UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

TEMA:

RED WLAN SEGURA PARA LA INTERCONEXIÓN DE LOS EDIFICIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Trabajo de graduación modalidad TEMI, presentado como requisito previo a la obtención del Título de Ingeniero en Electrónica y Comunicaciones.

AUTOR: Javier Santiago Seilema Valladares

TUTOR: Ing.Eduardo Chaso

Ambato – Ecuador

Octubre - 2011

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, nombrado por el H. Consejo Superior de Pregrado de la Universidad Técnica de Ambato:

CERTIFICO:

Que el trabajo de investigación: **"RED WLAN SEGURA PARA LA INTERCONEXIÓN DE LOS EDIFICIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL"** presentado por el Sr. Javier Santiago Seilema Valladares, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato; reúne los requisitos y méritos suficientes para ser sometido a la evaluación del jurado examinador que el H. Consejo de Pregrado designe.

Ambato, Octubre 2011

EL TUTOR

……..……

Ing. Eduardo Chaso

AUTORÍA

El presente trabajo de investigación titulado: "**RED WLAN SEGURA PARA LA INTERCONEXIÓN DE LOS EDIFICIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL**" es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Octubre 2011

…….

Javier Santiago Seilema Valladares

C.I. 180426933-8

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Edwin Morales e Ing. Geovanny Brito, revisó y aprobó el Informe Final del trabajo de graduación titulado **"RED WLAN SEGURA PARA LA INTERCONEXIÓN DE LOS EDIFICIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL"**, presentado por el señor Javier Santiago Seilema Valladares de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

…….

PRESIDENTE DEL TRIBUNAL

Ing. Oswaldo Paredes

…….	……
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR
Ing. Edwin Morales	Ing. Geovanny Brito

DEDICATORIA

El presente trabajo está dedicado con mucho cariño y entusiasmo a nuestro ser supremo Dios, quien me ha dotado de dones y virtudes. A mis padres Fausto y Bilma, pilares fundamentales en mi vida. A mis hermanos por ser quienes, día a día, a base de esfuerzo, cariño y comprensión, me ayudaron a culminar con este anhelo.

Javier S. Seilema V.

AGRADECIMIENTO

Mi más sincero agradecimiento a la Universidad Técnica de Ambato, en especial a mi querida Facultad de Ingeniería en Sistemas, Electrónica e Industrial, por los conocimientos brindados a mi persona.

Al Ing. Eduardo Chaso por su acertada dirección para culminar con éxito el presente proyecto.

A Erika por su constante apoyo y dedicación, a mis Amigos y Familiares que me apoyaron y confiaron en mi persona, mil gracias.

Javier S. Seilema V.

Índice General

APROBACIÓN DEL TUTOR i
AUTORÍA ii
APROBACIÓN DE LA COMISIÓN CALIFICADORA iii
DEDICATORIA iv
AGRADECIMIENTO v
Índice General vi
Índice de Figuras xii
Índice de tablas xiv
Índice de Ecuaciones xiv
Resumen Ejecutivo xv
Introducción xvi
CAPITULO I 1
EL PROBLEMA 1
1.1 Tema 1
1.2 Planteamiento del Problema 1
1.2.1 Contextualización 1
1.2.2 Análisis Crítico 2
1.2.3 Prognosis 3
1.3 Formulación del Problema 3
1.4 Preguntas Directrices 3
1.5 Delimitación del Problema 3
1.6 Justificación 3
1.7 Objetivos de la investigación 4
1.7.1 Objetivo General 4
1.7.2 Objetivos específicos 4
CAPITULO II 5
MARCO TEÓRICO 5
2.1 ANTECEDENTES INVESTIGATIVOS 5
2.2 FUNDAMENTACIÓN 5
2.2.1 CATEGORÍAS FUNDAMENTALES 5
2.2.2 RED WLAN SEGURA 6

