción requeriría la adquisición de nuevos switches, cables, conectores; además demandaría la ejecución de trabajos sobre la planta física que implicarían costos hasta en un 65% superior a los generados en la segunda opción. Por otra parte, la inversión a realizar en el caso de adoptar la primera alternativa de solución no garantizaría la eficacia de la misma en el tiempo, puesto que al depender de puntos físicos de conexión, no se asegura la extensibilidad de la red a mediano y largo plazo. En contraposición, la solución inalámbrica requeriría la adquisición de switches inalámbricos de costos inferiores a los switches convencionales; así como la adquisición de tarjetas de red inalámbricas para los equipos que accedan por esta vía a los recursos de la red institucional. Tal solución no requeriría cambios en la planta física de nuestra Institución, lo que disminuiría notablemente los costos de instalación de cableado y posterior certificación de los puntos de red. Lo anterior significaría que no importando los cambios que se realicen en la distribución de nuevas oficinas, el Departamento de Sistemas del Colegio Internacional SEK-QUITO

estaría en capacidad de ofrecer de manera instantánea el acceso a la red de nuevos equipos.

- **Extensión de la vida útil de la infraestructura de red.-**

La naturaleza de la solución inalámbrica respetaría la arquitectura de la red actual, al mismo tiempo que posibilitaría su extensibilidad en el tiempo de manera ordenada a mediano y largo plazo, así como la compatibilidad con nuevas tecnologías.

- **Mejora del servicio.-**

La solución inalámbrica representaría una mejora en el servicio con una inversión razonable, no sólo para hacer frente al aumento de la demanda por parte de las distintas áreas de la Institución, sino que también nos permitiría ofrecer de manera expedita conexión a la red a los docentes y estudiantes que posean equipos portátiles con dispositivos inalámbricos. Significaría también que cualquier profesor con equipo portátil podría trabajar de manera cómoda en cualquier lugar dentro de la Institución y acceder igualmente a Internet.

- **Tiempo de implementación**

Los tiempos de implementación de la solución inalámbrica serían razonablemente cortos, siempre y cuando se otorguen los recursos necesarios para la ejecución de las tres etapas que constituirían el proyecto, a saber: Fase de Diseño, Fase de Implementación y Fase de Pruebas. Estimamos necesario adquirir equipos para realizar pruebas que nos permitirían, entre otros aspectos: determinar la mejor ubicación de los switches inalámbricos, determinar el alcance efectivo de cada dispositivo y por lo tanto la cantidad de estos necesaria para hacer efectiva la solución; y lo más delicado, conocer los modelos de los dispositivos que garanticen la compatibilidad con el sistema operativo con la que opera la Institución

La solución inalámbrica se describe a continuación:

- En cada Sección se dispondría de un switch inalámbrico conectado a un punto de red o directamente al switch convencional que presta servicio en dicha área.

- A los equipos que necesiten acceder a la red y que no puedan debido a la ausencia de puntos físicos de acceso, se les instalará una tarjeta de red inalámbrica (dado el caso que no tuvieran), que se comunicaría con el switch inalámbrico más cercano. Se estudian dos posibilidades en cuanto al dispositivo a instalar en los equipos: la instalación de una tarjeta de red inalámbrica o la instalación de dispositivos USB de acceso inalámbrico. La última opción sería recomendable puesto que minimizaría el proceso de instalación; pero por otra parte, los aspectos de seguridad deben ser contemplados debido a la facilidad con la que pueden ser sustraídos tales dispositivos.
- Los dispositivos deben ser compatibles con Windows

La figura que se presentan a continuación muestra la vista de la solución propuesta

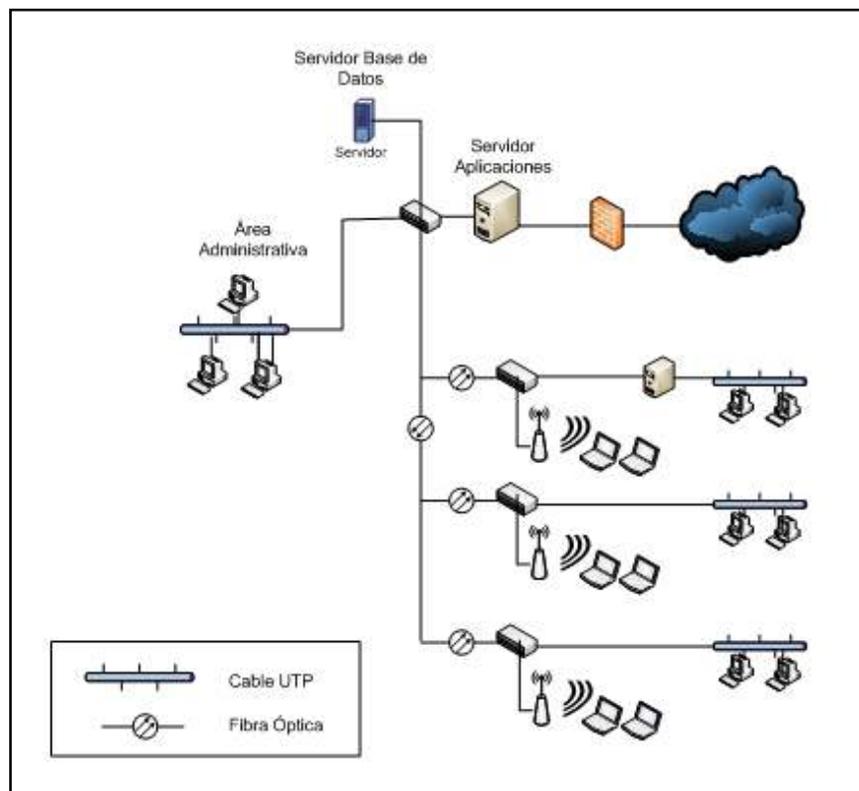


Figura 1.1 Topología de Red Inalámbrica Propuesta

1.5 OBJETIVOS

1.5.1 Objetivo General

Realizar el Proyecto de Análisis, Diseño e Implementación de una Red Inalámbrica en el Colegio Internacional SEK-QUITO, considerando aspectos de Seguridad dentro del Área Perimetral

1.5.2 Objetivos Específicos

- Analizar y determinar el tráfico que debe soportar la red de datos para los usuarios móviles del Colegio Internacional SEK-QUITO
- Determinar un diseño de red inalámbrica adecuado para los usuarios móviles del Colegio Internacional SEK-QUITO, con la finalidad de que la rapidez y la entrega garantizada de flujos de datos que van a circular en la red, permitan gestionarlo y administrarlo.
- Determinar los equipos necesarios que cumplan con los estándares de seguridad y administración de tráfico para la implementación de la solución.
- Implementar y configurar redes inalámbricas seguras en redes basadas en los sistemas operativos de Microsoft con los que trabaja el Colegio Internacional SEK-QUITO.

1.6 ALCANCE

Como aplicación práctica de la tesis se propondrá el análisis, diseño e implementación de una Red Inalámbrica con estándares de seguridad en el Colegio Internacional SEK-QUITO sede Ecuador, donde se someterá a pruebas de diferentes métodos de acceso

para determinar cuál de los modelos analizados es recomendable en cuanto a prestaciones de control de acceso se refiere.

1.7 MARCO TEÓRICO

1.7.1 Redes

1.7.1.1 Concepto de una Red

La más simple de las redes conecta dos computadoras, permitiéndoles compartir archivos e impresoras. Una red mucho más compleja conecta todas las computadoras de una empresa o compañía en el mundo. Una vez instalada la conexión se instala el sistema operativo de red NOS (Network Operating System). Hay dos tipos básicos de sistemas operativos de red: punto a punto y con servidor dedicado.

1.7.1.2 Topología de las Redes

Las redes de computadoras surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos. Pero los diferentes componentes que van a formar parte de una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de topología de la red. La topología idónea para una red concreta va a depender de:

- El número de máquinas a interconectar
- El tipo de acceso al medio físico que deseemos

Las principales topologías son:

a) Topología de Bus.-

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los hosts queden desconectados.

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, inconvenientes que se solucionan segmentando la red en varias partes. Es la topología más común en pequeñas LAN (Local Area Network), con hub o switch final en uno de los extremos.

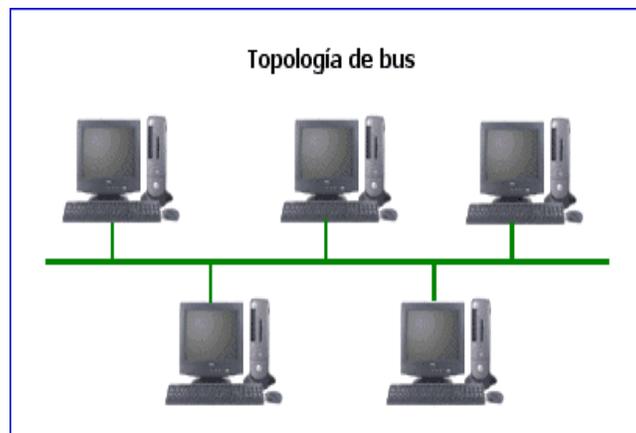


Figura 1.2 Topología de Bus

b) Topología de Anillo.-

Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos adyacentes. Los dispositivos se conectan directamente entre sí por medio de cables en lo que se denomina una cadena margarita. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

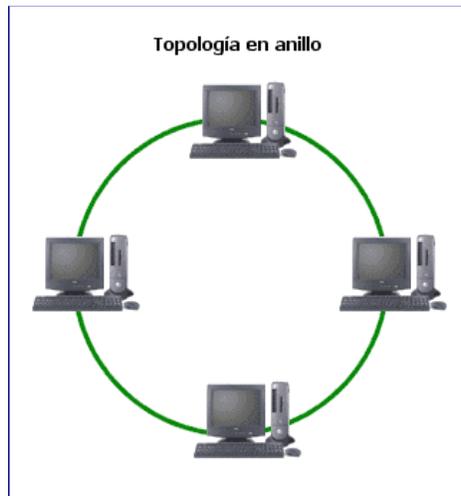


Figura 1.3 Topología de Anillo

c) Topología en Estrella.-

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un concentrador, pasa toda la información que circula por la red. La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

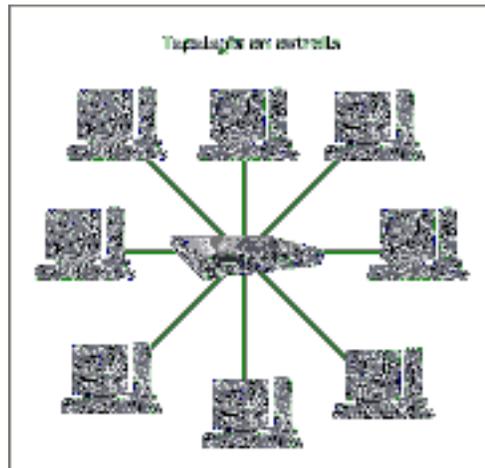


Figura 1.4 Topología en Estrella

1.7.1.3 Tipos de Redes

Actualmente existe una gran variedad de redes no sólo por el número sino también por la diversidad de protocolos que ellas utilizan. Las redes de acuerdo a la cobertura geográfica pueden ser clasificadas en LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).

a) LAN - Redes de Área Local.-

Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña. Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general broadcast), alta velocidad y topología. Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos.

b) MAN - Redes de Área Metropolitana.-

Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. La razón principal para

distinguirla de otro tipo de redes, es que para las MAN's se ha adoptado un estándar llamado DQDB (Distributed Queue Dual Bus) o IEEE 802.6. Utiliza medios de difusión al igual que las Redes de Área Local.

c) WAN - Redes de Amplia Cobertura.-

Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (end system). En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (conmutación). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión.¹

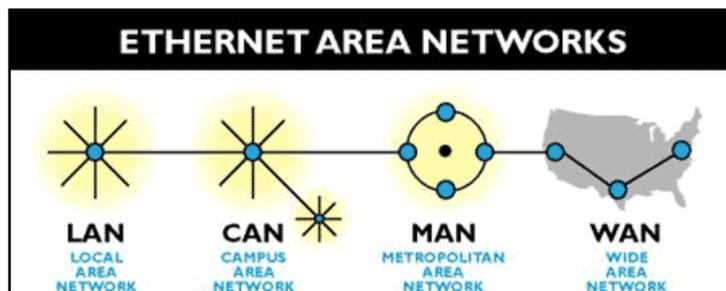


Figura 1.5 Tipos de Redes

1.7.1.4 Protocolos de Comunicación

Las reglas que regulan la comunicación dentro de una red se llaman protocolos. Un protocolo es por tanto un lenguaje, con su sintaxis, su semántica y su adecuada temporización. La sintaxis entronca con el cómo, la semántica con el qué (el significado), y la temporización con el cuándo.

a) Modelo OSI (Open System Interconnection).-

Fue definido por la ISO (Internacional Organization of Standards) en 1983. La propuesta OSI fue la siguiente: Para un terminal o host propusieron una estructura de 7 y 3 capas como puede apreciarse en la Figura 1.4

¹FRENZEL LOUIS E., "Sistemas Electrónicos de Comunicación", Alfaomega, 2003

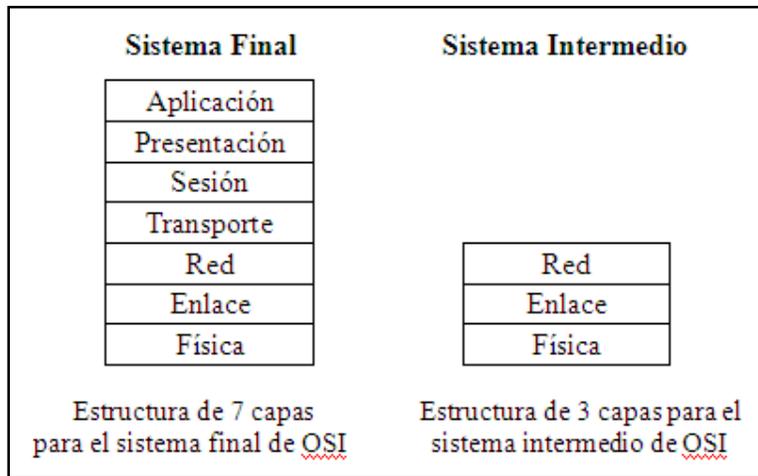


Figura 1.6 Modelo OSI

b) TCP/IP.-

El nombre TCP/IP proviene de dos protocolos importantes de la familia, el TCP (Transmission Control Protocol) y el IP (Internet Protocol). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto. El TCP/IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo ordenadores de escritorio, mini computadoras y computadoras centrales sobre redes de área local y área extensa.²

1.7.1.5 Equipos de Comunicación.

a) Puentes o Bridges.-

Los bridges trabajan en el nivel 2 de modelo OSI (Open System Interconnection), con direcciones físicas, por lo que filtra tráfico de un segmento a otro. Se utilizan cuando el tráfico no es excesivamente alto en las redes pero interesa aislar las colisiones que se produzcan en los segmentos interconectados entre sí.

² DOUGLAS COMER, TCP/IP, Vol 1, Prentice Hall, 1996.

b) Conmutadores Ethernet.-

Los conmutadores (Switch) Ethernet son una ampliación del concepto de puentes. Los conmutadores LAN tienen, básicamente dos arquitecturas, “store and forward” (almacenar y remitir) y “cut through” (cortar y atravesar). Inicialmente, los modelos “cut through”, tenían una ventaja de velocidad porque cuando un paquete entra en el conmutador, solo se examina la dirección del destino antes de remitirlo a su segmento de destino. Un conmutador “store and forward”, por otro lado, acepta y analiza el paquete completo antes de remitirlo a su destino.

c) Routers.-

Estos equipos trabajan a nivel 3 de la pila OSI, es decir pueden filtrar protocolos y direcciones a la vez. Los routers pueden interconectar redes distintas entre sí; eligen el mejor camino para enviar la información, balancean tráfico entre líneas, etc.

1.7.1.6 Tecnología de las Redes

En el siglo XXI, se presentan grandes desafíos, económicos, políticos, sociales y culturales, en los cuales las Telecomunicaciones tienen un rol de suma importancia, siendo el estudio de las redes el nexo de mayor relevancia para su desarrollo. El soporte que proporcionan las redes constituye de gran importancia para el desarrollo de los diferentes servicios y prestaciones en la obtención de nuevas y mejores conocimientos de la superautopista de la información.

Actualmente, el estudio de la tecnología de la redes busca una óptima infraestructura de última generación que nos permita comunicarnos con el resto del mundo, permitiendo de esta forma el más avanzado desarrollo de servicios de Telecomunicaciones.

El estudio de las tecnologías de redes ha permitido la interconexión de las mismas con la implementación de nuevas innovaciones o el mejoramiento de los sistemas ya existentes, mediante el acoplamiento de estándares de los diferentes hardwares de redes con su respectivo software y sistemas operativos compatibles.

a) Fast Ethernet.-

La tecnología Fast Ethernet nació a partir de la Ethernet, debido a que la tecnología Ethernet alcanza velocidades de hasta 10 Mbps mientras que la Fast Ethernet alcanza velocidades de 100 Mbps, que es la tecnología que actualmente es mayormente difundida en las computadoras que encontramos en el mercado. La velocidad de las redes y su disponibilidad son requerimientos críticos. Con más aplicaciones que requieren mayores velocidades en una LAN para tener un performance aceptable, los administradores de redes se enfrentan a una gran cantidad de opciones para implementar tecnologías de alta velocidad para una LAN.

b) Giga Ethernet.-

Es una extensión a las normas de 10-Mbps y 100-Mbps IEEE 802.3. Ofreciendo un ancho de banda de 1000 Mbps, Giga Ethernet mantiene compatibilidad completa con la base instalada de nodos Ethernet. Giga Ethernet soporta nuevos modos de operación Full-Duplex para conexiones conmutador-conmutador y conexiones conmutador-estación y modos de operación Half-Duplex para conexiones compartidas que usan repetidores y los métodos de acceso CSMA/CD (Carrier Sense Multiple Access / Collision Avoidance). Inicialmente operando sobre fibra óptica, Giga Ethernet también podrá usar cableados de par trenzado y coaxial.

Las implementaciones iniciales de Giga Ethernet emplean cableados de fibra de gran velocidad, los componentes ópticos para la señalización sobre la fibra óptica serán 780 nm (longitud de onda corta) para la serialización y deserialización. Está reforzándose la tecnología de fibra actual que opera a 1.063 Gbps para correr a 1.250 Gbps, proporcionando así los 1000 Mbps completos.

Para enlaces a más largas distancias, por encima de al menos 2 Km. usando fibra monomodo y por encima de 550 metros con fibra multimodo de 62.5. Usa los métodos de acceso CSMA/CD con soporte para un repetidor por dominio de colisión, mantiene total compatibilidad con las tecnologías 10 Base T y 100 Base T. ³

1.7.1.7 Estándares de la IEEE

IEEE (Institute of Electrical and Electronics Engineers), es la organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares para redes de la IEEE son los estándares de mayor importancia en de la actualidad.

A través de sus miembros, más de 360.000 voluntarios en 175 países, el IEEE es una autoridad líder y de máximo prestigio en las áreas técnicas derivadas de la eléctrica original: desde ingeniería computacional, tecnologías biomédica y aeroespacial, hasta las áreas de energía eléctrica, control, telecomunicaciones y electrónica de consumo, entre otras.

Mediante sus actividades de publicación técnica, conferencias y estándares basados en consenso, el IEEE produce más del 30% de la literatura publicada en el mundo sobre ingeniería eléctrica, en computación, telecomunicaciones y tecnología de control, organiza más de 350 grandes conferencias al año en todo el mundo, y posee cerca de 900 estándares activos, con otros 700 más bajo desarrollo.

A continuación los estándares para redes de la IEEE:

³ DOUGLAS COMER, TCP/IP, Vol 1, Prentice Hall, 1996.

Grupos de trabajo del IEEE	
Estándar	Características
IEEE 802.1	Cubre la administración de redes y otros aspectos relacionados con la LAN
IEEE 802.2	Protocolo de LAN de IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos
IEEE 802.3	Protocolo de IEEE para LAN que especifica la implementación de las capas físicas y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del Estándar IEEE 802.3 especifican implementaciones para fast Ethernet. Las variaciones físicas de las especificaciones IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT, y 10Broad36.
IEEE 802.4	Especifica el bus de señal pasante.
IEEE 802.5	Protocolo de LAN IEEE que especifica la implementación de la capa físicas y de la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa de acceso de transmisión de tokens a 4 Mbps ó 16 Mbps en cableado STP O UTP y de punto de vista funcional y operacional es equivalente a token Ring de IBM
IEEE 802.6	MAN (Red de Área Metropolitana)
IEEE 802.7	Emisión (Grupo técnico de recomendación)
IEEE 802.8	Fibra Óptica (Grupo técnico de recomendación)
IEEE 802.9	Redes de área local isosíncronas
IEEE 802.10	Seguridad de interoperación de redes de área local
IEEE 802.11	Redes de área local inalámbrica
IEEE 802.12	Prioridad de demanda
IEEE 802.14	Red de cable de comunicaciones de banda ancha
IEEE 802.15	Redes personales inalámbricas WPAN (Wireless Personal Area Network)
IEEE 802.16	Acceso inalámbrico de banda ancha

Tabla 1.1 Grupos de Trabajo del comité de normalización IEEE 802

Capítulo 2

2 REDES WLAN

En este capítulo se analizará la base teórica de los siguientes temas: Redes Inalámbricas y sus tipos, Ondas electromagnéticas, Técnicas de modulación, Técnicas de transmisión WLAN, Propagación de la onda, Funcionamiento Wi-Fi y Aplicaciones de Redes Inalámbricas.

2.1 Redes Inalámbricas

Una de las tecnología más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja, actualmente está siendo ampliamente investigada. Las redes inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentran en varios pisos.

La tecnología espectro disperso fue desarrollada en los años 40 en vísperas de la Segunda Guerra Mundial, para proteger comunicaciones militares. El espectro disperso es una tecnología inalámbrica que trabaja en la frecuencia 902 – 928 MHz, 2459 – 2483,5 MHz y 5,725 a 5,850 MHz, transmitiendo información en bandas que no requieren autorización regulatoria para su uso. Las llamadas aplicaciones industriales, científicas y médicas. La técnica de espectro disperso es actualmente la más utilizada en las redes LAN inalámbricas

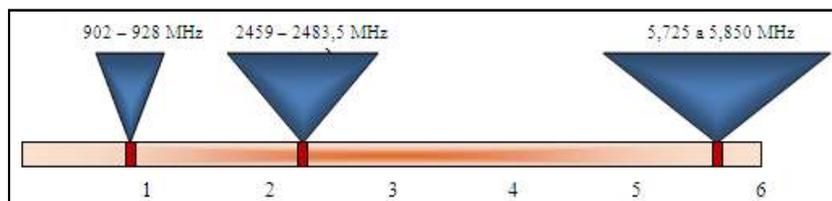


Figura 2.1 Disponibilidad del Espectro

Las bandas ISM (Industrial Scientific Medical) son bandas de frecuencias para uso comercial y sin licencia, son las utilizadas por los teléfonos inalámbricos domésticos, los microondas o los dispositivos Bluetooth.

En nuestro caso 802.11 utiliza el rango de frecuencias de 2,4 a 2,4835 GHz y la divide en canales (11 para EEUU y 9 para Europa), definiendo unos anchos de banda de 11, 5, 2 y 1 Mbps por canal.

Número de Canal	Frecuencia EEUU	Frecuencia Europa
1	2412	No disponible
2	2417	No disponible
3	2422	2422
4	2427	2427
5	2432	2432
6	2437	2437
7	2442	2442
8	2447	2447
9	2452	2452
10	2457	2457
11	2462	2462
Frecuencia en MHz		

Tabla 2.1 Bandas ISM

Cuando se tiene instalada la red inalámbrica, su utilización es prácticamente idéntica a la de una red cableada, los ordenadores que forman parte de la red se pueden comunicar entre sí y compartir toda clase de recursos, como ocurre en una con una red cableada, una red inalámbrica puede estar formada por tan solo dos ordenadores o por miles de ellos. Por todo lo anteriormente expuesto, las soluciones inalámbricas están poco a poco ocupando un lugar importante en las posibilidades que tienen los equipos informáticos de intercomunicarse.

Las redes inalámbricas hoy por hoy, también tienen algunos inconvenientes, tienen un menor ancho de banda (velocidad de transmisión), ya que las redes cableadas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica, las redes inalámbricas actuales ofrecen velocidades ideales de hasta 108 Mbps, las redes

cableadas ofrecen velocidades desde 100 Mbps hasta 1 Gbps. Y en general son más caras que las soluciones con cable, aunque en muchas ocasiones resultan no solo más baratas que la alternativa cableada, sino que se muestra como la solución más conveniente.

Las redes inalámbricas no vienen a reemplazar a las redes cableadas, sino que se convierten en una tecnología para resolver problemas de movilidad y accesibilidad de las estaciones.

Sin embargo se pueden fusionar las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de una institución o una oficina.

Existen dos amplias categorías de Redes Inalámbricas:

a) De Larga Distancia

Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps

b) De Corta Distancia

Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades de orden de 2 Mbps hasta los 108 Mbps

2.1.1 Redes Híbridas (LAN cableadas y MAN inalámbricas)

Es la fusión de las redes cableadas y las inalámbricas para que se pueda considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Considerando que las redes LAN cableadas son redes de computadoras cuya extensión se encuentra en el orden de los 10 metros a 1 Kilómetro que por lo general son redes pequeñas utilizadas en oficinas, escuelas o centros educativos que usualmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas.

Por otro lado se puede mencionar a la tecnología de redes MAN inalámbricas la cual es una colección de LAN's dispersadas geográficamente dentro de un campus (universidades, oficinas de gobierno o industrias) pertenecientes a una misma entidad en un área delimitada en kilómetros.

2.1.2 Tipos de Redes Inalámbricas

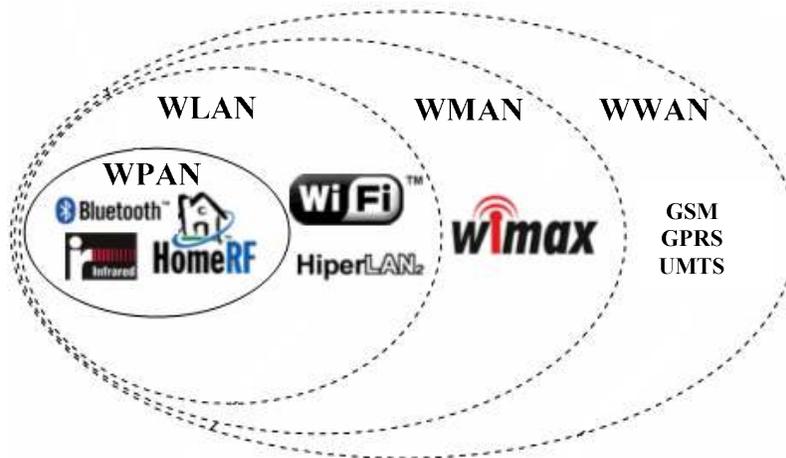


Figura 2.2 Tecnologías Inalámbricas

Las posibilidades que ofrecen las redes inalámbricas son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer alternativas de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red, por lo que con lo mismo que sucede con las redes con cable, las redes inalámbricas se pueden clasificar en diferentes tipos, o dependiendo del criterio al que se atienda, nosotros vamos a clasificarlas en función de las distancias a través de las que se pueden transmitir los datos.⁴

Las comunicaciones inalámbricas se dividen en los siguientes grupos de acuerdo con su alcance:

WPAN Redes de área personal inalámbricas	WLAN Redes de área local inalámbricas	WMAN Redes de área metropolitana inalámbricas	WWAN Redes de área extensa inalámbricas
< 10 metros	Edificios, hogares, campus	Ciudades	Regiones, globales
Bluetooth Infrarrojo DECT	Wi-Fi HomeRF HiperLAN	LMDS MMDS WiMax	2,5 G 3G

Tabla 2.2 Tipos de redes inalámbricas

2.2 Redes Inalámbricas de Área Personal

WPAN (Wireless Personal Area Network), son aquellas redes que tienen una cobertura de de los 10 metros como máximo. La finalidad de estas redes es la comunicación de dispositivos peer-to-peer, que en mucho la mayoría de los casos no requieren altos índices de transmisión de datos, permitiendo comunicación directa a corta distancia entre estos dispositivos.

⁴ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

Dispositivos con bajo índice de consumo de energía, haciendo que la tecnología WPAN sea el uso para una variedad de dispositivos personales que funcionan con batería (ordenador, teléfonos móviles, PDA). Tradicionalmente estos dispositivos personales se interconectaban utilizando cables, entonces es como nació la comunicación inalámbrica para este tipo de redes, suponiendo un gran avance en cuanto a versatilidad, confiabilidad y comodidad.

Bluetooth

Bluetooth describe un método de interconectividad móvil universal, por lo que se ha convertido en la solución inalámbrica ideal para interconectar dispositivos como teléfonos móviles, portátiles para conexión a Internet, asistentes personales digitales que pudieran conectarse al PC para coordinar sus contactos, e incluso para poder imprimir desde un ordenador de forma inalámbrica y muchos otros dispositivos, utilizando una conexión inalámbrica de corto alcance basado en radio frecuencia.

Cada dispositivo está equipado con un chip transmisor / receptor de 1 Mbps en la banda ISM de 2,4 GHz de bajo consumo, aunque la velocidad real permitida gira entorno a los 725 Kbps, con una distancia de operatividad para conexión de dispositivos de hasta 10 m. además no se necesita de soporte para la conectividad de los dispositivos ya que la sincronización automática y sin tener línea de vista entre estos.

Bluetooth puede considerarse como una red inalámbrica de corto alcance muy segura; en cierta medida, es lo que se viene a llamar una PAN (Personal Area Network), de uso particular y restringido a un entorno cercano.⁵

DECT

DECT (Digital Enhanced Cordless Telecommunications), teniendo como objetivo facilitar las comunicaciones inalámbricas entre terminales telefónicos, trabaja en la banda de frecuencias de 1,9 GHz, teniendo en la actualidad una velocidad máxima de 2 Mbps, aunque la idea es que se logre alcanzar velocidades de hasta los 20 Mbps y conseguir alcances de hasta 17 Km.

⁵ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

Infrarrojo

Radiación electromagnética invisible para el ojo humano, estos sistemas de comunicación se basan en la emisión y recepción de haces de luz infrarroja, la totalidad de los mandos a distancia de los aparatos domésticos utilizan comunicación por infrarrojo, como también tenemos los PDA, teléfonos móviles hasta ordenadores.⁶

2.2.1 Grupos de Trabajo

Para compensar las diferentes necesidades de comunicación dentro de un área personal la IEEE ha establecido un grupo de trabajo 802.15 para las WPAN

Cada uno de los cuatro grupos de trabajo en la que se divide la tecnología WPAN, tienen sus características e intereses específicos satisfaciendo necesidades específicas de comunicación y así encargándose del desarrollo de estándares.

IEEE 802.15	
Grupo de Trabajo	Enfoque
802.15.1	Basado en las especificaciones de Bluetooth
802.15.2	Modelo de coexistencia entre las WLAN y WPAN
802.15.3	Estándar nuevo de alta velocidad (20 Mbps o superiores), complementariamente diseñado para consumir poca energía y ofrecer soluciones a bajo costo
802.15.4	Investiga y desarrolla soluciones que requieren una baja transmisión de datos

Tabla 2.3 Grupo de Trabajo 802.15

⁶ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

2.3 Redes Inalámbricas de Área Local

Las redes WLAN (Wireless Local Area Network) se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una tarjeta de red inalámbrica, con o sin antena, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos

La principal ventaja de este tipo de redes WLAN, a nivel regulatorio mundial es que no necesitan licencia para su instalación, ya que las frecuencias de trabajo en las que operan este tipo de redes están en la banda ISM, son frecuencias libres y no requiere licencia para la transmisión de datos, sin embargo el CONATEL (Consejo Nacional de Telecomunicaciones) es el ente de regulación del sector de telecomunicaciones del país, regula la utilización de esta banda a través de permisos de redes privadas, con trámites sencillos, correspondientes a este tipo de redes, lo cual disminuye notablemente el costo final de su implementación, además la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información e todos los lugares por donde puedan estar trabajando. Y se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de los terminales en caso necesario.

El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una interfaz física

Home RF

Con una finalidad muy parecida a Bluetooth, HomeRF pretende la conectividad sin cables dentro del hogar. Al igual que WECA (Wireless Ethernet Compatibility Alliance) o Bluetooth, el HomeRF Working Group, es un grupo de compañías encargadas de asegurar la plena interoperabilidad de los dispositivos fabricados bajo este estándar.

El HomeRF se basa en el protocolo de acceso compartido SWAP (Share Wireless Access Protocol) que define una interface común inalámbrica para soportar tráfico de voz datos, e interoperar con las redes públicas de telefonía e Internet.

Esta especificación permite que los ordenadores, periféricos, teléfonos y electrodomésticos puedan comunicarse con otros dispositivos de similar naturaleza sin utilización de cables.⁷

La instalación de este estándar sin cables dentro del hogar haría posible que los distintos usuarios puedan compartir voz y datos entre ordenadores, periféricos, teléfonos inalámbricos y PDA's, pudiendo tener acceso a cualquiera de estos dispositivos desde cualquier punto y permitiendo, por ejemplo, el desvío automático de llamadas entrantes hacia los diferentes dispositivos según las necesidades de cada miembro de la familia.

HyperLAN

El ETSI (Instituto de Estándares de Telecomunicaciones Europeo), crea durante los años 1991 y 1996 el proyecto HyperLAN, en el cual su objetivo primordial era conseguir una tasa de transferencia mayor que la ofrecida por las especificaciones IEEE 802.11, y que se lo utilizara en configuraciones ad-doc con dispositivos portátiles.

Actualmente, el ETSI dispone de la especificación HyperLAN2, que fue desarrollado dentro del proyecto BRAN (Broadband RadioAccess Networks) de ETSI, que mejoró notablemente las características de sus antecesoras, ofreciendo una mayor velocidad de transmisión en la capa física de 54 Mbps para lo cual emplea el método de modulación OFDM (Orthogonal Frequency Digital Multiplexing), opera en el espectro localizado en la banda 5 GHz y ofrece soporte QoS.

Además este estándar está diseñado para proporcionar comunicaciones multimedia de gran capacidad entre diferentes redes de banda ancha con terminales móviles. Cuenta con dos modos de funcionamiento: Centralizado que es una estructura con puntos de acceso y modo directo que es una estructura de red ad-hoc.

⁷ DIANE TEARE, CATHERINE PAQUET. "Campus Network Design Fundamentals", Indianapolis: Cisco Press, 2006.

Wi-Fi

En el caso de las redes locales inalámbricas, el sistema que se está imponiendo es el normalizado por IEEE con el nombre 802.11 conocido como Wi-Fi (Wireless Fidelity), llegando a velocidades de 54 Mbps en la actualidad en las comunicaciones, y en versiones más recientes hasta 100 Mbps.

Wi-Fi se caracteriza por ser un sistema de envío de datos en las redes computacionales que utilizan ondas de radio en lugar de los cables. Wi-Fi una marca de la Wi-Fi Alliance que anteriormente era denominado WECA (Wireless Ethernet Compatibility Alliance), organización mundial que adopta, prueba y certifica que los equipos cumplan con los estándares 802.11.

Existen varios tipos de Wi-Fi, cada uno de estos basados en el estándar 802.11 aprobado, tendiendo una aceptación internacional debido a que las bandas en que operan se encuentran disponibles casi universalmente.⁸

2.3.1 Grupos de Trabajo

El estándar para WLAN 802.11 fue creado por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), que describe y especifica una interoperabilidad inalámbrica para la comunicación de datos para una velocidad de 2 Mbps, con una modulación de señal de espectro expandido por DSSS (Secuencia directa), aunque también contempla opción de espectro expandido FHSS (Por salto de frecuencia) en la banda de 2.4 GHz.

El estándar WLAN IEEE 802.11 ha sufrido diferentes extensiones para obtener modificaciones y mejoras, de esta manera, tienen las siguientes especificaciones:

⁸ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

IEEE 802.11	
Grupo de Trabajo	Enfoque
802.11a	54 Mbps WLAN en la banda 5 GHz
802.11b	11 Mbps WLAN en la banda 2.4 GHz
802.11c	Cruce sin enlaces
802.11d	Modo mundial. Adaptación a los requerimientos regionales
802.11e	QoS y extensiones que fluyen a través de 802.11a/g/h
802.11f	Tránsito para 802.11a/g/h
802.11g	54 Mbps WLAN en la banda 2,4 GHz
802.11h	802.11 ^a con DFS y TPC. “Europa”
802.11i	Autenticación y encriptado (AES, 802.11x)
802.11j	802.11 ^a con canales adicionales por encima de 4.9 GHz “Japón”
802.11k	Intercambios de información y puntos de acceso
802.11l	No se usa debido al peligro de confusión tipográfica
802.11m	Mantenimiento, publicación de actualizaciones estándar
802.11n	Nueva navegación de WLAN de redes de al menos 100 Mbps

Tabla 2.4 Grupo de Trabajo 802.11

Las redes inalámbricas se reparten en dos clases principales subdivididas por la banda de frecuencias. Las primeras tecnologías utilizaban la banda de 2.4 GHz mientras que las más modernas usaban la de 5 GHz.

- **IEEE 802.11**
Es el primer estándar disponible que describe una interfaz inalámbrica en la banda ISM de 2.4 GHz con velocidad de 2 Mbps, usando FHSS (Salto de Frecuencias) o DSSS (Secuencia directa).
- **IEEE 802.11a**
Extensión del 802.11 que describe una interfaz inalámbrica en la banda ISM de 5 GHz con velocidades de comunicación de datos de 54 Mbps, usando OFDM.
- **IEEE 802.11b**
Extensión del 802.11 que describe una interfaz inalámbrica en la banda ISM de 2.4 GHz con velocidades de comunicación de datos de 11 Mbps, usando DSSS.
- **IEEE 802.11c**
IEEE 802.11c especifica métodos para la comunicación inalámbrica o lo que es lo mismo métodos para conectar diferentes tipos de redes mediante redes inalámbricas
- **IEEE 802.11d**
IEEE 802.11d normalmente se le conoce como el método mundial y se refiere a las diferentes regiones en tecnologías como a cuantos y cuales son los canales disponibles para usarse en las distintas regiones del mundo. Como usuario solo necesitamos especificar el país en el que queremos usar la tarjeta WLAN y el controlador se ocupa del resto
- **IEEE 802.11e**
El protocolo IEEE 802.11e define la calidad de servicio y las extensiones para el flujo de medio para 802.11a/h y g, el objetivo es ajustar las redes de 54 Mbps para aplicaciones multimedia y de voz sobre IP, o lo que es lo mismo, telefonía a través de redes IP e Internet. La red debe soportar valores de transmisión de datos garantizados para servicios individuales o retrasos de propagación mínimos para que sean útiles con multimedia o voz.

- **IEEE 802.11f**

El protocolo 802.11f describe como se tratan los estándares de las comunicaciones de clientes de móviles fuera de zona entre puntos de acceso.

- **IEEE 802.11g**

El protocolo 802.11g es el estándar compatible con 802.11b que describe una interfaz inalámbrica en la banda ISM de 2.4 GHz con velocidades de comunicación de datos de 22 Mbps, incluso a 54 Mbps como el 802.11a. Usa OFDM.

- **IEEE 802.11h**

Por otro lado tanto 802.11h, que opera en la banda de 5 GHz, consiguen un rendimiento nominal de 54 Mbps. 802.11h referido a Estados Unidos como de compatibilidad en Europa, es la variante europea del estándar americano. Sus dos características más importantes son la selección dinámica y la potencia de transmisión variable, obligatorias para cada mercado europeo según el Instituto Europeo de Estándares de comunicación con el fin de asegurar que los sistemas tengan una capacidad de transmisión razonable.

2.3.2 Ubicación de las WLAN dentro de las tecnologías inalámbricas

Estos últimos años la comunicación inalámbrica ha evolucionado notablemente con el uso de teléfonos es solo el inicio de la comunicación inalámbrica, ya que estas continúan apostando a convertir el aire en el mejor medio de transporte de datos

Las redes inalámbricas WLAN, son todo un hecho debido a su utilización en la solución de aplicaciones específicas. Sin embargo estos estándares pecan quizás de ser una solución más bien general y dirigida a entornos de trabajo en grupos y empresas que puedan sacar el máximo partido a sus capacidades. Por esto han surgido otras nuevas tecnologías como Bluetooth o HomeRF entorno al protocolo 802.11b utilizando también el rango de frecuencias de 2.4 GHz especializadas en ofrecer una conectividad inalámbrica enfocada a usos mucho más específicos.

Por si toda esta competitividad no fuera suficiente, la ETSI Instituto de Estándares de Telecomunicaciones Europeo es responsable de haber llevado a cabo durante los años 1991 y 1996 el proyecto HyperLAN que también da soluciones inalámbricas.

Estas soluciones aparentemente pueden parecer similares, sin embargo hay grande diferencias entre ellas, lo que hace que sean complementarias.⁹

2.4 Redes Inalámbricas de Área Metropolitana

Las redes inalámbricas de área metropolitana, WMAN (Wireless Metropolitan Area Network), son las que dentro de un área metropolitana permiten a los usuarios establecer conexiones inalámbricas, tienen una cobertura de unos cientos de metros hasta varios kilómetros lo que permite comunicar varios edificios de oficinas de una ciudad o campus universitarios, si altos costos que suponen las instalaciones de cables de fibra o cobre y el alquiler de líneas. Sobre todo las WMAN, sirven como copias de seguridad para las redes con cable, en caso que las líneas principales alquiladas para las redes con cables no estén disponibles.

WMAN utiliza ondas de radio o luz infrarroja para transmitir datos, protocolos como LMDS (Local Multipoint Distribution Service) servicio local de distribución multipunto, MMDS (Microwave Multipoint Distribution Service), servicio de distribución de canal múltiple o WiMAX (Worldwide Interoperability for Microwave Access) interoperabilidad mundial para accesos d microondas, ofrecen soluciones de este tipo, el grupo de trabajo IEEE 802.16 para los estándares de acceso inalámbrico de banda ancha sigue desarrollando especificaciones para normalizar el desarrollo de estas tecnologías.

Existen dos topologías primordiales: sistemas con comunicación punto a punto a alta velocidad entre dos emplazamientos fijos y sistemas que permiten crear una red punto multipunto, entre emplazamientos fijos.

⁹ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

LMDS

Tecnología inalámbrica vía radio para comunicación entre puntos fijos, por lo que no es una tecnología para ser utilizada por terminales en movimiento. Opera en rangos de frecuencia de 2 y 20 GHz.

LMDS utiliza un transmisor central emitiendo su señal a una distancia de 5 kilómetros, los receptores por lo general se ubican en lugares con línea de vista con el transmisor central.

WiMAX

WiMAX es una organización sin fines de lucro creado por fabricantes de equipos inalámbricos, promoviendo el uso de las tecnologías IEEE 802.16a y ETSI HiperMAN y asegurar su interoperabilidad entre sí, operan en la banda de 2 a 11 GHz con la finalidad de que no necesiten visibilidad directa, sino que al contrario edificios, árboles u obstáculos no limiten grandemente su aplicación.

Una estación base típica de WiMAX tiene un alcance de 50 kilómetros, y puede ofrecer servicio a más de 6 empresas (a 2 Mbps) y cientos de hogares (a 256 Kbps) simultáneamente, WiMAX puede ser una alternativa a xDSL, por lo que incluso se le conoce como WDSL (Wireless DSL), por lo que actualmente se está trabajando a velocidades de hasta 72 Mbps, en un futuro se espera poder aumentar esta velocidad.

2.5 Redes Inalámbricas Globales

Los sistemas inalámbricos de cobertura global que existen son los sistemas de telefonía celular. Las tecnologías WWAN (Wireless Wide Area Network) actuales se conocen como sistemas de segunda generación 2G, entre los principales encontramos a los sistemas GSM (Global System for Mobile Communications) sistema global para comunicaciones móviles, CDPD (Cellular Digital Packet Data) y CDMA (Code Division Multiple Access) acceso múltiple por división de código. Algunos de estos sistemas tienen capacidades limitadas de movilidad y son incompatibles entre sí, a

tecnologías de tercera generación 3G, que seguirán un estándar global y proporcionarían capacidades de movilidad internacional.

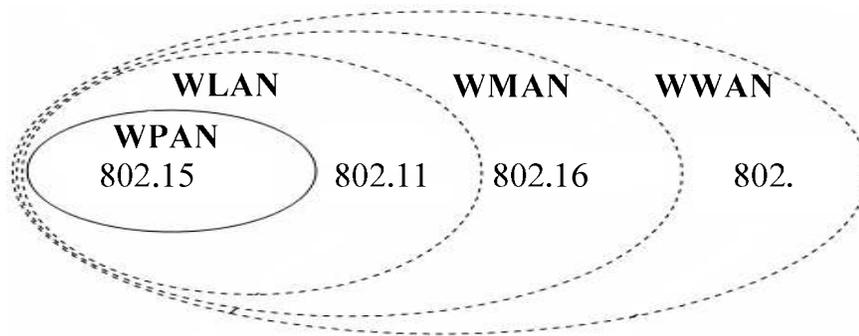


Figura 2.3 Posicionamiento Estándares Wireless

GSM

GSM es una tecnología estandarizada por el CEPT (Conference of European Post and Telecommunications), en la actualidad es el sistema 2G más extendido, es un sistema que puede transmitir datos a 13 Kbps sin necesidad de utilizar un módem, para conectar un teléfono móvil solo hace falta conectar un cable y un software apropiado.

CDMA

CDMA es una tecnología desarrollada por la empresa Qualcomm, esta tecnología se caracteriza por la nueva forma de establecer comunicación inalámbrica multiusuario con un aprovechamiento de la capacidad seis veces mejor que TDMA.

3G

La tercera generación afronta el objetivo de conseguir un sistema global común, por lo que las tres regiones importantes desde el punto de vista del desarrollo tecnológico (Europa, Norteamérica y Asia) tomaron caminos distintos.

Esto comenzó cuando la UIT (Unión Internacional de Telecomunicaciones), anunció su iniciativa de crear un nuevo sistema de comunicaciones móviles al que llamó FPLMTS (Future Public Land Mobile Telecommunications System) que luego pasaría a llamarse IMT2000 (International Mobile Communications) el objetivo de estas era definir un marco dentro d la cual puedan coexistir distintas tecnologías 3G, la visión de disponer

un sistema universal de comunicaciones hizo que los grupos de intereses llegaran a un acuerdo de tecnología única conocida como WCDMA (Wideband CDMA), donde se desarrollan tres modos opcionales bajo esta tecnología:

- **UMTS**

UMTS (Universal Mobile Telecommunications System), estándar europeo como evolución de la arquitectura GSM, ofreciendo servicios de voz, fax, mensajes multimedia y servicios de datos de hasta 2 Mbps.

- **CDMA 2000**

Evolución del estándar americano, es una de las primeras tecnologías 3G que se apareció en el mercado, permitiendo transmitir datos hasta 300 Kbps.

- **TD SCDMA**

TD SCDMA (Time Division Synchronous Code Division Multiple Access), combinación de técnicas TDMA y CDMA, permitiendo interoperar con las redes 2G

2.6 Ondas electromagnéticas

Las OEM (Ondas Electromagnéticas), son ondas o rayos de energía generados por fuentes naturales o artificiales, que se propagan esféricamente en todas las direcciones a través del medio, por lo tanto es el nombre que se le dio a todos los tipos de radiación. Todas las ondas electromagnéticas viajan a la velocidad de la luz y tienen una longitud de onda y una frecuencia.

Fórmula:

$$c = \lambda \times f$$

Donde:

$$c = 3 \times 10^8 \text{ m/s}$$

$$\lambda = \text{longitud de onda (m)}$$

$$f = \text{frecuencia (Hz)}$$

La fórmula nos dice que la longitud de la onda de cualquier onda electromagnética en metros multiplicado por la frecuencia de esa misma onda electromagnética en hercios, va hacer siempre igual a al velocidad de la luz 300.000 Km por segundo, cuando viaja en el vacío. Las ondas electromagnéticas exteriorizan las siguientes propiedades: reflexión, refracción, difracción y dispersión.

Las ondas electromagnéticas comprenden un amplio rango de frecuencias (y correspondientemente, de longitudes de onda). Este rango de frecuencias y longitudes de onda es nombrado espectro electromagnético.

La parte del espectro más conocido a los seres humanos es probablemente la luz, la porción visible del espectro electromagnético. La luz se sitúa aproximadamente entre las frecuencias de $7,5 \cdot 10^{14}$ Hz y $3,8 \cdot 10^{14}$ Hz, correspondientes a longitudes de onda desde cerca de 400 nm a 800 nm.

También estamos expuestos a otras zonas del espectro electromagnético, incluyendo los campos de la red de distribución eléctrica *CA (Corriente Alterna)*, Rayos-X, Ultravioleta (en las frecuencias más altas de la luz visible), Infrarrojo (en las frecuencias más bajas de la luz visible) y muchas otras. Radio es el término utilizado para la porción del espectro electromagnético en la cual las ondas pueden ser transmitidas aplicando corriente alterna a una antena. Esto abarca el rango de 3 Hz a 300 GHz, pero normalmente el término se reserva para las frecuencias inferiores a 1 GHz.

Cuando se habla de radio, la totalidad de la gente piensa en la radio FM, que usa una frecuencia de alrededor de 100 MHz. Entre la radio y el infrarrojo encontramos la región de las microondas con frecuencias de 1 GHz a 300 GHz, y longitudes de onda de 30 cm a 1 mm.

En el siguiente gráfico resume los rangos de frecuencias del espectro electromagnético.

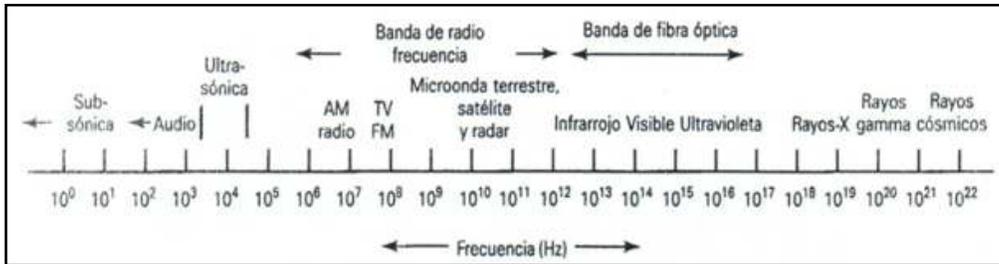


Figura 2.4 Espectro Electromagnético

2.6.1 Espectro Radioeléctrico

Es un recurso natural del Estado y constituye el elemento básico para el funcionamiento de los sistemas de radiocomunicaciones. Conjunto de ondas cuya frecuencia se fija convencionalmente por debajo de 3000 GHz y que se propagan por el espacio sin guía artificial.

La constitución de la UIT establece que los estados miembros tendrán en cuenta que las frecuencias y las órbitas asociadas, incluida la de los satélites geoestacionarios, son recursos naturales limitados que deben utilizarse de forma racional, eficaz y

Las entidades de regulación de cada estado son los encargados de ejercer la soberanía que a este corresponde sobre el espectro radioeléctrico, elaborando y estableciendo la política de su utilización, ejecutando su planificación, reglamentación, administración y control.

Asimismo le corresponde velar que el uso del espectro radioeléctrico se realice en beneficio de la nación, coadyuve al desarrollo económico y social sostenible y proporcione bienestar y seguridad a la población, asegurando en particular la obtención de los siguientes objetivos.

En la siguiente tabla se van a listar las distintas bandas de radiofrecuencia, junto con el nombre de las ondas transmitidas en cada banda:

ESPECTRO RADIOELÉCTRICO				
Margen de Frecuencias	Bandas de Frecuencias			Tipo Propagación
3 - 30 KHz	Frecuencia muy baja	Miriamétricas	Onda Larga	Terrestre
	VLF (Very Low Frequency)			
30 - 300 KHz	Frecuencia baja	Kilométricas	Onda Media	
	LF (Low Frequency)			
300 - 3000 KHz	Frecuencia media	Hectométricas	Onda Corta	
	MF (Medium Frequency)			
3 - 30 MHz	Frecuencia alta	Decamétricas	Espacial	
	HF (Hight Frequency)			
30 - 300 MHz	Frecuencia muy alta	Métricas	Espacial	
	VHF (Very Hight Frequency)			
300 - 3000 MHz	Frecuencia ultra elevada	Decimétricas	Espacial	
	UHF (Ultra Hight Frequency)			
3 - 30 GHz	Frecuencia superelevada	Centimétricas	Espacial	
	SHF (Super Hight Frequency)			
30 - 300 GHz	Frecuencia extremadamente alta	Milimétricas	Espacial	
	EHF (Extra Hight Frequency)			

Tabla 2.5 Espectro Radioeléctrico

2.6.2 El Uso del Espacio, del Tiempo y del Espectro en Redes de RF

El método de acceso, tal como la modulación de radio y el ancho de banda disponible, es importante para determinar la eficiencia y la capacidad de un sistema de radio. Uno de los aspectos más importantes de la eficiencia del tiempo es la asignación de frecuencia consolidada y el tráfico de cargas de usuarios no relacionados entre si.

Independientemente del rango, un conjunto de enlaces puede únicamente dar servicio a una fracción del área total. Para una cobertura total del área, se debe de usar canales independientes, derivados por frecuencia, código o tiempo. No es fácil minimizar el número de canales independientes o conjunto de enlaces para una cobertura total.¹⁰

Para el diseño de una red inalámbrica, los siguientes factores son importantes:

- Es necesaria una relación señal-interferencia, para una comunicación correcta.
- Se requiere de un margen expresado en estadísticas para generar esta relación, aún en niveles de señal variables
- La posición de las antenas que realizan la transmisión. La cual puede ser limitada por las estaciones y perfectamente controlada por puntos de acceso fijos.
- La función de la distancia para el nivel de la señal. Esta dada por el valor promedio de la señal, considerando las diferencias en la altura de la antena de las terminales y los impedimentos naturales en la trayectoria.

2.6.3 Comportamiento de RF

El comportamiento para las Redes Inalámbricas de Radio Frecuencia, la FCC (Comisión Federal de Comunicaciones) ha permitido la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia: 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Para disminuir la interferencia, las regulaciones de FCC estipulan que una técnica de señal de transmisión llamada spread spectrum

¹⁰ JESÚS GARCÍA TOMÁS, “Alta velocidad y calidad de servicios en redes IP”, Alfaomega, 2006.

modulation, la cual tiene potencia de transmisión máxima de 1 Watt deberá ser utilizada en la banda ISM (Bandas industriales, científica y médicas). Esta técnica ha sido utilizada en aplicaciones militares. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. Así, la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía abajo del nivel de ruido ambiental de tal manera que la señal no sea detectable.

2.7 Propagación de la onda

En ciertas ocasiones es imposible interconectar dos puntos de red por medio físico, razón por la que es necesario utilizar el espacio libre (atmósfera de la tierra) como medio de transmisión, la propagación en el espacio libre de las OEM (Ondas electromagnéticas) se llama RF (Propagación de la radiofrecuencia o Propagación de Radio), propagándose en línea recta en varias direcciones al mismo tiempo. En el vacío, las ondas de radio se propagan 3,8 m/s.¹¹

Y en cualquier otro medio, la señal se vuelve más débil debido a la:

- Reflexión
- Refracción
- Difracción
- Absorción

2.7.1 Refracción

Es el cambio de dirección de un rayo conforme pasa oblicuamente de un medio a otro, con diferentes velocidades de propagación, la velocidad de propagación de las OEM es inversamente proporcional a la densidad del medio, y ocurre siempre que se pasa de un medio a otro de diferente densidad.

¹¹ JESÚS GARCÍA TOMÁS, “Alta velocidad y calidad de servicios en redes IP”, Alfaomega, 2006.

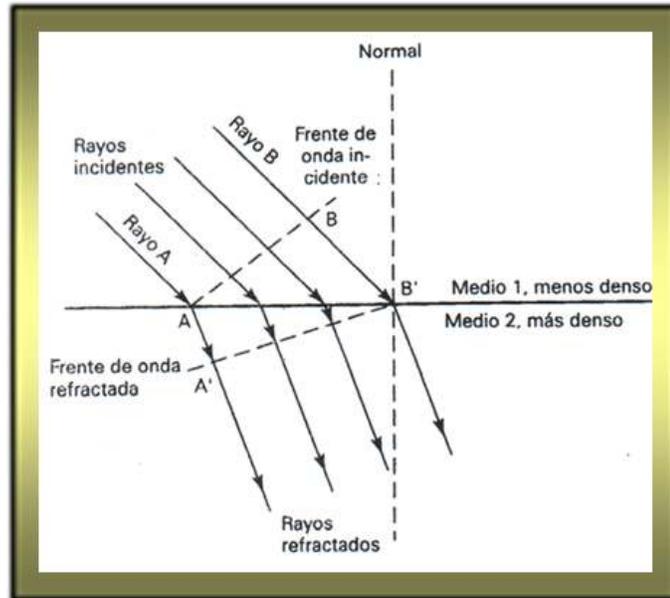


Figura 2.5 Refracción

En la refracción se toma muy en cuenta los siguientes parámetros:

- Ángulo de incidencia: ángulo entre la onda incidente y la normal.
- Ángulo de refracción: ángulo entre la onda refractada y la normal.
- El ángulo de refracción depende del índice de refracción de los dos materiales.
- Índice de refracción: Es la relación de la velocidad de propagación de un rayo de luz en el espacio libre a la velocidad de propagación de la luz en un material dado, y está dada por la siguiente fórmula.

Fórmula:

$$\eta = \frac{c}{v}$$

- Donde:

η = índice de refracción

c = velocidad de la luz en el espacio libre (3×10^8 m/s)

v = velocidad de la luz en un material dado

La refracción también ocurre cuando un frente de onda se propaga en un medio que tiene un gradiente de densidad que es perpendicular a la dirección de propagación.

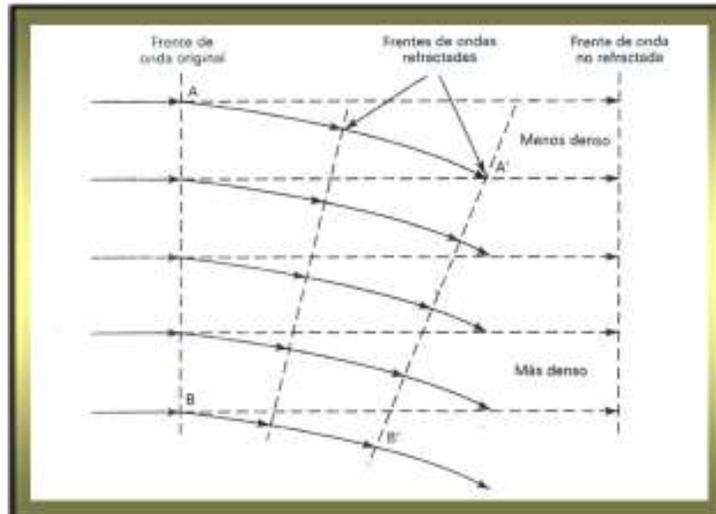


Figura 2.6 Representación de la Refracción con la Densidad

2.7.2 Reflexión

Ocurre cuando una onda incidente choca con una barrera de dos medios y algo (o todo) de la potencia incidente no entra en el segundo material, debido a que se conserva el medio de propagación, el ángulo de reflexión es igual al ángulo de incidencia. Sin embargo, la intensidad de campo de voltaje reflejado es igual o menor que la intensidad de campo de voltaje incidente.

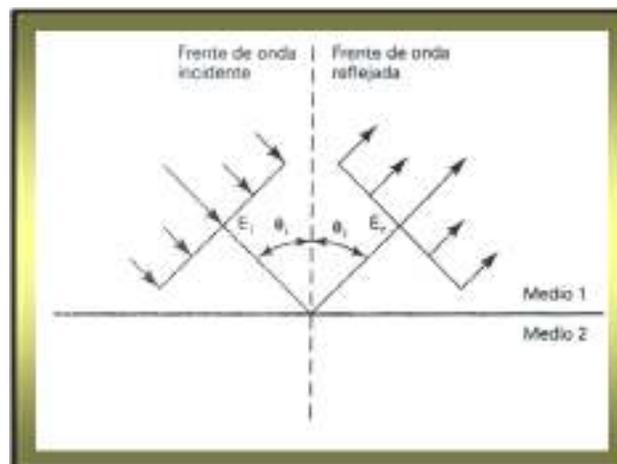


Figura 2.7 Reflexión

Tenemos los siguientes tipos de reflexión:

- **Reflexión Difusa**

Se produce ante la presencia de una superficie irregular que provoca que el frente de onda incidente se refleje en varias direcciones de una forma aleatoria.

- **Reflexión Especular**

Reflexión sobre una superficie perfectamente lisa.

- **Superficie Semiáspera**

Intermedia entre irregular y lisa, este tipo de superficie provoca los dos tipos de reflexión.

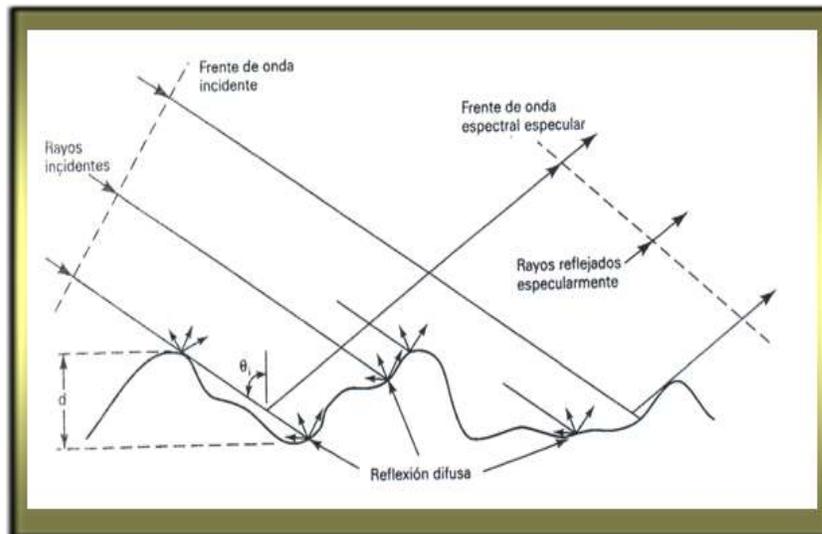


Figura 2.8 Representación de la Reflexión

2.7.3 Difracción

Es la redistribución de energía de un frente de onda cuando pasa cerca del extremo de un objeto opaco, este fenómeno permite que las OEM se propaguen a la vuelta de las esquinas. Para explicar este fenómeno se utiliza el principio de Huygens.

- **Principio De Huygens**

Indica que cada punto de un frente de onda esférica determinado se puede considerar como una fuente secundaria de puntos de OEM, desde donde se irradian hacia fuera otras ondas secundarias

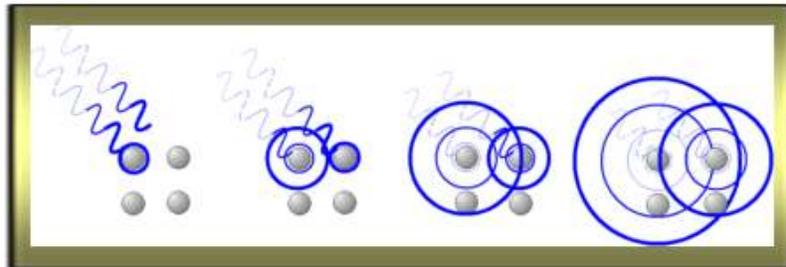


Figura 2.9 Principio De Huygens

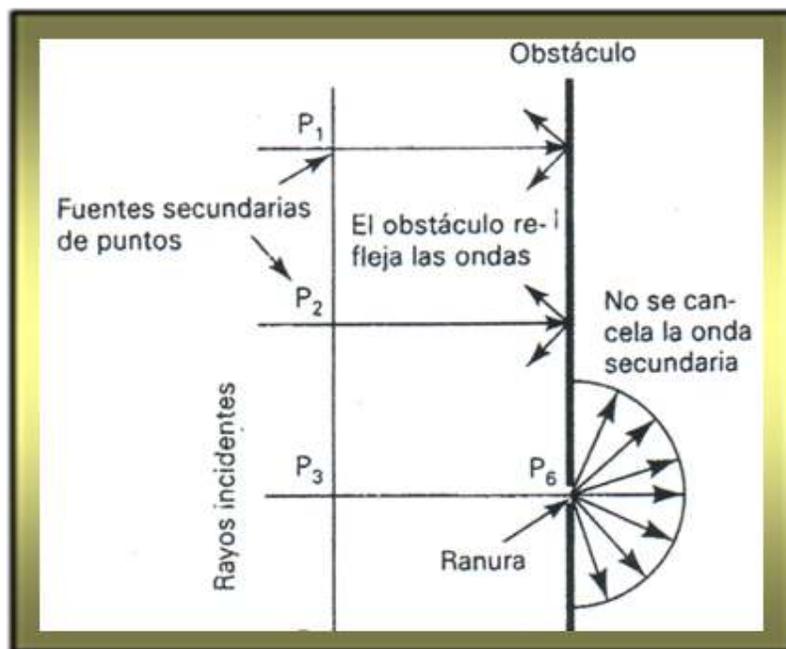


Figura 2.10 Representación de la Difracción

2.7.4 Absorción

Es la pérdida de densidad de potencia cuando una onda se propaga en el espacio no libre, transfiriéndose la energía a los átomos y moléculas que conforman la atmósfera.

La absorción de RF depende de la frecuencia de la onda, siendo relativamente insignificante debajo de los 10 GHz, la absorción de las ondas no depende de la distancia de la fuente sino de la distancia que recorre la onda, en condiciones de lluvia o neblina la absorción es mayor.

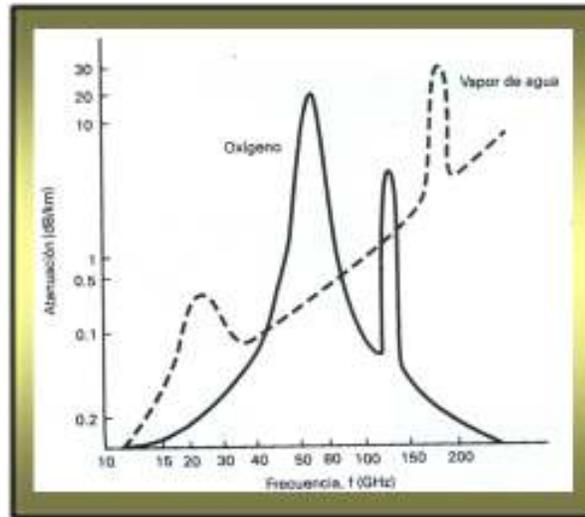


Figura 2.11 Absorción Atmosférica

2.8 Técnicas de modulación

Según la American National Standard for Telecommunications, la modulación es el proceso de variar una o todas las características de una señal portadora, con la finalidad de alcanzar largas distancias, por ejemplo utilizando una señal de alta frecuencia.

2.8.1 Técnicas de modulación Básica

Las tres características que se tiene en una onda portadora básica y que pueden ser modificadas son:

- Amplitud
- Frecuencia
- Fase

Los métodos de modulación básicos son:

- Modulación de la amplitud (ASK)
- Modulación de la frecuencia (FSK)
- Modulación de la fase (PSK)

La mayoría de los sistemas de comunicación utilizan una de las técnicas anteriormente mencionadas, las siguientes son algunos casos extremos de estas técnicas:

- ASK (Amplitude Shift Keying), codificación por desplazamiento de amplitud, desactiva la amplitud durante toda la trayectoria, requiriendo un medio en la que la respuesta de amplitud sea estable, por lo que este tipo de modulación es bastante perceptivo a ruidos y distorciones
- FSK (Frequency Shift Keying), codificación de desplazamiento de frecuencia, salta a una frecuencia extrema, es usado normalmente para transmisiones de datos en bajas velocidades
- PSK (Phase Shift Keying), desplaza la fase 180 grados

2.8.2 Técnicas de Modulación WLAN

Los estándares 802.11 soportan varias técnicas de modulación, en función de la velocidad de datos utilizable:

- BPSK (Binary Phase Shift Keying), codificación de desplazamiento de fase binaria, utilizando una fase para representar un 1 binario y otra para representar un 0 binario, para un total de un 1 bit de datos binarios, se utiliza para transmitir datos a 1 Mbps en 802.11b mientras que hasta unos 6 Mbps en 802.11a, codificando 125 Kbps por canal
- QPSK (Quadrature Phase Shift Keying), codificación por desplazamiento de fase en cuadratura, la portadora sufre cuatro cambios en la fase, representando 2 bits binarios de datos, se utiliza para transmitir datos a 2 Mbps en 802.11b mientras que hasta unos 12 Mbps en 802.11a, codificando 250 Kbps por canal
- CCK (Complementary Code Keying), codificación complementaria de código, utilizando un conjunto de funciones complejas, conocido como códigos

complementarios, para enviar datos, se utiliza para transmitir datos a 5,5 y 11 Mbps en 802.11b

- 16QAM (16 level Quadrature Amplitude Modulation), codifica 4 bits por hercio, se utiliza para transmitir datos a 24 Mbps en 802.11a
- 64QAM (64 level Quadrature Amplitude Modulation), codifica 8 ó 10 bits por ciclo, se utiliza para transmitir datos a 54 Mbps en 802.11a

802.11g utiliza las mismas técnicas de modulación que 802.11a, y soporta la modulación CCK, por tal razón 802.11g soporta clientes de 54 Kbps siendo compatible con clientes 802.11a.¹²

2.9 Técnicas de transmisión WLAN

Los estándares 802.11 especifican varias técnicas de transmisión, dependiendo de la tecnología. El 802.11a y el 802.11g utilizan OFDM y 802.11b utiliza FHSS o DSSS, cada una de estas técnicas se construye a partir de las técnicas de modulación explicadas anteriormente.

2.9.1 Spread Spectrum

El principio de funcionamiento del Espectro Ensanchado consiste en multiplicar la fuente digital de información por un código de mayor velocidad binaria que la fuente.

En principio la multiplicación por un código aumenta artificialmente el ancho de banda, disminuyendo la eficiencia espectral del sistema. Sin embargo el SS (Spread Spectrum) permite la coexistencia de múltiples transmisiones en la misma frecuencia y al mismo tiempo. Mediante el uso de códigos diferentes para cada transmisión, éstas no se interfieren significativamente entre ellas.

¹² DIANE TEARE, CATHERINE PAQUET. “Campus Network Design Fundamentals”, Indianapolis: Cisco Press, 2006.

No se puede decir que las comunicaciones mediante espectro ensanchado son medios eficientes de utilización del ancho de banda. Sin embargo rinden al máximo cuando se los combina con sistemas existentes que hacen uso de la frecuencia

Existen dos tipos de radio spread spectrum:

- DSSS (Secuencia directa)
- FHSS (Salto de Frecuencia)

2.9.1.1 DSSS

DSSS (Direct Sequency Spread Spectrum), en este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada

2.9.1.2 FHSS

FHSS (Frequency Hopping Spread Spectrum), este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, con saltos de ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 MHz que son utilizadas por hornos de Microondas.¹³

¹³ DIANE TEARE, CATHERINE PAQUET. "Campus Network Design Fundamentals", Indianapolis: Cisco Press, 2006.

2.9.1.3 Ventajas y Desventajas de Spread Spectrum

El espectro ensanchado tiene muchas propiedades únicas y diferentes que no se pueden encontrar en ninguna otra técnica de modulación. Para verlo mejor, se listan debajo algunas ventajas y desventajas que existen en los sistemas típicos del espectro ensanchado

Ventajas

- Resiste todo tipo de interferencias, tanto las no intencionadas como las malintencionadas, siendo más efectivo con las de banda estrecha
- Se puede compartir la misma banda de frecuencia con otros usuarios

Desventajas

- Ineficiencia del ancho de banda
- La implementación de los circuitos es en algunos casos muy compleja

2.9.2 OFDM

La modulación por división ortogonal de frecuencia, en inglés OFDM (Orthogonal Frequency Division Multiplexing), también llamada modulación por multitono discreto, en inglés DMT (Discreet Multitone Modulation), es una modulación que consiste en enviar la información modulando en QAM o en PSK un conjunto de portadoras de diferente frecuencia

Normalmente se realiza la modulación OFDM tras pasar la señal por un codificador de canal con el objetivo de corregir los errores producidos en la transmisión, entonces esta modulación se denomina COFDM (Coded OFDM).¹⁴

¹⁴ DIANE TEARE, CATHERINE PAQUET. "Campus Network Design Fundamentals", Indianapolis: Cisco Press, 2006.

2.9.2.1 Características de la modulación OFDM

La modulación OFDM es muy robusta frente al multitrayecto, que es muy habitual en los canales de radiodifusión, frente al desvanecimiento debido a las condiciones meteorológicas y frente a las interferencias de RF. Debido a las características de esta modulación, las distintas señales con distintos retardos y amplitudes que llegan al receptor contribuyen positivamente a la recepción, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia

Entre los sistemas que usan la modulación OFDM destacan:

- La televisión digital terrestre
- Wireless LAN
- El sistema de transmisión inalámbrica de datos Wi-MAX

2.10 Cómo funciona Wi-Fi

Las redes Wi-Fi, pueden estar formadas por dos ordenadores o miles de ellos, para que uno de estos equipos susceptibles de formar parte de la red pueda comunicarse de forma inalámbrica necesita la instalación de un adaptador de red (con transmisor, receptor y antena), conocido como equipo terminal de red.

Complementariamente a los adaptadores de red, las redes Wi-Fi pueden disponer de infraestructura AP (Access Point), puntos de acceso que son estaciones base utilizados para gestionar las comunicaciones entre los distintos terminales, por lo que se les conoce con el nombre general de estación.

Las estaciones se comunican entre sí, por lo que utilizan la misma banda de frecuencia, por lo que tienen instalados el mismo conjunto de protocolos, por lo que el estándar IEEE 802 sólo define las dos primeras capas, el resto de capas son idénticas a las utilizadas en las redes locales cableadas.

Relación Modelo OSI			
Modelo OSI			Protocolos
7	Aplicación	IP	HTTP, FTP, SMTP
6	Presentación		DNS, LDAP
5	Sesión		UDP, TCP
4	Transporte		ICMP, RSVP
3	Red		LLC, MAC
2	Enlace	IEEE 802	Físico
1	Físico		

Tabla 2.6 Relación de los protocolos de red local

2.10.1 Modelo OSI para redes inalámbricas

Se debe asignar una importancia esencial al concepto de que el equipo WLAN actual sea considerado como elementos de red y no simplemente radios. De acuerdo con esto, es adecuado revisar el radio tanto en la capa 1 o elemento de capa física y por lo menos uno de los dos subconjuntos de la capa 2, conocido como el control de acceso al medio o capa MAC

A modo de recordatorio, OSI por sus siglas que significan “sistemas abiertos de interconexión” y su modelo de referencia es un modelo de arquitectura de red que se acepta en todo el mundo. Este modelo esta formado por siete capas, cada una de las cuales sirve para funciones de red particulares como:

- Direccionamiento
- Control de flujo
- Control de errores
- Cifrado
- Transferencia confiable

La capa más baja, capa 1 es la que más cerca de la tecnología de medios que en este caso sería el radio. Las dos capas OSI inferiores (Capa 1 y Capa 2) están implementadas en el hardware y software, mientras que las 5 capas superiores solo se implementan en el software. La capa más alta (Capa de aplicación) es la más cercana al usuario. El modelo de referencia OSI se usa universalmente como un método para enseñar y entender el funcionamiento de las redes.

2.10.2 Capas IEEE802

La norma IEEE 802, se relaciona con las dos primeras capas del sistema OSI, como habíamos mencionado anteriormente: la capa física y la del enlace y a esta última se la divide en dos por lo que el resultado son 3 capas:

- **PHY**
PHY (Physical Layer), la capa física es la que encarga de definir los métodos por los que se divide la señal
- **MAC**
MAC (Medium Access Control), la capa control acceso al medio, es la que se encarga del control de acceso al medio físico, en el caso de Wi-Fi el medio físico es el espectro radioeléctrico.
- **LLC**
LLC (Logical Link Control) es la capa que se encarga del control del enlace lógico, definiendo como pueden acceder múltiples usuarios a la capa MAC.

2.10.3 Capa Física

La capa física de las redes 802.11a permite la transmisión a 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Los datos son transmitidos por 52 subportadoras que se modulan utilizando BPSK (6 y 9 Mbps), QPSK (12 y 18 Mbps), 16-QAM (24 y 36 Mbps) o 64-QAM (48 y

54 Mbps). El propósito de las 5 subportadoras es aumentar la calidad de la señal recibida.

El estándar 802.11 permite las tres variantes de la capa física; espectro extendido de secuencia directa DSSS, espectro extendido de saltos de frecuencia FHSS y la transmisión por rayos infrarrojos. Debido a que el estándar 802.11b actual soportan distintas velocidades de datos y tanto FHSS como DSSS soportan velocidades desde 1 a 2 Mbps

Por lo tanto, como principio práctico casi todos los dominios de colisión no usan más de tres puntos de acceso debido a que solo están disponibles tres canales que no se traslapan, y obtener la cantidad máxima del espectro para una transmisión específica permite las velocidades más altas además de un enlace más sólido

La cantidad de puntos de acceso no se debe confundir con el número de clientes que se pueden agregar, debido a que un solo punto de acceso puede dar servicio a 2000 clientes aproximadamente, aunque no al mismo tiempo puesto que pasaría mucho tiempo antes de que el ancho de banda estuviera disponible.

Normalmente los puntos de acceso con el mejor desempeño como por ejemplo los que fabrica Cisco, pueden dar servicio hasta 256 clientes al mismo tiempo por punto de acceso, aunque esto no sería favorable en términos de capacidad de acceso y desempeño.

Más aún, debido a las limitaciones de rango de los dispositivos, la cantidad de área física que normalmente se requiere para 20000 usuarios incapacitaría las asociaciones entre puntos de acceso y clientes.

La parte más importante que se debe subrayar aquí es que normalmente no se deben colocar más de tres puntos de acceso en un solo dominio de colisión, debido a que un despliegue nominal los colocaría en los canales 1, 6 y 11 respectivamente.¹⁵

¹⁵ DIANE TEARE, CATHERINE PAQUET. "Campus Network Design Fundamentals", Indianapolis: Cisco Press, 2006.

2.10.3.1 Elementos de la Capa física

La capa física tiene dos subcapas, las cuales son el protocolo de convergencia de la capa física PLCP (Physical Layer Convergence Procedure) procedimiento de convergencia de la capa física y la subcapa dependiente del medio físico PMD (Physical Medium Dependent) dependiente del medio físico. La diferencia entre las dos es que la capa PLCP se encarga de aspectos como la codificación Barres y CCK, además de la técnicas de modulación como QPSK y la técnica de propagación DSSS, mientras que la capa PMD crea la interfaz hacia la capa MAC para sensibilidad de portadora a través de su comprobación de canal libre CCA (Clear Channel Assessment).

El PLCP consiste de un preámbulo de 144 bits que se usa para sincronizar los Access point con los clientes, determinar la ganancia del radio y establecer la CCA. Este preámbulo está formado de 128 bits para la sincronización, seguido de un campo de 16 bits que consiste del patrón 1111001110100000. Esta secuencia se usa para marcar el inicio de una trama y se conoce como el delimitador de inicio de trama SFD. Los siguientes 48 bits se conocen en conjunto como el encabezado PLCP, el cual cuenta con tres campos: señal, servicio y longitud; además de revisión de errores en el encabezado HEC (Header Error Control), lo que asegura la integridad del encabezado y el preámbulo.

El campo de señal indica la velocidad a la que será transmitida la carga, la cual para 802.11b 1, 2, 5.5 u 11 Mbps. 802.11g y 11a también cuentan con velocidades de hasta 54 Mbps. El campo de servicio está reservado para un uso futuro. El campo de longitud indica el tamaño de la carga e incluye los 16 bits de HEC que se efectúa mediante una revisión de redundancia cíclica CRC (Cyclic Redundancy Check).

El PLCP siempre se transmite a 1 Mbps debido a que la confiabilidad y solidez de la señal son muy importantes y tienen prioridades sobre la velocidad. Sin embargo, este encabezado no impacta la velocidad general de un enlace, debido a que 24 bits de cada paquete se envían a 1 Mbps. Como se nota aún en este punto no se asignado un destino para la trama. Debido a que la carga del encabezado de 192 bits se trasmite a 1 Mbps, 802.11 tienen cuando mucho solo 85% de eficiencia en la capa física. No obstante que las partes internas del radio.

2.10.4 MAC

Los diferentes métodos de acceso de IEEE 802 están diseñados según el modelo OSI y se encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC.

Además, la capa de gestión MAC controlará aspectos como sincronización y los algoritmos que precisa o propone el modo infraestructura. Por último, veremos el aspecto y los tipos de tramas MAC.

Sensor de Portadora

La búsqueda de portadora se refiere a la frecuencia real o energía de radio que es transmitida por un radio 802.11 y que se recibe y reconoce como nativa del dominio de colisión. Hay que recordar que la información reside dentro de la onda portadora (el estándar 802.11, 11b, 11a, 11g realizan la tarea del sensor de portadora con prevención de colisiones (CSMA/CA) para asegurar que la cantidad de colisiones dentro de un dominio se mantenga a un nivel mínimo.

Protocolo de acceso al medio CSMA/CA y MACA

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA (Carrier Sense Multiple Acces / Collision Avoidanc). Este algoritmo funciona tal y como describimos a continuación:

1. Antes de transmitir información una estación debe testear el medio, canal inalámbrico, para determinar su estado (libre / ocupado).
2. Si el medio no está ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada espaciado entre tramas IFS.
3. Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
4. Una vez finalizada esta espera debida a la ocupación del medio la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera

adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5. Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición (Tiempo IFS es el tiempo de intervalo entre tramas).

2.10.4.1 Funciones principales de la Capa MAC

Exploración

Existen dos tipos activa y pasiva. En este contexto “exploración” se refiere a los clientes, por ejemplo, tarjetas PCMCIA y dispositivos parecidos que buscan puntos de acceso y puentes para grupos de trabajo. La exploración pasiva es obligatoria dentro del protocolo 802.11 y se realiza cuando los clientes exploran cada uno de los canales disponibles. Esta exploración se efectúa con el fin de encontrar una señal óptima. La exploración pasiva es importante debido a que todas las instalaciones 802.11 tienen canales traslapados para la cobertura de un área, con el fin de asegurar los niveles de desempeño más alto y una cobertura omnipresente (en todas las direcciones)

La exploración activa es un protocolo opcional y en esencia efectúa el mismo proceso que una exploración pasiva, la única diferencia es que el cliente envía una trama de prueba. La diferencia entre activa y pasiva es que cuando un cliente explora de manera activa no espera las señales radioeléctricas programadas regularmente que envían los puntos de acceso

Autenticación

La autenticación es el proceso mediante el cual los clientes previamente aprobados pueden integrarse a un dominio de colisión. La autenticación ocurre antes de la asociación, debido a que es durante el proceso de asociación en el que las direcciones del protocolo de Internet (IP) son reveladas por el punto de acceso y asignadas al cliente. La retención de esta información es muy importante para prevenir la falsificación de direcciones, un término de seguridad que se refiere a la emulación de un cliente o punto de acceso autorizado en la WLAN. Existen dos tipos de autenticación:

- **Autenticación de sistema abierto**

Obligatoria dentro de la especificación 802.11. Se realiza cuando el cliente envía una solicitud con SSID (Service Set Identifier es una contraseña asignada y distribuida por el administrador de la red, que los puntos de acceso reconocerán después de recibirlas desde los clientes) a un punto de acceso, el cual a su vez responde con la autorización o desaprobación de la autenticación.

- **Autenticación de clave compartida**

El fundamento del protocolo WEP (Wired Equivalent Privacy), que se reconoce como un protocolo de seguridad ineficaz para cualquier tipo de WLAN, pero en particular en aquellas que se usan en las redes de empresas pequeñas y medianas, en comparación con las WLAN que se usan en compañías, empresas colegios, y campus universitarios.

Asociación

Después de que se ha realizado el proceso de autenticación, la tarjeta del cliente inicia una asociación cuando envía una trama de solicitud de asociación que contiene un SSID y las velocidades de datos soportadas. El punto de acceso responde mediante una trama de respuesta de asociación que contiene un identificador de asociación junto con otra información relacionada con el punto de acceso específico, por ejemplo una dirección IP.

Modo de ahorro de energía

La capa MAC proporciona la opción de reducir el uso de energía, lo que puede ser importante donde los usuarios tienen clientes, por ejemplo: tarjetas PCMCIA en

computadores portátiles o PDA. Cuando está activado el modo de ahorro de energía, el cliente envió un mensaje al punto de acceso indicando que se irá a dormir, lo que se realiza por medio del bit de estado localizado en el encabezado de cada trama que se envía desde el cliente. Al recibir la solicitud de ir a dormir enseguida el punto de acceso coloca en el búfer los paquetes correspondientes al cliente.

Fragmentación

Es el contexto del protocolo 802.11 y se refiere a la capacidad de un punto de acceso para dividir paquetes en tramas más pequeñas. Con frecuencia esto se hace de modo que la interferencia RF solo elimina a los paquetes más pequeños. Hay que recordar que un dispositivo receptor debe enviar un paquete ACK al dispositivo transmisor para conformar que ha recibido un paquete en forma exitosa. Tiene sentido que algunos paquetes tendrán que ser retransmitidos

En estos casos, mientras más pequeña sea la retransmisión, será mejor el desempeño general dentro de un dominio de colisión, debido a que los otros clientes no tendrán que esperar hasta que la retransmisión se haya completado

Además de evitar las colisiones y las pérdidas de señal, la capa MAC es responsable de identificar las direcciones fuente y de destino del paquete que se envía, además del CRC. Cada nodo en una red inalámbrica es identificado mediante su dirección MAC y usa un esquema de direccionamiento que es idéntico al de Ethernet, el cual es un valor de 6 bytes-48 bits.

Capa de Transporte

El Protocolo Inalámbrico de Datagramas WDP proporciona un servicio fiable a los protocolos de las capas superiores de WAP y permite que la comunicación de forma transparente sobre los protocolos portadores válidos.