2.2.2.1 TELECOMUNICACIONES 6
2.2.2.1.1 Características de un sistema de telecomunicación 6
2.2.2.1.2 Radiocomunicación 7
2.2.2.1.3 Transmisión y recepción 7
2.2.2.1.4 Sistemas AM y FM 7
2.2.2.2 REDES 8
2.2.2.2.1 Clasificación 9
2.2.2.2.2 Redes fijas, inalámbricas, móviles y celulares 10
2.2.2.2.3 Protocolos de redes 11
2.2.2.2.4 Arquitectura de Redes 12
2.2.2.3 REDES WLAN 14
2.2.2.3.1 Características 15
2.2.2.3.2 Funcionamiento 15
2.2.2.3.3 Estándares 16
2.2.2.3.4 Seguridad 18
2.2.2.3.5 WLAN - Hotspot 19
2.2.2.3.6 Diseño 19
2.2.2.3.7 Implementación 21
2.2.3 INTERCONECCIÓN ENTRE LOS EDIFICIOS DE LA FISEI 22
2.2.3.1 CENTRALIZACIÓN DE LA INFORMACIÓN 22
2.2.3.2 INTERCONECTIVIDAD DE REDES 24
2.2.3.2.1 Cómo se interconectan las redes 25
2.2.3.3 INTERCONECCIÓN ENTRE EDIFICIOS 26
2.3 Hipótesis 27
2.4 Variables 27
2.4.1 Variable independiente 27
2.4.2 Variable dependiente 27
CAPITULO III 28
METODOLOGÍA 28
3.1 Enfoque 28
3.2 Modalidad básica de la investigación 28
3.2.1 Investigación bibliográfica 28

3.3 Nivel o tipo de investigación 28
3.4 Población y muestra 29
3.4.1 Población 29
3.4.2 Muestra 29
3.5 Operacionalización de variables 30
3.5.1 Variable independiente 30
3.5.2 Variable dependiente 31
3.6 Recopilación de la información 32
3.7 Procesamiento de la información 32
CAPITULO IV 33
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 33
4.1 Verificación de la hipótesis 39
4.1.1 Frecuencias Observadas 40
4.1.2 Frecuencias Esperadas 40
4.1.3 Modelo lógico 40
4.1.4 Nivel de significancia y regla de decisión 40
4.1.4.1 Grado de libertad 40
4.1.4.2 Grado de significancia 41
4.1.5 Calculo del Chi-cuadrado 41
CAPITULO V 43
CONCLUSIONES Y RECOMENDACIONES 43
5.1 Conclusiones 43
5.2 Recomendaciones 44
CAPITULO VI 45
PROPUESTA 45
6.1 Datos informativos 45
6.2 Antecedentes de la propuesta 45
6.3 Justificación 46
6.4 Objetivos 46
6.4.1 Objetivo General 46
6.4.2 Objetivos Específicos: 46
6.5 Análisis de la factibilidad 47

6.5.1 Factibilidad técnica 47
6.5.2 Factibilidad operativa 47
6.5.3 Factibilidad económica 47
6.6 Fundamentación 47
6.6.1 Modelo OSI 47
6.6.1.1 Capa física 47
6.6.1.2 Capa de enlace de datos 48
6.6.1.3 Capa de red 48
6.6.1.4 Capa de transporte 48
6.6.1.5 Capa de sesión 48
6.6.1.6 Capa de presentación 49
6.6.1.7 Capa de aplicación 49
6.6.2 TCP 49
6.6.3 IP 49
6.6.4 Router 49
6.6.5 Access Point 49
6.6.6 Switch 50
6.6.7 Wi-Fi y sus Estándares 50
6.6.8 802.11 50
6.6.9 802.11g 51
6.6.10 802.11n 51
6.6.10.1 MIMO 51
6.6.11 802.11g y 802.11n trabajando en conjunto 53
6.6.12 Arquitectura de red para el estándar 802.11 54
6.6.13 Formato de un paquete de datos (trama) en 802.11 55
6.6.14 CSMA/CA 55
6.6.15 Canales/Frecuencias utilizados por 802.11b/g/n en la banda de 2.4GHz . 56
6.6.16 Roaming entre Access points 57
6.6.16.1 Los Beacons y cómo funciona el Roaming entre APs. 57
6.6.16.2 La Problemática del Roaming 58
6.6.17 Técnicas de transmisión de datos en 802.11g/n 58
6.6.17.1 Modulación 58