Debido a que este protocolo proporciona un interfaz común a los protocolos de las capas superiores, las capas de seguridad, sesión y aplicación pueden trabajar independientemente de la red inalámbrica que dé soporte al sistema.

Este protocolo ofrece servicios de transmisión a los protocolos superiores realizando las funciones de:

- Número de puerto.
- Segmentación y re ensamblado.
- Detección de errores.
- Permite a las aplicaciones de usuario funcionar de forma transparente sobre distintos servicios portadores disponibles.

2.11 Estructura Wi-Fi

2.11.1 Distintas direcciones IP

Cada ordenador que pertenece a una red local tiene que disponer de una dirección IP, esta dirección en una red local se la conoce como dirección de IP privada, tienen la misma apariencia que una dirección IP del Internet, solo que estas se las conoce como dirección pública.

Una dirección IP está formada por una cadena de cuatro cifras separadas por un punto. Cada una de estas cifras pueden hallarse entre 0 y 255. Las direcciones IP privadas pueden ser asignadas arbitrariamente por el administrador de la red local mientras que las direcciones IP públicas son asignadas por la IANA, administradores del Internet.

Para que una dirección IP privada sea compatible con el Internet, debe estar dentro de los rangos siguientes:

- Clase A. 10.0.0.0 a 10.255.255.255
- Clase B. 172.16.0.0 a 172.31.255.255
- Clase C. 192.168.0.0 a 192.168.255.255

Estas direcciones no están reconocidas por la red Internet, si ningún paquete de datos está en los rangos anteriormente indicados, podrá progresar dentro de Internet, y para

que una dirección de red local este conectada al Internet, es el router el que se encarga de traducir las direcciones IP privadas en públicas y viceversa, y que así se pueda llevar a cabo la comunicación, mediante NAT (Network Address Translation).¹⁶

2.11.2 DHCP

DHCP (Dynamic Host Configuration Protocol), es el protocolo de configuración dinámica de máquinas instalado en un servidor de una red local, especifica un método para asignar una dirección IP dinámicamente a los ordenadores de una red de área local conectados a un router con parámetros de red necesarios para que un sistema pueda comunicarse efectivamente.

DHCP permite configurar muchos parámetros más como la máscara de subred, la puerta de enlace, los servidores DNS y WINS, etc. DHCP cumple muy bien las funciones en redes de tamaño mediano.

El funcionamiento consiste, cuando un cliente DHCP (ordenador de la Intranet) se inicia, este envía un mensaje de difusión DHCP Discovery (broadcast) respectivamente. El servidor almacena los campos del paquete CHADDR (dirección Ethernet origen, MAC) de manera que el servidor DHCP pueda detectarlo, en dicho mensaje indica que ha iniciado y que necesita una dirección IP.

El servidor DHCP al escuchar la petición, contesta a esta con una difusión DHCP Offer, el servidor determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDR. El servidor especifica la dirección IP en el registro YIADDR. Como la cual se ha dado en los demás parámetros y lo envía al cliente en el DHCP Request, el cliente selecciona la configuración de los paquetes recibidos de DHCP Offer. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor en el DHCP REQUEST, cuando el servidor DHCP recibe el mensaje DHCP REQUEST del cliente, que inicia la fase final

¹⁶ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

del proceso de configuración. Esta fase implica el envío de un paquete al cliente en el DHCP Acknowledge, este paquete incluye el arrendamiento de duración y cualquier otra información de configuración que el cliente pueda tener solicitada. En este punto, indica que el proceso se ha completado, por lo que el servidor DHCP devuelve una especie de acuse de recibido al cliente, el cual puede empezar a usar esta nueva IP sin problemas.

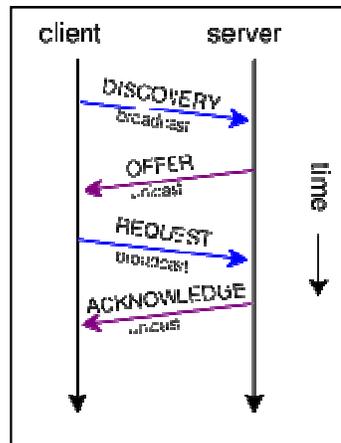


Figura 2.12 Funcionamiento DHCP

Para la utilización de este modo de asignación de direcciones, se debe habilitar el modo DHCP, tanto en el router, como en cada ordenador de la red, caso contrario se debería configurar una dirección estática en cada ordenador.

DHCP asigna direcciones IP al momento que el ordenador se enciende, este puede tener direcciones IP cada vez que se enciende, sin embargo DHCP se puede configurar para que asigne siempre la misma dirección IP a un mismo ordenador, o sino lo hará de forma aleatoria.

2.11.3 NAT

NAT (Network Address Translation), es un método que nos permite conectar múltiples ordenadores de una red local hacia el Internet, proceso de salida que consiste en enmascarar o mapear direcciones IP locales en una o más direcciones globales

permitiendo la salida de paquetes hacia el Internet, y el proceso inverso es tomar las direcciones globales con la que viene el requerimiento y desenmascararla o mapearla nuevamente en una dirección IP local.¹⁷

Funcionamiento

NAT cambia la dirección origen en cada paquete de salida, dependiendo del método también cambia el puerto de origen, estas traducciones se van almacenando en una tabla, para recordar que dirección y puerto le corresponde a cada dispositivo cliente y así poder saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla, será descartado.

NAT tiene muchas formas de funcionamiento, entre las principales tenemos:

- **Estático**

Consiste en que una dirección IP privada se traduzca a una dirección IP pública la cual siempre será la misma, permitiendo que el ordenador tenga una dirección IP de red privada pero sea visible en Internet.

- **Dinámico**

Consiste en que una dirección IP privada se mapea a una IP pública, basándose en una tabla de direcciones de IPs registradas (públicas), y cada vez que esta IP privada requiera acceso a Internet, el router elegirá una dirección de la tabla.

Utilizar NAT ayuda a mantener la seguridad en las empresas, por lo que los paquetes entrantes o salientes deben ser expuestos a un proceso de translación que permite calificar o autenticar el requerimiento para garantizar que uno es consecuencia del otro.

¹⁷ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

2.11.4 DMZ

DMZ (Demilitarized Zone), es el servidor de seguridad interno y la red interna que concentra segmentos de red para los servidores de infraestructura, los servidores de base datos y administración y los servidores corporativos.

La zona desmilitarizada DMZ se halla entre la red interna y la red de perímetro generalmente Internet, y está separada de ellas por servidores de seguridad a ambos lados. Esta red aguanta servidores que proporcionan dos grupos básicos de servicios. El primero es el servicio Web de aplicaciones para el usuario, formado por servidores en los que se ejecuta ISS (Internet Information Server). Este grupo ofrece los servicios Web fundamentales y se comunica con los clientes de Internet a través de los protocolos de transporte estándar de Internet, como HTTP o HTTPS.

Estos servidores se reúnen en clústeres con el servicio Equilibrio de la carga en la red. El segundo grupo de servidores proporciona servicios de red como el Sistema de nombres de dominio DNS (Domain Naming System). Todos los servidores de la red DMZ también pueden comunicarse con recursos internos, como los servidores de bases de datos y otros componentes adicionales que formen parte de la red interna.

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ's dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS. Las conexiones que se

realizan desde la red externa hacia la DMZ se controlan generalmente utilizando PAT (Port Address Translation).¹⁸

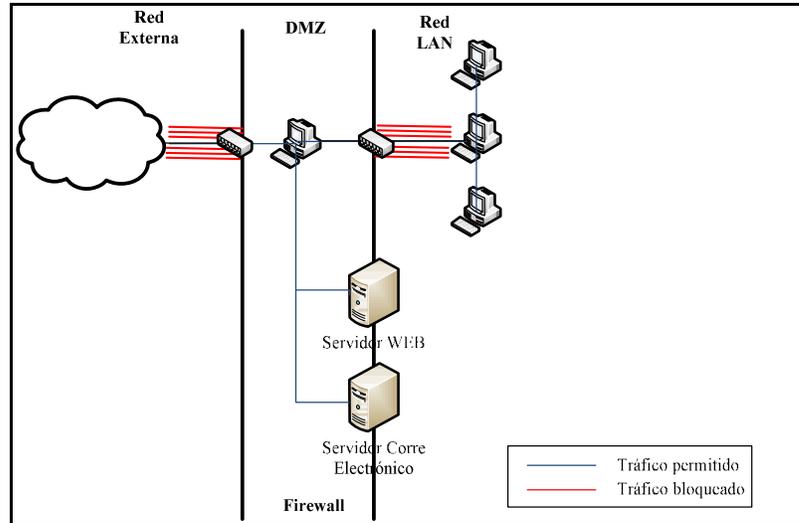


Figura 2.13 Arquitectura DMZ

Los servidores en la DMZ se denominan anfitriones bastión ya que actúan como un puesto de avanzada en la red de la organización.

Por lo general, la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está autorizado.
- El tráfico de la red externa a la red interna está prohibido.
- El tráfico de la red interna a la DMZ está autorizado.
- El tráfico de la red interna a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la organización. Debe observarse que es posible instalar las DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

¹⁸ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

2.12 Aplicaciones de Redes Inalámbrica

Originalmente las redes WLAN fueron diseñadas para su empleo en redes empresariales. En este tipo de aplicaciones una WLAN, compuesta por varios puntos de acceso inalámbricos, se conecta a una red cableada que nos permite acceder a todos los servicios disponibles en la empresa. Pero en la actualidad las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicación tanto en el ámbito residencial como en entornos públicos.

2.12.1 Aplicaciones Indoor

Definiendo así aquellas aplicaciones que dan cobertura en el interior de edificios, ambientes cerrados, oficinas, casas, aeropuertos, etc, cuyo radio de acción se remite a distancias menores a los 200 metros. El radio de cobertura depende del entorno físico y de las especificaciones técnicas del equipo. En aplicaciones indoor se pueden dar cualquiera de las configuraciones ad-hoc e infraestructura con baja potencia de irradiación.

La ventaja de esta aplicación es que muchas aplicaciones requieren conexiones móviles de laptops a la red LAN de una organización, por ejemplo, para resolver trabajos como: tareas de inventario en depósito, recolección de datos, etc. Esto es posible ya que las laptops pueden moverse libremente desde una área a otra sin perder conexión a la red LAN.

2.12.2 Aplicaciones Outdoor

Estas aplicaciones utilizan para dar servicio de largo alcance, pudiendo cubrir áreas de cobertura de varios kilómetros. Entre estas aplicaciones podemos mencionar: enlaces punto a punto, enlaces punto a multipunto y servicio de Internet inalámbrico.

En estas aplicaciones entran en juego diversos dispositivos con antenas autorizadas, que trabajan con línea de vista, según el alcance y la capacidad.

2.12.2.1 Enlaces Punto a Punto

Con este tipo de enlaces 802.11b, podemos unir dos LAN's a 11 Mbps que pueden distar varios kilómetros entre sí, podemos enlazar una PC con una LAN remota o realizar enlaces para unir dos ordenadores entre sí. Además permiten conectar puntos distantes (varios kilómetros) a través de un vínculo de datos a 11 Mbps.

2.12.2.2 Enlaces Punto a Multipunto

Enlaces punto a multipunto pueden proveer enlaces de datos a 11 Mbps entre distintos puntos de una zona o ciudad. Ahora podemos unir las redes de varias sucursales de manera sencilla y económica.

2.12.2.3 Servicio de Internet Inalámbrico

Con suma facilidad se puede ser ISP inalámbrico (Proveedor De Servicio de Internet) en barrios, cooperativas, universidades, edificios, sucursales de una forma sencilla y económica, etc.

Capítulo 3

3 SEGURIDAD PARA REDES INALÁMBRICAS

Este capítulo permite explorar lo que se refiere a Seguridades para Redes Inalámbricas, el vasto conjunto de tecnologías, técnicas y metodologías inalámbricas que se tienen en la actualidad y proporcionar un análisis de estas cuestiones con el fin de mejorar la comprensión de los principios correspondientes a la seguridad, la amenaza en los entornos inalámbricos y a las contramedidas criptográficas que se pueden aplicar de manera efectiva en las comunicaciones inalámbricas.

3.1 Principios de seguridad

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. Como el medio es compartido, todos los datos sobre una red Wireless pueden interceptados. Debido a esto varios son los riesgos que se pueden dar, como por ejemplo: se podría perpetuar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal de mayor potencia que capte la comunicación de las estaciones clientes, en vez del punto de acceso legítimo, logrando así interceptar la red inalámbrica. La posibilidad de comunicarnos entre estaciones clientes directamente (Ad-Hoc), sin pasar por un punto de acceso, también es un riesgo ya que permitirá atacar directamente a una estación cliente, si esta ofrece servicios TCP/IP o comparte ficheros, existiendo además la posibilidad de duplicar las direcciones IP o MAC de estaciones legítimas o autorizadas. Los puntos de acceso también están expuestos a un ataque (Infraestructura) para averiguar sus passwords, por lo que una configuración incorrecta facilitaría la irrupción de sistemas inalámbricos.

Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica. Por ejemplo, si varias empresas tienen su oficina matriz en un mismo edificio, y todas ellas poseen red inalámbrica, el equipo de un empleado podría encontrarse en cierto momento en el área de influencia de dos o más

redes diferentes, y dicho empleado podría conectarse (intencionalmente o no) a la red de una compañía que no es la suya.

Aún peor como las ondas de radio pueden salir del edificio, cualquier persona que posea un equipo móvil y entre en el área de influencia de la red, podría conectarse a la red de la empresa.

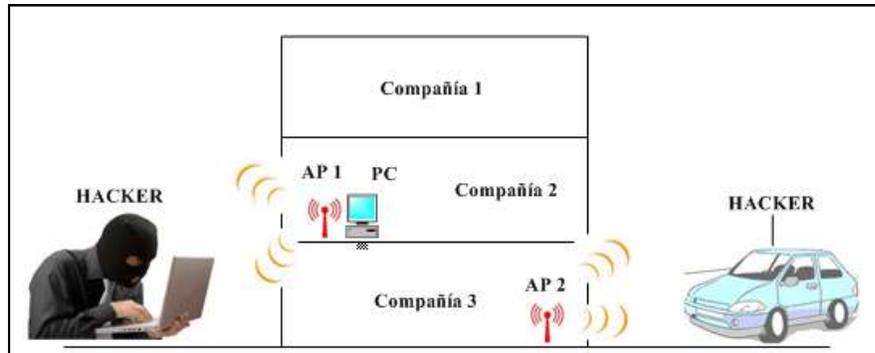


Figura 3.1 Acceso no autorizado a una red Wireless

Lo grave de esta situación es que muchos administradores de redes parece no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbricos en la red de una empresa. Es muy común encontrar redes en las que el acceso a Internet se protege adecuadamente con un firewall bien configurado, pero al interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio.

Cualquier persona que desde el exterior capte la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en el Internet, emplear la red de la compañía como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software o información, introducir virus o software maligno, entre muchas otras cosas. Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía. La mal configuración de un acceso inalámbrico, es desgraciadamente muy común. Existen dos prácticas bien conocidas para localizar redes inalámbricas:

- **El Warchalking**

Consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en el muro, indicando la presencia del punto de acceso y si tiene configurado algún tipo de seguridad o no. De este modo, otras personas pueden conocer la localización de la red.

- **El Wardriving**

Propio para localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita de un computador portátil con una tarjeta WLAN, una antena adecuada, un GPS para localizar los puntos de acceso en un mapa, y software para detección de redes inalámbricas, que se consigue libremente en el Internet.

Por esto debemos contar con herramientas sólidas de seguridad en nuestras comunicaciones con el fin de evitar interferencias y “escuchas” a nuestras comunicaciones de datos por parte de sistemas ajenos a nuestra red. El estándar IEEE 802.11b contemplando mecanismos de autenticación y encriptación. La meta es hacer una red Wireless tan segura como una red cableada, para lo cual siempre debemos considerar aspectos como:

- **Los clientes necesitan privacidad:** Cuan robustos y costosos deben ser los protocolos
- **Fácil de usar:** Si la implementación es muy difícil, entonces no se va usa

Los ataques más comunes a una red cableada o Wireless generalmente son:

- Amenazas a la seguridad física de la red.
- Acceso no autorizado.
- Ataques desde dentro de la red.
- Escuchas ilegales.
- Interferencias aleatorias e intencionales.

Por lo tanto las medidas utilizadas para asegurar la integridad de una red cableada también se aplican a una red Wireless.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquier intruso con herramientas suficientes pueda introducirse en una red

3.1.1 Vulnerabilidades de una WLAN

Las vulnerabilidades son aquellas características de nuestras situaciones, sistemas o instalaciones que pueden ser exploradas por aquellos que plantean la amenaza, con el fin de causarnos algún daño. Una vulnerabilidad para lo cual no exista una amenaza creíble no requiere que los procesos de seguridad pongan en marcha una respuesta.

Las WLAN son vulnerables a ataques especializados, muchos de estos ataques explotan los puntos débiles de la tecnología porque la seguridad de las WLAN 802.11 es relativamente nueva. También existen muchos puntos débiles de configuración porque algunas empresas no utilizan las funciones de seguridad WLAN en todos sus equipos. Hay personas que se benefician de las vulnerabilidades de las WLAN, que están intentando constantemente descubrir y explotar nuevas debilidades, en muchos de los casos, esas vulnerabilidades se comparten públicamente en Internet, y entre las principales vulnerabilidades de seguridad del 802.11 tenemos:

- Débil autenticación, solo del dispositivo
- Cifrado débil de los datos
- No se tiene integridad del mensaje

Las vulnerabilidades de seguridad 802.11 pueden ser en muchos de los casos un obstáculo para la implementación de una WLAN dentro de una empresa, por lo que las

empresas fabricantes de dispositivos de puntos de acceso desarrollan suites de seguridad proporcionando mejoras robustas en cuanto a cifrado y autenticación se refiere.¹⁹

3.1.2 Amenazas WLAN

Los gestores consideran posibles consecuencias de los ataques derivados de una amplia variedad de amenazas. Cada ataque que se puede llegar a atener puede dirigirse contra una vulnerabilidad diferente, e incluso muchos de estos intentos pueden pasar desapercibidos. Muchas de las veces, las amenazas de la información y a los sistemas de información se relacionan con una línea específica de ataques o un conjunto específico de vulnerabilidades.

Si las tecnologías inalámbricas fueran seguras, las amenazas contra las WLAN no fueran un problema, sin embargo con la existencia de estas vulnerabilidades, los intrusos presentan una amenaza eminente, entre las principales amenazas a la seguridad tenemos:

- **Amenazas no estructurales**
Consisten principalmente en individuos inexpertos que utilizan fácilmente las herramientas de pirateo disponibles.
- **Amenazas estructurales**
Proviene de intrusos más motivados y técnicamente más instruidos, son personas que conocen en profundidad las vulnerabilidades del sistema inalámbrico.
- **Amenazas externas**
Son individuos y organizaciones que trabajan desde el exterior de la empresa, individuos que no tienen acceso autorizado a la red inalámbrica, trabajan a su manera sobre una red, principalmente desde el exterior o puntos cercanos a la red.

¹⁹ DIANE TEARE, CATHERINE PAQUET. "Campus Network Design Fundamentals", Indianapolis: Cisco Press, 2006.

- **Amenazas internas**

Se producen cuando alguien tiene acceso autorizado a la red con una cuenta en un servidor, o tiene acceso físico al cableado.

3.1.3 Ataques contra las WLAN

Los métodos de ataque inalámbrico se pueden clasificar en las siguientes categorías:

- **Ataque de reconocimiento**

Es el descubrimiento y asignación no autorizados de sistemas, servicios o vulnerabilidades. El reconocimiento implica el uso de comandos o utilidades comunes para aprender tanto como sea posible del sitio de la víctima

- **Ataques de acceso**

Se refiere a la posibilidad de que un intruso no autorizado obtenga acceso a un dispositivo para el que no dispone de una cuenta o una contraseña. Entrar o acceder a sistemas no autorizados implican normalmente de herramientas que exploten las vulnerabilidades.

- **Ataque de denegación del servicio**

La DoS (Denial of Service), denegación del servicio, se da cuando un intruso deshabilita o corrompe redes, sistemas o servicios inalámbricos con la intención de denegar el servicio a los usuarios autorizados. Los ataques DoS en la mayoría de los casos, un ataque de este tipo implica la ejecución de herramientas automatizadas.

3.1.4 Debilidades de las Wi-Fi

En muchos de los estudios y pruebas realizadas a las redes inalámbricas IEEE 802.11 no tienen altos niveles de seguridad, en estos estudios se hace referencia a posibles ataques como los siguientes:

- Se hace posible descifrar un mensaje basado en la fragilidad del IV (Vector de inicialización) y en la utilización de códigos estáticos.
- Se hace posible la creación de mensajes utilizando los mensajes existentes.
- Se hace posible ataques que permiten descifrar la información contenida en las cabeceras de los paquetes, haciendo posible reenviarlos a otras estaciones para descifrar su contenido.
- Se hace posible que los ataques puedan crear una tabla de IV (vectores de inicialización) y claves permitiendo descifrar fácilmente los mensajes interceptados.

3.2 Mecanismos de Seguridad en las Redes Inalámbrica

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red inalámbrica, cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas, el protocolo IEEE 802.11 provee seguridad mediante dos atributos: autenticación y el cifrado o criptografía.

3.2.1 Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbrica que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hace impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones o de puntos de acceso, la situación se toma inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas. De este modo, el atacante puede hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un

punto de acceso el problema es más serio, porque el punto de acceso contiene toda tabla de direcciones válidas en su memoria de configuración.²⁰

3.2.2 WEP

El protocolo WEP (Wired Equivalent Protocol), es un sistema criptográfico, o de encriptación estándar, de clave estática propuesto por el comité 802.11, implementado en la capa MAC y soportado por la mayoría de los fabricantes de soluciones inalámbricos.

Este protocolo fue diseñado en particular para las redes Wireless y que pretende mediante una clave, que deben conocer todos los integrantes, asegurar la red haciendo invisible el tráfico, como el nombre lo indica, la intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security. El algoritmo RC4 se utiliza para cifrar las transmisiones realizadas a través del aire

Se trata de un secreto compartido entre dos dispositivos inalámbricos que desean comunicarse entre sí. WEP utiliza una clave de red, de 40 o 104 bits de tamaño, para la autenticación y encriptación de datos.

Esto puede llevar a confusión, porque los proveedores pueden expresar una clave de 40 bits como 64 bits de tamaño, o una clave de 104 bits como de 128 bits. En cada conjunto, los sistemas son los mismos, ya que el tamaño real de la clave es de 40 y 104 bits respectivamente. Los otros 24 bits son para un parámetro de inicialización que no es configurable por el usuario.

Otro mecanismo de seguridad definido en el estándar IEEE 802.11 es el conocido como el identificador de servicio SSID (Service Set Identifier), de una red inalámbrica. El SSID, que se establece en cada cliente inalámbrico y punto de acceso, define la red

²⁰ TOMASI WAYNE, “Sistemas de Comunicaciones Electrónicas”, Prentice Hall, 1996.

lógica para el grupo de dispositivos inalámbricos de red comparten ese SSID particular. Cada usuario (cliente o punto de acceso) de una red WLAN recibe su propia identificación SSID que es asignada al momento de configurar la red inalámbrica.²¹

3.2.3 Autenticación

Autenticación es el proceso de validar a un usuario o sistema antes de que se produzca la comunicación, es decir, verificar que una entidad, en este caso un cliente terminal, es realmente quien dice ser. Es siempre un paso previo para autorizar a un cliente a comunicarse con otro o con el punto de acceso en el área de cobertura.

Existen diferentes opciones para realizar el proceso de autenticación. Para las WLAN la autenticación puede ser en “Open System” o con “Sharred Key”.

3.2.3.1 OSA

OSA (Open System Authentication), este sistema es un tipo de autenticación definido por el estándar 802.11 para autenticar todas las peticiones que recibe. Todos los clientes que inician el proceso de autenticación ante un AP son registrados en la red. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar aunque el WEP este activado, por lo que es un mecanismo poco fiable.

El propio sistema es una vulnerabilidad en sí mismo, absolutamente todos los clientes que piden ser autenticados en la red lo son.

²¹ RANDALL K. NICHOLS & PANOS C. LEKKAS, “Seguridades Para Comunicaciones Inalámbricas”, Edigrafos S.A., 2004

3.2.3.2 SKA

SKA (Shared Key Authentication), la autenticación por clave compartida, es un proceso sencillo. Se basa en un desafío entre el cliente y el punto de acceso, en donde ambos comparte una llave secreta para iniciar dicha autenticación, siendo el cliente el dispositivo móvil que desea ser autenticado y el punto de acceso el que recibirá dicha petición.

El cliente, envía una trama (management frame) indicando que el método a usar es de llave compartida. Al recibir el AP esta trama, enviará una nueva con los 128 bytes de texto para ser usado como desafío. Estos bytes se generan por el PRNG (Pseudo Random Number Generator) usando dicha llave y un vector de inicialización.

Una vez recibida esta segunda trama por el cliente, se copia el contenido del desafío en el cuerpo de una nueva trama, que a su vez es encriptada con WEP usando la llave compartida más un nuevo vector de inicialización (esta vez es elegido por el cliente). Una vez realizado todo esto se envía al punto de acceso, para que cuando reciba esta trama proceda a:

- Desencriptarla
- Comprobar si el CRC es válido
- Verificar la validez del desafío

Una vez realizado este proceso de manera satisfactoria, el punto de acceso autentifica al cliente. Una vez completado este paso, se realiza de manera inversa. De esta manera se produce una autenticación mutua y el cliente es registrado en la red.

3.2.3.3 CNAC

CNAC (Closed Network Access Control), la autenticación cerrada es un sistema basado en el ESSID (Extended Service Set ID), que pretende controlar el acceso a la red inalámbrica. El ESSID es un código alfanumérico que está incluido en todos los AP's y en los clientes que participan dentro de la red para permitir el acceso solamente a aquellas estaciones cliente que conozcan el código, actuando este como contraseña.²²

3.2.3.4 ACL

ACL (Access Control List), lista de control de acceso, es un mecanismo de seguridad confeccionado con las direcciones físicas de cada cliente, es decir su dirección MAC. Utiliza esta dirección para permitir el acceso a la red, a aquellas MAC que consten en la lista del control de acceso establecida por el AP, como direcciones válidas.

3.2.4 802.1x

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 a una red.¹¹ 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 suplicante, o equipo del cliente, que desea conectarse con la red

²² STALLINGS WILLIAM, "Comunicaciones y Redes de Computadoras", Pearson Educación, 2004.

- El servidor de autorización (autenticación), que contiene toda la información necesaria para saber cuáles equipos o usuarios están autorizados para acceder a la red
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto..) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza

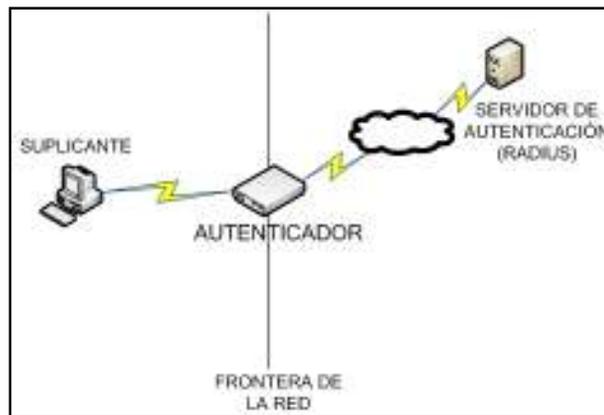


Figura 3.2 Arquitectura de un sistema de autenticación 802.1x

3.2.5 WAP

WPA (Wi-Fi Protected Access) 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.

El protocolo WAP fue promulgado para:

- Mejorar la productividad y el servicio. La información en tiempo real está disponible en todo momento y en todo lugar dentro de la organización, mejorando en gran medida la flexibilidad y la movilidad de los empleados.

- Mejorar la velocidad, la simplicidad y el costo de la instalación de infraestructuras. Eliminar los tendidos de cable a través de conductos, paredes y falsos techos.

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.

3.2.5.1 Comparación Modelos OSI, TCP/IP y WAP

Los protocolos WAP, está compuesta por los siguientes niveles:

- Nivel de aplicación
- Nivel de sesión
- Nivel de transacción
- Nivel de seguridad
- Nivel de transporte

MODELO TCP/IP	MODELO OSI	MODELO WAP
Proceso	Aplicación	Aplicación WAE
	Presentación	
Transporte	Sesión	Sesión WSP
	Transporte	Transacción WTP
Internet	Red	Seguridad WTLS
	Control de enlace	
Físico	Físico	Transporte WDP
		Nivel de adaptación

Figura 3.3 Modelos OSI, TCP/IP y WAP

- El nivel de aplicación, operando como entorno de aplicaciones inalámbricas WAE (Wireless Application Environment), proporciona un entorno en el que desarrollar y ejecutar aplicaciones y servicios para dispositivos inalámbricos y portátiles.
- El nivel de sesión, operando como protocolo de sesión WSP (WAP Session Protocol), proporciona un estado compartido entre los elementos de red a lo largo de una secuencia de solicitudes múltiples.
- En el nivel de transacción, operando como protocolo WTP (WAP Transaction Protocol), proporciona el procesamiento de transacciones, aunque con una fiabilidad más bien cuestionable, proporcionando mecanismos de flujo de datos.
- En el nivel de seguridad, operando el protocolo WPTLS (Wireless Transport Layer Security), proporciona funciones de autenticación, confidencialidad y conexiones seguras entre aplicaciones.
- En el nivel de transporte, que opera desde el entorno el protocolo WDP (WAP Datagram Protocol), protege a los niveles superiores con respecto a los servicios portadores pertenecientes al operador de telecomunicaciones.²³

3.3 Medidas de Protección

En el área de los estándares para WLAN, podemos comprobar que la seguridad se describe una y otra vez como una opción. Aunque se le presta la apropiada atención en todas las evaluaciones de redes WLAN, la seguridad se contempla, fundamentalmente, como un obstáculo para incrementar la velocidad de transmisión de datos, y solo después se la considera como un mecanismo apropiado sobre el usuario, si bien las mejoras más recientes en los estándares incluyen algunos avances en el tema de seguridad.²⁴

La única manera de poder conseguir seguridad es manteniendo unas técnicas de protección adecuadas, haciendo conciencia de no hay ninguna técnica de protección es

²³ DIANE TEARE, CATHERINE PAQUET. "Campus Network Design Fundamentals", Indianapolis: Cisco Press, 2006.

²⁴ JOSÉ A. CARBALLAR, "Wi-Fi Cómo construir una red inalámbrica", Alfaomega, 2005.

eficaz al cien por ciento, en un principio, las barreras de seguridad básicas que pueden tenerse en cuenta para cada uno de los riesgos son los siguientes:

- **Pérdida de equipo**

Precauciones mínimas para evitar pérdida o robo del equipo, no dejar grabados en el equipo los nombres de usuario y contraseña.

- **Infección de virus**

Utilizar software antivirus, porque los ataques exteriores se pueden presentar en virus, caballos de troya, etc.

- **Uso equivocado por personas autorizadas**

Es fundamental implantar políticas de seguridad donde se defina cuáles son los puntos importantes que se deben tener en cuenta en relación con la seguridad.

- **Fraudulento por personas no autorizadas**

Muchas de las veces se deja las configuraciones por defecto, y los intrusos si algo conocen muy bien son las configuraciones por defecto, por lo cual es recomendable cambiar las claves de acceso y activar las medidas de seguridad no configuradas por defecto.

Capítulo 4

4 ANÁLISIS DE LA RED EN EL COLEGIO INTERNACIONAL SEK-QUITO

En este capítulo se realizará un análisis del estado actual de la red, su configuración, administración, equipos de Internetworking, y demás configuraciones técnicas que se utilizan.

4.1 Análisis de la infraestructura Colegio Internacional SEK-QUITO

Tradicionalmente hemos visto que a los diferentes bloques o secciones se les ha ido dotando distintos servicios de mayor o menor nivel tecnológico. Tales como: calefacción, aire acondicionado, suministro eléctrico, megafonía, seguridad, etc., características que no implican dificultad, y que permiten obtener un edificio automatizado.

Cuando a estos bloques o secciones se les proporciona de un sistema de gestión centralizado, con posibilidad de interconexión entre ellas, y además de una infraestructura de comunicaciones (voz, datos, textos, imágenes), empezamos a hablar de secciones inteligentes o racionalizadas, como es el caso de los bloques o secciones del Colegio Internacional SEK-QUITO.

4.1.1 Infraestructura LAN

Las instalaciones tienen 4 bloques o secciones principales (Administración, Preescolar, Primaria y Secundaria) los cuales forman parte de la infraestructura de la red LAN de la Institución.

En este punto se toma en cuenta la infraestructura del lugar, es decir sus dimensiones, facilidades y dificultades que pueda presentar para poder determinar el cableado horizontal que dispone la Institución.

En el Anexo A se detalla las dimensiones y el esquema de la distribución del cableado estructurado que dispone la misma.

En la actualidad, el Colegio Internacional SEK-QUITO posee una infraestructura de voz y datos principalmente, disgregada según las diferentes aplicaciones y entornos y dependiendo de las modificaciones y ampliaciones que se ha ido realizando, por ello es posible que coexistan multitud de hilos, cada uno para su aplicación y correspondiente uso.

Todo ello se puede resumir en los siguientes puntos:

- Convivencia de cable de varios tipos diferentes, telefónico, coaxial, pares apantallados, pares sin apantallar con diferente número de conductores, etc.
- Peligro de interferencias, averías y daños personales, al convivir en muchos casos los cables de transmisión con los de suministro eléctrico.
- Coexistencia de diferentes tipos de conectores.
- Trazados diversos de los cables a través de la Institución. Según el tipo de conexión hay fabricantes que eligen la estrella, otros el bus, el anillo o diferentes combinaciones de estas topologías.
- Posibilidad de accidentes. En diversos casos la acumulación de cables en el falso techo o canaletas ubicadas a lo largo de la Institución.
- Dificultades en el mantenimiento en trazados u accesibilidad de los mismos

Ante esta problemática parece imposible encontrar una solución que satisfaga los requerimientos técnicos de los fabricantes y las necesidades actuales y futuras de los mismos. Sin embargo entran en juego varios factores que permiten modificar este panorama:

- Tendencia a la estandarización de Interfaces por parte de gran número de fabricantes.
- Estándares internacionalmente reconocidos para RDSI (Red Digital de Servicios Integrados).
- Evolución de grandes sistemas informáticos hacia sistemas distribuidos y redes locales.

- Generalización del PC o compatible en el puesto de trabajo como terminal conectado a una red.
- Tecnologías de fabricación de cables de cobre de alta calidad que permite mayores velocidades y distancias.
- Aparición de la fibra óptica y progresivo abaratamiento del costo de la electrónica asociada.
- Además de todo ello alguna compañías han tenido la iniciativa de racionalizar dichos sistemas, así como dar soluciones comunes.

Las técnicas de cableado estructurado se aplican en:

- Instituciones donde la densidad de puestos informáticos y teléfonos es muy alta: oficinas, centros de enseñanza, etc.
- Donde se necesite gran calidad de conexión así como una rápida y efectiva gestión de la red: hospitales, fábricas automatizadas, centros oficiales, aeropuertos, terminales y estaciones de autobuses, etc.
- Donde a las instalaciones se les exija fiabilidad debido a condiciones extremas: barcos, aviones, estructuras móviles, fábricas que exijan mayor seguridad ante agentes externos.

4.1.1.1 Mapa de la Red

El trabajo de administrador de una red de computadores es algo que no debe llevarse a la ligera. Un buen administrador debe tener en cuenta hasta los más pequeños detalles. Es por eso que una buena cantidad de trabajo es ahorrado, al tener documentado qué cosas componen tu red.

Desde el punto de vista de un usuario común y corriente, el mapa de red no le es muy útil. Pero en fin, supongamos que hay que revisar un desperfecto en la red y no tenemos idea de dónde podría estar ubicado el error. Claro, ahora sí que es importante nuestro mapa. En vez de andar verificando en el suelo, encaramándose al techo o rompiendo

paredes o techos falsos, es mucho más simple ver por dónde pasaba el cable, o puede ser bastante más económico saber en qué punto del hub estaba ubicado tal o cual cable de red. En el Anexo A se detalla el esquema de la distribución del cableado de la red.

Mapa de Red	
IP ADDRESS	NAME
192.168.5.254	Servidor 1
192.168.5.253	Servidor 2
192.168.5.201	Administración
192.168.5.202	Dirección
192.168.5.203	Admisiones
192.168.5.204	Recepción 1
192.168.5.205	Recepción 2
192.168.5.206	Rectorado
192.168.5.207	Almacén
192.168.5.208	BI
192.168.5.209	Contabilidad 1
192.168.5.210	Contabilidad 2
192.168.5.211	Caja 1
192.168.5.212	Caja 2
192.168.5.231	Recepción
192.168.5.232	Contabilidad 1
192.168.5.233	Pre Escolar
192.168.5.234	Secretaría Primaria
192.168.5.235	Biblioteca
192.168.5.236	Secretaría Secundaria
192.168.5.246	Música 1
192.168.5.247	Música 2
192.168.5.214	Jefatura Primaria
192.168.5.215	Secretaría Primaria
192.168.5.216	Biblioteca
192.168.5.217	Sicología
192.168.5.218	Jefatura Secundaria
192.168.5.219	Secretaría Secundaria
192.168.5.250	Sistemas
192.168.5.251	Sistemas

Tabla 4.1 Mapa de Red

4.1.1.2 Medios LAN

Una vez realizado el análisis del sistema de redes cableadas LAN se determinó que la tecnología utilizada es la de punto multipunto.

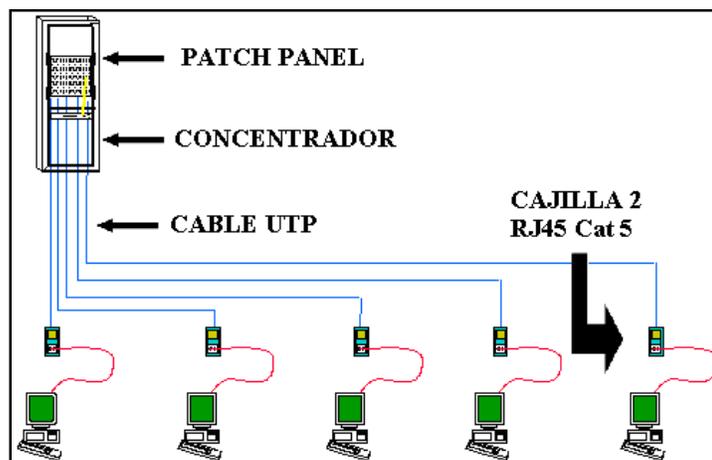


Figura 4.1 Esquema de Cableado Estructurado

Los medios utilizados en la capa física que define especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales son los que mencionaremos a continuación:

El medio físico utilizado en la red alámbrica es el cable UTP (Unshielded Twisted Pair) de par trenzado debido a que ofrece ventajas referentes a movilidad, facilidad de crecimiento y expansión, integración a altas velocidades de transmisión de datos compatibles con todas las redes LAN que soporten velocidades superiores a 100 Mbps, flexibilidad para el mantenimiento de las instalaciones dispositivos y accesorios para cableado estructurado.

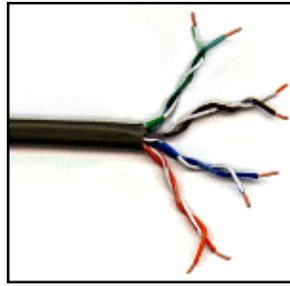


Figura 4.2 Cable UTP

Otros elementos físicos para la conexión para cable UTP son los siguientes:

- Conector RJ 45 macho (PLUG).

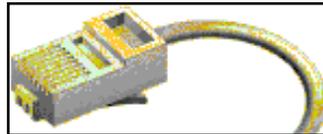


Figura 4.3 PLUG

- Conector RJ 45 hembra (JACK)



Figura 4.4 JACK

Otro medio físico utilizado en la red alámbrica es la fibra óptica que no es susceptible a la interferencia electromagnética y ofrece velocidades de datos más altas que cualquiera. El cable de fibra óptica no transporta impulsos eléctricos sino que son haces de luz.



Figura 4.5 Fibra Óptica

En la siguiente figura, mostramos como esta distribuido cada medio en la red alámbrica del Colegio Internacional SEK-QUITO.

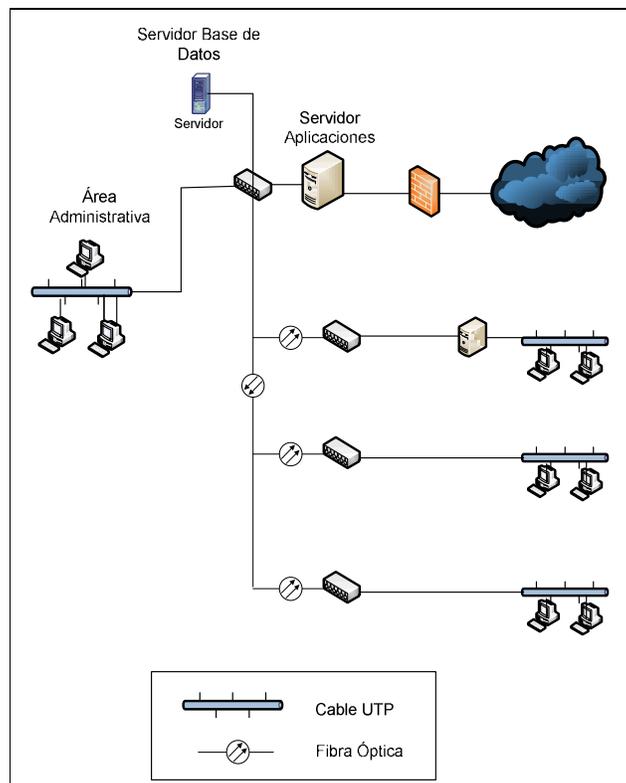


Figura 4.6 Medios LAN Colegio Internacional SEK-QUITO

Cabe mencionar que las canaletas se alojarán los cables UTP Cat5e que unirán los puntos de red con el rack de distribución más cercano, con sus respectivos cajetines, así mismo cada punto de acceso dispondrán de ponchado directo de plugs, jacks y del patch panel según la normativa EIA/TIA 568B o EIA/TIA 568A, y el medio utilizado.

4.1.2 Comprobación de la red LAN

La red actual es una red Gigabit Ethernet, las computadoras que trabajan en los bloques o secciones poseen tarjetas de red 10/100, es decir, el ancho de banda de la red interna es de 100 Mbps (teóricamente).

La salida a Internet que tiene el Colegio internacional SEK-QUITO cuenta con una antena ubicada en los techos del área administrativa, que brinda un enlace directo al backbone del ISP ECUANET, mediante el servidor Dell Power Edge 2850, este enlace es de 2048 Mbps de ancho de banda. El servicio de Internet lo comparten los diferentes bloques o secciones, lo que quiere decir que el ancho de banda para estas secciones se divide. ECUANET provee acceso al backbone de Internet con alto desempeño y altas velocidades. Este servicio le proporciona una conexión permanente a Internet y le permite configurar las opciones de acuerdo a las necesidades específicas que tenga cada empresa.

La conexión a Internet Institucional provee las siguientes características:

- Latencia: 112 ms hacia portales de investigación como yahoo y google.
- Confiabilidad: VER 10 e -12.
- Pérdida de paquetes: 0%
- Capacidad: Hasta 10 Gbps

4.1.3 Rendimiento de la red LAN

La evaluación del rendimiento de la red LAN, se realiza a través del software NetLimiter 2.0.10 Pro que brinda la facilidad de medir el ancho de banda y sirve para saber con exactitud lo que pasa en la red interna y el uso que da el personal del Colegio Internacional SEK-QUITO, como por ejemplo: el ancho de banda utilizado, los protocolos más utilizados, los riegos de los virus, los web sites más visitados, etc.

La información que se detalla en el cuadro resumen representa el flujo de información durante el año lectivo 2007 y 2008.

Los datos presentados a continuación, nos dan información como el día más activo, la tasa de transmisión, la tasa de recepción, promedio de información enviada por día, total de información recibida, etc.

Cuadro Resumen	
Número de días	200
Pedidos exitosos	31388161
Pedidos error	0
Totales Número de Eventos	223682386
Promedio Eventos por día	1118411
Totales Número de Visitantes autenticados	132
Día más activo	08/24/2007
Totales Bytes transferidos	1664,13 GB
Promedio transferidos por día	8,32 GB
Totales Bytes enviados	18,27 GB
Totales Bytes recibidos	1645,85 GB
Totales Número de Attacks	8,30 GB
Totales emergencias Eventos	13
Promedio emergencia Eventos por día	0
Totales alerta Eventos	280271
Promedio alerta Eventos por día	1401
Totales críticos Eventos	21502
Promedio críticos Eventos por día	107
Totales Error Eventos	2
Promedio Error Eventos por día	0

Tabla 4.2 Resumen General del Flujo de Información del Colegio Internacional SEK-QUITO

4.2 Inspección y descripción de la infraestructura

El Colegio Internacional SEK-QUITO se encuentra ubicado en la ciudad de Quito, las instalaciones se encuentran ubicadas en el sector norte de Quito con dirección C/ Carmen Olmo Mancebo y Guayacanes.

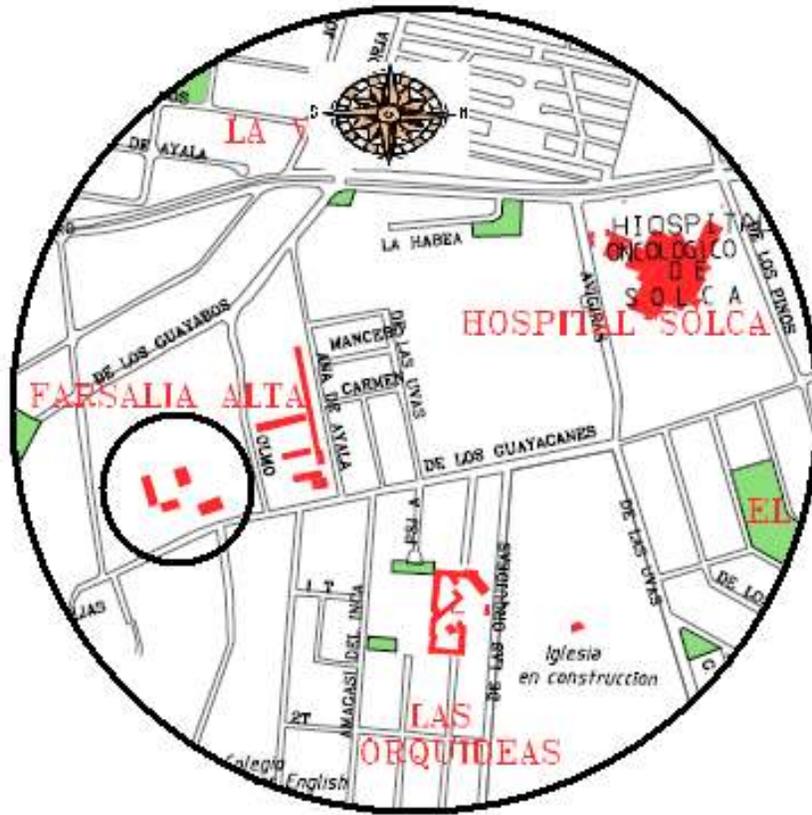


Figura 4.7 Ubicación del Colegio Internacional SEK-QUITO
Respecto a la Ciudad de Quito.

4.2.1 Inspección de la infraestructura

Al realizar la inspección de campo, para tener una visión general de la infraestructura del Colegio Internacional SEK-QUITO, se pudo confirmar lo que anteriormente se había dicho, es decir que está conformada por bloques, que estos se encuentran en una sección, y además cuenta con varios espacios abiertos que sirven para la recreación de los estudiantes.



Figura 4.8 Bloques y Espacios Abiertos del Colegio Internacional SEK-QUITO

4.2.2 Inspección de equipos activos existentes

Luego de haber hecho una inspección de campo, y de analizar las áreas de infraestructura que dispone la Institución, el área de sistemas realizó en aulas, salas de profesores, salas de música, racks y demás lugares donde se desarrollen las actividades a que se refiere esta inspección, controles de equipos, aparatos, dispositivos y sistemas de comunicación, con el fin de comprobar que se mantienen todas las características técnicas en cuya virtud se otorgó el certificado de aceptación, por parte de las autoridades del Colegio Internacional SEK-QUITO en su debido tiempo, que aplicaciones y servicios tiene cada punto de acceso, para lo cual se utilizaron herramientas necesarias para dicha inspección (testadores, seguidores de tonos, software de monitoreo de IPs, sniffer), todo esto con el único propósito de documentar lo que se tiene físicamente en la red de la Institución (mapa de red, inventario de equipos de comunicación, inventario de equipos de computación), información que nos ayudará hacer un diseño más operativo, eficaz y eficiente, para la solución que se dará posteriormente, hacia las necesidades y requerimientos de la misma.

4.3 Documentación de análisis e inspecciones de la red LAN

4.3.1 Equipos existentes

Los datos recogidos en la inspección de equipos activos y equipos existentes muestran en general, que en algunos casos equipos HP-Compaq Pentium III (Aulas) y en la mayoría de los casos equipos Dell Pentium IV (Laboratorios de Informática de Preescolar, Primaria y Secundaria), equipos Dell de escritorio y portátiles Core Duo 2 (Oficinas Administrativas).

Los principales dispositivos que se utilizan en las comunicaciones, las redes y el cableado estructurado en la actualidad son:

- 01 Rack de pared LAN-PRO.
- 06 Concentradores Switch CYSCO 10/100 de 16 puertos, Modelo CATALYST 2900 SERIES XL, Fast Ethernet a 100 Mbps en puntos estratégicos de la Institución.
- 06 Fast Ethernet Media Converter
- 03 Patch Panel LAN-PRO de 24 puertos

4.3.2 Direcciones IP

La red del colegio Internacional SEK-QUITO utiliza la clase de red C, debido a que no se tiene previsto interconectar más de 256 computadoras.

Para configurar las direcciones IP en cada una de las PCs se utilizan las propiedades de conexiones de área local y seleccionamos las propiedades del Protocolo de Internet TCP/IP de Windows.

Dentro de las propiedades del protocolo TCP/IP incluimos las direcciones IP establecidas, la máscara de subred, la puerta de enlace predeterminada y las direcciones de DNS definidas por el proveedor de Internet, a los computadores con IP estática, mientras que a los otros computadores les asignaremos mediante servicio DHCP, esta tecnología consiste que el servidor DHCP corre el servicio manteniéndose a la escucha de peticiones broadcast DHCP, y cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con una información adicional.

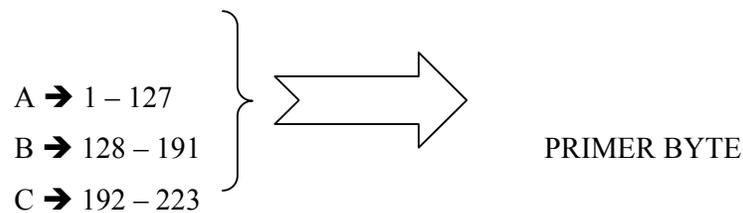
El protocolo es tan fundamental que en ocasiones, se le llama nivel IP al nivel de red. Tienen una estructura de 4 bytes (32 bits)



Esta estructura de 4 bytes se divide en 2 grupos:

- ID → identificación # máximo de clientes registrados a un servicio.
- # HOST → # de máquinas que puedo tener conectadas en una red local.

Dependiendo de la dirección IP que se vaya a emplear tenemos tres clases de red (A, B, C).



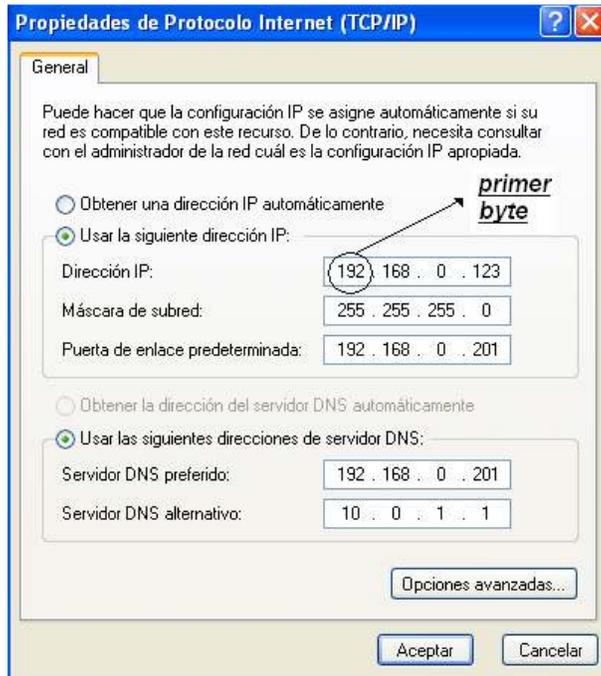
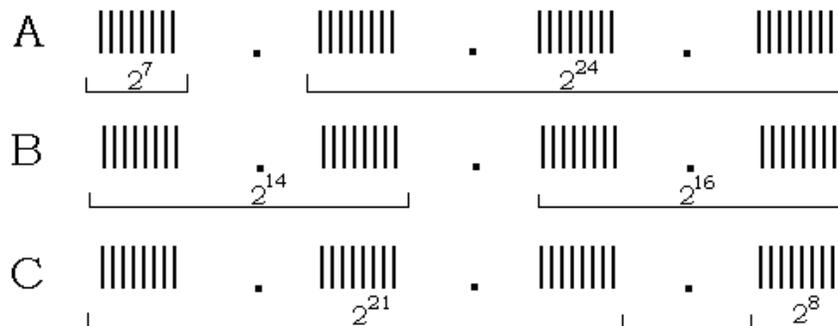


Figura 4.9 Direcciones IP y Máscara de Subred

El primer byte que colocamos en la dirección nos va a definir la clase de red que vamos a utilizar. A continuación detallamos los rangos de la dirección IP con su respectiva clase, ID y HOST, de acuerdo a la norma establecida para este protocolo se resta 1 bit por cada byte para la realización de comprobación de la red esto solo le afecta al ID.



Por tal razón a continuación describimos un máximo de ID (clientes registrados al servicio) y de HOST (máquinas de la red) de acuerdo a la clase seleccionada.

Clase	ID	HOST
A	$2^7 \rightarrow 128$	$2^{24} \rightarrow 16777216$
B	$2^{14} \rightarrow 16384$	$2^{16} \rightarrow 65536$
C	$2^{21} \rightarrow 2097152$	$2^8 \rightarrow 256$

Tabla 4.3 Clientes registrados – Máquinas de red

4.3.3 Máscara de Subred

Dependiendo de la clase de red que utilizaremos el protocolo TCP/IP define automáticamente una máscara de red, condicionado al ID. Si es necesario ampliar la red en varias subredes podemos cambiar el último dígito de la máscara de la red.

Clase	Máscara de Subred
A	255. 0. 0. 0
B	255. 255. 0. 0
C	255. 255. 255. 0

Tabla 4.4 Máscara de Subred

En el Anexo B se puede verificar como se han distribuidos las direcciones IP estáticas.

4.3.4 Dirección Proxy

El Servidor Proxy es un programa que se instala en un ordenador por cada Red LAN en nuestro caso es uno solo para la red interna, el mismo que permite que varios

ordenadores conectados a una misma red local puedan compartir un mismo acceso a Internet o conexión a Internet de manera simultánea.

La traducción de la palabra "Proxy" es "apoderado" o "sustituto", es decir una persona que toma la identidad de otra para determinada tarea, por lo que para la conexión a Internet, un Proxy es un servidor que sirve de intermediario entre un cliente y otro servidor.

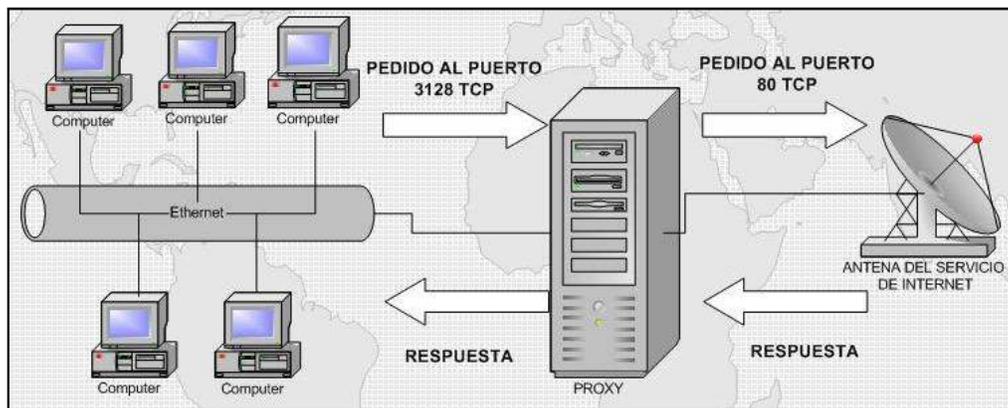


Figura 4.10 Conexión a través de Proxy

El cliente hace un requerimiento a un puerto específico del servidor Proxy (3128TCP), y hace un pedido a otro servidor. El Proxy se conecta con el servidor que el cliente desea contactar y hace el pedido al puerto verdadero de la aplicación (80TCP), y, luego de recibir la respuesta proveniente del servidor final, el Proxy se la envía al cliente original.

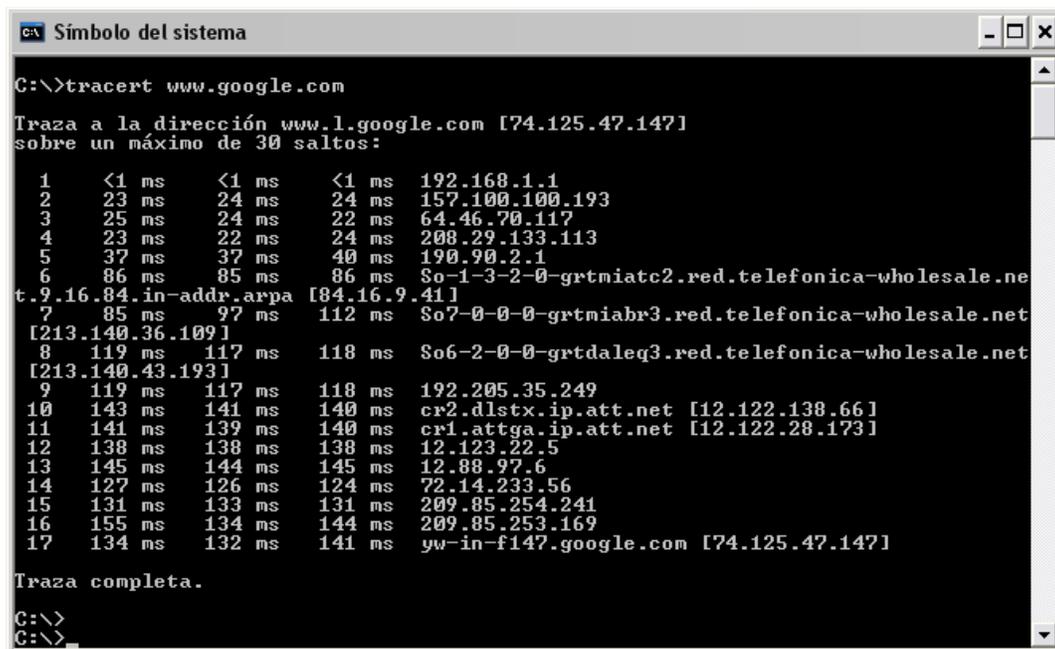
Con esta característica, el Proxy Server ofrece muchas ventajas, entre las que podemos anotar:

- Un solo punto de Acceso al Servicio de Internet
- Seguridad: El Proxy también actúa como una barrera (firewall) pero en solo una dirección, es decir que permite limitar el acceso al Internet de los clientes internos al exterior.
- Dirección IP única: La dirección IP es la que identifica de forma unívoca a cada máquina en Internet. Si se utiliza un Proxy basta con una dirección IP para toda la red local en lugar de tener una IP para cada uno de los ordenadores.
- Conexión automática (autodialing): No es necesario que el ordenador que actúa

como Proxy esté conectado permanentemente a Internet. Con esta función, cada vez que un usuario realiza una petición, el Proxy establece la conexión. Del mismo modo el Proxy la desconecta cuando no hay ninguna petición, todo ello automáticamente.

- Menor tráfico de red: El Proxy almacena automáticamente en la memoria las páginas Web a las que se accede con mayor frecuencia, con lo que se reduce la cantidad de información que es necesario recuperar a través de Internet.

No se ha visto la necesidad de configurar un firewall a nivel de nuestros servidores Proxy por cuanto los ataques desde fuera de la red podrían provenir del servidor del servicio de Internet ya que ellos nos brindan el servicio a través de su Proxy. Lo cual podemos verificar aplicando el comando de consola TRACEROUT, que nos muestra la ruta que está recorriendo un paquete hasta llegar a su destino.



```
C:\>tracert www.google.com
Traza a la dirección www.l.google.com [74.125.47.147]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms    192.168.1.1
 2  23 ms    24 ms    24 ms    157.100.100.193
 3  25 ms    24 ms    22 ms    64.46.70.117
 4  23 ms    22 ms    24 ms    208.29.133.113
 5  37 ms    37 ms    40 ms    190.90.2.1
 6  86 ms    85 ms    86 ms    So-1-3-2-0-grtmiatc2.red.telefonica-wholesale.net
 7  85 ms    97 ms    112 ms   So7-0-0-0-grtmiabr3.red.telefonica-wholesale.net
 8  119 ms   117 ms   118 ms   So6-2-0-0-grtdaleq3.red.telefonica-wholesale.net
 9  119 ms   117 ms   118 ms   192.205.35.249
10  143 ms   141 ms   140 ms   cr2.dlstx.ip.att.net [12.122.138.66]
11  141 ms   139 ms   140 ms   cr1.attga.ip.att.net [12.122.28.173]
12  138 ms   138 ms   138 ms   12.123.22.5
13  145 ms   144 ms   145 ms   12.88.97.6
14  127 ms   126 ms   124 ms   72.14.233.56
15  131 ms   133 ms   131 ms   209.85.254.241
16  155 ms   134 ms   144 ms   209.85.253.169
17  134 ms   132 ms   141 ms   yw-in-f147.google.com [74.125.47.147]

Traza completa.
C:\>
C:\>
```

Figura 4.11 Tracert www.google.com

Un punto a tomar en cuenta es que existen también paredes de concreto que separan a los diferentes departamentos, dependencias varias, aulas, causando atenuación de la señal.

Es necesario hacer un análisis más minucioso y detallado de los equipos que tendríamos por alumno y en que zona de la Institución se encontrarían.

- **Determinación de la población objeto de estudio**

La población objeto de estudio corresponde a las personas del Colegio Internacional SEK-QUITO, que para el caso de estudio es igual a 1195 personas entre alumnos, docentes y personal administrativo.

- **Técnica de muestreo**

Muestreo aleatorio simple

Una muestra aleatoria simple es seleccionada de tal manera que cada muestra posible del mismo tamaño tiene igual probabilidad de ser seleccionada de la población. Para obtener una muestra aleatoria simple, cada elemento en la población tenga la misma probabilidad de ser seleccionado, el plan de muestreo puede no conducir a una muestra aleatoria simple. Por conviencia este método puede ser reemplazado por una tabla de números aleatorios.²⁵

- **Cálculo de la muestra**

El cálculo de la muestra se o realiza mediante la siguiente fórmula

$$n = \frac{z^2 * N(p * q)}{e^2(N - 1) + z^2 * (p * q)}$$

Donde:

N = Número de personas del Colegio Internacional SEK-QUITO

p = Prob. de acceso a Internet (Nivel de aceptación)

q = Prob. de no acceso a Internet (Nivel de rechazo)

z = Coef. Estandarización de la curva normal (Nivel de confianza)

e = Error estándar

²⁵ www.monografias.com/trabajos11/tebas/tebas.shtml#met

Para completar la información de la fórmula es necesario calcular los coeficientes de p y q a través de una prueba piloto.

Por medio de la prueba piloto se determinará el tamaño de muestra de las posibles demandantes con disponibilidad de equipos con dispositivo inalámbrico para acceso a Internet, basándose en la pregunta base.

Con estas observaciones se puede identificar la probabilidad de éxito o fracaso en la pregunta y aplicando la fórmula de cálculo del método probabilístico se definirá el tamaño de la muestra.

Para desarrollar la prueba piloto se realizaron 10 encuestas a las personas escogidas; los resultados de la aplicación de esta prueba se detallan a continuación:

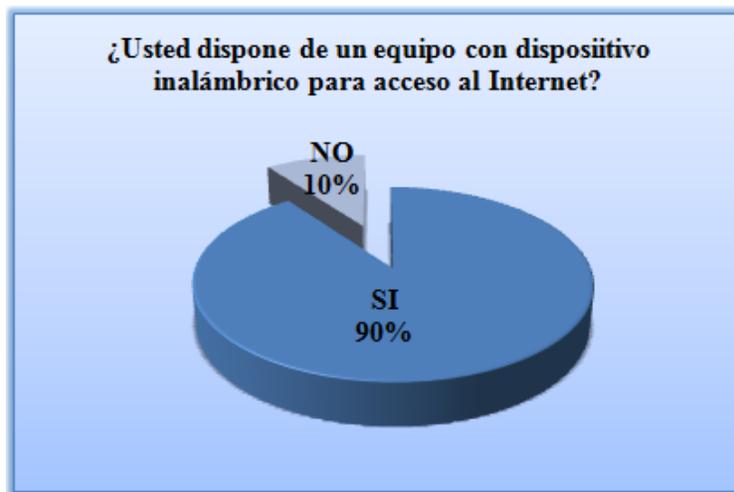


Figura 4.12 Resultados de la prueba piloto

Por lo tanto la probabilidad de disponibilidad de equipos con dispositivo inalámbrico para acceso a Internet es del 90% y una posibilidad de no consumo es igual a 10%

Entonces:

Datos:	
p =	90,00%
q =	10,00%
N =	1195
z =	1,96
e =	5,00%

$$n = \frac{1.96^2 * 0,9 * 0,1 * 1195}{0,05^2 * (1195 - 1) + 1.96^2 * 0,9 * 0,1}$$

Una vez aplicada la fórmula, se obtuvo una muestra igual a 124 personas del Colegio Internacional SEK-QUITO, a los cuales se les aplicara la encuesta

Descripción	Frecuencia	Porcentajes
Alumnos Primaria	51	41,1
Alumnos Secundaria	60	48,4
Docentes	9	7,2
Administrativo	4	3,3
Total:	124	100

Tabla 4.5 Personas Promedio

De las personas encuestadas un 36% se encuentra en la sección primaria, un 40% lo tenemos en la sección secundaria, un 20% pertenecen a los docentes y mientras que un 4% son del área Administrativa. Lo que indica que la mayoría de las personas encuestadas son de secundaria, por lo tanto la red inalámbrica a implementar se acopla perfectamente a las personas que demandan este servicio, ya que podríamos decir que un implemento obligatorio el acceso a Internet en la actualidad.

- **Segmento Alumnos de Primaria**

Respuesta	Porcentajes	Personas
Tamaño del mercado	41,1	491
Si disponen equipos inalámbricos	30	147
No disponen equipos inalámbricos	70	344

Tabla 4.6 Alumnos de Primaria con disponibilidad de equipos inalámbricos

El 30% dijo que si dispone de equipos inalámbricos para acceso a Internet, lo que representa cuantitativamente 147 personas.

- **Segmento Alumnos de Secundaria**

Respuesta	Porcentajes	Personas
Tamaño del mercado	48,4	578
Si disponen equipos inalámbricos	60	346
No disponen equipos inalámbricos	40	232

Tabla 4.7 Alumnos de Secundaria con disponibilidad de equipos inalámbricos

El 60% dijo que si dispone de equipos inalámbricos para acceso a Internet, lo que representa cuantitativamente 346 personas.

- **Segmento Docentes**

Respuesta	Porcentajes	Personas
Tamaño del mercado	7,2	86
Si disponen equipos inalámbricos	35	30
No disponen equipos inalámbricos	65	56

Tabla 4.8 Docentes con disponibilidad de equipos inalámbricos

El 35% dijo que si dispone de equipos inalámbricos para acceso a Internet, lo que representa cuantitativamente 30 personas.

- **Segmento Administración**

Respuesta	Porcentajes	Personas
Tamaño del mercado	3,3	40
Si disponen equipos inalámbricos	40	16
No disponen equipos inalámbricos	60	24

Tabla 4.9 Alumnos de primaria con disponibilidad de equipos inalámbricos

El 40% dijo que si dispone de equipos inalámbricos para acceso a Internet, lo que representa cuantitativamente 16 personas.

En el estudio realizado tendríamos unas 539 personas entre alumnos, docentes y personal administración que en el transcurso del día tendrían acceso al Internet con equipos inalámbricos propios. Y es muy importante recalcar que la solución más óptima en la biblioteca y lugares de concentración de los alumnos, sería colocar dos puntos de acceso para proveer de mejor manera conectividad, mantener las tasas de transmisión altas y cubrir las necesidades de cobertura.

Este estudio mas particularizado apunta a detectar características referidas fundamentalmente a los consumidores en nuestro caso alumnos de primaria y secundaria, docentes y personal administrativo, La tabla del coeficiente de estandarización de la curva se encuentra en el Anexo D.

4.4 Requerimientos del Colegio Internacional SEK-QUITO

La misión del Colegio Internacional SEK-QUITO privilegia la formación integral de sus estudiantes, por lo que, es imprescindible mantener una constante actualización de los recursos e infraestructura utilizada para su labor. Por esta razón hay que tomar en cuenta, los siguientes requerimientos:

- La infraestructura física que soporta la red institucional se torna insuficiente para atender el volumen creciente de puntos de acceso por parte de usuarios que solicitan acceso a la red. La creación, remodelación o mudanzas de direcciones, oficinas o aulas, en los distintos departamentos ha exigido la extensión de la red a tal nivel que actualmente imposibilitados agregar nuevos puntos de acceso, además del número limitado de puertos que ofrecen los switchs instalados, de ahí que existe la imperiosa necesidad de implementar un sistema de intercomunicación mediante el cual los trámites administrativos, coordinaciones, y más acciones de orden educativo puedan ser realizadas con mayor prontitud y efectividad.
- El manejo de un sistema administrativo, escolástico y financiero (WEBSEK, Fórum Profesores y Fórum Alumnos), implementado por el Colegio

Internacional SEK-QUITO amerita que la información sea manejada en forma integral por todas las dependencias inmersas en la labor educativa, sobre todo aquella referente a datos personales de los estudiantes, información socioeconómica, record académico, control de asistencia, entre otros; esto permitiría mayor certeza en la entrega de la misma a los clientes internos y externos de cada proceso realizado en la Institución (departamentos, docentes, alumnos, padres de familia, estamentos educativos superiores).

- El desarrollo mismo del proceso educativo, cada vez más exigente en el manejo de tecnologías informáticas de comunicación (TICs), requiere de la utilización del Internet como recurso didáctico y fuente de consulta e investigación para estudiantes y docentes de la Institución. De esta necesidad se desprende además que en las áreas de recreación y relax de los estudiantes deben estar conectados en red para el aprovechamiento de los servicios propios que prestan las redes.
- El análisis anterior evidencia la necesidad de dinamizar el proceso educativo tanto en su manejo administrativo como pedagógico, por lo que, de ser atendido, se requiere implementar el uso de nuevas técnicas de información y comunicación; como el uso de la tecnología Wireless sobre la Institucional, con la finalidad de ampliar su capacidad de comunicación.

4.5 Informe de la red del Colegio Internacional SEK-QUITO

Luego de realizar el trabajo descrito anteriormente en la red del Colegio Internacional SEK-QUITO, me permito concluir que el Colegio Internacional SEK-QUITO cuenta con una estructura de red alámbrica en todas sus dependencias. Tanto en las áreas administrativas en sus oficinas, áreas docentes en sus aulas y áreas de estudiantes en sus laboratorios, se soportan con esta estructura de red y con todos los servicios de Internet, correo electrónico y capacidad de compartir archivos e impresoras.

Complementariamente al servicio de biblioteca tradicional, los estudiantes cuentan con computadores con acceso a Internet, así mismo para los docentes existen puntos de acceso en las salas de profesores, pero muchas veces estos puntos de acceso se encuentran ocupados, incrementándose de uso por parte de los docentes especialmente a finales de mes cuando hacen el ingreso de notas a través del Internet, por estas razones se requiere implementar una estructura de red inalámbrica para que puedan tener acceso a Internet y demás servicios que brinda la red.

Adicionalmente a esto, existen otras áreas de mayor demanda para el servicio inalámbrico por diferentes razones como son: la biblioteca (prestación de computadores portátiles con tarjetas inalámbricas), áreas recreativas en cada bloque, pasillos, bar y en los lugares donde se concentran los alumnos (computadores personales, celulares, agendas electrónicas con tarjetas inalámbricas de alumnos y docentes), todas aquellas son áreas que se encuentran sin ningún servicio de red por lo cual es indispensable que se les brinde conectividad y los servicios mencionados anteriormente.

Capítulo 5

5 DISEÑO WLAN COLEGIO INTERNACIONAL SEK-QUITO

En este capítulo se presenta el estado actual de la red y sus necesidades, con la finalidad de recomendar una propuesta de diseño de red inalámbrica institucional propuesta para solucionar cuyo objeto es solucionar el problema de datos del Colegio Internacional SEK-QUITO.

5.1 Principios del Diseño (PDIOO)

PDIOO es conocido como el ciclo de vida de una red en la cual describe las fases múltiples con las cuales una red existe. En la siguiente figura se ilustra el ciclo de vida:

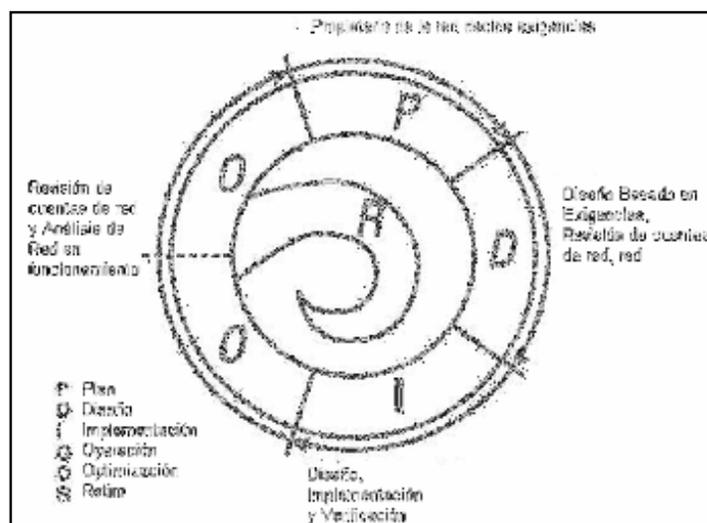


Figura 5.1 Ciclo de Vida de una Red

- **Plan:** Se identifican los requisitos detallados de la red y la red existente es revisada.
- **Diseño:** La red es diseñada según los requisitos iniciales y los datos adicionales obtenidos durante el análisis de la red.

- **Implementación:** La red es construida según el diseño aprobado.
- **Operación:** En esta fase la red es operacional y supervisada.
- **Optimización:** Detección, corrección de problemas.
- **Retiro:** A pesar de no ser parte del ciclo de vida PDIOO esta fase es necesaria cuando cierta parte de la red es obsoleta.

El ciclo PDIOO describe todas las fases de una red. La tarea de diseñar una red es obviamente una parte integral de este ciclo vital e influyente en todas ellas. El diseño de red debería incluir las siguientes tareas:

- Determinación de requisitos, a través de informes técnicos y de negocio se puede determinar los requisitos más importantes de red como por ejemplo: redundancia, disponibilidad de ancho de banda, seguridad, acceso a Internet, calidad de servicio, etc.
- Análisis de la red existente, si esta existe: Si se trata de un re-configuración de una red existente es probable restringir el diseño de red por ejemplo el cableado estructurado existente por motivos de costo. Se debe determinar que se puede cambiar para beneficios de los usuarios.
- Diseño preliminar, implica considerar todos los requisitos de la red y determinar las mejores soluciones que el dueño de la red necesite.
- Diseño final, consiste en producir una red con todas las especificaciones técnicas de configuración, presentando esquemas detallados de la red.
- Despliegue de la red, consiste en un planeamiento de cómo debe ser hecha la documentación, quien lo realiza y el impacto que tendrá en la red existente. La puesta en marcha de la red es la verificación final del diseño.
- Monitoreo, realiza estadísticas con información acerca de cómo la red está trabajando, supervisando las anomalías y problemas que requieran de reajustes para la optimación de la misma.
- Backup de la configuración de la red, es importante mantener todo el diseño de la red documentada, por tal motivo esta tarea incluye puntos como son: requisitos, estado de la red existente, diseños preliminares, planes de contingencia, seguridad, etc.

A continuación se ilustra en la siguiente figura las tareas del diseño de la red:

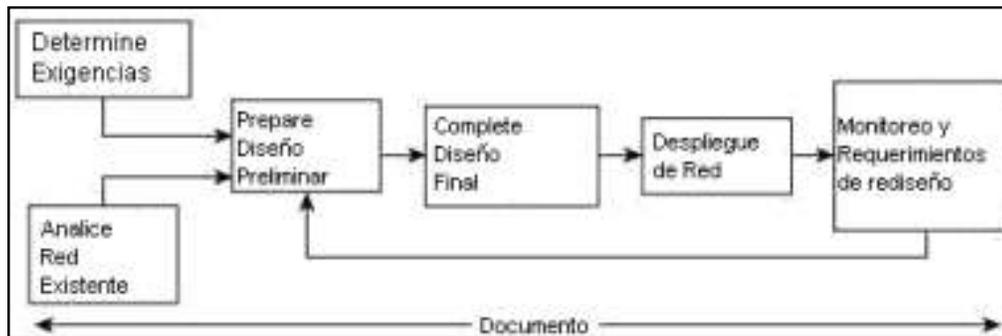


Figura 5.2 Tareas del Diseño de la Red

5.2 Estudio del diseño WLAN Colegio Internacional SEK-QUITO

Actualmente las instalaciones del Colegio Internacional SEK-QUITO cuentan con una estructura de red alámbrica en todas sus dependencias. Tanto los profesores como los estudiantes cuentan con esta estructura de red y con todos los servicios que brindan ésta: Internet, correo electrónico y capacidad de compartir archivos e impresoras.

A diferencia de los profesores que cuentan con sus estaciones de trabajo en la mayoría de las aulas o en las salas de profesores, los estudiantes cuentan con los laboratorios de informática, que muchas veces se satura o se encuentran ocupados, por esta razón se podría implementar una estructura de red inalámbrica complementaria para que puedan tener acceso a este servicio.

Adicionalmente a esto, existen otras áreas de mayor demanda para el servicio inalámbrico y de mayor necesidad, como son: la biblioteca y áreas de recreación. Estos lugares se encuentran sin ningún servicio de red adicionales por lo cual es indispensable que se les de conectividad y los servicios mencionados anteriormente.

Debido a las diferencias en la configuración, colocación y entorno físico de los componentes, cada infraestructura es una instalación única. Antes de instalar el sistema, debe realizarse una inspección de emplazamiento para determinar el uso óptimo de los componentes de red y para maximizar el alcance, la cobertura y el rendimiento de la

infraestructura. Las siguientes son algunas de las condiciones operativas y ambientales que se debe tener en consideración:

- **Velocidades de transmisión de datos**

La sensibilidad y el alcance son inversamente proporcionales a las velocidades de transmisión de datos (bits). El alcance de radio máximo se consigue con la velocidad más baja que sea factible.

- **Tipo de antena y ubicación**

Un factor importantísimo para maximizar el alcance de la radio es la configuración correcta de la antena. Como regla general, el alcance aumenta en proporción a la altura de la antena.

- **Entornos físicos**

Las áreas despejadas o abiertas proporcionan un mejor alcance de la radio que las áreas cerradas o probadas.

- **Obstáculos**

Una obstrucción física, como una estantería o un pilar, puede entorpecer el rendimiento de cualquier dispositivo WLAN. No se deben colocar dispositivos WLAN cerca de las superficies metálicas u otras superficies reflexivas

- **Materiales de construcción**

El material utilizado en la construcción influye mucho en la penetración de la señal de radio.

5.2.1 Matriz (Equipos-Solución)

En conjunto, a todo el cableado estructurado de la infraestructura del Colegio Internacional SEK-QUITO, lo vamos a llamar SISTEMA y a cada parte en la que se vaya a subdividir se lo llamará SUBSISTEMA. Se llama estructurado porque obedece a esta estructura definida. Las variaciones existentes son, el tipo de componentes utilizados según el ambiente donde se unen, como por ejemplo cables y elementos especiales para ambientes ácidos o húmedos.

Los componentes del sistema de red la interna son:

- **Puesto de Trabajo**

El concepto de Área de Trabajo está asociado al concepto de punto de conexión. Comprende las inmediaciones físicas de trabajo habitual (mesa, silla, zona de movilidad, etc.) del o de los usuarios. El punto que marca su comienzo en lo que se refiere a cableado es la roseta o punto de conexión. En el ámbito del área de trabajo se encuentran diversos equipos activos del usuario tales como teléfonos, ordenadores, impresoras, etc. La naturaleza de los equipos activos existentes condicionan el tipo de los conectores existentes en las rosetas, mientras que el número de los mismo determina si la roseta es simple (1 conector), doble (2 conectores), triple (3 conectores), etc.

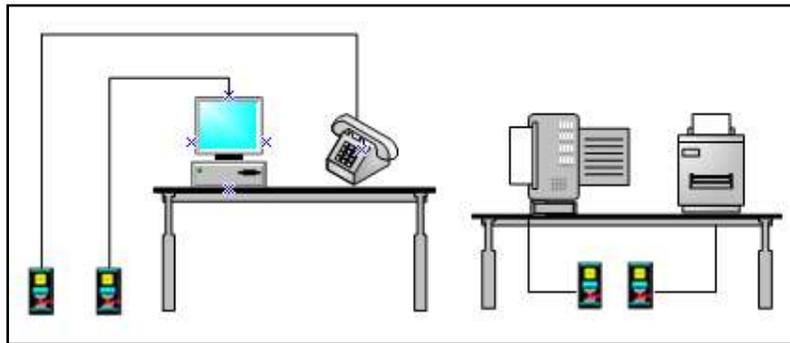


Figura 5.3 Diagrama de Puestos de trabajo

El cableado entre la roseta y los equipos activos es dependiente de las particularidades de cada equipo activo, por lo que debe ser contemplado en el momento de instalación de éstos.

- **Subsistema Horizontal**

Este subsistema comprende el conjunto de medios de transmisión (cables, fibras) que unen los puntos de distribución de planta con el conector o conectores del puesto de trabajo. Ésta es una de las partes más importantes de la red interna debido a la distribución de los puntos de conexión en la Institución. En esta red, los puntos de conexión están colocados donde el cliente necesita y se cablea por donde mejor conviene.

- **Subsistema Vertical**

Está constituido por el conjunto de cables que interconectan las diferentes plantas y zonas entre los concentradores (switch) y administración (también llamado troncal donde se encuentra el rack principal). Para el caso de las instalaciones del Colegio Internacional SEK-QUITO, este tipo de sistemas esta constituido del cableado de Fibra Óptica que da conectividad a los distintos puntos de la Institución.

Utilización:

- Para circuitos de ancho de banda vocal se usan hilos de pares de teléfono.
- Para uniones de datos entre plantas cercanas sin mucha demanda, cable de categoría.
- Cable de fibra óptica par la comunicación de datos entre plantas lejanas o con mucha densidad

El tipo de fibra óptica que se utiliza en esta red interior es fibra multimodo que es más barata y las pérdidas no son muy grandes a ser recorridos cortos. En los extremos de la fibra se colocan conectores ST adecuados, y éstos van al equipo de comunicaciones, que adaptan la señal eléctrica/óptica.

En definitiva, entre administradores de distintas plantas están conectados dos sistemas paralelos uno de pares y otro de fibra, así como enlaces con cable o mangueras de categoría 5. Los cables de pares y pares trenzados terminan en un repartidor o panel de parchado. Los cables de fibra óptica terminan en un repartidor con conectores ST.

Para el subsistema de administración se usan paneles de parchado para cables de par trenzado sin apantallar o fibra óptica. Estas regletas van por el techo lo que facilita la instalación del armario metálico, este armario permite albergar distintos dispositivos.



Figura 5.4 Servidores de la red del Colegio Internacional SEK-QUITO

De todos los equipos Wireless cotizados y que se analizaron las especificaciones técnicas, los más importantes son los pertenecientes a la serie de productos CISCO-Aironet 1310 para aplicaciones de ambientes exteriores (outdoor).

Los cuatro principales requisitos de diseño de una solución WLAN son las siguientes:

- **Alta disponibilidad**

Se consigue con la redundancia del sistema y del diseño adecuado del área de cobertura. La redundancia del sistema incluye AP redundantes en frecuencias separadas. El diseño adecuado del área de cobertura se refiere a la contabilidad de la itinerancia, la negociación automática de la tasa cuando la fuerza de la señal se debilita, la selección de la antena correcta.

- **Escalabilidad**

La escalabilidad se consigue soportando varios AP por área de cobertura que utilizan varias frecuencias y canales no superpuestos. Los AP también pueden efectuar el equilibrado de la carga.

- **Manejabilidad**

Se logra utilizando dispositivos WLAN empresariales que soportan protocolos de administración remota, como SNMP, SSH, Telnet y HTTP.

- **Interoperabilidad**

Se consigue adhiriéndose a los estándares (como por ejemplo, IEEE 802.11a, b y g), y participando en asociaciones de interoperabilidad como la Wi Fi Alliance. Además los dispositivos WLAN deben acatar las directrices locales, estatales y federales en cuanto a emisiones de RF.

5.2.2 Requisitos de Diseño

Para el análisis y diseño de la Red Inalámbrica del Colegio internacional SEK-QUITO, se ha tomado en cuenta los presentes objetivos financieros y técnicos.

5.2.2.1 Objetivo Financiero

Este proyecto como objetivo fundamental es reducir costos de operación a los señores jefes departamentales facilitando todas las actividades que hasta el día se realizan siendo estos procesos largos e inseguros, además se pretende entregar mejores facilidades para hacer un proceso de producción continuo, esto implica el aumento de la productividad, optimización de los recursos destinados a las personas involucradas; el costo inicial del proyecto será recuperado con el aumento de productividad de los usuarios jefes departamentales.

5.2.2.2 Objetivo Técnico

Teniendo en cuenta que la Institución es una de las principales entidades educativas en la ciudad de Quito, la responsabilidad de no quedarse rezagada en el uso de nuevas tecnologías y de optimizar sus recursos hace que busque nuevas formas que los usuarios accedan a la información que la empresa ofrece.

Permitir movilidad al personal de la Institución dentro de la misma y así poder mejorar los procesos para paso de información del resto de departamentos.

Buscar la mejor opción que se adapte a las necesidades de la Institución para brindar un servicio de calidad pero sobre todo seguir permitiendo el funcionamiento de todas las aplicaciones que son de primordial necesidad para que el negocio siga funcionando en su totalidad.

5.3 Situación Actual de la Red

Todos los componentes por los que se encuentra conformada la red de datos de la Institución serán listados a continuación, con su respectivo análisis y detalle.

Estos datos son tomados del Colegio Internacional SEK-QUITO, mirando siempre las falencias y fortalezas que la red de datos posee para así poder tener un resultado óptimo en el diseño que desea mostrar.

5.3.1 Servicios de Red que dispone el Colegio Internacional SEK-QUITO

a) Servicios Generales

- Control de acceso por dominio
- Servicio de Internet – Intranet
 - Navegación WEB:
 - Control de acceso por usuario
 - Control de acceso por contenido
 - Control de acceso por horario
 - Web – mail
 - POP3
- Compartir archivos

b) Tipo de conexión a Internet

- Ecuonet
- Enlace dedicado 2Mbps

c) Servidores de red

- Proxy
- Servidor de Correo + Dominio + DNS
- Servidor de Antivirus (PANDA(+ Dominio + Impresión
- Servidor de Aplicaciones (Departamento de contabilidad y cobranzas)
 - WEBSEK
 - LOGIC
- Servidor FTP + Terminal remota
- Servidor de Fax

5.3.2 Densidad de Usuarios

La cantidad de usuarios con la cual se encuentra funcionando la Institución se ubican diseminados por todos los pisos y bloques en la cual el Colegio Internacional SEK-QUITO tiene a su poder, los usuarios de la Institución por ser esta pionera a nivel nacional, tienen como factor común el constante movimiento por las sucursales así como por todas las áreas en la que se ven involucrados los usuarios.

5.3.3 Número de Puntos de Red y Host

En la siguiente tabla se muestra un detalle de todos los puntos de datos que se encuentran instalados y libres en cada bloque, así como también se muestran cuantos puntos de datos se encuentran siendo ocupados por los usuarios.

Bloque	Número de puntos de red	Hosts Habilitados
Administración	25	22
Bloque I	22	19
Bloque II	35	34
Bloque III	35	33
Bloque IV	45	44
Total	162	152

Tabla 5.1 Puntos de Datos y Hosts Habilitados

5.3.4 Requerimientos de los usuarios

Al ser una Institución cuyo objetivo es la educación de calidad a nivel nacional e internacional, los requerimientos de los usuarios es de encontrar datos e información en Internet, e incluso las visitas de alumnos y personal docente hacia las bases de datos para consulta e ingreso de notas si son muy comunes por tal motivo el uso de Internet necesita que tenga un buen ancho de banda. Por tal motivo la velocidad se incremento de 1Mbps a 2Mbps para que sea suficiente para los usuarios.

5.3.5 Escalabilidad de la Red Actual

Al momento de ser diseñada la red en sus inicios se tuvo en cuenta este factor, pero actualmente con el crecimiento de la Institución y por supuesto el incremento de personal y alumnos, los puntos de datos en cada bloque fueron escanciando hasta llegar al punto que ya no hay puntos de red disponibles en la mayoría de bloques en la que el Colegio Internacional SEK-QUITO funciona. Por lo cual no soportaría un incremento excesivo de usuarios pero si se tiene proyectado espacio para el incremento de usuarios de forma mesurada y planificada.

Los puntos de datos que se encuentran a disponibilidad del Colegio internacional SEK-QUITO son un total de 152 puntos, los cuales son únicamente para transmisión de datos, esta cantidad de puntos de datos abastecen sin ningún problema a la necesidad de la empresa, estos valores se pueden observar con detalle en la tabla 5.1.

5.3.6 Disponibilidad de la Red Actual

Por políticas de la Institución el mantenimiento que se proporciona a los equipos de comunicación y servidores se lo hace varias veces al año haciendo que el servicio de la red se vea comprometida durante una hora en el tiempo que se realiza dicho mantenimiento, este mantenimiento consiste en verificación de todos los puntos de datos de los equipos de comunicación así como actualizaciones de ciertos procedimientos o programas en los servidores.

El mantenimiento que se da a los equipos es el siguiente:

- Mantenimiento de equipos comunicación cada 6 meses.
- Servidores cada 3 meses
- La caída del servicio por motivos sin explicación es alrededor de 30 minutos cada 6 meses.

Horas laborales semanal	Horas laborales fin de semana	Total horas laborales mes	Horas laborales semestral	Red caída horas al semestre
12	7	67	12227.5	4.5

Tabla 5.2 Datos de disponibilidad de red actual

Con los datos explicados en la tabla 5.2, se consigue hallar el coeficiente de disponibilidad de la red 99,96321, este cálculo es hallado únicamente para la red sin acceso al Internet, es decir la red de datos o Intranet.

5.3.7 Calidad

A continuación se muestra los parámetros de calidad de la red de datos del Colegio Internacional SEK-QUITO, para observar los parámetros de throughput se presenta en la tabla 5.3 los elementos para el cálculo de este.

Archivo / Directorio	Tiempo (segundos)	Tamaño (Kbytes)
/PRH/LOGIC_user.dat	<0.001	0.052
/PRH/Dates.dat	<0.001	1.784
/PRH/Trig.dat	0.001	8.643
/PRH/Dat_ext.dat	0.001	9.8.42
/PRH/Time.dat	0.002	11.214

Tabla 5.3 Parámetros de throughput

En la tabla 5.3 se muestra la ubicación y nombre del archivo descargado, el tiempo de respuesta y el tamaño del archivo, gracias a las estadísticas de la tabla se puede mencionar que el retardo es de 0.003 segundos en la red.

En la figura 5.4 se muestra el tamaño de los paquetes en la red de datos del Colegio internacional SEK-QUITO en un periodo de tiempo de 10 minutos.

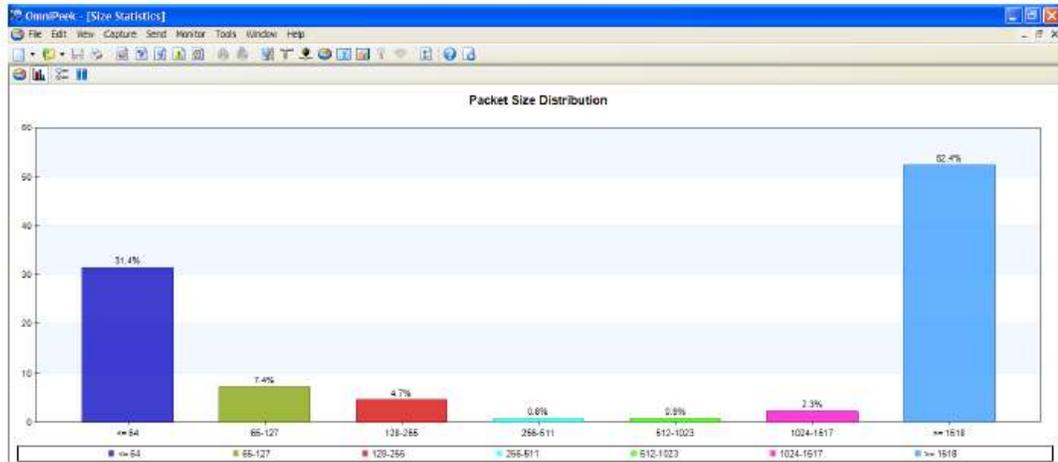


Figura 5.5 Tamaño de Paquetes

Como se muestra en la figura 5.5 se puede observar la utilización que tiene la red en un periodo de tiempo corto a horas pico, esta utilización es cuando se desea ingresar al servidor de LOGIC.

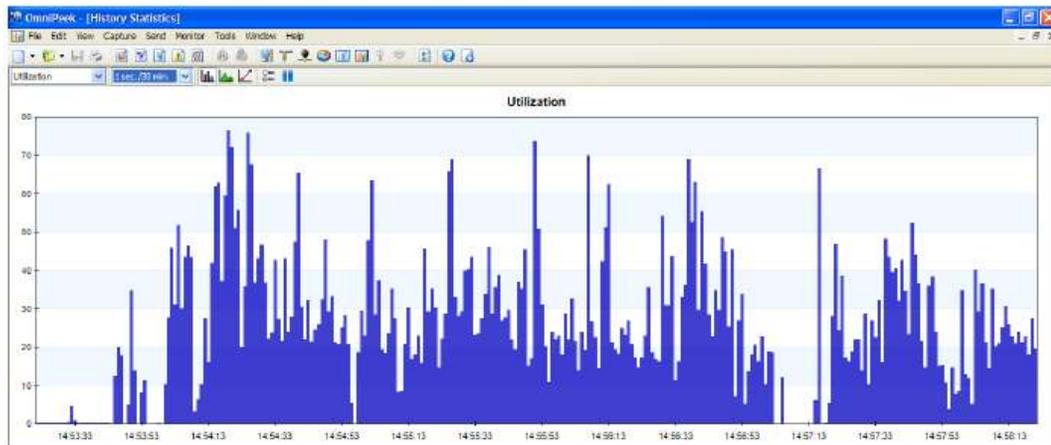


Figura 5.6 Utilización de la Red

5.3.8 Seguridad

La seguridad para la red de datos en el Colegio internacional SEK-QUITO ha sido dividida en dos partes, la seguridad lógica orientada a la seguridad de aplicaciones o de los servicios que la red actualmente provee y la seguridad física esta orientada a la protección de los equipos y el cableado de la red.

5.3.8.1 Seguridad Lógica

La seguridad lógica que se encuentra implementada en el Colegio Internacional SEK-QUITO, se encuentra definida según el recurso que se debe proteger, es decir existen normas de seguridad creadas para el uso del Internet, para accesos a aplicaciones propias de la Institución, para operaciones propias de cada computador. El objetivo es tener un control de la red y así poder otorgar o denegar permisos ya sea para acceso a la red como para impedir que los usuarios puedan instalar o desinstalar las aplicaciones y así poder estropear al normal funcionamiento del computador.

Cada usuario al momento de ingresar a su computador, se genera un script en el cual se genera una unidad y ésta apunta a una carpeta que se encuentra en el servidor de respaldos, cuya finalidad es que los usuarios coloquen toda la información relevante y si ocurre algún percance no se pierda nada.

El uso de Internet se encuentra limitado por 3 tipos de perfiles en general los cuales son según la necesidad u obligaciones que posee con la Institución, esto se lo hace pese a que todos los usuarios tienen acceso a Internet, a continuación se detalla cual es el nombre de usuario así como sus permisos y restricciones.

- **ALUMNOS:** Son la gran mayoría de los usuarios de la Institución, el uso del Internet viene dado y permitido por 3 factores fundamentales:
 - **Horario:** Los usuarios solo pueden navegar desde las 8:00 a.m. hasta 16:00 p.m.
 - **Navegación por tipo de archivo:** Se encuentra prohibido la descarga de documentos de audio o videos.

- **ADMINISTRATIVOS:** Este grupo de usuarios son todos los usuarios, dirigentes, jefes de estudios, personal del área administrativa, poseen la restricción en muy pocas categorías de acceso al Internet, y es para evitar el contagio con virus o troyanos.

- **DIRECTORES:** No poseen ninguna restricción en específica.

5.3.8.2 Seguridad Física

La seguridad de los equipos de comunicación y servidores no es la mejor ya que en el cuarto de equipos se encuentra las personas del área contable y el acceso a la habitación se ve comprometida por usuarios los cuales pueden ocasionar un daño irreparable en la red.

5.3.9 Topología Física

La topología física implica como se encuentra conectado físicamente los equipos de comunicación y las terminales; además se toma muy en cuenta de cómo es la distribución física de los usuarios así como el material de la institución donde se encuentra el colegio Internacional SEK-QUITO.

5.3.9.1 Dimensionamiento de las Instalaciones

Las instalaciones del Colegio Internacional SEK-QUITO, consta de cuatro bloques los mismos que tienen una dimensión de 480 metros cuadrados. Como se muestra en el Anexo , en el que se detalla el esquema de los bloques y el área de trabajo de los diferentes departamentos.

5.3.9.2 Distribución

La Institución en su edificación tiene distribuido en cada bloque los diferentes departamentos de la siguiente manera:

Bloque I:

- Departamento Administrativo
 - Director General
 - Jefe Administrativo
 - Secretarías
 - Copiadora / Impresora

- Departamento de Contabilidad
 - Jefe de Contabilidad
 - Auxiliar de Contabilidad
 - Tesorero
- Departamento de Admisiones
 - Jefe de Admisiones
- Departamento de Servicios
 - Jefe de Servicios
 - Auxiliar de Servicios
- Departamento de Preescolar
 - Jefe de estudios de Preescolar
 - Laboratorio de Computación de Preescolar
 - Sala de Profesores de Preescolar
 - Docentes de Preecolar
 - Impresora

Bloque II:

- Departamento de Primaria
 - Jefe de estudios de Primaria
 - Laboratorio de Computación de Primaria
 - Sala de Profesores de Primaria
 - Docentes de Primaria
 - Impresora

Bloque III:

- Biblioteca
 - Laboratorio de Computación Biblioteca
 - Secretaria de Primaria
 - Docentes de Primaria y Secundaria
 - Impresora

Bloque IV:

- Departamento de Secundaria
 - Jefe de estudios de Secundaria
 - Secretaria de Secundaria
 - Laboratorio de Computación de Secundaria
 - Sala de Profesores de Secundaria
 - Laboratorios de Secundaria
 - Docentes de Secundaria
 - Impresora

- Capacitación
Capacitación
Secretaria

5.3.9.3 Materiales que componen el área de trabajo de las instalaciones

Para poder realizar un diseño de red inalámbrico es importante identificar los materiales de los que esta hecho las instalaciones ya que esto permite determinar el nivel de pérdida de señal debido a la atenuación que se presentan por la característica de absorción de señal de los materiales.

Las instalaciones del Colegio Internacional SEK-QUITO que se encuentran ubicado en el sector de Monteserrín al norte de la ciudad, se encuentran construido en su totalidad de hierro y hormigón armado en su parte externa, con vidrios de color transparente.

Las divisiones de las oficinas en cada bloque se encuentran realizadas por modulares los cuales son de madera forrados con tela con una altura de 1.6 metros. La estructura de los modulares está conformada por armazones de aluminio. Los muebles de las oficinas son de madera.

El material del cual se encuentra en las instalaciones son de interferencia media, a excepción del aluminio que se encuentran en las armazones de los modulares que son de interferencia alta, pero ya que su presencia tiene un porcentaje no tan significativa se lo puede tomar como un nivel de atenuación media.

En resumen, no existen elementos que no puedan alterar la señal de los equipos inalámbricos en una forma representativa.

5.3.9.4 Esquema de Distribución física

En el Anexo A se muestra el esquema de la red del Colegio Internacional SEK-QUITO, este esquema es expuesto desde el punto de vista de conexión física.

La conexión de entre bloque y bloque, se lo realiza por medio de un switch 3Com 4800G el cual es de 48 puertos, en esta conexión se encuentra la granja de servidores. Las características del equipo de interconexión se puede observar en el Anexo B.

En los siguientes bloques las conexiones de los equipos se lo realiza con un switch 3Com SuperStack 3226 el cual posee 24 puertos, en estos bloques tienen sus propios equipos pues los otros equipos que se encuentran en Bloque I, no abastecen en puertos para cubrir las necesidades de los mismos. Las características del equipo de interconexión se puede observar en el Anexo C.

5.3.10 Topología Lógica

A continuación se describe como se encuentra conformada la topología de la red del Colegio internacional SEK-QUITO, esta distribución muestra de forma detallada como se encuentra jerarquizada la red de datos de la Institución.

5.3.10.1 Esquema de Red Actual

En el anexo E se muestra la topología que posee la red, este diseño es de tipo plano ya que no se encuentra capas o se distingue una jerarquía la cual no separa reglas de negocio en cada nivel.

El direccionamiento IP que posee la Institución es de tipo estático para el área administrativa e impresoras en red y para el resto de usuarios será mediante servidor DHCP, por tal motivo a los servidores se les asignado direcciones IP

estáticas, con una máscara de red 255.255.255.0. Esta distribución se le puede apreciar en la siguiente tabla:

Mapa de Red		
Nº	IP ADDRESS	NAME
1	192.168.5.254	Servidor 1
2	192.168.5.253	Servidor 2
3	192.168.5.201	Administración
4	192.168.5.202	Dirección
5	192.168.5.203	Admisiones
6	192.168.5.204	Recepción 1
7	192.168.5.205	Recepción 2
8	192.168.5.206	Rectorado
9	192.168.5.207	Almacén
10	192.168.5.208	BI
11	192.168.5.209	Contabilidad 1
12	192.168.5.210	Contabilidad 2
13	192.168.5.211	Caja 1
14	192.168.5.212	Caja 2
15	192.168.5.231	Recepción
16	192.168.5.232	Contabilidad 1
17	192.168.5.233	Pre Escolar
18	192.168.5.234	Secretaría Primaria
19	192.168.5.235	Biblioteca
20	192.168.5.236	Secretaría Secundaria
21	192.168.5.246	Música 1
22	192.168.5.247	Música 2
23	192.168.5.214	Jefatura Primaria
24	192.168.5.215	Secretaría Primaria
25	192.168.5.216	Biblioteca
26	192.168.5.217	Sicología
27	192.168.5.218	Jefatura Secundaria
28	192.168.5.219	Secretaría Secundaria
29	192.168.5.250	Sistemas
30	192.168.5.251	Sistemas

Tabla 5.4 IP's Fijas – Área Administrativa

Impresoras en Red		
Nº	IP ADDRESS	NAME
1	192.168.5.231	Recepción
2	192.168.5.232	Contabilidad
3	192.168.5.233	Sala de Profesores Preescolar
4	192.168.5.234	Secretaria Primaria
5	192.168.5.235	Biblioteca
6	192.168.5.236	Secretaria Secundaria

Tabla 5.5 IP's Fijas – Impresoras en Red

En el direccionamiento IP para los computadores que se conecten mediante DHCP se lo ha hecho desde 192.168.5.1 hasta 192.168.5.200. El servidor Web de la Institución se encuentra en la Institución. El dominio registrado para el sitio Web es www.sekquito.com/

5.3.11 Red inalámbrica

La red del Colegio Internacional SEK-QUITO no posee una red inalámbrica, por esto los usuarios solo pueden acceder a los servicios que provee la red conectándose por medio de patch cords.

5.4 Propuesta WLAN Colegio Internacional SEK-QUITO

El proyecto tiene como finalidad analizar y diseñar el segmento inalámbrico de la red de datos para la Institución, otorgando así la facilidad a los usuarios que necesitan tener movilidad con su equipo por las oficinas de la Institución, este segmento de la red se ve necesaria ya que los usuarios en sus constantes reuniones o movimientos por la Institución no pueden seguir con su trabajo normal.

El diseño que se presenta tiene como objetivo hacer que los usuarios continúen recibiendo todos los servicios que la red les proporciona,

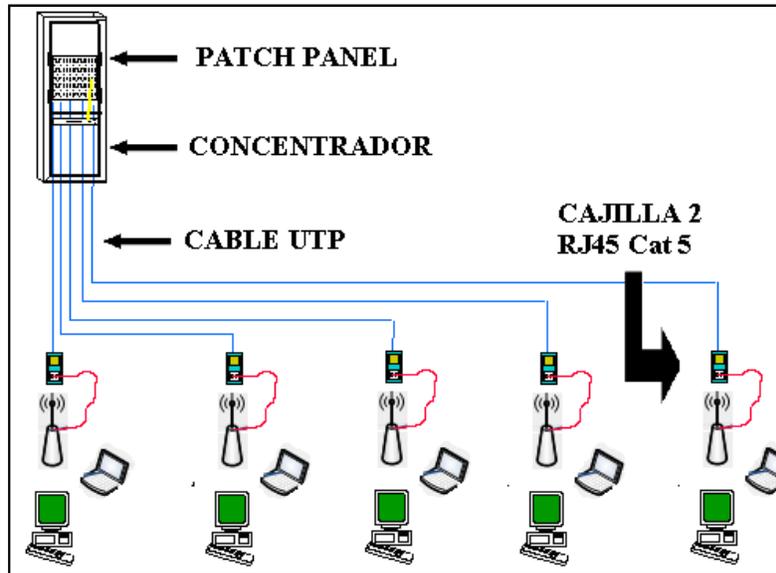


Figura 5.7 Esquema de Cableado Estructurado hacia los Puntos de Acceso

Criterios de Diseño de Red Inalámbrica

La propuesta de diseño de red que se presenta, tiene que cumplir los requisitos básicos de conectividad, es decir brindar los servicios que el segmento cableado lo hace; siempre brindando una buena transmisión y recepción de datos.

Brindar soporte a todos los usuarios que realicen uso de este segmento de red, sin ninguna preocupación de saber cuantos usuarios simultáneos se encuentran conectados a la red.

El segmento inalámbrico debe tener la capacidad de llegar a todas las áreas de trabajo de la empresa siempre brindando una óptima calidad de señal, detectar y evitar pérdidas de señal además.

Brindar seguridad en el segmento inalámbrico, con el fin de mantener todos los datos de la Institución en total confidencialidad.

Todos los aspectos de red antes mencionados pueden ser solucionados por medio de la buena ubicación de los puntos de acceso y la correcta configuración de los equipos evitando así un mal diseño.

Al diseñar una red inalámbrica, la cual va a dar servicio a cada bloque de las oficinas y aulas que la Institución actualmente posee tal como lo muestra la siguiente figura, es decir todos los puntos de acceso van a ser colocados de manera esquemática de forma horizontal, esto implica que se tiene que diseñar evitando la interferencia ²⁶co-canal e interferencias ²⁷inter-canales de las señales de los dispositivos inalámbricos y así limitar la capacidad de la red inalámbrica.

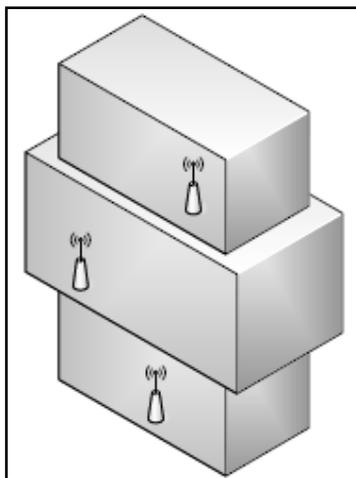


Figura 5.8 Puntos de acceso en cada bloque

Siguiendo los consejos para diseños de redes inalámbricas, se asignará canales para múltiples bloques, es decir se asignarán canales 1, 4, 7, 11 con el afán de que canales adyacentes usen el mismo canal, en la siguiente figura se presenta un esquema de asignación para múltiples bloques.

²⁶ **Co-canal:** Interferencia que se provoca al transmitir sobre el mismo canal.

²⁷ **Inter-canal:** Interferencia que se provoca sobre los canales adyacentes.

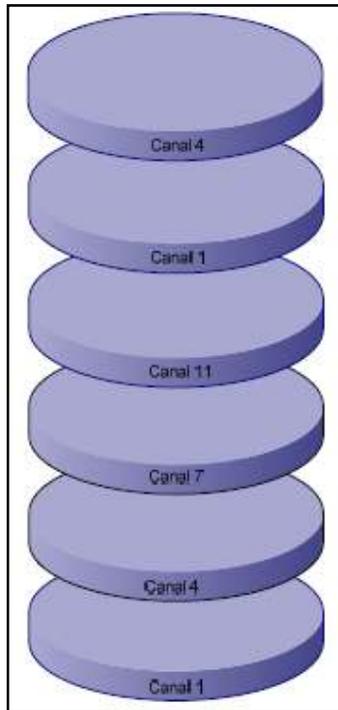


Figura 5.9 Asignación de canales múltiples bloques

Los puntos de acceso que se ubican en cada bloque serán ubicadas tomando referencia desde el bloque inferior al superior se muestra en la siguiente tabla:

Bloque	Canal
Bloque I	1
Bloque III	4
Bloque IV	7
Biblioteca	11
Bloque IV (Pasillo)	1

Tabla 5.6 Asignación de canales para cada bloque

Esquema De La Red Cableada hacia los puntos de acceso

En este punto se toma en cuenta la infraestructura del lugar, es decir sus dimensiones, facilidades y dificultades que pueda presentar para poder determinar el diseño óptimo para la implementación del cableado estructurado.

En el Anexo C se detalla el esquema de la distribución del cableado estructurado con sus respectivos puntos de red, concentradores, computadores y puntos de acceso que se requieren instalar.

Los dispositivos que utilizará el Cableado Estructurado diseñado es el siguiente:

- 03 concentradores Switch CISCO 10/100 de 16 puertos, los cuales ofrecen la potencia del Fast Ethernet a 100 Mbps. 03 Rack de pared LAN-PRO.
- 03 Patch Panel LAN-PRO de 24 puertos.
- 3 Patch Cords 1M
- Un rollo cable UTP NEXXT SOLUTIONS CAT 5e 100 pies
- Canaletas
- 3 back box y wall plate de 2 puertos

El cableado será de tipo horizontal, los puntos de red serán ponchados con la normativa EIA/TIA 568A. Las canaletas van distribuidas según los esquemas del Anexo A realizado para cada punto de acceso, en donde alojaremos los cables UTP Cat 5e que unirán los puntos de red con el rack de distribución más cercano con sus respectivos cajetines.

Análisis de Cobertura para el diseño y ubicación de los puntos de acceso en la infraestructura del Colegio Internacional SEK-QUITO

La infraestructura del Colegio Internacional SEK-QUITO tiene 4 bloques, los cuales reciben conectividad cada uno por medio de su red de fibra óptica. Debido al costo de los equipos de redes inalámbricas y a la cantidad de usuarios que tiene cada bloque dentro la red interna, se procedió a realizar el diseño basándose principalmente en esta característica, la cantidad.

Es decir que unos bloques serán los que proveerán conectividad así mismos como a las áreas adyacentes como es el caso de Administración, Preescolar y un parte de Primaria, con esto se logra reducir el costo de instalación de la red inalámbrica. Los bloques con mayor número de usuarios o críticos son: el Bloque IV (Secundaria), y el Bloque III (Área de la biblioteca).



Figura 5.10 Bloque I (Administración y Preescolar)



Figura 5.11 Bloque II y III (Primaria)



Figura 5.12 Bloque IV (Secundaria)



Figura 5.13 Biblioteca y Áreas de recreación

El diseño se basa en colocar un Punto de Acceso es un punto céntrico con la ayuda de los planos arquitectónicos de los bloques antes mencionados y mediante computadores portátiles y computadoras con tarjetas inalámbricas verificar en cada punto de trabajo de la infraestructura los siguientes parámetros:

- Áreas de cobertura
- Velocidad de transmisión
- Fuerza de la señal
- Calidad de la señal

5.4.1 Ubicación de puntos de acceso

Es importante realizar una inspección del emplazamiento. Antes de instalar los AP de WLAN, debe investigar unas cuantas cosas acerca de la instalación de la infraestructura:

- Radiofrecuencia
- Ubicación de la instalación
- Número de conexiones que se servirán
- Rendimiento
- Cobertura de la WLAN

Una buena inspección del emplazamiento ayuda a determinar lo siguiente:

- Viabilidad de la cobertura deseada
- Interferencia de radiofrecuencia
- Ubicaciones óptimas para la instalación

- Espaciado entre AP
- Limitaciones de la conectividad cableada

La inspección de un emplazamiento nos va a permitir instalar correctamente la WLAN para tener un acceso inalámbrico consistente y fiable. Un ingeniero debe tener conocimientos de los equipos inalámbricos y cableados, como hubs, routers, switches y cualquier medio alternativo.²⁸

La inspección de un emplazamiento también nos va a servir para determinar el número de AP que son necesarios por toda la instalación para conseguir la cobertura y el ancho de banda deseados. La inspección determina la ubicación de esos AP y detalla la información necesaria para realizar la instalación.

Además una inspección del emplazamiento determina la viabilidad de la cobertura deseada en función de los obstáculos como las limitaciones de la conectividad cableada, los ruidos derivados de la radio y los requisitos de la aplicación. La definición de esta viabilidad permite al cliente instalar correctamente la WLAN y tener acceso inalámbrico consistente y fiable.

La infraestructura del Colegio Internacional SEK-QUITO tiene 4 bloques, los cuales reciben conectividad cada uno por medio de su red de fibra óptica. Debido al costo de los equipos de redes inalámbricas y a la cantidad de usuarios que tiene cada bloque dentro de la red interna, se procedió a realizar el diseño basándose principalmente en esta característica la cantidad. Es decir que unos bloques serán los que proveerán conectividad así mismos como a las áreas adyacentes como es el caso de Administración, Preescolar y un parte de Primaria, con esto se logra reducir el costo de instalación de la red inalámbrica. Los bloques con mayor número de usuarios o críticos son: el Bloque IV (Secundaria), y el Bloque III (Área de la biblioteca).

Basados en el estándar del hardware CISCO, los sistemas outdoor router permiten crear nuevas infraestructuras de red inalámbricas o expandir infraestructuras inalámbricas existentes. Los sistemas CISCO outdoor están basados en los siguientes componentes:

²⁸ JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.

- Central Outdoor Routers (COR's)
- Remote Outdoor Routers (ROR's)
- Outdoor Router Client (ORC's)

Los productos Outdoor Routers (OR) son una completa solución en hardware y software para enlaces outdoor inalámbricos de alta velocidad incluyendo acceso inalámbrico a Internet. Los OR's a más de contar con una interfase Ethernet alámbrica, pueden soportar dos interfases inalámbricas, pudiendo así tener los siguientes modos de operación:

- Central Outdoor Router
- Remote Outdoor Router
- IEEE 802.11b Access Point

El diseño se basa en colocar un Punto de Acceso, que es un punto céntrico con la ayuda de los planos arquitectónicos de los bloques y mediante computadores portátiles y computadoras con tarjetas inalámbricas de verifican cada punto de trabajo de la infraestructura los siguientes parámetros:

- Áreas de cobertura
- Velocidad de transmisión
- Fuerza de la señal
- Calidad de la señal

Un punto a tomar en cuenta es que existe también paredes de concreto que separan a los diferentes departamentos, dependencias varias, aulas, causando atenuación de la señal. Cabe recalcar que la solución más óptima es colocar dos puntos de acceso en áreas céntricas de los bloques para proveer mejor conectividad, mantener las tasas de transmisión altas y cubrir las necesidades de cobertura.

Con esta breve descripción de los equipos y de su utilidad para aplicaciones en ambientes exteriores e interiores, en la siguiente tabla, se indican todos los equipos existentes con los cuales se va a diseñar la red inalámbrica y su respectiva ubicación:

Descripción de los Equipos			
Item	Equipo	Descripción	Cantidad
1	CISCO-AIRONE T serie 1310	Canales de operación: 802.11b/g: 11(EEUU), 13 (Europa), 14 (Japón) Frecuencia: 2.4 GHz Encriptación: 40 bit (=64 bit) 128 bit WLAN Standards: IEEE 802.11g/b	3
2	LINKSYS WAP54G	Antena: Detachable Antenna x 2 Canales de operación: 802.11b/g: 11(EEUU), 13 (Europa), 14 (Japón) Frecuencia: 2.4 GHz Encriptación: 40 bit (=64 bit) 128 bit	2
3	Antena Omnidireccional	Para techo (AIR-ANT1728) 5,2 dBi	3
4	Antena Dipolar	2,2dBi	2

Tabla 5.7 Descripción de los Equipos

Ubicación Equipos		
	Equipo	Ubicación
1	CISCO-AIRONET serie 1310	Bloque I
1	CISCO-AIRONET serie 1310	Bloque III
1	CISCO-AIRONET serie 1310	Bloque IV
1	LINKSYS	Biblioteca
1	LINKSYS	Bloque IV (Pasillo)

Tabla 5.8 Ubicación de los Equipos

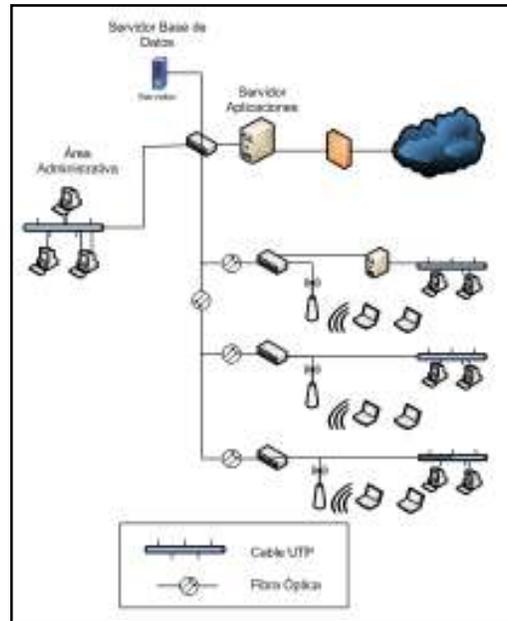


Figura 5.14 Ubicación de los Equipos

5.4.2 Mapas de Cobertura

Las distancias tipo para estos dispositivos Wireless 802.11g, son de 100 metros para espacios cerrados y hasta 400 metros en espacios abiertos. Como podremos comprobar en las pruebas, lo de 100 metros en espacios cerrados es muy cuestionable si, como en nuestro caso, tenemos que atravesar paredes de 50 centímetros de grosor. Es importante averiguar el rendimiento que necesitan los usuarios para determinar la ubicación de los AP. Los requisitos de ancho de banda para la conectividad inalámbrica determina potencialmente el número de AP necesarios. Si se requiere una velocidad constante y esa velocidad es bastante alta, la cobertura será inferior y se necesitarán muchos AP.

En algunos entornos, el ancho de banda y la carga del AP son factores de diseño determinantes para la implementación de una WLAN. Una forma de asegurarse de que una pequeña área de usuarios utiliza el AP seleccionado consiste en manipular la configuración de potencia del AP para ajustar el tamaño de la celda. Este ajuste crea células que cubren áreas específicas. Los niveles de potencia se pueden controlar tanto en el AP como en los clientes. Como se observa en el diseño lógico (Anexo A), los puntos de acceso van conectados a los puertos de los switch del Backbone de fibra óptica de los bloques: uno, tres y cuarto; los que darán conectividad vía inalámbrica a los equipos ya sean computadoras portátiles o computadoras personales.

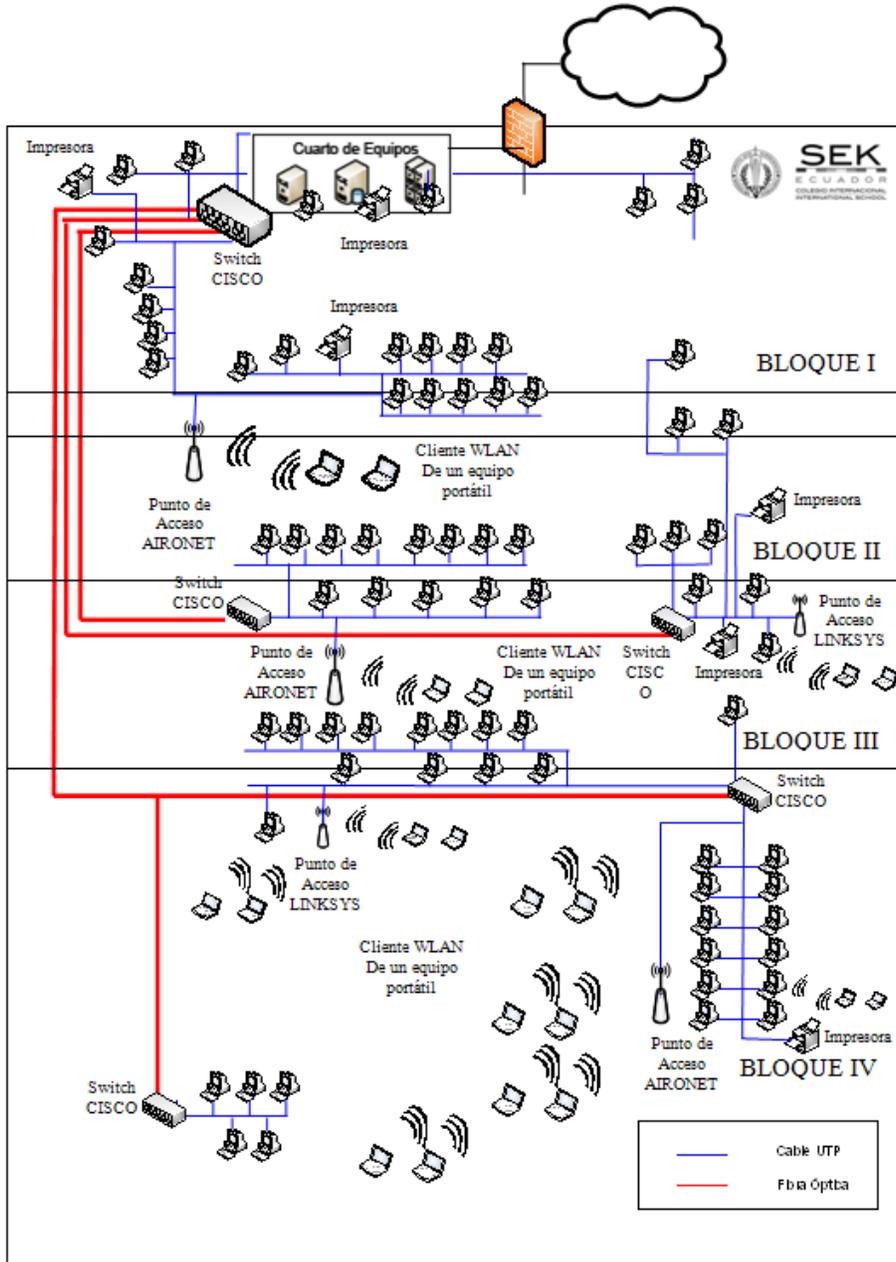


Figura 5.15 Diseño físico WLAN propuesto para el Colegio Internacional SEK-QUITO

Los mapas de cobertura son gráficos que indicarán la propagación de la señal de los equipos inalámbricos de acuerdo a las características de las antenas, en nuestro caso se utilizó equipos con características promedio como las siguientes: estándar 802.1 g, velocidad de transmisión de hasta 108 Mbps, tecnología de modulación OFDM y seguridad inalámbrica PSK, WEP 128 bit y WEP 64 bit.

Para la medición de nivel de señal se utilizó el software Wireless Monitor, el mismo que proporciona la siguiente información:

- Nombre SSID
- MAC del punto de acceso
- Canal en el que se encuentra funcionando el punto de acceso
- Tipo de dispositivo inalámbrico
- Relación Señal a Ruido
- Fuerza de la señal
- Intervalo de Beacon enviado

Para la realización de las pruebas de estado de conexión se usó el comando ping el cual sirve para comprobar el IP alcanzado y registrar resultados como el tiempo exacto que tardan los paquetes de eco en ir y volver a través de la red hacia un equipo remoto, pérdidas, tiempos máximos y mínimos, este tiempo es el mismo que se tomará en cuenta en las mediciones de monitoreo a realizarse.

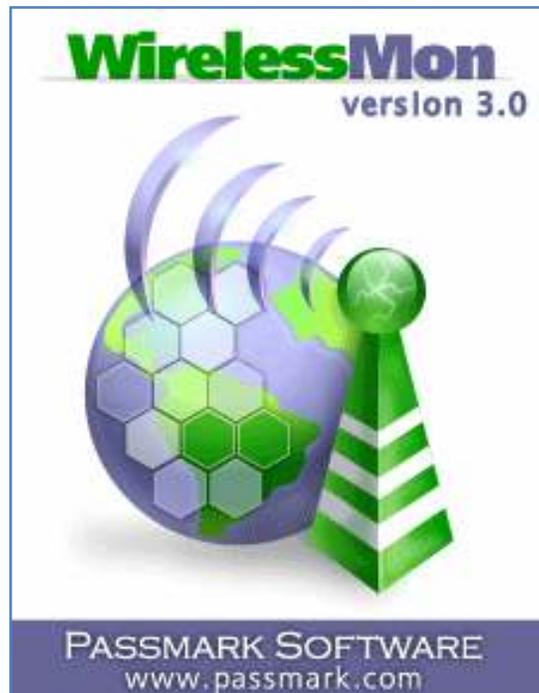


Figura 5.16 Software para el monitoreo del diseño de la red WLAN

Este software se encuentra libre en el Internet, presenta una interfaz como la que ilustra a continuación y permite de una manera rápida e interactiva saber algunos parámetros de las redes inalámbricas.

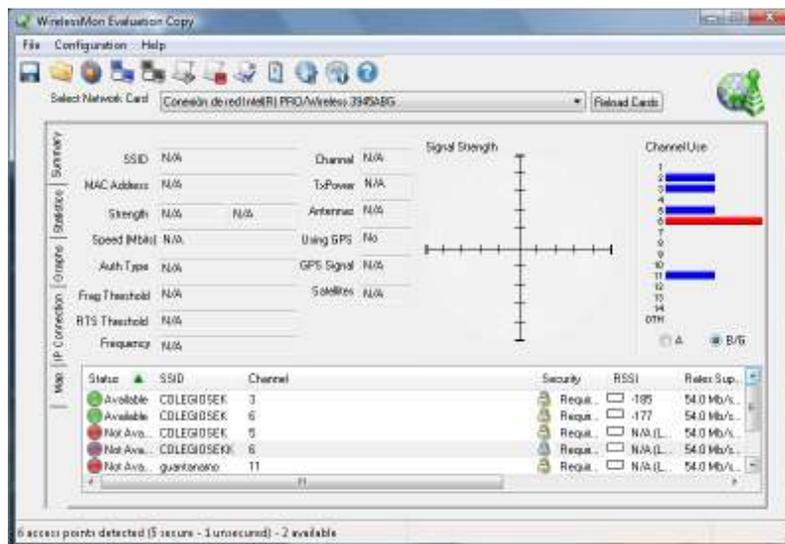


Figura 5.17 Interfaz gráfica del software utilizado para mediciones

Como son: el canal que está trabajando el punto de acceso, la frecuencia de operación, el nombre SSID y la fuerza de la señal por medio de un indicador.

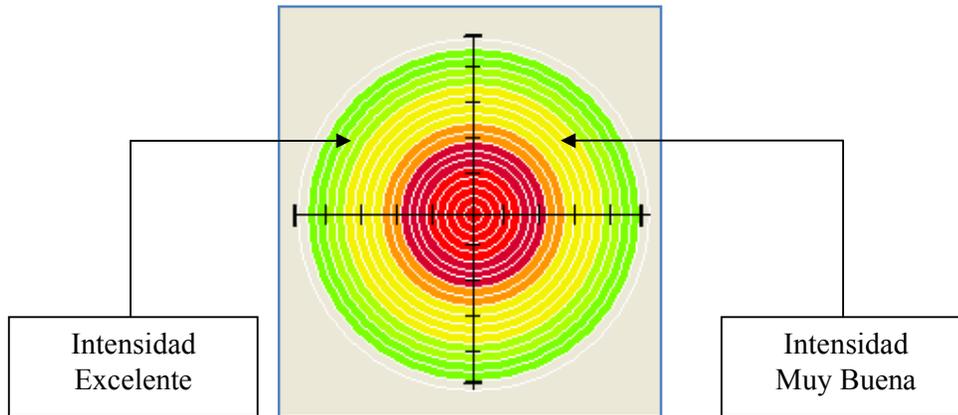


Figura 5.17 Interfaz gráfica del software utilizado para mediciones

También presenta si el punto de acceso utiliza alguna encriptación, el tipo de modulación utilizada y enlista todos los puntos de acceso disponibles dentro del área de cobertura.

5.4.2.1 Cobertura Horizontal

Esta cobertura fue analizada de acuerdo al bloque en el que se va a ubicar el AP ya que la topología de cada bloque es diferente al igual que la densidad de usuarios.

Se realizaron mediciones en varias distancias de la ubicación del AP mismo que fue situado en el centro del espacio que se desea dar cobertura a los usuarios. El resultado obtenido de varias pruebas fue que se enviaron 40 paquetes de datos en un tiempo promedio, esto se presenta en los gráficos de monitoreo en el siguiente capítulo.

Con esto se puede ver que la señal se va degradando mientras más lejos se encuentra el equipo del AP, pero sin embargo se sigue manteniendo una recepción buena para la utilidad que se le va a dar a la red, además se pudo determinar los niveles de velocidad

de conexión para la Institución, los mismos que son detallados a continuación en las siguientes tablas:

BLOQUE I, II y ADMINISTRACIÓN		
DISTANCIA	3 a 6 mts.	6 a 9 mts.
VELOCIDAD	108 Mbps	108 Mbps
POTENCIA	-36 dBm	-44 dBm

Tabla 5.9 Medición cobertura horizontal Bloque I, II y Administración

BLOQUE III		
DISTANCIA	3 a 6 mts.	6 a 9 mts.
VELOCIDAD	108 Mbps	108 Mbps
POTENCIA	-35 dBm	-45 dBm

Tabla 5.9 Medición cobertura horizontal Bloque III

BLOQUE IV		
DISTANCIA	3 a 6 mts.	6 a 9 mts.
VELOCIDAD	108 Mbps	108 Mbps
POTENCIA	-34 dBm	-45 dBm

Tabla 5.10 Medición cobertura horizontal Bloque IV

BIBLIOTECA		
DISTANCIA	0 a 3 mts.	3 a 6 mts.
VELOCIDAD	108 Mbps	108 Mbps
POTENCIA	-20 dBm	-34 dBm

Tabla 5.11 Medición cobertura horizontal BIBLIOTECA

BLOQUE IV (PASILLO)		
DISTANCIA	0 a 3 mts.	3 a 6 mts.
VELOCIDAD	108 Mbps	108 Mbps
POTENCIA	-23 dBm	-34 dBm

Tabla 5.12 Medición cobertura horizontal Bloque IV (PASILLO)

5.4.2.2 Direccionamiento IP para equipos inalámbricos

Para el diseño de la nueva red inalámbrica se debe asignar direcciones IP estáticas a los puntos de acceso y para ello como se muestra en la siguiente tabla:

Tipo	Ubicación	Dirección IP.
Punto de acceso	Bloque I	192.168.5.229
Punto de acceso	Bloque III	192.168.5.228
Punto de acceso	Bloque IV	192.168.5.227
Punto de acceso	Biblioteca	192.168.5.226
Punto de acceso	Bloque IV (Pasillo)	192.168.5.225

Tabla 5.13 Direcciones IP para equipos inalámbricos

5.4.2.3 Seguridad

Para otorgar seguridad al segmento inalámbrico de la red de datos se vio necesaria la implementación de un servidor el cual se levantarán dos servicios para proporcionar gestión y seguridad al segmento inalámbrico.

El primer servicio es SYSLOG el cual se encargará de llevar un histórico de todas las acciones o actividades que se generan en los equipos inalámbricos, con ello se pretende detectar algún intruso o algún ataque que han sufrido los equipos inalámbricos. El tipo de autenticación que se va a realizar es por medio de WPA el cual utilizará para la encriptación el protocolo de autenticación extensible EAP y conjuntamente utilizará TLS para la seguridad de transmisión.

5.4.2.4 Resumen de segmento inalámbrico

Característica	Descripción
SSID	COLEGIOSEK
Canal	Depende del bloque de ubicación del punto de acceso
Autenticación	WPA
Protocolo de autenticación	EAP
Frase secreta	MMJle6782

Tabla 5.14 Resumen de segmento inalámbrica

5.5 Administración WLAN Colegio Internacional SEK-QUITO

Son los puntos de distribución o repartidores donde se interconectan los diferentes subsistemas y están ubicados en el Área de Administración.

- **Administración principal**

Este subsistema es el repartidor principal de Colegio Internacional SEK-QUITO, y es donde llega el cable de la red pública y donde se está ubicada la central y todos los equipos servidores.

- **Administración de planta**

Los componen los pequeños repartidores que se ubican por las distintas plantas de la Institución.

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Para hacer más eficiente la administración de la red, se dividen en dos partes así:

- Monitoreo, o proceso de observar el comportamiento de la red y de sus componentes, para detectar problemas y mejorar su funcionamiento.
- Control, o proceso de cambiar el comportamiento de la red en tiempo real ajustado parámetros, mientras la red está en operación, para mejorar el funcionamiento.

Sus objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos apropiados
- Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- Reducir costos por medio del control de gastos, y de mecanismos de cobro.

- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

El sistema de administración de red opera bajo los siguientes pasos básicos:

- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.
- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.
- Transportación de la información del equipo monitoreando al centro de control.
- Almacenamiento de los datos coleccionados en el centro de control.
- Análisis de parámetros de los datos coleccionados en el centro de control.
- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

5.5.1 Elementos involucrados en la Administración de Red

- **Objetos:** son los elementos de más bajo nivel y constituyen los aparatos administrados.
- **Agentes:** un programa o conjunto de programas que colecciona información de administración del sistema en un nodo o elemento de la red. El agente genera el grado de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de:
 - Notificación de problemas
 - Datos de diagnóstico
 - Identificador del nodo
 - Características del nodo

- **Administrador del sistema:** es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

5.5.2 Operaciones de la Administración de Red

La administración de fallas maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

- Detección de fallas
- Diagnóstico del problema
- Seguimiento y control

- **Control de Fallas**

Esta operación tiene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

- **Administración de cambios**

La administración de cambios comprende la planeación, la programación de eventos e instalación.

- **Administración del comportamiento**

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye el número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

- **Servicios de contabilidad**

Este servicio provee datos concernientes al cargo por uso de la red. Entre datos proporcionados están los siguientes:

- Tiempo de conexión y terminación
- Número de mensajes transmitidos y recibidos
- Nombre del punto de acceso al servicio
- Razón por la que terminó la conexión

- **Control de inventarios**

Se debe llevar un registro de los nuevos componentes que se incorporen a los de los movimientos que se hagan y de los cambios que se lleven a cabo

- **Seguridad**

Autorización de acceso a los usuarios, es decir, solo personal autorizado

- **Confidencialidad**

Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

La administración de la red del Colegio Internacional SEK-QUITO se encarga principalmente de asegurarla correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos así como de administración remota de fallas, configuración, rendimiento, seguridad e inventarios.

5.5.3 Funciones de Administración definidas por OSI y aplicadas en la red del Colegio Internacional SEK-QUITO

Las cinco funciones de administración básicas definidas por OSI son las siguientes:

- **Configuración**

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red.

- **Fallas**

La función de fallas incluye la detección, el aislamiento y la corrección de fallas.

- **Contabilidad**

La función de contabilidad permite el establecimiento de cargos a usuarios por uso de los recursos de la red

- **Comportamiento**

La función de comportamiento mantiene el comportamiento de la red en niveles aceptables.

- **Seguridad**

La función de seguridad provee mecanismos para autorización, control de acceso, confidencialidad y manejo de claves.

Capítulo 6

6 IMPLEMENTACIÓN DE WLAN COLEGIO INTERNACIONAL SEK-QUITO

En este capítulo se describirá la información relacionada con la instalación y configuraciones básicas de un punto de acceso (AP), y de los servicios que estos poseen.

6.1 Implementación WLAN Colegio Internacional SEK-QUITO

802.11g opera exactamente en la misma banda de 802.11b es decir en la banda de 2.4 GHz. Esta banda proporcionada para esta tecnología (802.11g), también da como resultado distintas dificultades, como el alcance limitado de las ondas, por no ser infinito y estar restringido a un área determinada, normalmente está definido entre 10 y 300 metros, dependiendo de factores como la potencia del punto de acceso, apantallamiento de la señal, etc. Otro inconveniente que sobresale es la seguridad, uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi Fi, porcentajes muy elevados indican la instalación de redes que por la simplicidad de su implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes abiertas, sin proteger la información que por ellas circulan. La industria LAN inalámbrica comenzó la transmisión desde 900 MHz hasta 2.4 GHz a mediados de los noventa.

El estándar 802.11g proporciona una velocidad de datos máxima de 54 Mbps, no tan alta como la de Ethernet (100Mbps), pero sustancialmente más grande que 802.11b y mucho más adecuada para las necesidades de desempeño de las empresas actuales como es el Colegio internacional SEK-QUITO.

Como propósito de ilustración y sin tomar en cuenta los aspectos de despliegue físico y el número de usuarios, la siguiente tabla lista la capacidad de los distintos estándares, la cual se deriva de multiplicar la velocidad de datos máxima por el número de canales.

Estándares Básicos			
Estándar	Velocidad	Canales	Capacidad
802.11b	11 Mbps	3	333 Mbps
802.11g	54 Mbps	3	162 Mbps
802.11a	54 Mbps	8	432 Mbps

Tabla 6.1 Estándares 802.11, números de canales y capacidad

Una vez más, esta es una simplificación que no toma en cuenta la diferencia entre velocidad de datos y el rango. Tampoco considera la parte práctica de los aspectos físicos o financieros de diseñar una LAN inalámbrica para un desempeño de 54 Mbps. No se quiere sugerir que un solo usuario podría disfrutar de un enlace que proporciona una velocidad de datos de 162 Mbps. Lo que se desea ilustrar es que el número de canales disponibles tiene un impacto enorme en la capacidad de la red al igual que la velocidad de datos.

El beneficio de 802.11g es un desempeño más alto además de ofrecer la compatibilidad con productos anteriores. Además el esbozo de la especificación 802.11g también señala que los dispositivos 802.11g deben soportar el tipo de transmisión DSSS y los tipos de modulación BPSK, QPSK, CCK de 802.11b. Este requerimiento junto con el hecho de que 802.11g opera en la misma banda de frecuencia de 2.4 GHz que usa 802.11b proporciona compatibilidad con los productos anteriores.

Debido a que 802.11g opera en la misma porción del espectro de frecuencia que 802.11b, 802.11g usa exactamente las mismas antenas que 802.11b. Esto significa que 802.11g ofrecerá una línea muy completa y variada de antenas. Esto también significa que los usuarios tendrían una gran posibilidad de dejar en su lugar las antenas de 2.4 GHz y cables que ya están instalados para 802.11b y simplemente reemplazar los puntos de acceso 802.11b con los 802.11g lo cual reduce de manera significativa el costo de una instalación en términos de mano de obra y equipos.

Sin embargo, junto con la característica importante de compatibilidad con productos anteriores también aparece el contratiempo clave de 802.11g. Debido a que opera en la misma banda de 2.4 GHz que usa 802.11b, 802.11g está sujeto a la capacidad y

problemas de interferencia de 802.11b., la banda de 2.4 GHz solo permite el uso de 3 canales. La banda está saturada con dispositivos 802.11b y teléfonos inalámbricos además del uso de dispositivos Bluetooth.

6.1.1 Configuración de los puntos de acceso

Un punto de acceso actúa como punto de comunicación central para los usuarios de una red inalámbrica. Un AP puede enlazar redes cableadas e inalámbricas. Es importante mantener una configuración sencilla hasta conseguirse la conectividad. En instalaciones grandes se pueden configurar varios AP para que los usuarios inalámbricos puedan moverse entre ellos sin interrupción. Los AP de CISCO también proporcionan seguridad, monitorización y manejabilidad a nivel empresarial. Por último, un AP puede actuar como repetidor inalámbrico, o como un punto de extensión de la red inalámbrica.

A continuación examinaremos la información sobre la instalación y las configuraciones básicas de un punto de acceso CISCO, que son los equipos que utilizaremos según el diseño WLAN en el Colegio Internacional SEK-QUITO planteado.

El control y la configuración de un AP se pueden realizar a través de la línea de comandos y de interfaces web. La administración también se puede realizar utilizando protocolos tradicionales, como SNMP (Simple Network Management Protocol). La variedad de opciones de antena pueden proporcionar un mayor alcance y una velocidad más alta, dependiendo de la instalación. Un AP puede ser de una sola banda, aunque también puede ser de banda doble.

Un AP tiene las siguientes características:

- **Administración de redes integrada**

El soporte SNMP y de syslog para interactuar con la administración de la actual es esencial. También se necesita una administración web funcional o desde la línea de comandos.

- **Seguridad del Sistema**

Debe ser posible restringir el acceso al sistema de administración del AP a una lista de usuarios. El cifrado debe estar soportado, así como la Privacidad equivalente al cableado (WEP).
- **Filtrado**

Los protocolos de filtrado para evitar o permitir el uso de protocolos específicos a través del AP. También deben existir controles para el envío y filtrado de paquetes de unidifusión y multidifusión.
- **Firmware**

El firmware debe ser actualizado y debe soportar la copia y el restablecimiento de una configuración.
- **Asignación de reserva o en espera**

Esta característica permite que el AP actúe como copia de seguridad de otro AP a fin de proporcionar una conectividad ininterrumpida a la red.
- **Modo universal para los viajeros internacionales**

La regulación de la frecuencia varía ligeramente de unas partes a otras. Esta función permite que un visitante japonés que está utilizando el modo universal en un dispositivo cliente pueda asociarse a un AP en EEUU y cambiar automáticamente a la configuración regional.
- **Equilibrado de la carga**

Esta característica direcciona automáticamente los dispositivos cliente al AP que ofrece la mejor conexión a la red, en base a factores como el número de usuarios, las tasas de error por bits, ancho de banda de radio disponible, y fuerza de la señal, para mejor comprensión en el Anexo E tenemos el manual y especificaciones técnicas de los equipos a utilizar Aironet 1310 de CISCO.



Figura 6.1 Punto de Acceso Aironet 1310 de CISCO

Conexión al Punto de Acceso

Los pasos a seguir para la conexión de un AP:

- Conecte el cable Ethernet RJ45 al puerto Ethernet de la parte posterior del AP
- Conecte el otro extremo del cable Ethernet a la LAN Ethernet 10/100
- Conecte el adaptador de corriente a un receptáculo de alimentación adecuado
- Inserte el conector de alimentación en la parte posterior del AP. Al ponerse en marcha, los tres LED del AP parpadean lentamente siguiendo una secuencia ámbar, rojo y verde. Esta secuencia tarda unos minutos en completarse



Figura 6.2 Conectores Aironet 1310 de CISCO

Indicadores LED

Los LED de un AP informan de su estado. Cuando el AP está encendido, normalmente los tres LED parpadean. Tras su inicio, los colores de los LED representan lo siguiente:

- Los LED verdes indican una actividad normal.
- Los LED ámbar indican errores o avisos.
- Los LED rojos significan que la unidad no está funcionando correctamente o está actualizándose.

Características de la Antena omnidireccional de 5,2 dBi de CISCO para techo

La antena omnidireccional de 5,2 dBi de CISCO para techo, está diseñada para su instalación en la rejilla metálica de un techo suspendido. Debe instalarse con el extremo del agujero apuntando hacia el techo. Esta antena no esta diseñada para lugares con techos bajos, debido a la posibilidad de tropezar con ella y poder dañarla. Esta antena está polarizada verticalmente, pero tiene un haz ligeramente inclinado hacia abajo, lo que permite que su patrón de cobertura abarque las áreas situadas debajo del techo.



Figura 6.3 Antena omnidireccional de 5,2 dBi de CISCO para techo

- **Patrón de radiación**

El patrón de radiación es un gráfico o diagrama polar sobre el que se representa la fuerza de los campos electromagnéticos radiados por una antena. La forma del patrón de radiación depende del modelo de antena. Las antenas omnidireccionales emiten en todas direcciones y tienen menor alcance que las antenas direccionales. El patrón de radiación puede ser representado en dos planos perpendiculares conocidos como azimut y elevación.

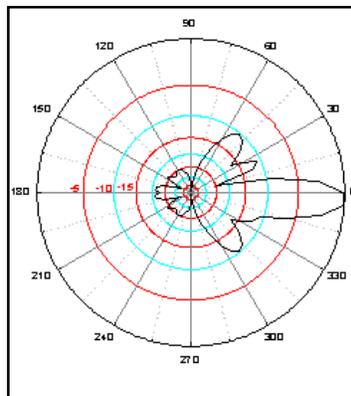


Figura 6.4 Ejemplo de patrón de radiación Azimut de la antena

- **Polarización**

El campo de radiación que emite desde un transmisor 802.11 tendrá tanto un elemento electromagnético como un magnético. En las representaciones clásicas o tradicionales los elementos electromagnéticos se conocen como el campo E y el campo magnético se denomina campo H dentro de un campo de radiación, los elementos E y H de la radiación de energía desde una fuente se mueven en una dirección que es perpendicular a la dirección del campo de radiación.

Cuando el campo E está orientado en forma vertical, se dice que el campo de radiación tienen una polarización vertical. Si el campo E está orientado horizontalmente, se dice que el campo de radiación tiene una polarización horizontal. También existe un fenómeno conocido como polarización circular, lo que significa que el campo E gira. Lo importante de observar acerca de la polarización es que tanto la antena transmisora como la receptora deben tener la misma polarización, con el fin de proporcionar el desempeño máximo de un enlace de radio.

Las formas de polarización más comunes son las siguientes:

- **Vertical**

Cuando el campo eléctrico generado por la antena es vertical con respecto al horizonte terrestre.

- **Horizontal**

Cuando el campo eléctrico generado por la antena es paralelo al horizonte terrestre

- **Circular**

Cuando el campo eléctrico generado por la antena va rotando de vertical a horizontal, y viceversa, creando movimientos circulares en todas direcciones.

- **Elíptica**

Cuando el campo eléctrico se mueve como en la polarización circular pero con desigual fuerza e las distintas direcciones. Generalmente, este tipo de polarización no suele ser intencionado.

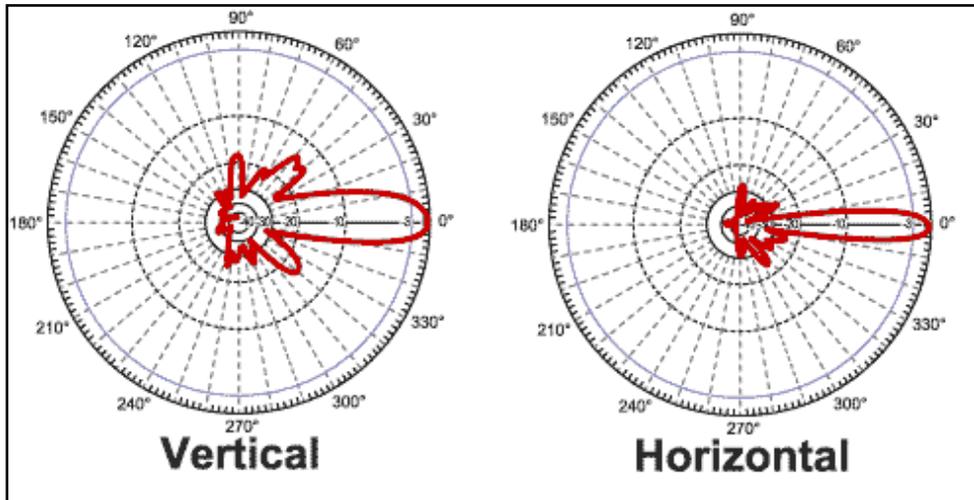


Figura 6.5 Modelos de Ganancia de una Antena

- **Medidas de Seguridad**

Antes de instalar la antena hay que anticipar los posibles riesgos, tales como:

- El contacto con las líneas de alta tensión. Las antenas, los mástiles, las torres, o los cables pueden apoyarse o caerse sobre las líneas de alta tensión.

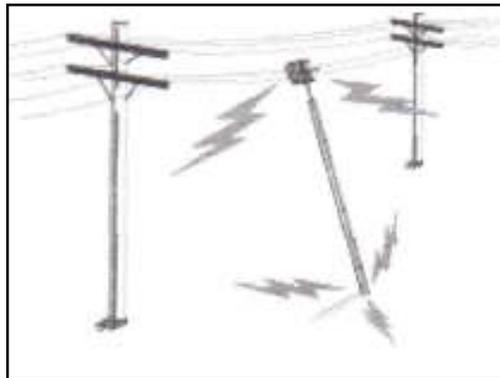


Figura 6.6 Seguridad con las Líneas de Alta Tensión

- Caídas de rayos. Debemos asegurarnos en tener una conexión a tierra de la antena para prevenir la caída de un relámpago, aumento estático o corto circuito dentro del equipo que se conecta a la antena.

- **Pérdida de Propagación**

La pérdida de propagación ocurre cuando una onda de radio se topa con un obstáculo, parte de su energía absorbe y se convierte en otro tipo de energía, mientras que otra parte se atenúa y sigue propagándose. Es posible que la otra parte se refleje. La atenuación se da cuando la energía de una señal se reduce en el momento de la transmisión. La atenuación se mide en belios (símbolo: B) y equivale al logaritmo de base 10 de la intensidad de salida de la transmisión, dividida por la intensidad de entrada. Por lo general, se suelen usar los decibelios (símbolo: dB) como unidad de medida. Cada decibelio es un décimo de belio. Siendo un belio 10 decibelios, la fórmula sería:

$$R \text{ (dB)} = (10) * \log (P2/P1)$$

Cuando R es positivo, se denomina amplificación, y cuando es negativo se denomina atenuación. En los casos de transmisiones inalámbricas, la atenuación es más común.

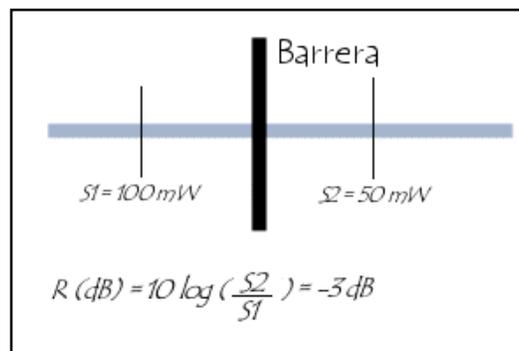


Figura 6.7 Atenuación

La atenuación aumenta cuando sube la frecuencia o se aumenta la distancia. Asimismo, cuando la señal choca con un obstáculo, el valor de atenuación depende considerablemente del tipo de material del obstáculo. Los obstáculos metálicos tienden a reflejar una señal, en tanto que el agua la absorbe.



Figura 6.8 Bloque I (Administración y Preescolar)



Figura 6.9 Bloque II y III (Primaria y Secundaria)



Figura 6.10 Bloque IV (Secundaria)

Un AP se puede configurar de varias formas:

- Puerto de consola: requiere un cable totalmente cruzado
- Telnet: requiere que el AP tenga una dirección IP conocida
- Navegador web: requiere que el AP tenga una dirección IP conocida.

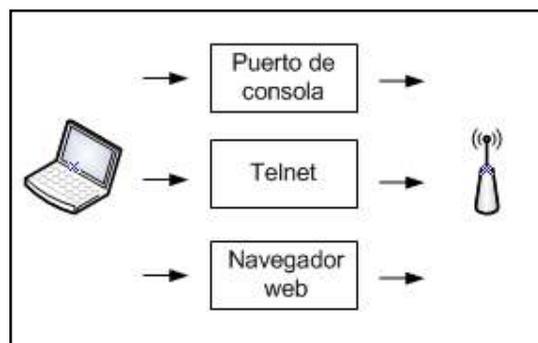


Figura 6.11 Opciones de Conexión

Configuración

Antes de empezar la configuración, es importante obtener la siguiente información:

- El nombre del sistemas
- El identificador del conjunto de servicio SSID (Service Set Identifier) con distinción de mayúsculas y minúsculas para la red de radio
- Si no esta conectado a un servidor DHCP, asigne una dirección IP única para el AP
- Si el AP no está en la misma subred que el PC, utilice una dirección de Gateway predeterminado y máscara de subred
- Un nombre de comunidad SNMP y el atributo de archivo SNMP si SNMP está en uso
- La dirección MAC de la etiqueta de la parte inferior del AP si IPSU está en uso

Si está configurado el AP en una red nueva, puede que parte de esta información la tenga que configurar un instalador o administrador de redes.²⁹

6.1.1.1 Propiedades configurables en el punto de acceso

Existen modelos de puntos de acceso que solamente son puntos de acceso de red local inalámbrica. Sin embargo, es habitual encontrar modelos de puntos de acceso que, además incluyen en su interior un router, un switch. Por este motivo las propiedades que son configurables en cada modelo de punto de acceso pueden variar dependiendo de todo lo que sea capaz de hacer. En cualquier caso, las propiedades principales propias de las funciones de punto de acceso son las siguientes:

- **Nombre de red**

Al nombre de red se le conoce también como SSDI (Service Set Identifier). Los puntos de acceso suelen incluir un nombre de red por defecto. No obstante, es recomendable sustituir este nombre por cualquier otro que se considere adecuado.

²⁹ FRENZEL LOUIS E., “Sistemas Electrónicos de Comunicación”, Alfaomega, 2003

- **Canal**

Aquí se deberá introducir el número de canal que se considere apropiado. Hay que tener en cuenta que, aunque el sistema me permita elegir cualquier canal, existen limitaciones regulatorias para el uso de los canales dependiendo del área geográfica en que nos encontremos.

- **Seguridad**

Los equipos Wi Fi disponen de determinadas características de seguridad que pueden ser configuradas en el punto de acceso y los adaptadores de cada ordenador que forme parte de la red. Es importante que los parámetros de seguridad que aquí se configuren sean los mismos que los se configuren en cada ordenador.

Adicionalmente los puntos de acceso ofrecen distintas características que ayudan a gestionar la red. Algunas de estas características son las siguientes:

- **Bajada automática de velocidad**

Esta característica permite que, cuando empeoren las condiciones de difusión de la señal radioeléctrica, el sistema pueda bajar la velocidad de transmisión para mantener la comunicación abierta.

- **Selección de los ordenadores autorizados**

Los puntos de acceso CISCO incluyen la facilidad de incluir una lista de acceso. Esta característica es interesante cuando se desea incrementar la seguridad de la red, pero no resulta práctica cuando se desea disponer de una red inalámbrica abierta a nuevos usuarios.

- **Emitir el nombre de red**

Los puntos de acceso emiten generalmente su nombre de red para permitirles a los posibles usuarios que puedan asociarse a la red con facilidad. No obstante si se desea aumentar la seguridad de la red, puede deshabilitarse esta opción.

- **Clave de acceso**

El punto de acceso dispone de una clave para impedir el acceso a sus funciones de configuración. El fabricante configura a todos sus equipos con una misma

clave de acceso (generalmente admin), pero el usuario debe cambiar esta clave para aumentar la seguridad de su equipo.

- **Habilitar la red inalámbrica**

Algunos equipos permiten que su función de punto de acceso pueda ser habilitada o deshabilitada. Esto es útil, fundamentalmente, cuando el punto de acceso dispone también de las funciones de router o switch.

Especificaciones Técnicas

- **Estándares**

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x

- **Administración del dispositivo**

- Web-Based – Internet Explorer
- Telnet
- AP Manager
- SNMP

- **Tasas de transferencia**

- Para 802.11g:
108, 54, 48, 36, 24, 18, 12, 9 and 6 Mbps
- Para 802.11b:
11, 5.5, 2 and 1 Mbps

- **Seguridad**

- 64, 128, 152 bit WEP
- WPA – Wi Fi Protected Access
- WPA – TKIP/PSK/AES
- 802.1x (EAP-MD5/TLS/TTLS/PEAP)
- MAC Address Access Control List

- **Rango de Frecuencia Inalámbrica**
 - 2,4 GHz to 2,483 GHz

- **Alcance de Operación**
 - Indoors
 - 98ft (30m) @ 54Mbps
 - 105ft (32m) @ 48Mbps
 - 121ft (37m) @ 36Mbps
 - 148ft (45m) @ 24Mbps
 - 197ft (60m) @ 18Mbps
 - 223ft (66m) @ 12Mbps
 - 253ft (77m) @ 9Mbps
 - Outdoors
 - 312ft (95m) @ 54Mbps
 - 951ft (290m) @ 11Mbps
 - 1378ft (420m) @ 6Mbps

- **Tipo de Modulación**
 - For 802.11g:
 - OFDM:
 - BPSK @ 6 and 9 Mbps
 - QPSK @ 12 and 18 Mbps
 - 16QAM @ 24 and 36 Mbps
 - 64QAM @ 48 and 54 Mbps
 - DSSS:
 - DBPSK @ 1 Mbps
 - DQPSK @ 2 Mbps
 - CCK @ 5.5 and 11 Mbps
 - For 802.11b:
 - DSSS:
 - DBPSK @ 1 Mbps
 - DQPSK @ 2 Mbps
 - CCK @ 5.5 and 11 Mbps

- **Potencia de Transmisión**

- For 802.11g:

- 31mW (15dBm) @ 54 and 108Mbps

- 40mW (16dBm) @ 48Mbps

- 63mW (18dBm) @ 36, 24, 18, 12, 9 and 6 Mbps

- For 802.11b:

- 63mW (18dBm) @ 11, 5.5, 2 and 1Mbps

- **Sensibilidad del receptor**

- For 802.11g:

- 1Mbps: -94dBm

- 2Mbps: -91dBm

- 5.5Mbps: -89dBm

- 6Mbps: -91dBm

- 9Mbps: -90dBm

- 11Mbps: -86dBm

- 12Mbps: -89dBm

- 18Mbps: -87dBm

- 24Mbps: -84dBm

- 36Mbps: -80dBm

- 48Mbps: -76dBm

- 54Mbps: -73dBm

- For 802.11b:

- 1Mbps: -94dBm

- 2Mbps: -90dBm

- 5.5Mbps: -88dBm

- 11Mbps: -85dBm

Uso del asistente de configuración

El software en el Access Point, tiene las siguientes características:

- Para la configuración se necesita un computador con sistema operativo Windows que tenga instalado un adaptador Ethernet para acceder al software que viene en el punto de acceso Aironet 1310 CISCO
- Se necesita un navegador de Internet que puede ser el Internet Explorer

A continuación se presentará gráficamente el proceso de instalación del software:

- El acceso al AP será a través de un navegador WEB, para acceder a la configuración del punto de acceso, abrimos un navegador web e introducimos la dirección IP del AP en el cuadro de dirección del navegador, luego introducimos los datos de usuario y contraseña, posteriormente nos aparecerá la GUI del AP, como se muestra en la figura:

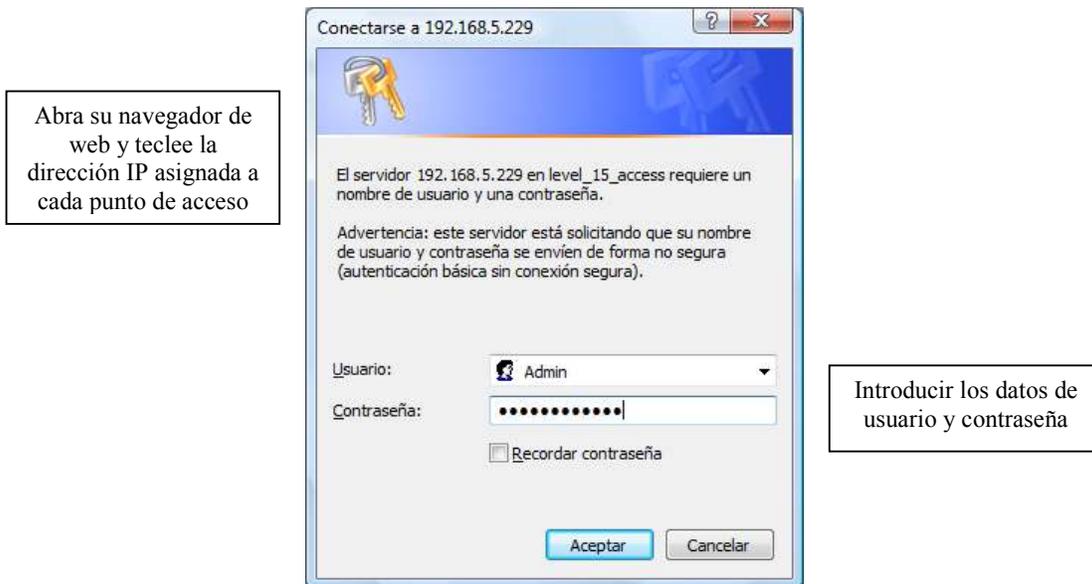


Figura 6.12 Conexión al CISCO Aironet 1310

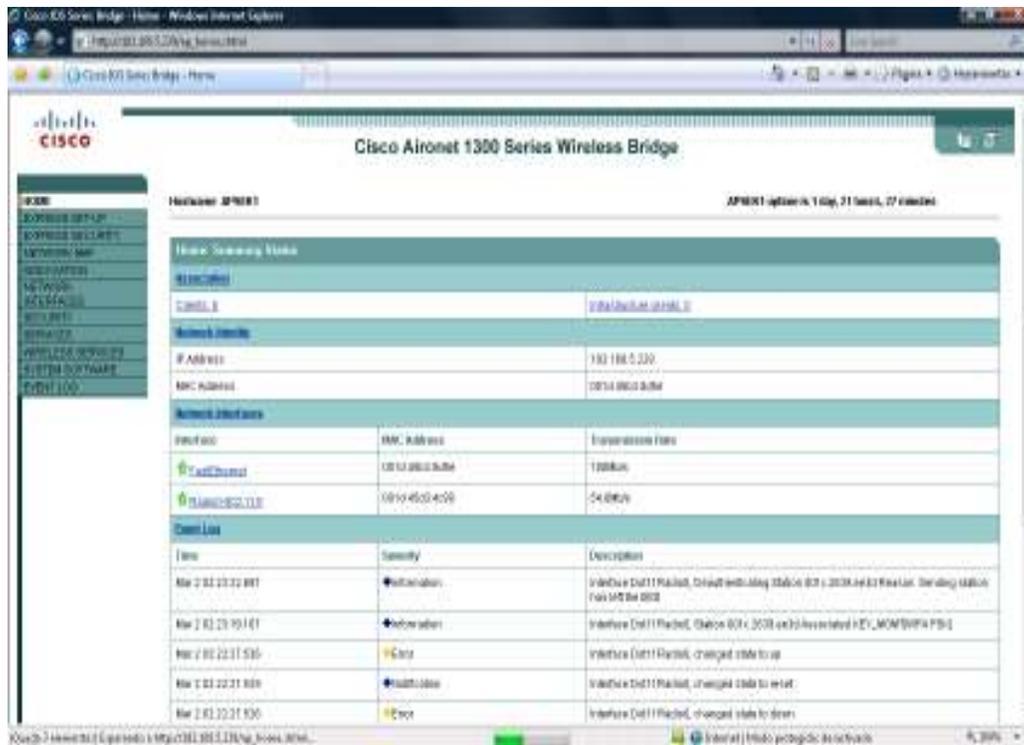


Figura 6.13 GUI del IOS

Una vez que el AP está configurado inicialmente, la página HOME, resume las estaciones asociadas, los eventos del sistema y el estado de los puertos, esta página también proporciona muchos enlaces a otras páginas que contienen información detallada.

La anterior figura muestra los enlaces y botones que aparecen en la página de administración del IOS mientras que en la siguiente tabla proporcionaremos una descripción de los mismos:

Comandos	
IOS	Descripción
EXPRESS SETUP	Muestra la página Express Setup, donde se incluyen los ajustes básicos, como el nombre del sistema, la dirección IP y el SSID
NETWORK MAP	Muestra una lista de los dispositivos de infraestructura de la WLAN
ASSOCIATION	Muestra una lista de todos los dispositivos de la WLAN, con sus nombres de sistema, papel en la red y las relaciones “padre-cliente”
NETWORK INTERFACES	Muestra el estado y las estadísticas de las interfaces de radio y Ethernet y proporciona enlaces a las páginas de configuración de cada interfaz
SECURITY	Presenta un resumen de los ajustes de seguridad y proporciona enlaces a las páginas de configuración de la seguridad
SERVICES	Muestra el estado de varias características del AP y enlaces a las páginas de configuración de Telnet/SSH, CDP, DNS, filtros, etc.
SYSTEM SOFTWARE	Muestra el número de versión del firmware que el AP está ejecutando y proporciona enlaces a las páginas de configuración para la actualización y la administración del firmware
EVENT LOG	Muestra el registro de eventos del AP y proporciona enlaces a las páginas de configuración donde puede seleccionar los eventos que se incluirán en avisos, establecer los niveles de severidad del evento y establecer los métodos de notificación.

Botones de acción (no aparecen en la figura)

APPLY	Guarda los cambios efectuados en la página y permanece en la página
REFRESH	Actualiza la información de estado o las estadísticas visualizadas en una página
CANCEL	Descarta los cambios introducidos en la página y permanece en la página
BACK	Descarta los cambios introducidos en la página y regresa a la página anterior

Tabla 6.2 Descripción de los botones de comando

6.1.1.2 Selección del canal

Una vez que se ha establecido que el punto de acceso y el sistema de antenas es compatible, el primer punto a considerar por los usuarios debe ser la de estar dentro de las limitaciones de la potencia de transmisión. Este es un aspecto que solo se relaciona con los productos de puentes de punto a punto y punto a multipunto, los cuales a menudo están basados en dispositivos Wi Fi.

La FCC limita el total de potencia de transmisión y la ganancia de la antena menos cualquier pérdida en el cable, a no más de 36 dB o 4 watios. Esta potencia de radiación isotrópica efectiva (EIRP) permite un poco más de flexibilidad en la parte del usuario y el fabricante.

A pesar de que la asignación FCC para la banda ISM de 2.4 GHz está definida entre 2.4 y 2.4835 GHz, los dispositivos Wi Fi que operan en esa banda funcionan en términos de canales, las especificaciones 802.11b y 802.11g definen los canales disponibles en la banda FCC para su uso de la manera siguiente:

ID de canal (MHz)	Frecuencia
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462

Tabla 6.3 Canales y bandas de frecuencia de red 802.11g,b

Los resultados anteriores de las especificaciones 802.11b y 802.11g sugieren de manera errónea que el usuario tiene once disponibles en la banda de 2.4 GHz. El usuario en realidad no tiene más de tres canales que no se traslapan. Se requiere de un mínimo de 22 MHz de ancho de banda para la transmisión Wi Fi en la banda de 2.4 GHz.

Los únicos canales disponibles de estos que permiten la amplitud de 11 MHz en ambas direcciones sin interferir con otro canal o extenderse más allá de la frecuencia asignada (excediendo las bandas laterales) son los canales 1,6 y 11.

A pesar de que no existe restricción legal sobre el diseño de una LAN inalámbrica que tenga un uso menor o mayor de un canal, normalmente es recomendable usar los tres canales, ni más ni uno menos, para alcanzar el mejor balance entre capacidad y la confiabilidad.

6.1.1.3 Conexión con la red LAN

Básicamente la nueva red Inalámbrica se la implantará a partir del cableado vertical existente en el Colegio internacional SEK-QUITO. La tecnología a implementare será la de una Red en Infraestructura.

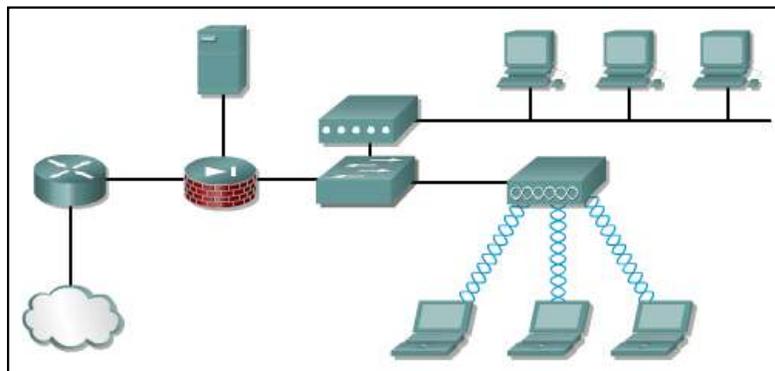


Figura 6.14 Topología de una Red en Infraestructura

Se re-utilizarán los servidores ubicados en el rack principal de la Institución, además del cableado de fibra óptica que recorre todos los bloques. Para el caso de la ubicación de los puntos de acceso, se realizará un estudio de potencias de recepción, calidad de la señal de recepción, ancho de banda, etc. Para así asegurarnos de que el diseño de la nueva red inalámbrica va a ser el óptimo.

Dependiendo de la cantidad de información que requieran las secciones, departamentos de la infraestructura del Colegio Internacional SEK-QUITO, se realizará el estudio previo para saber la cantidad de puntos de acceso por planta que necesitamos.

6.1.1.4 Comprobar el funcionamiento

Fuentes de Interferencia

Para redes inalámbricas que operan en la banda de frecuencia de 2.4 GHz, los hornos microondas pueden ser una importante fuente de interferencia. Los hornos emiten sobre los 750 W de potencia a 50 pulsos por segundo con un ciclo de radiación de 10 ms. Por lo tanto, para una tasa de datos de 2 Mbps, la longitud máxima de los paquetes está restringida a 20000 bits o 2500 octetos.

La radiación emitida barre de 2,4 a 2,45 GHz y se mantiene estable por un corto periodo a 2,45 GHz. Aunque las unidades son blindadas, un buen monto de energía puede todavía interferir con la transmisión. Otras fuentes de interferencia en la banda de frecuencia de 2,4 GHz incluyen a las fotocopiadoras, motores de ascensores y equipos médicos.

Obstrucción de propagación de señales

Para la implementación se considera algunos parámetros como el nivel de atenuación de las paredes internas y externas de la Institución, cuan más lejos las señales viajen, depende de los materiales de construcción de las paredes, divisiones y otros objetos.

Barrera	Nivel de Atenuación	Ejemplos
Cartón, Yeso	bajo	Paredes internas
Madera/Material sintético	bajo	Divisiones
Asbesto	bajo	Techos
Vidrio	bajo	Ventanas
Ladrillos/Mármol	medio	Interiores u otras paredes
Agua	medio	Acuarios
Concreto	alto	Pisos
Metal	muy alto	Cabinas de acero

Tabla 6.4 Cuadro comparativo de obstrucciones de propagación

También se tiene en cuenta los valores de atenuación que tienen los diferentes tipos de paredes. Así:

Material	Atenuación
Madera (15 mm)	2.5 a 3.5 dB
Tabla roca	0.2 a 3.5 dB
Bloque de concreto	8.0 a 15 dB
Fibra de vidrio	Aprox. 38 dB

Tabla 6.5 Obstrucción de señales de materiales

Índices de calidad

Para evaluar la calidad de una señal existen técnicas cualitativas y métodos cuantitativos. Las técnicas cualitativas permiten evaluar una señal de manera subjetiva, de forma que la señal se observa y analiza con la intención de detectar patrones que puedan indicar la presencia de irregularidades. Estas técnicas son, por lo regular, utilizadas para apuntar posibles causas y determinar estrategias en la solución de problemas. Las mediciones cuantitativas, por el contrario, proveen un dato numérico que se compara con algún parámetro recomendado o correspondiente a alguna especificación. Una medida cuantitativa es sumamente confiable, mientras que las técnicas cualitativas dependen de la percepción particular y de la experiencia.

El tipo de modulación que utilizara el Access Point dependerá de los valores de la tasa de transferencia que se obtiene del lugar donde se encuentra el cliente, así:

Para 802.11g:

OFDM:

- BPSK @ 6 and 9 Mbps
- QPSK @ 12 and 18 Mbps
- 16QAM @ 24 and 36 Mbps
- 64QAM @ 48 and 54 Mbps

DSSS:

- BPSK @ 1 Mbps
- DQPSK @ 2 Mbps
- CCK @ 5.5 and 11 Mbps

Para velocidades de 54 Mbps, que es lo que se busca en este diseño, se tiene que la modulación digital a utilizarse es 64 QAM.

Identificar el problema que aqueja a una señal digital en los diagramas de constelación consiste en reconocer el patrón que provoca una desviación respecto a la posición ideal de los símbolos. Si cada punto en la constelación corresponde a la posición ideal del símbolo correspondiente, entonces la señal es perfecta y no contendrá errores.

6.1.2 Configuración de los ordenadores

Cualquier ordenador que se desee conectar de forma inalámbrica a una red con puntos de acceso necesita disponer de un adaptador de red (tarjeta Wi Fi) y configurarse adecuadamente para que el adaptador se entienda con el punto de acceso de la red deseada.

El proceso de instalación de estos dispositivos es idéntico tanto para la configuración de redes inalámbricas en modo ad hoc, como para el modo de infraestructura (con puntos de acceso).

En cuanto a lo que hay que configurar desde el ordenador, hay que llevar a cabo dos tipos de configuraciones:

Configurar el adaptador de red

Los adaptadores de red se configuran con una aplicación que viene en el equipo. Los parámetros a configurar son los siguientes:

- **Tipo de red**

En este caso, el tipo de red que hay que configurar es el BSS también conocido como infraestructura o con puntos de acceso

- **Nombre de red**

El nombre de red debe ser el mismo que el configurado en el punto de acceso, incluidos los caracteres en mayúscula y minúscula. Al parámetro nombre de red también se le conoce como Network Name o SSID (Service Set Identifier). Muchas aplicaciones de configuración de adaptadores de red ofrecen la posibilidad de realizar una búsqueda automática de todas las redes del entorno que son recibidas por el adaptador en ese momento.

- **Canal**

En este caso no es necesario configurar el canal porque el adaptador lo tomará automáticamente del punto de acceso

- **Seguridad**

Es importante que los parámetros de seguridad que aquí se configuren sean los mismos que los configurados anteriormente en el punto de acceso. Si se tienen dudas, simplemente se dejan deshabilitados los parámetros de seguridad.

Configurar el protocolo TCP/IP

Configurar el protocolo TCP/IP en un ordenador suele suponer configurarle una dirección IP, una máscara de subred, una puerta de enlace y un servidor DNS. No obstante, en el caso de los puntos de acceso, todas estas configuraciones suelen sustituirse por configurar cada ordenador para que obtenga las direcciones IP de forma automática. El punto de acceso ya se encarga de pasarle a cada ordenador los datos necesarios para establecer la comunicación.

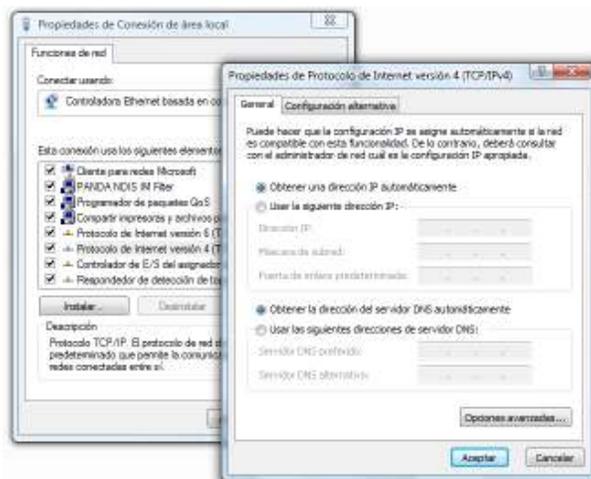


Figura 6.15 Configuración de la tarjeta

La operación de configurar el protocolo TCP/IP y el adaptador de red hay que repetirla con cada ordenador que se desee conectar al punto de acceso.

Cualquier ordenador con un adaptador Wi Fi que tenga configurados correctamente los parámetros anteriores y que estén dentro del área de cobertura radioeléctrico de cualquier punto de acceso de la red formará parte de ella y por tanto, podrá compartir sus recursos y tener acceso a los recursos (configurados como compartidos) del resto de ordenadores.

Esto quiere decir que, para añadir nuevos ordenadores a la red, simplemente hay que copiar los parámetros de cualquiera de los ordenadores ya conectados y configurárselos al nuevo ordenador.

Se debe aclarar que un mismo ordenador puede tener guardadas distintas configuraciones de red, distintos perfiles. Esto es especialmente útil para aquellos casos en los que un mismo ordenador se conecta a distintas redes. En estos casos no es necesario introducir todos los parámetros cada vez que se cambia de red, sino que elegir el perfil correspondiente.

Las pruebas de cobertura permitirán diagnosticar la calidad del enlace inalámbrico entre las estaciones OR. Cabe recalcar que las pruebas de cobertura son de tipo experimental, para lo cual se tomaron dos consideraciones: medir la calidad de los enlaces de las estaciones remotas con la estación central y la cobertura de un punto de acceso (AP) en un ambiente interno.

Calidad de los enlaces

Como se indico anteriormente en el diseño de la red inalámbrica, existen tres enlaces, uno en la parte en el I Bloque (Administración y Precolar), en el III Bloque (Primaria y Biblioteca) y IV Bloque (Secundaria y Zonas Recreativas). Para medir la calidad de los enlaces, nos valemos del propio software de monitoreo Wireless Link test que viene el Manager de los equipos CISCO.

Al escoger un enlace para monitorearlo, el software mencionado nos mostrará los siguientes parámetros: nivel de la señal, nivel de ruido (SNR), cantidad de paquetes enviados y recibidos y la cantidad de paquetes perdidos. El nivel de la señal nos indica cuán grande es la señal de radio recibida por cada uno de los dispositivos de enlace. Un nivel bajo de señal indica que uno de los dispositivos de enlace se encuentra fuera del rango de cobertura.

El ruido indica el nivel de interferencia producido por otro dispositivo (inalámbrico) que se encuentre en las proximidades de las estaciones. Existen dos tipos de ruido: ruido local que indica la interferencia en las proximidades de un seleccionado punto de acceso y ruido remoto que indica la interferencia en las centrales de un dispositivo de enlace.

Cuando la fuente de interferencia es identificada, dicha fuente debe ser eliminada o mediante el uso del indicador Wireless Link Test optimizamos la estación o la ubicación de la antena para los dispositivos CISCO y obtener un buen desempeño.

La SNR es el primer indicador para validar la calidad de comunicación entre dos dispositivos inalámbricos. La SNR indica cuán grande es el nivel de la señal de radio recibida con respecto al nivel de ruido percibida por la estación de monitoreo y la estación remota. Un valor bajo indica una situación de casi fuera de rango de cobertura o un alto nivel de interferencia.

La calidad de la señal es una medida de la claridad de la señal para diagnosticar las reflexiones de la señal por superficies reflectoras de radiofrecuencia, tal es el caso de los componentes estructurales de acero expuestos. Las reflexiones de la señal podrían llevar a la pérdida de paquetes reduciendo el rendimiento de la red inalámbrica.

6.1.2.1 Gestión de la Red

Existen aplicaciones que permiten vigilar y gestionar el funcionamiento de la red. De hecho existen dos tipos de aplicaciones: las que se instalan en las estaciones,

aplicaciones cliente, y las que instala el administrador para vigilar la red, aplicaciones de red. La mayoría de estos programas se basan en el protocolo SNMP (Simple Network Management Protocol).

Las aplicaciones clientes están relacionadas con la tarjeta de red inalámbrica de que se disponga. Suele ser el propio proveedor del adaptador de red el que facilita la aplicación. Estas aplicaciones facilitan información sobre la calidad de la señal, el estado de la conexión, SSID, WEP, etc. Las aplicaciones cliente permiten definir distintos perfiles para que el usuario pueda utilizar la misma tarjeta en distintas redes.

Las aplicaciones de red ofrecen herramientas tanto para el seguimiento como para la gestión de la red. La mayoría de los puntos de acceso vienen acompañados de un software de este tipo.

6.1.2.2 Medir Velocidad

La velocidad máxima a la que transmite Wi Fi es de 54 Mbps, no obstante, esta velocidad puede ser menor dependiendo de la distancia entre emisor y receptor y de las condiciones del entorno. También hay diferencias si los equipos se encuentran en el interior de un edificio o en el exterior en espacio abierto. La transmisión en el exterior suele ser de mayor calidad porque existen menos interferencias y menos equipos intentando competir por el uso del espectro radioeléctrico.

A pesar de lo anterior, la percepción de la velocidad es algo relativo, 1 Mbps es una buena velocidad para la mayoría de las aplicaciones que tenemos hoy en día, no obstante se percibirá como lenta, si se pretende transmitir un archivo de gran tamaño o acceder al directorio de un ordenador remoto, pero en el resto de casos es una velocidad suficiente.

Si desea comprobar la velocidad a la que se está haciendo uso de la red, la mayoría de las aplicaciones cliente de las tarjetas Wi Fi permite comprobar este dato, además de otros como la relación señal ruido, nivel de recepción de la señal recibida, etc.

6.2 Conexión a Internet

Los expertos dicen que en un futuro próximo la mayor parte de la información estará en Internet. Esto nos permitirá disponer de la información independientemente donde nos encontremos, siempre podremos acceder a nuestras bases de datos, catálogos de fotos, documentos, etc.

Las redes inalámbricas hacen que todos los dispositivos conectados a la red pueda compartir una única conexión a Internet, cada usuario puede navegar por sus propias páginas, leer su correo o hacer cualquier otro uso de Internet. Lo que sí es cierto que el ancho de banda de la conexión será compartido entre todos los usuarios. Por tanto es posible que en algunos momentos la conexión vaya algo más lenta de lo habitual, pero en general la navegación será bastante buena. Si no lo fuera siempre se puede contratar una velocidad mayor de acceso a Internet o contratar más de una línea de acceso.

La inmensa mayoría de los modelos de punto de acceso ya tienen integrada la posibilidad de compartir una conexión a Internet. Esto es posible porque el punto de acceso tiene integrada la función de router. El router es un equipo que hace de intermediario entre Internet y cada uno de los ordenadores de la red privada.

Evidentemente para compartir un acceso a Internet, lo primero es disponer del acceso. Las empresas que facilitan los servicios de acceso a Internet se conocen con el nombre de proveedores de acceso ISP (Internet Service Provider).

6.2.1 Acceso a Internet

La red Internet es una red global interconectada con prácticamente todos los tipos de redes públicas de telecomunicaciones existentes en la actualidad. Esto quiere decir que cualquier persona que tenga acceso a una red de comunicaciones podrá tener acceso a través de ésta a la red Internet.

La red pública más extendida es la red telefónica básica. Esto hace que una gran parte de los usuarios de Internet utilicen esta red como su acceso habitual.

Existen dos formas de disponer de una conexión completa a Internet:

- Desde un ordenador que forma parte de una red local de una empresa, universidad u otra institución y que está conectada a Internet a través de un router. Se necesita un ordenador con una tarjeta o adaptador de red.
- Desde un ordenador doméstico estableciendo una conexión telefónica a una empresa denominada genéricamente proveedor de acceso a Internet. Se necesita un ordenador conectado a la línea telefónica a través de un modem. Se debe abonar el coste de la llamada telefónica durante el tiempo de conexión a red, además de la tarifa del proveedor del acceso.

6.2.1.1 Ancho de Banda

Cuando hablamos de acceso a Internet, se habla de comunicación digital, la palabra ancho de banda hace referencia a la velocidad con la que se transmiten los datos, entre dos puntos (los bits por segundo).

El ancho de banda de acceso a Internet es la velocidad con la que se está conectado con esta red. El estar conectado a Internet con banda estrecha significa estar conectado a baja velocidad significa disponer de alta velocidad.

La frontera entre la banda ancha y estrecha no está claramente definida. No obstante, se entiende que la velocidad que se puede alcanzar utilizando un canal telefónico es banda estrecha y las velocidades superiores son banda ancha. Por lo cual la frontera entre ambas bandas se encuentra en 64 Kbps. Igual o menor es banda estrecha, superior es banda ancha.

El ancho de banda teórico es el ancho de banda de transmisión de datos, es decir, el flujo total de bits que puede enviar por segundo. En este valor se toma en cuenta toda la información que envía en cada sesión que realiza: bits de control, encabezados de transmisión y datos de usuario. Todos estos bits necesitan ser enviados en cada sesión para proveer la comunicación; los datos de usuario son una parte del flujo de datos pero no son su totalidad por lo que se debe tener siempre en cuenta.

El ancho de banda real o tasa efectiva es el ancho de banda de la transmisión de datos de usuario. Este valor muestra un valor aproximado del ancho de banda utilizado para transferir un archivo o datos entre un punto y otro y siempre es menos que el ancho de banda teórico.

6.2.2 Acceso de Banda Ancha

Los proveedores de acceso denominados ISP, son los intermediarios que facilitan el acceso a Internet a las personas o empresas interesadas. Los proveedores de acceso suelen ofrecer a sus clientes la posibilidad de acceder a Internet por cualquiera de los siguientes sistemas:

- **Baja Velocidad**

O banda estrecha, mediante un módem de red telefónica básica o RDSI. Para ello, le facilitan al cliente un nombre de usuario y clave.

- **Alta Velocidad**

O banda ancha, mediante circuito dedicado. En este caso dependiendo del tipo de proveedor de acceso de que se trate, puede ofrecer un tipo de solución tecnológica u otra: ADSL, Frame Relay, etc.

El estar conectado a Internet con banda ancha, quiere decir que se dispone de un gran ancho de banda o lo que es lo mismo se está conectado a Internet a alta

velocidad. En la práctica, significa disponer de una conexión igual o superior a 128Kbps. La posibilidad de acceder a Internet con banda ancha está haciendo que surjan servicios que se aprovechen la alta velocidad. Por ejemplo, la posibilidad de incorporar video está dando paso a popularizar aplicaciones como tele vigilancia, tele información o videoconferencia. Las ventajas principales de los servicios de acceso a Internet con banda ancha son las siguientes:

- Alta velocidad, ofreciendo una velocidad a Internet de hasta 2 Mbps
- Siempre conectado, no hace falta perder tiempo estableciendo una conexión, la conexión de banda ancha esta siempre activa y funcionando
- Voz y datos simultáneamente, funciona de forma completamente independiente al servicio telefónico
- Tarifa plana, ofrece la posibilidad de disponer del servicio de acceso a Internet las 24 horas al día por un bajo costo.

6.2.3 Conexión de Wi-Fi con Internet

La conexión de una red inalámbrica Wi Fi con Internet se lleva a cabo a través del punto de acceso. En el mercado existen distintos modelos de puntos de acceso con distintas características. No obstante, las facilidades que puede presentar un punto de acceso para su conexión a Internet son las siguientes:

- Disponer de un puerto 10/100Base-T (RJ-45 o Ethernet, también conocido como uplink por donde poder conectarse al módem ADSL o al switch
- Disponer internamente de la funcionalidad hub. Esto facilitaría de dos a cuatro puertos exteriores 10/100Base-T (RJ-45 o Ethernet) por donde poder conectarse a la red local cableada con conexión a Internet.
- Un puerto serie RS-232 a donde se le puede conectar un módem tradicional de red telefónica (V90 a 56 Kbps). Esta conexión a Internet a baja velocidad podría ser utilizada como acceso principal a Internet o como acceso secundario de seguridad en el caso de que falte la conexión principal de banda ancha.

La conexión de una red Wi Fi a Internet pasa, generalmente por conectar el punto de acceso a una red cableada que ya dispone de acceso que incluye la funcionalidad de router. Por lo que el punto de acceso podría ser configurado, por ejemplo con unas

mejores medidas de seguridad, para compartir más de una dirección IP pública entre sus usuarios.

6.2.3.1 Instalación conexión entre Wi-Fi e Internet

Las interconexiones entre un punto de acceso Wi Fi y un módem ADSL pueden diferir levemente de unos fabricantes a otros; no obstante, los conceptos básicos son los mismos.

La interconexión de la red Wi Fi con el módem ADSL consiste en interconectar ambos equipos mediante un cable 10/100 Base-T (RJ45). Para ello, primeramente hay que comprobar que tanto la red Wi Fi como la conexión ADSL están instaladas y funcionando correctamente de forma independiente.

Si la conexión ADSL está funcionando conectada directamente a un ordenador, el trabajo consiste en sustituir el ordenador por el punto de acceso. Esto supone configurar el punto de acceso con los mismos parámetros con los que está configurado el ordenador y cambiar la conexión del cable del ordenador al punto de acceso.

6.2.3.2 Configuración del punto de acceso

Para configurar el punto de acceso, se debe ejecutar el software de utilidad que acompaña a los equipos Wi Fi. Este software permite verificar las conexiones, modificar las configuraciones, y en general gestionar las comunicaciones de la unidad Wi Fi. Cada fabricante llama a este software de una manera. Por cierto, es siempre una buena manera de acceder al web del fabricante de los dispositivos Wi Fi para comprobar si existe una versión más moderna de los controladores, firmware y software de utilidad de estos dispositivos Wi Fi. Si así fuera, es recomendable instalar las versiones más modernas de la web antes que las versiones más antiguas.

Cuando se pone en marcha el software de configuración del punto de acceso y una vez introducida la identificación del punto de acceso y su clave habrá que buscar la opción de configuración del puerto Ethernet. Para terminar, se sale del programa de configuración aceptando los cambios, esto hará que la nueva configuración se transmita al punto de acceso y todo quede listo para utilizar el acceso a Internet.

6.2.4 Pruebas y Monitoreo WLAN Colegio Internacional SEK-QUITO

No existe una forma exacta de saber el rango de cobertura del AP. Paredes de concreto, metales, pisos reforzados, obstáculos podrían detener la señal y reducir el rango de cobertura, por esta razón, el procedimiento a seguir fue moverse con una laptop, con su tarjeta inalámbrica, e irse alejando del AP dentro del ambiente y de esta manera obtener el máximo rango de cobertura.

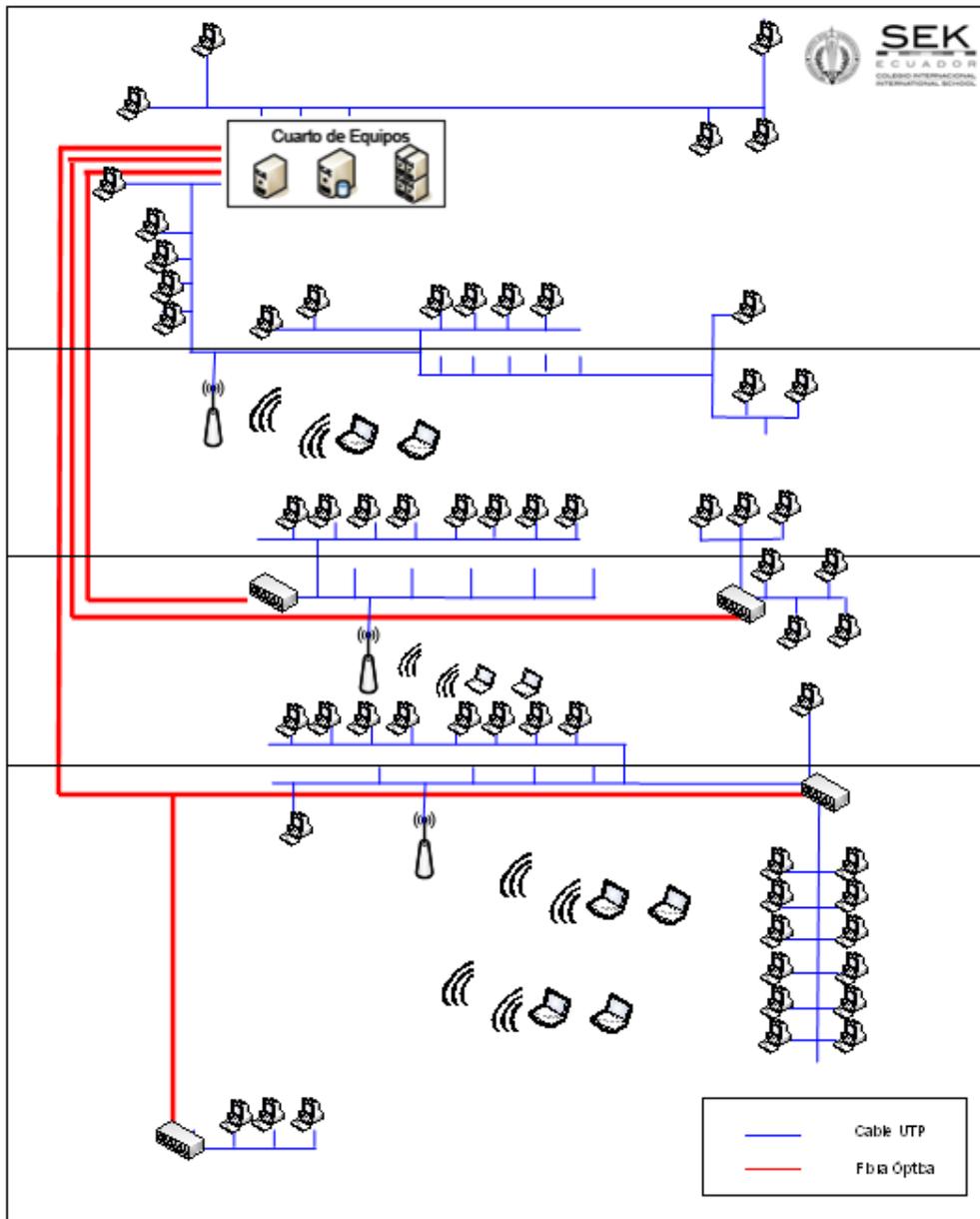


Figura 6.16 WLAN del Colegio Internacional SEK-QUITO

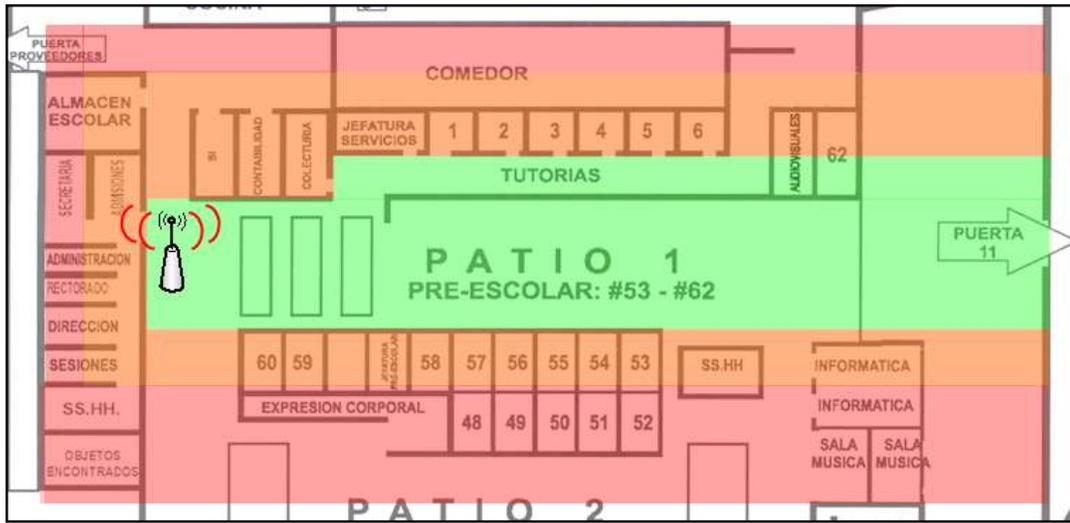


Figura 6.17 Mapa de Cobertura Experimental Bloque I (Administración y Preescolar)

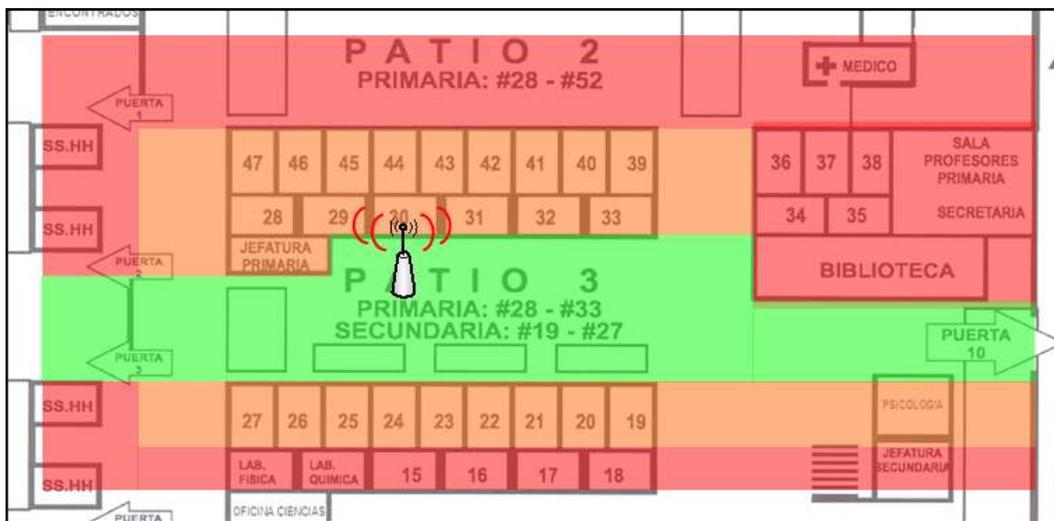


Figura 6.18 Mapa de Cobertura Experimental Bloque II y III (Primaria y Secundaria)

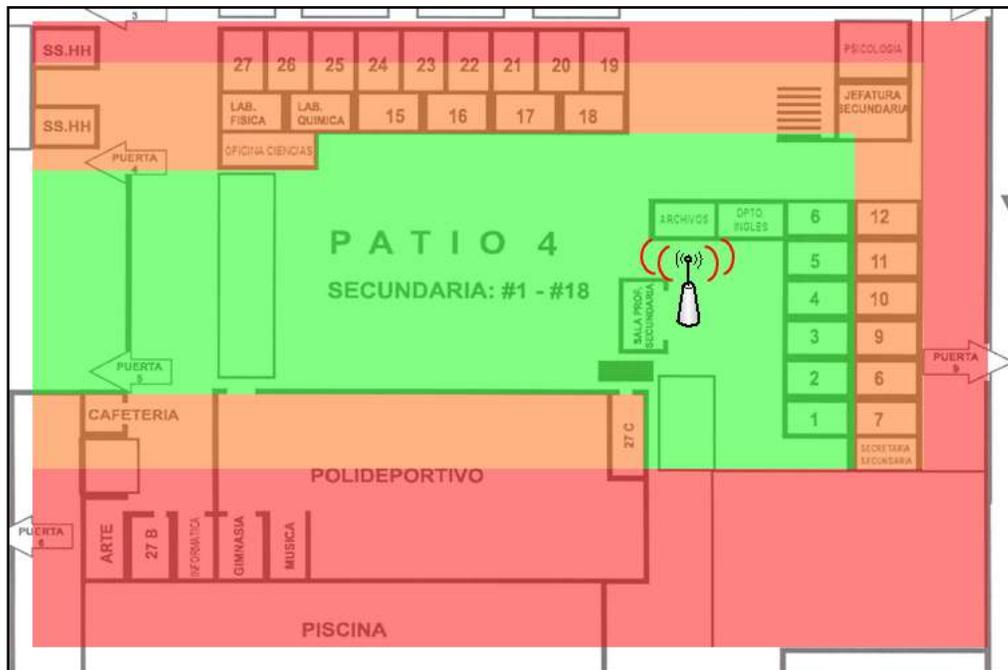


Figura 6.19 Mapa de Cobertura Experimental Bloque IV (Secundaria)

Como se muestra en las figuras, en las zonas abiertas existe una cobertura total de calidad excelente, a las cercanías de esta cobertura es buena y mientras más nos apartamos del AP la señal se va debilitando hasta no tener conexión. Si se desea ampliar el rango de cobertura para ambientes internos, se debe añadir AP's y ubicarlos en los distintos lugares para que cubran las zonas que no tienen conexión.

Como se indicó anteriormente, ciertos puntos de acceso además de dar conectividad al bloque donde se encuentra instalado, también darán conectividad a las áreas adyacentes, es decir el punto de acceso ubicado en el Bloque I, dará conectividad a los equipos de dicho de dicho bloque y a los equipos ubicados en el área administrativa como a los equipos ubicados en un área de primaria, el punto de acceso ubicado en el Bloque III, dará conectividad a los equipos ubicados en dicho bloque y a los equipos ubicados en el en la otra área de primaria, logrando así dar conectividad a todos los equipos del Colegio Internacional SEK-QUITO.

Las mediciones que se muestran en las siguientes figuras se realizaron para medir la intensidad de la potencia de la señal a distintas distancias y así poder verificar rangos

de coberturas de equipos inalámbricos. Este análisis se realizó para irradiación de señal de manera horizontal.

BLOQUE I, II Y ADMINISTRACIÓN

- **Distancia:** 6 metros



Figura 6.20 Medición a 6 metros en el Bloque I, II y Administración

- **Distancia:** 9 metros



Figura 6.21 Medición a 9 metros en el Bloque I, II y Administración

BLOQUE III

- **Distancia:** 6 metros



Figura 6.22 Medición a 6 metros en el Bloque III

- **Distancia:** 9 metros



Figura 6.23 Medición a 9 metros en el Bloque III

BLOQUE IV

- **Distancia:** 6 metros



Figura 6.24 Medición a 6 metros en el Bloque IV

- **Distancia:** 9 metros



Figura 6.25 Medición a 9 metros en el Bloque IV

BIBLIOTECA

- **Distancia:** 3 metros



Figura 6.26 Medición a 3 metros en Biblioteca

- **Distancia:** 6 metros



Figura 6.27 Medición a 6 metros en Biblioteca

BLOQUE IV (PASILLO)

- **Distancia:** 3 metros



Figura 6.28 Medición a 3 metros en el Bloque IV (Pasillo)

- **Distancia:** 6 metros

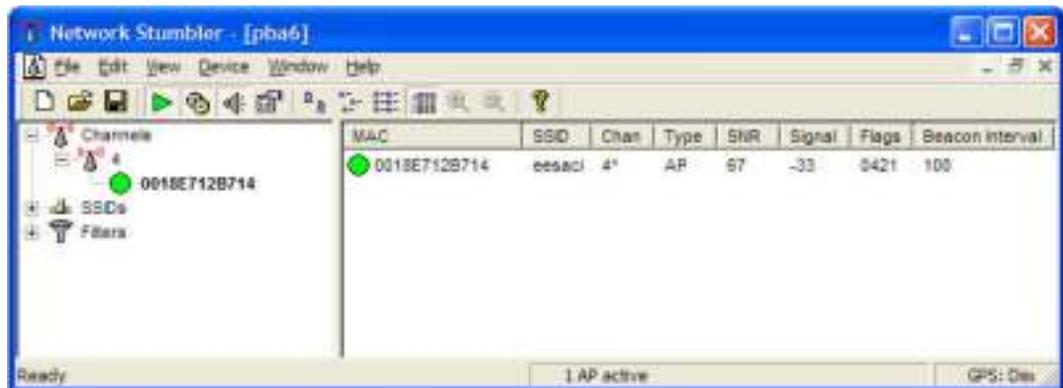


Figura 6.29 Medición a 6 metros en el Bloque IV (Pasillo)

6.2.4.1 Comprobar el acceso a Internet

Para comprobar si el acceso a Internet está funcionando correctamente simplemente hay que abrir el navegador y ver si se puede acceder a cualquier página web, si las páginas web se pueden ver sin problemas, perfecto esto funciona. Si por el contrario, si se tiene como respuesta el mensaje de que la página no se puede mostrar, entonces tenemos un problema.

Antes de darlo todo por perdido, conviene intentar acceder a distintas páginas. Es posible que nos hayamos equivocado a la hora de introducir el nombre de la página. Si aun así, seguimos teniendo problemas, debemos comprobar la conexión a Internet desde ese ordenador conectándole directamente al módem ADSL. Si no funciona, si no funciona debemos configurar dicha conexión en el ordenador siguiendo las instrucciones de la guía de usuario del módem DSL.

Si el ordenador puede acceder a Internet desde el módem DSL pero no desde la conexión inalámbrica y por otro lado, la conexión inalámbrica de este ordenador funciona adecuadamente, sólo nos quedan dos puntos por comprobar: o el cable de conexión entre el punto de acceso y el módem no es el correcto o no está bien conectado, o el punto de acceso no está bien configurado. Para lo cual debemos comprobar todos estos términos.

En cuanto al cable, existen dos tipos de cables Ethernet categoría 5 (RJ45): cruzado y no cruzado. Los cables de tipo no cruzado no suelen tener ningún tipo de marca mientras que los de tipo cruzado suelen tener una marca especial, por ejemplo, una marca negra donde se puede leer Crossover, o similar. Asegúrese que está utilizando un cable Ethernet categoría 5 (RJ45) no cruzado para conectar el módem ADSL con el punto de acceso.

Por último, si se tiene alguna duda en la configuración del punto de acceso, consultar el manual de usuario del equipo.

Capítulo 7

7 DEFINICIÓN DE POLÍTICAS Y ESTÁNDARES DE SEGURIDADES EN LA WLAN COLEGIO INTERNACIONAL SEK-QUITO

En este capítulo se analizarán los objetivos de las seguridades en la WLAN del Colegio Internacional SEK-QUITO, que son mantener la integridad, proteger la confidencialidad y garantizar la disponibilidad, y que por lo tanto todas las redes deben ser protegidas para alcanzar su mayor potencial.

7.1 Creación de Estándares de Seguridad

El Colegio Internacional SEK-QUITO es una institución de educación secundaria que tiene una población de aproximadamente 1100 alumnos, repartidos en dos sistemas: Un sistema de primaria. Cuenta también con un sistema de bachillerato el cual es catalogado como secundario, el cual contempla un Bachillerato Nacional y otro Bachillerato Internacional. Todas ellas administradas por una plantilla de aproximadamente 70 personas entre profesores y personal administrativo.

Debido a ser una institución de élite en donde en su mayoría necesitan de un punto de acceso hacia el Internet, es cada vez mayor la necesidad de contar con recursos informáticos que apoyen al crecimiento educativo del alumno y fortalezcan los conocimientos por parte de los maestros. Es bien sabido que la tecnología se mueve a pasos agigantados y los profesores se apoyan en muchas ocasiones de los recursos electrónicos para sus clases y el desarrollo de los trabajos. Muchas de estas herramientas se adquieren por medio de la red Internet.

Con el aumento en las necesidades de recursos de red, el departamento de Sistemas del Colegio internacional SEK-QUITO, creó aulas informáticas para cada sistema y apoyan al alumno en las necesidades de cómputo que requiere en las diferentes materias, mas

esto no fue suficiente y se empezaron a instalar servicios sin restricciones de acceso inalámbrico en diferentes secciones de la Institución, logrado que cualquier persona, ya sea o no del Instituto, pueda gozar de los beneficios de este servicio. Cabe mencionar que muchos de los alumnos y maestros cuentan con equipos portátiles y estos en su mayoría contienen tarjetas inalámbricas. Se presentaron varios problemas, uno fue que debido a la gran población con la que cuenta la Institución tanto de alumnos como personal y las variadas características de los equipos de acceso inalámbrico, es muy difícil llevar una administración por medio de listas de acceso en cada equipo, dejando así el servicio abierto. Un problema mas es que el Colegio Internacional SEK-QUITO, se encuentra ubicado en un sector en donde existe una gran cantidad de población en sus alrededores que potencialmente puede aprovecharse y explotar el recursos sin discreción, ocasionando saturación en nuestra red y lo que puede ser peor ataques a nuestros servidores o realizar algún ataque a un sitio remoto utilizando nuestra infraestructura de red.

La meta principal era que un alumno independientemente de su ubicación, pudiera disponer de los recursos inalámbricos. Es por ello que se pensó en un proyecto que pueda resolver los siguientes puntos:

- Ubicar todos los equipos inalámbricos de la Institución así como su cobertura
- Analizar la factibilidad de configurar los conmutadores de datos a los que se encontraban conectados estos puntos de acceso
- Diseñar un esquema de protección para todos los equipos inalámbricos
- Diseñar la manera de implementar este sistema, tomando en cuenta de que muchos maestros y alumnos no cuentan con mucho conocimiento respecto a hardware.
- Sacar estadísticas de uso y monitoreo de tráfico en la red inalámbrica.

Una vez planteado lo anterior, se procedió a tratar de realizar estos puntos de la manera más fácil posible.

La mayoría de los incidentes de seguridad inalámbrica se producen porque los administradores de los sistemas no implementan las contramedidas disponibles. Por consiguiente, el asunto no es solamente confirmar la existencia de una vulnerabilidad

técnica y encontrar una contramedida que funcione. También es crítico verificar que la contramedida está en su sitio y que funciona correctamente.

Aquí es donde la rueda de seguridad WLAN, que es un proceso de seguridad continuo, se muestra eficaz. Esta rueda promueve la aplicación de medidas de seguridad a la red. Y lo que es más importante, también promueve el hecho de volver a probar y aplicar medidas de seguridad actualizadas de forma continua.

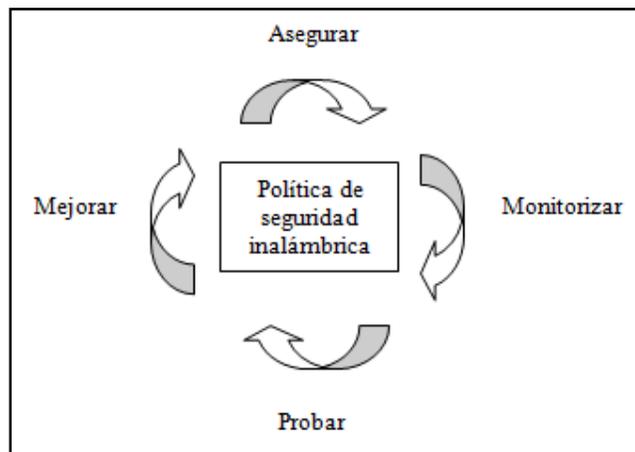


Figura 7.1 Rueda de Seguridad en una WLAN

Como se muestra en la figura la seguridad WLAN es un proceso continuo construido alrededor de una política de seguridad inalámbrica. Los cuatro pasos de la rueda de seguridad WLAN son los siguientes:

- **Paso 1: Asegurar**

Este paso implementa las soluciones de seguridad WLAN para detener o evitar el acceso o las actividades no autorizadas y para proteger la información utilizando lo siguiente:

- Autenticación 802.1x
- Encriptación o cifrado
- Integridad
- Filtros de tráfico
- Deshabilitar o asegurar los servicios
- Control de área de cobertura inalámbrica

- **Paso 2: Monitorizar**

Este paso implica las siguientes acciones:

- Detectar violaciones de la política de seguridad de la WLAN
- Auditar el sistema implicado, anotar registros y detectar intrusiones en tiempo real
- Detectar los AP falsos
- Validar la implementación de seguridad del paso 1 de la rueda de seguridad WLAN

- **Paso 3: Probar**

Este paso valida la eficacia de la política de seguridad de la WLAN mediante la auditoría del sistema y la búsqueda de vulnerabilidades inalámbricas y cableadas.

- **Paso 4; Mejorar**

Este paso implica las siguientes acciones:

- Utilizar la información de los pasos 3 y 4 para mejorar la implementación WLAN
- Ajustar la política de seguridad a medida que se identifiquen vulnerabilidades y riesgos en el ámbito inalámbrico.

Una política de seguridad inalámbrica eficaz funciona para garantizar que los recursos de red de la empresa están protegidos ante el sabotaje y el acceso no apropiado, lo que incluye el acceso intencionado y accidental. Todas las funciones de seguridad inalámbrica deben configurarse de conformidad con la política de seguridad de la Institución.

Complementariamente a las seguridades inalámbricas que se implementen, se debe mencionar que en el servidor 192.168.5.254, se encuentra instalado el software Websense, el mismo que proporciona una combinación única de inteligencia web, de contenidos y de usuarios para bloquear las amenazas en sus lugares de origen y controlar con exactitud el quién, qué, dónde y cómo de la seguridad de la red del Colegio Internacional SEK-QUITO.

Websense

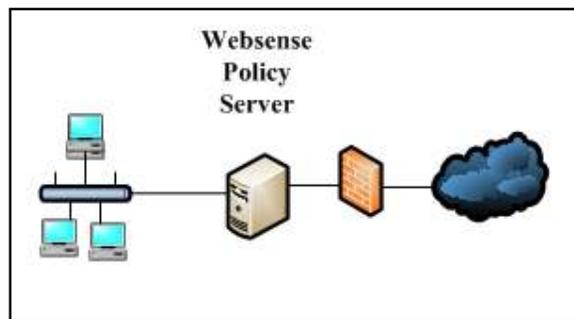


Figura 7.2 Websense Policy Server

La Web está evolucionando rápidamente y adquiriendo mayor dinamismo con las aplicaciones Web 2.0 interactivas. Pero también está siendo utilizada cada vez más para el lanzamiento de numerosos y diversos ataques. Abundan los sitios web maliciosos y sitios inocentes de terceros son víctimas de malware y crimeware incorporados. Las amenazas de phishing continúan evolucionando con ataques más sofisticados y destinados a objetivos puntuales. Se utilizan con mayor frecuencia las explotaciones de navegadores y sistemas operativos, incluidas las explotaciones de vulnerabilidades del día cero utilizadas por el spyware, el crimeware, los ataques de phishing y las instalaciones de keylogging.

Nuevas amenazas demandan nuevas tecnologías

Muchas amenazas web pueden omitir las defensas perimetrales como los firewalls. Las defensas del punto final, como el software antivirus a nivel del escritorio están diseñadas para prevenir amenazas pero sólo pueden proteger contra amenazas existentes y conocidas. Es claro que las empresas necesitan una solución de defensa más completa y profunda.

Websense descubre las amenazas en sus lugares de origen

Websense combina tecnología de vanguardia y conocimientos exhaustivos sobre Internet para encontrar nuevas amenazas antes de que éstas lo encuentren a la Institución.

Websense ofrece:

- Tecnología automatizada que recorre continuamente Internet, 600 millones de sitios web por día, para detectar nuevo malware antes de que se realicen ataques. Al detectar una amenaza en su lugar de origen, Websense puede bloquearla en todas partes, desde el correo electrónico hasta el correo web, desde URL estáticas hasta sitios Web 2.0 dinámicos.
- Defensa de múltiples niveles para coartar ataques de botnets y bloquear mensajes de phishing, acceder a URL infectadas y comunicaciones caseras de botnets.³⁰



Figura 7.3 Websense

7.2 Implementación de las política y estándares de para la WLAN Colegio Internacional SEK-QUITO

El estándar IEEE 802.11 incluye WAP para proteger los usuarios autorizados de una WLAN ante una escucha casual. El estándar IEEE 802.1 WAP especifica una clave

³⁰ www.websense.com

estática que puede explotarse y utilizarse universalmente, y que será utilizada como política para la WLAN Colegio Internacional SEK-QUITO. Al utilizar WAP, tanto el cliente inalámbrico como el AP deben tener una clave WAP coincidente.

El estándar IEEE 802.11 ofrece dos esquemas para definir las claves WAP para ser utilizadas en una WLAN. En el primer esquema, un conjunto de cuatro claves predeterminadas son compartidas por todas las estaciones, incluyendo clientes y AP, de un subsistema inalámbrico. Cuando un cliente obtiene las claves predeterminadas, puede comunicarse con seguridad con las demás estaciones del subsistema. El problema de las claves predeterminadas es que cuando se distribuyen ampliamente, es más probable que se vean comprometidas. El equipo WLAN de CISCO utiliza este primer esquema, que es compatible Wi Fi.

El segundo esquema cada cliente establece una relación clave-asignación con otra estación. Es la forma de funcionamiento más segura, porque son menos estaciones las que tienen las claves. No obstante la distribución de dichas claves unidifusión se complica a medida que aumenta el número de estaciones.

Configuración de la seguridad de una WLAN

Daremos unos de los diez pasos top ten de la configuración de seguridades en los equipos Aironet1310 de CISCO:

- Tener una política de seguridad inalámbrica
- Tener una seguridad física fuerte y una instalación correcta
- Controlar los niveles de potencia, la cobertura de la antena y el tamaño de la célula
- Evitar los ajustes predeterminados para las contraseñas, los SSID, etc.
- Desactivar los protocolos, servicios, la difusión de los SSID, etc., innecesarios.
- Utilizar WAP
- Utilizar contraseñas sólidas
- Utilizar filtros de capas 2,3 y 4
- Mantener actualizado el firmware

- Administrar los dispositivos a través de conexiones SSH o SSL

Además, debemos tener algunas recomendaciones de seguridad para el tráfico de administración de la red:

- Active la autenticación del usuario para la interfaz de administración
- Elija unas cadenas de comunidad sólidas para el protocolo simple de administración de redes SNMP, y modifíquelas a menudo
- Considere el uso de SNMP de sólo lectura si la infraestructura de administración lo permite
- Desactive los protocolos de administración inseguros y no esenciales proporcionados por el fabricante
- Limite el tráfico de administración a una subred cableada dedicada
- Donde sea posible, cifre todo el tráfico de administración remoto

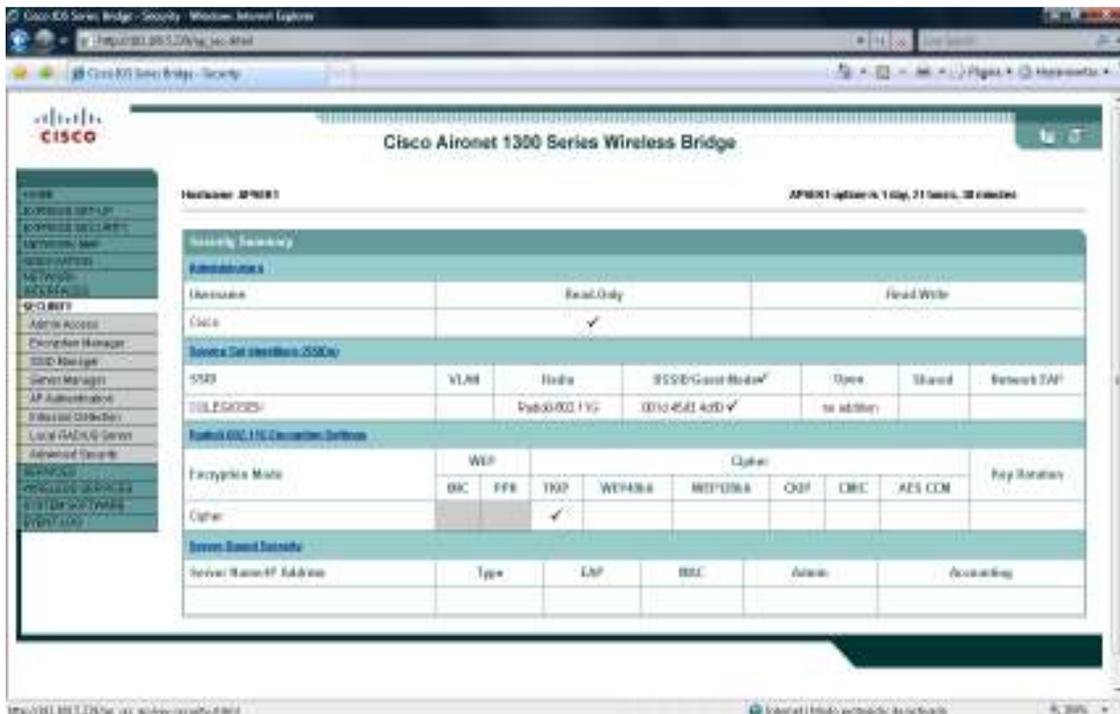


Figura 7.4 Opción Seguridad

7.2.1 Pruebas y Monitoreo WLAN Colegio Internacional SEK-QUITO

El registro de eventos a través de SNMP es muy importante en el proceso de seguridad global. Como se muestra en la siguiente figura, para SNMP se pueden definir niveles de notificación de eventos.

Para hacer la prueba de implementación de seguridades, seguimos el siguiente procedimiento:

- Con un ordenador vamos autenticarnos al punto de acceso del Colegio Internacional SEK-QUITO

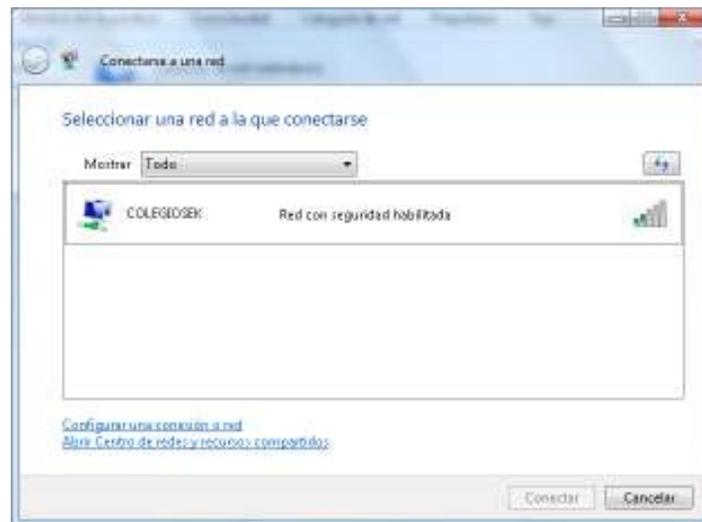


Figura 7.5 Autenticación Punto de Acceso

- Introducimos la contraseña para el cifrado, podemos esconder los caracteres o no, según lo deseado.

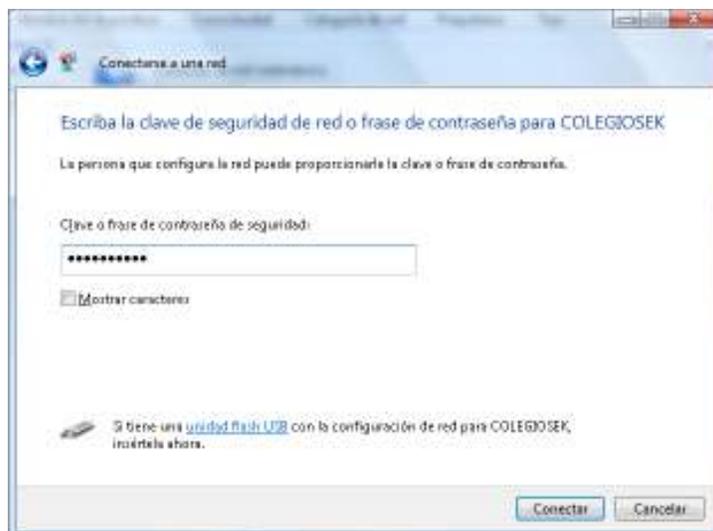


Figura 7.6 Contraseña

- Vemos que la conexión ya es real, y se pone de manifiesto en un icono de la Área de notificación de la barra de tareas. Aun así para comprobarlo, podemos hacer doble clic sobre ese icono. Y si ese icono no saliera podemos hacerlo mediante acceso al panel de control y en conexiones de red y veremos fácilmente el icono que caracteriza a este tipo de conexión inalámbrica, pues simplemente doble clic en él y también nos saldrá la misma pantalla. Pero siempre sale el icono a menos que este ocultado por nosotros.

Existe un sistema completo de seguridad basado en las siglas AAA que significan:

- **Autenticación**
Permite que un usuario demuestre su identidad a partir de la aplicación de una llave que generalmente será un ID y una contraseña. Cuando el usuario valida en un sistema dado, se dice que esta autenticando o demostrando su identidad. A raíz de esto el sistema puede actuar de muchas formas.
- **Autorización**
La autorización se refiere a los esquemas necesarios para gestionar a un usuario autenticado los recursos que podrá utilizar. Generalmente esta

parte del esquema de seguridad proporciona información sobre los permisos de los recursos a los cuales el usuario autenticado tiene acceso.

- **Contabilidad**

Se refiere al chequeo directo de los procesos, aplicaciones, tiempo, etc. que el usuario utiliza durante su tiempo de validación. Es decir, después que un usuario ha validado y sus recursos han sido autorizados, este puede efectuar diferentes procesos dentro del sistema, al control de estos procesos se le denomina contabilidad.

Algunas de las principales debilidades en WLAN

- Autenticación de dispositivo pero no de usuarios.
- Pobre encriptación de datos.
- Pobre integridad de datos.

Capítulo 8

8 CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

- Se ha podido cumplir con los objetivos planteados al inicio del proyecto, que era la realización del diseño e implementación de una Red Inalámbrica para el Colegio Internacional SEK-QUITO, los mismos que permitieron obtener datos reales acerca de las deficiencias que la Institución sufría.
- La implementación de la tecnología de redes inalámbricas nos permite una gran movilidad, reducción de costos de infraestructura y además una gran escalabilidad de la red entre otros, para que todo esto funciones de una manera adecuada se debe tomar en cuenta la seguridad ya que la confidencialidad en estas es vulnerable.
- El uso del diseño jerárquico en la actualidad en las instituciones es muy necesario ya que permite una alta velocidad de acceso a los datos por parte de los usuarios y clientes.
- Todo mecanismo de seguridad siempre debe estar ligado a políticas de seguridad creadas por las personas encargadas del área de tecnología, permitiendo esto alcanzar un alto grado de seguridad en los segmentos de la red que no son controlados de manera física o tangible.
- La migración de redes a nuevos diseños como son las redes jerárquicas donde las reglas del negocio en cada nivel se separan permitiendo una mayor administración, son cada vez más comunes, pues la aparición de nuevas tecnologías provoca dicha migración.
- La adición de un segmento inalámbrico a la red existente, provoca que la red de datos se vuelva mucho más versátil permitiendo a los usuarios movilizarse sin la preocupación de quedarse sin conectividad.

- La principal característica que define las organizaciones educativas de hoy en día es la presencia y dependencia de los sistemas informáticos bajo la forma de Redes Locales Inalámbricas, las cuales representan la punta de lanza de una organización educativa.
- La población del Colegio Internacional SEK-QUITO sigue en aumento, por tal motivo las áreas de estudio siguen creciendo obligando a la Institución seguir creciendo de acuerdo a las necesidades de la sociedad por consiguiente, el diseño y la implementación de Redes Inalámbricas fue inevitable para facilitar la comunicación, la transmisión de datos e información y la descentralización de servicios que actualmente se prestan en la biblioteca, laboratorios de informática y salas de profesores.
- El instalar redes WLAN en nuestros bloques, biblioteca, áreas de recreación, etc., nos ofreció muchas ventajas para el trabajo diario de los alumnos, docentes y personal administrativo. Estas son algunas ventajas ofrecidas al implementar una red inalámbrica de computadoras:
 - Compartición de programas y archivos.
 - Compartición de los recursos de la red.
 - Compartición de bases de datos.
 - Posibilidad de utilizar software de red.
 - Uso del Correo Electrónico.
 - Creación de grupos de trabajo.
 - Gestión centralizada.
 - Seguridad.
 - Mejoras en la organización de la Institución.
- Las pruebas de cobertura de la Red Inalámbrica permitieron diagnosticar la calidad de los enlaces en ambientes externos y el rango de cobertura que los AP tenían en ambientes internos, siendo pruebas de tipo experimental.
- Para que no exista ningún problema de traslapamiento entre estaciones de trabajo con el AP que es designado, se utilizaron los canales 1,6 y 11. A pesar de que no existe restricción legal sobre el diseño de una LAN Inalámbrica que tenga un uso menor o mayor de un canal, normalmente es recomendable usar los tres canales, ni más ni uno menos, para alcanzar el mejor balance entre capacidad y la confiabilidad.

8.2 RECOMENDACIONES

- Las universidades como centros de investigación siempre deben de buscar tecnologías que permitan dar el mismo o mejor servicio a menor costo, así como explotar el conocimiento y la iniciativa de los alumnos, bajo la acertada guía de los docentes.
- Se debe instruir a los usuarios sobre el buen uso de las computadoras portátiles, educando a que los usuarios no abusen de los recursos compartidos que otras computadoras puedan proporcionar.
- Los encargados del área tecnológica deben tener en claro como funciona el diseño jerárquico de la red, diferenciando para que sirve cada capa para así poder implementar nuevas tecnologías o añadir nuevos requerimientos de la red.
- Se recomienda realizar un estudio con la finalidad de implementar VoIP, en el Colegio Internacional SEK-QUITO, ya que todas las áreas sin excepción poseen servicio de Internet de banda ancha, facilitando de esta manera la comunicación entre ellas en forma gratuita.
- Implementar en la Carrera de Sistemas de la UISEK una asignatura teórica como práctica en que se estudie el desarrollo de estas nuevas tecnologías que significan la solución a problemas de la sociedad abaratando costos y dando un buen servicio.
- Realizar continuamente una evaluación a la solución implementada para el Colegio Internacional SEK-QUITO con la finalidad de tener en cuenta los estándares y tecnologías nuevas y de mayor penetración, lo cual nos ahorrará dinero, tiempo y problemas de incompatibilidad y nos brindará una comunicación rápida, eficiente y transparente.
- Se debe contar con herramientas de seguridad en la red con el fin de evitar interferencias o interceptaciones a nuestras comunicaciones de datos por parte de sistemas ajenos a nuestra red.
- Es recomendable cambiar todas las configuraciones que vienen pregrabadas por defecto por el fabricante en los equipos a utilizar, para garantizar que ningún intruso tenga acceso a los mismos y pueda realizar daños a la red.

- Se recomienda dar un mantenimiento a los equipos inalámbricos por lo menos cada tres meses, evitando así que estos se deterioren e impidan el correcto funcionamiento de la Red Inalámbrica del Colegio internacional SEK-QUITO.
- El personal que estará a cargo de la Red, debe dar capacitación a todos los alumnos, docentes y personal administrativo ya sea en relación a las ventajas que obtendrán con la infraestructura implementada.
- Es recomendable que el Administrador de Red realice una buena administración de los recursos y aplique políticas de seguridad a la red, para que ésta funcione correctamente y sea explotada por los usuarios de manera óptima.

ANEXOS

ANEXO A

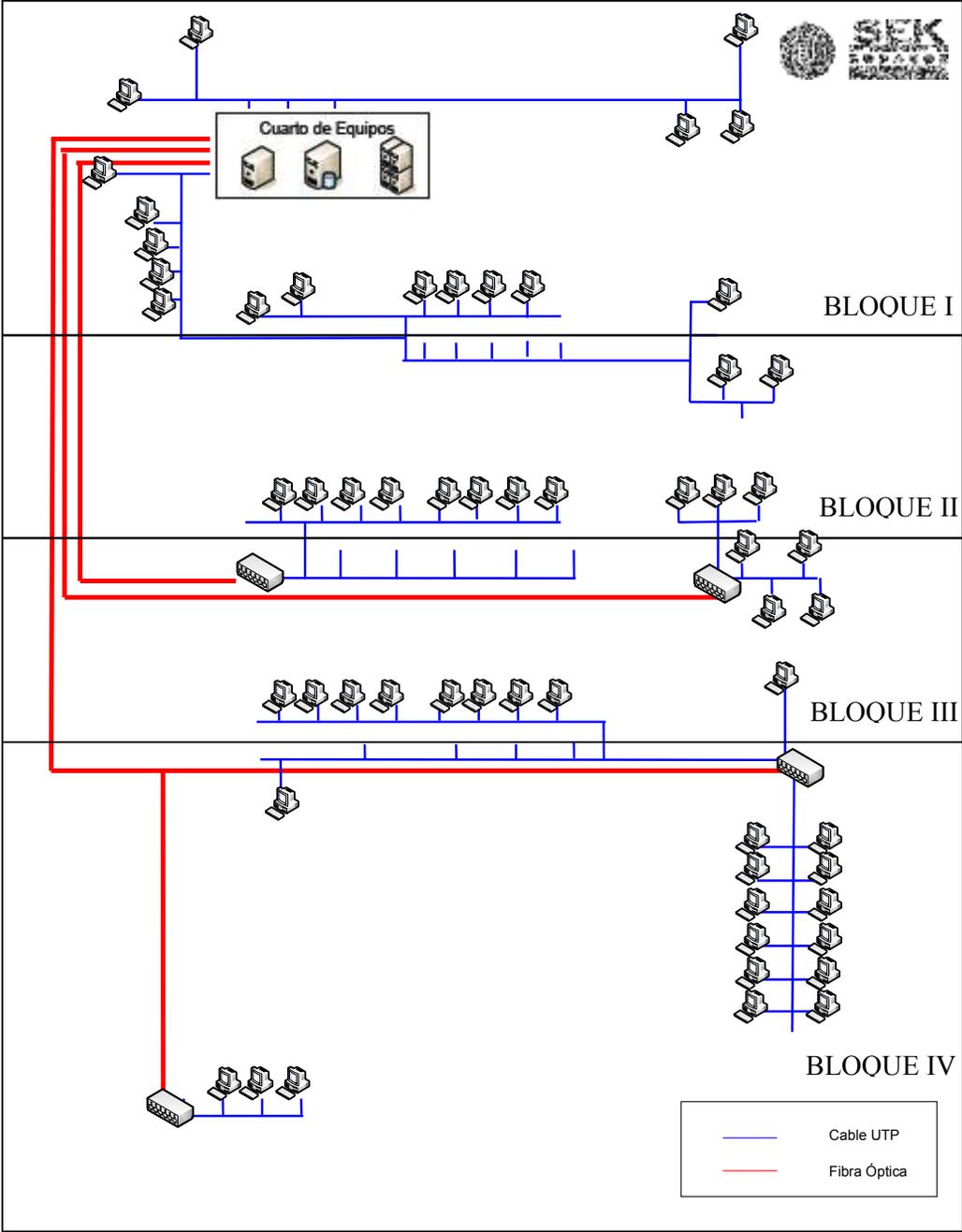
ESQUEMA DE LA DISTRIBUCIÓN DEL CABLEADO DE LA RED

En el siguiente mapa de red se detallan las direcciones IP que tiene cada punto de red en al anterior anexo:

Mapa de Red		
N°	IP ADDRESS	NAME
1	192.168.5.254	Servidor 1
2	192.168.5.253	Servidor 2
3	192.168.5.201	Administración
4	192.168.5.202	Dirección
5	192.168.5.203	Admisiones
6	192.168.5.204	Recepción 1
7	192.168.5.205	Recepción 2
8	192.168.5.206	Rectorado
9	192.168.5.207	Almacén
10	192.168.5.208	BI
11	192.168.5.209	Contabilidad 1
12	192.168.5.210	Contabilidad 2
13	192.168.5.211	Caja 1
14	192.168.5.212	Caja 2
15	192.168.5.231	Recepción
16	192.168.5.232	Contabilidad 1
17	192.168.5.233	Pre Escolar
18	192.168.5.234	Secretaría Primaria
19	192.168.5.235	Biblioteca
20	192.168.5.236	Secretaría Secundaria
21	192.168.5.246	Música 1
22	192.168.5.247	Música 2
23	192.168.5.214	Jefatura Primaria
24	192.168.5.215	Secretaría Primaria
25	192.168.5.216	Biblioteca
26	192.168.5.217	Sicología
27	192.168.5.218	Jefatura Secundaria
28	192.168.5.219	Secretaría Secundaria
29	192.168.5.250	Sistemas
30	192.168.5.251	Sistemas

ANEXO B

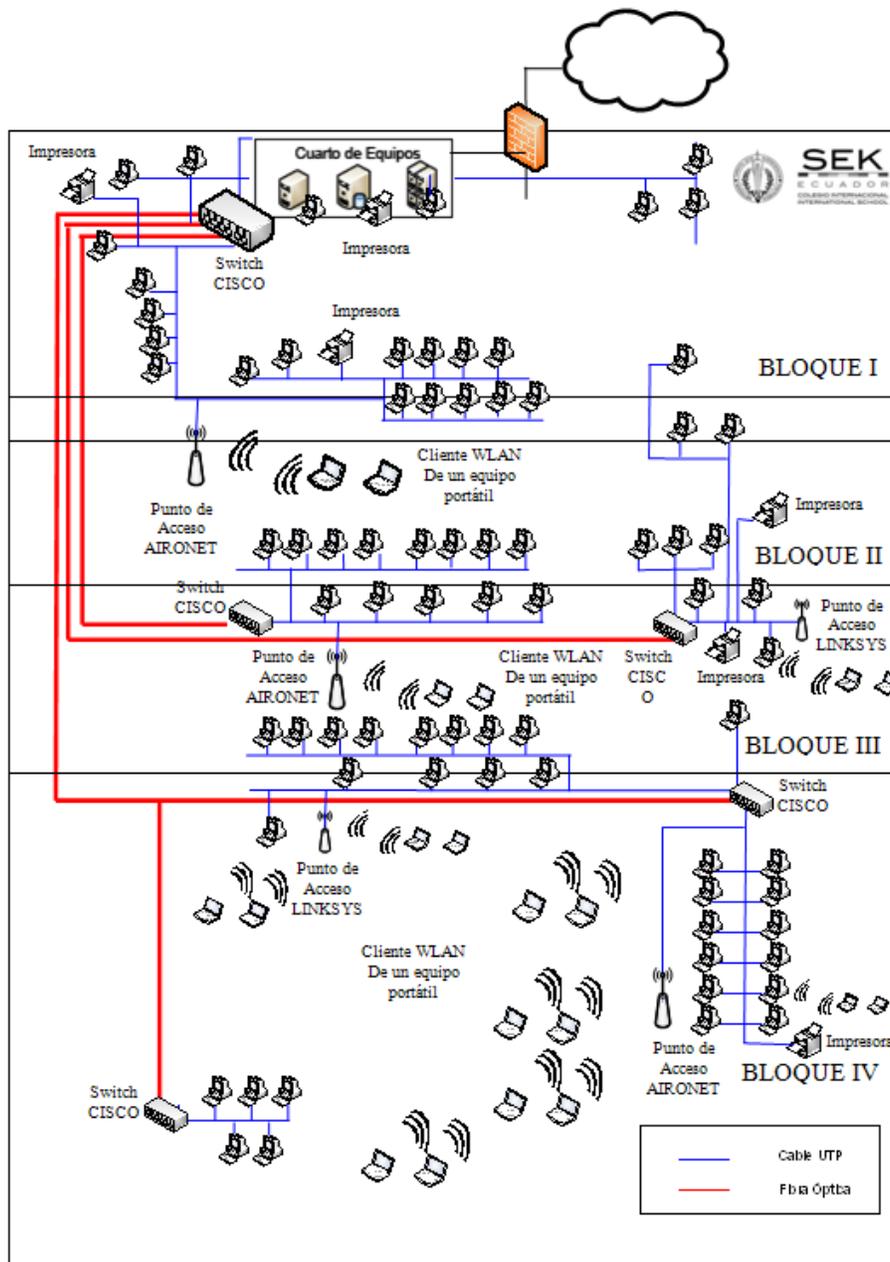
ESQUEMA DE CONEXIÓN FÍSICA DEL COLEGIO INTERNACIONAL SEK-QUITO



ANEXO B – Esquema Conexión Física Colegio Internacional SEK-QUITO

ANEXO C

DISEÑO WLAN PROPUESTO PARA EL COLEGIO INTERNACIONAL SEK-QUITO



ANEXO C – Diseño WLAN propuesto para el Colegio Internacional SEK-QUITO

ANEXO D

DATASHEET 3COM 4800G

Premium Gigabit Switches with Enhanced IPv4/IPv6 Networking, and Maximum Security, Convergence and Intelligence

OVERVIEW

The 3Com® Switch 4800G Gigabit Family delivers outstanding security, reliability and multi-service support capabilities for robust switching at the edge or aggregation layer of large enterprise networks and campus networks, or in the core layer of medium- and small-sized enterprise networks. The family is comprised of Layer 2/3/4 Gigabit Ethernet switches that can accommodate the most demanding applications, providing resilient and secure connectivity and the latest traffic-prioritization technologies to optimize applications on converged networks.

Designed for maximum flexibility, these models are available with 24 or 48 Gigabit ports. The family offers Power over Ethernet (PoE) and non-PoE models, with optional 10-Gigabit expansion capability and SFP mini-GBIC Gigabit combo ports for fiber flexibility. An additional, all-SFP model with dual power supplies, for highest availability applications, allows for very flexible fiber with copper Gigabit connectivity.

Each of the five 3Com Switch 4800G models comes in a convenient, stackable 1U-high enclosure:

- › Switch 4800G 24-Port: 24 10/100/1000 Mbps ports with two dual-port 10-Gigabit slots; includes four SFP Gigabit combo ports
- › Switch 4800G 48-Port: 48 10/100/1000 Mbps ports with two dual-port 10-Gigabit slots; includes four SFP Gigabit combo ports
- › Switch 4800G PWR 24-Port: 24 10/100/1000 Mbps PoE ports with two dual-port 10-Gigabit slots; includes four SFP Gigabit combo ports
- › Switch 4800G PWR 48-Port: 48 10/100/1000 Mbps PoE ports with two dual-port 10-Gigabit slots; includes four SFP Gigabit combo ports
- › Switch 4800G 24-Port SFP: 24 SFP Gigabit ports with two dual-port 10-Gigabit slots and dual removable power supplies, with up to two power-cord inputs; includes eight 10/100/1000 Mbps combo ports



from top: 3Com Switch 4800G 24-Port, Switch 4800G 48-Port, Switch 4800G 24-Port SFP, Switch 4800G PWR 24-Port, Switch 4800G PWR 48-Port

KEY BENEFITS

HIGH EXPANDABILITY FOR INVESTMENT PROTECTION

All models in the 3Com Switch 4800G Gigabit Family include auto-sensing 10-, 100- and 1000-Mbps connections, giving you the ability to gradually upgrade your edge connections to higher bandwidth while retaining full compatibility with slower desktops. Support for dual-speed SFPs facilitates connections to both 100 and 1000 MB fiber cabling, making network migration easier.

Two expansion slots, each supporting available 1-port or 2-port 10-Gigabit extension modules, allow for the adoption of 10-Gigabit interfaces for high bandwidth unit-to-unit local connections and uplinks, helping you to protect your network investment.

Every Switch 4800G model has the ability to pass and route IPv4 and IPv6 data. As an IPv4/IPv6 dual-stack platform, the switches are IPv4- and IPv6-ready, supporting the major L3 routing protocols, multicast protocols and policy routing mechanisms and ensuring a seamless migration from IPv4 to IPv6.

Premium Security

Multiple layers of security are built into each Switch 4800G. Management access can be limited to known stations and unauthorized access can be prevented by encrypting management traffic with SSH for CLI access, SSL/HTTPS for web access and SNMPv3 for SNMP management access.

Advanced processor queuing mechanisms prevent Denial of Service (DOS) attacks while DHCP servers preserve data integrity. Enhanced Access Control Lists (ACLs) restrict users to certain areas of your network. Unicast Reverse Path Finding (uRPF) technology verifies the authenticity of a route from the receiving interface to the source address, deleting the data packet if the route does not exist and preventing malicious network attacks that are based on source address spoofing.

Advanced network access control features, including IEEE 802.1X and MAC-based network login, ensure that only authorized users get access to the network.

Multilayer Reliability

3Com 4800G switches interoperate with a number of link reliability technologies including Rapid Ring Protection Protocol (RRPP), a fast ring protection mechanism created by 3Com. If a link or node on the Ethernet ring fails, RRPP rapidly moves traffic to a backup link, ensuring normal operations without impacting network convergence time. Other network resiliency features include Spanning Tree, Rapid Spanning Tree and Multiple Spanning Tree protocol support.

Hardware resiliency, delivered with available redundant power system support, allows for the continued operation of the switch in the event of a power supply failure, and supplements power for full PoE operation across all ports. For high-availability fiber connections, the Switch 4800G 24-Port SFP comes with dual 1+1 redundant power supplies with dual power inputs. All switches in this family include fault detection and alarms, power supply and fan monitoring, and remote management.

KEY BENEFITS (CONTINUED)

Redundant Power System Support

Four 3Com Switch 4800G models support a redundant power system (RPS) connection.

RPS units provide these benefits:

- › For PWR switches, an RPS can deliver more power budget for IEEE 802.3af Power over Ethernet than what the switches alone can provide. For example, the 48-port PWR switch has a PoE power budget of 370 Watts, which means that approximately half of the ports can provide the full 802.3af PoE power of 15.4 Watts. With an RPS providing power, all 48-ports can provide a full 15.4 Watts of PoE power.
- › They deliver redundant power to switches so there is continued operation should the main switch unit power supply fail. This allows for continuous operation of advanced Enterprise networks, particularly important for converged networks running IP phones on the network.

3Com switches are compatible with these RPS solutions:

Eaton Powerware RPS

3Com's recommended premium solution is made by Eaton Powerware. Eaton is an industry leader in enterprise-capable power solutions, and they designed and released an RPS line for 3Com with standard -48V DC connections, one that stands up to the rigors of an enterprise switch network with Power over Ethernet. The units have a customizable design, can be built for highest N+1 redundancy, support a full stack up to eight-high of PoE switches, support integrated battery backup units, and can be remotely monitored.

H3C RPS 1000

The H3C RPS 1000 is manufactured by H3C, a 3Com company. The RPS 1000 is a 1U high design which operates with one or two power rectifiers, providing -48V DC connections for H3C and 3Com-branded stackable switches. The unmanaged unit supports up to two connections at 25A for PWR switches, and up to six connections at 8A for non PWR switches, with support of 1+1 power redundancy.

H3C RPS 500

The H3C RPS 500 is manufactured by H3C, a 3Com company. The RPS 500 is a fixed configuration 1U high design with a single rectifier and a single power connection. It can provide -48V and +12V DC connections for H3C and 3Com-branded non-PWR stackable switches.

The table below summarizes RPS support for the 3Com Switch 4800G.

Switch 4800G Model	RPS Support	Eaton Powerware	H3C RPS 1000	H3C RPS 500
PWR 24-Port	Yes [-48V]	Yes	Yes	No
PWR 48-Port	Yes [-48V]	Yes	Yes	No
24-Port	Yes [+12V]	No	No	Yes
48-Port	Yes [+12V]	No	No	Yes
24-Port SFP	No- use 2x PSU for power redundancy			

Table 1: Redundant power supply support for the 3Com Switch 4800G

ANEXO E

DATASHEET SUPERSTACK 3226



3Com® SuperStack® 3 Switch 3200 Family

DATA SHEET



- Wirespeed, Layer 2/3 switches with 10/100 desktop connections and Gigabit downlinks
- Dynamic Layer 3 routing simplifies implementation
- IEEE 802.1X network login and RADIUS authentication

Key Benefits

Performance

Wirespeed, non-blocking Layer 2/3 switching for 10/100 desktop connections with built-in Gigabit downlinks. Packet prioritization gives optimal performance to real-time applications such as voice and video. Link aggregation of the downlinks enables high-performance connectivity to the core of the network, with resiliency to improve availability and uptime. Layer 3 switching at the edge enables fast switching of traffic between local subnets while offloading routers in the core of the network.

Flexibility

Available in managed 50- or 26-port configurations, with 48 or 24 auto-sensing 10/100 ports and two dual-personality ports for 10/100/1000 or SFP connectivity.

Ease of Use

Supports dynamic routing through RIP, with automatic updating of the Layer 3 network without any manual intervention. Much easier than implementing static routes.

Automatically auto-negotiates speed and duplex mode of cables connected to it preventing misconfiguration of the network. Switches detect and adjust to cross-over or straight-through cable connections— a feature called auto MDI/MDIX— eliminating the need for specific crossover cables.

Scalability

Supports up to 2,000 external routes, allowing the switch to scale as the network grows—ideal for deployments at the edge of a network. Supports up to 255 VLANs and standards-based IEEE 802.3ad trunking (LACP).

Rate limiting enables the bandwidth on each port to be restricted, preserving network bandwidth and allowing maximum control of network resources.

Security

Supports IEEE 802.1X network login to secure user entry into the network, with access control directed from a central standards-based RADIUS server for ease of management. Intrusion prevention features protect the network and will discard all packets from unauthenticated users.

Port-based Access Control Lists further enhance security. Communication of attached stations can be restricted to certain destinations, in essence segmenting the network into more secure areas.

Management of the switch can be implemented using Secure Shell (SSH) and Secure Sockets Layer (SSL/HTTPS) encryption (56 or 168 bit) preventing unauthorized remote access to the switch over IP networks or from a web browser.

Network Control

Network management through embedded web interface, command line interface, or an SNMP management station. Network management is further simplified with the use of 3Com Network Supervisor for configuration and troubleshooting of multiple devices on the network.

Limited Lifetime Hardware Warranty
Limited Lifetime Hardware Replacement. See www.3com.com/warranty for details.

Service

3Com products are backed by 3Com Global Services and authorized partners with demonstrated expertise in network assessment, implementation, and maintenance. Ask about 3Com's Network Health Check, installation services, and maintenance service packages available in your area.

3Com® SuperStack® 3 Switch 3200 family switches are wrespeed, Layer 3 switches with 10/100 desktop connections and Gigabit downlinks for high performance connectivity to the rest of the network. These switches support dynamic Layer 3 routing, simplifying the implementation of Layer 3 networks by automatically configuring and updating the switch with all topology changes. This ability to dynamically reconfigure the routing provides a significant benefit over the use of static routes, avoiding the drawback of many Layer 3 switches which require manual intervention when changing the topology of the network.

The SuperStack 3 Switch 3200 is optimized for edge desktop connections. Layer 3 switching for the network's edge, with the Switch 3200's hardware-based wrespeed routing, improves performance by routing locally without data having to travel back to the network core. This is especially useful in organizations having or anticipating multiple subnets in their workgroups, where even local traffic may otherwise need to be routed via a core switch.

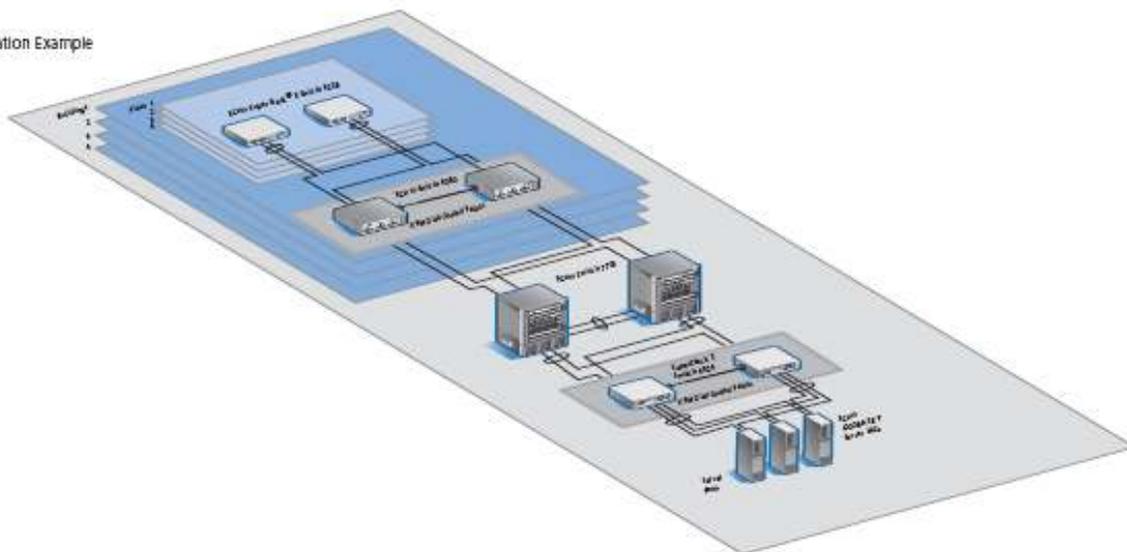
Also, for edge-optimized deployment, the SuperStack 3 Switch 3200 supports the learning of up to 2,000 IP routes through an uplink to a core router using Router Internet Protocol (RIP). This high number of routes enables the switch to operate in larger networks than can other switches which have significantly smaller numbers of routes.

The SuperStack 3 Switch 3200 also supports core-level switching in smaller networks, with local routing for 32 IP interfaces and up to 14 routes distributed from other local Layer 3 devices.

The SuperStack 3 Switch 3200 family confirms 3Com's commitment to strong network security. Its implementation of IEEE 802.1X network login security helps ensure all users are authorized before being granted access to any network resource. User authentication is carried out using any standards-based RADIUS server, avoiding any proprietary authentication mechanisms.

Containment of users to specific areas of the network can be easily controlled through Access Control Lists (ACLs), restricting the IP addresses with which a port can communicate.

Configuration Example



3COM® SUPERSTACK® 3 SWITCH 3200 FAMILY DATA SHEET

Features

PERFORMANCE	
Switching capacity	SuperStack 3 Switch 3226, 8.8 Gbps; Switch 3250, 13.6 Gbps
Forwarding rate	Switch 3226, 6.6 Mpps; Switch 3250, 10.1 Mpps Store-and-forward switching; latency <12 µs
LAYER 2 SWITCHING	
MAC Address	8K MAC addresses
VLAN	255 VLANs (IEEE 802.1Q)
Link Aggregation	IEEE 802.1ad (LACP), Gigabit ports only
Auto-negotiation	Auto-negotiation of port speed, duplex, and connection (MDI/MDIX)
Traffic control	IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex Supports Broadcast Storm Suppression (3,000 pps threshold)
Spanning Tree Protocol / Rapid Spanning Tree Protocol	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Backward-compatible with Spanning Tree Protocol (STP) Fast-start mode Spanning tree enable/disable per port
LAYER 3 SWITCHING	
Routes	Hardware based routing 2,001 IP routes: 1,990 dynamic and 10 static Address Resolution Protocol (ARP) entries with 1 user default route
IP Routing	32 IP Interfaces Multi-netting (multiple IP interfaces per VLAN) Routing Information Protocol (RIP), v1 and v2 <ul style="list-style-type: none"> • Split Horizon • Split Horizon with poisoned reverse • Triggered updates • MD5 authentication of the RIP packets • Password authenticated RIP packets • Host route advertisements
Multicast	Filtering for 64 multicast groups Internet Group Management Protocol (IGMP) snooping on Layer 2 interfaces IGMP v1 and v2 IGMP Querier
Network protocol	Dynamic Host Configuration Protocol (DHCP) Helper/Relay UDP Helper ARP, ARP Proxy
CONVERGENCE	
Priority Queues	Four hardware queues per port Weighted Round Robin queuing
Traffic Prioritization	Priority based on: <ul style="list-style-type: none"> • DiffServ Code Point (DSCP) • IEEE 802.1p Class of Service (CoS) VLAN priority • TCP/UDP destination port number • Default port priority • Auto classification of 3Com NBX® telephony traffic
Bandwidth Management	Port-based bandwidth management: <ul style="list-style-type: none"> • 1 Mbps increments (10/100 ports) • 8 Mbps increments (Gigabit ports)

ANEXO F

**TABLA DE ÁREAS DE LA CURVA NORMAL ENTRE LA
ORDENADA MÁXIMA Y LA ORDENADA EN Z**

BIBLIOGRAFÍA

- [1] UYLES BLACK, “Redes de Computadoras”, Alfaomega, 2003.
- [2] FRENZEL LOUIS E., “Sistemas Electrónicos de Comunicación”, Alfaomega, 2003
- [3] DOUGLAS COMER, TCP/IP, Vol 1, Prentice Hall, 1996.
- [4] RON SEIDE, “Cómo Funcionan Las Redes Inalámbricas”, RÚSTICA, 2005.
- [5] STALLINGS WILLIAM, “Comunicaciones y Redes de Computadoras”, Pearson Educación, 2004.
- [6] DIANE TEARE, CATHERINE PAQUET. “Campus Network Design Fundamentals”, Indianapoli: Cisco Press, 2006.
- [7] JESÚS GARCÍA TOMÁS, “Alta velocidad y calidad de servicios en redes IP”, Alfaomega, 2006.
- [8] JOSÉ MANUEL DÍAZ, “Fundamentos de redes inalámbricas”, Rigorma Grafic S.I, Impreso en España, Traducido de: “Fundamentals of Wireless LANs Companion Guide (Cisco Networking Academy Program), 2005
- [9] TOMASI WAYNE, “Sistemas de Comunicaciones Electrónicas”, Prentice Hall, 1996.
- [10] RANDALL K. NICHOLS & PANOS C. LEKKAS, “Seguridades Para Comunicaciones Inalámbricas”, Edigrafos S.A., 2004
- [11] JOSÉ A. CARBALLAR, “Wi-Fi Cómo construir una red inalámbrica”, Alfaomega, 2005.
- [12] JESÚS GARCÍA TOMÁS, Alta velocidad y calidad de servicios en redes IP, Alfaomega, 2002.
- [13] www.mailxmail.com Información Redes
- [14] www.monografias.com Información Redes Inalámbricas
- [15] www.cybercursos.com Información Redes Inalámbricas
- [16] www.microsoft.com Información Redes Inalámbricas
- [17] www.es.wikipedia.org/wiki/Wikipedia:Portada Wikipedia Enciclopedia
- [18] <http://www.wirelessmon.com/> Software IP PBX
- [19] www.cisco.com Información Equipos Inalámbricos
- [20] www.conatel.gov.ec Legislación Redes Inalámbricas Ecuador
- [21] www.monografias.com/trabajos11/tebas/tebas.shtml#met Monografías

- [22] www.hyperlink.com Equipos Inalámbricos
- [23] www.websense.com Filtro de Contenidos WEB
- [24] Personal del Colegio Internacional SEK-QUITO