6.6.17.2 Multiplexación 58
6.6.17.3 OFDM 59
6.6.17.4 PSK 59
6.6.17.5 QAM 60
6.6.17.6 QoS 61
6.6.18 Servidor de Autenticación 61
6.6.18.1 Servidor 61
6.6.18.2 Radius 61
6.6.18.3 Servidor Radius 62
6.6.18.4 Servidor Web 62
6.6.18.5 SSL 63
6.6.18.6 Base de datos 63
6.6.18.7 Sofware Libre 63
6.6.18.8 Licencia GPL 63
6.6.18.9 GNU/Linux 64
6.7 Metodología 66
6.8 Modelo operativo 66
6.8.1 Análisis del sistema 66
6.8.2 Requerimientos 68
6.8.2.1 Software 68
6.8.2.1.1 Software de diseño de la red inalámbrica 68
6.8.2.1.2 Servidor radius 69
6.8.2.2 Hardware 70
6.8.3 Diseño de la red inalámbrica 71
6.8.3.1 Calidad de servicio o QoS 71
6.8.3.2 Cálculo del ancho de banda 72
6.8.3.3 Diseño lógico y físico 73
6.8.3.4 Ubicación de los puntos de acceso en el edificio principal 74
6.8.3.5 Ubicación de los puntos de acceso en el edificio dos 77
6.8.3.6 Cálculos de cobertura realizados con el modelo Okumura-Hata 79
6.8.3.7 Sistema de respaldo de comunicación 86
6.8.4 Sistema de autenticación para la WLAN 86

6.8.4.1 Instalación del sistema operativo Linux 87
6.8.4.2 Configuración de servicios y aplicaciones necesarias 93
6.8.4.2.1 Servidor Web Apache 97
6.8.4.2.2 Servidor Radius Freeradius 104
6.8.4.2.3 Servidor Mysql 107
6.8.4.2.4 Chillispot 109
6.8.4.2.5 Daloradius 111
6.8.4.3 Configuración de Equipos 113
6.8.4.3.1 Configuración del Router inalámbrico: 114
6.8.4.3.2 Configuración del AP – 2 115
6.8.4.3.3 Configuración del AP – 3 118
6.8.4.3.4 Configuración del AP – 4 120
6.8.4.3.5 Configuración del AP – 5 123
6.8.5 Pruebas de Acceso 125
6.9 Presupuesto 127
6.10 Administración 128
6.11 Conclusiones y Recomendaciones 128
6.11.1 Conclusiones 128
6.11.2 Recomendaciones 129
6.12 BIBLIOGRAFÍA 130
6.12.1 LINKOGRAFÍA 130
6.13 ANEXOS 133
6.13.1 ANEXO 1: Encuesta realizada a los alumnos de la FISEI 134
6.13.2 ANEXO 2: Manual del software de simulación AirMagnet Planner 135
6.13.3 ANEXO 3: Manual de Daloradius 147
6.13.4 ANEXO 4: Especificaciones del router y puntos de acceso 156

Índice de Figuras

Fig. 2.1: Sistemas AM y FM 8
Fig. 2.2: Topologías de red 10
Fig. 2.3: Relación gráfica entre OSI y TCP/IP 13
Fig. 2.4: Diagrama de una red WLAN 14
Fig. 4.1: Gráfico porcentual - Pregunta 1 34
Fig. 4.2: Gráfico porcentual - Pregunta 2 35
Fig. 4.3: Gráfico porcentual - Pregunta 3 36
Fig. 4.4: Gráfico porcentual - Pregunta 4 37
Fig. 4.5: Gráfico porcentual - Pregunta 5 38
Fig. 6.1: Diversidad de espacio en el receptor 52
Fig. 6.1: Ejemplo de Channel Bonding 53
Fig. 6.3: Arquitectura de 802.11 54
Fig. 6.4: Formato de una trama 802.11 55
Fig. 6.5: Distribución de canales en 802.11 57
Fig. 6.6: Representación gráfica de OFDM 59
Fig. 6.7: Modulación PSK 60
Fig. 6.8: Modulación QAM 60
Fig. 6.9: Diagrama de la red inalámbrica 73
Fig. 6.10: Cobertura del AP-1 en edificio principal de la FISEI 74
Fig. 6.11: Cobertura del AP-2 en edificio principal de la FISEI 75
Fig. 6.12: Cobertura del AP-3 en edificio principal de la FISEI 76
Fig. 6.13: Cobertura del AP-1, AP-2 y AP-3 en edificio principal de la FISEI 77
Fig. 6.14: Cobertura del AP-4 en edificio dos de la FISEI 78
Fig. 6.15: Cobertura del AP-5 en edificio dos de la FISEI 79
Fig. 6.16: Arranque desde el CD de instalación 88
Fig. 6.17: Comprobación del estado del CD de instalación 88
Fig. 6.18: Inicio de la instalación en modo gráfico 89
Fig. 6.19: Partición del disco duro 89
Fig. 6.20: Configuración del gestor de arranque 90
Fig. 6.21: Configuración del direccionamiento IP del servidor 90
Fig. 6.22: Selección de la región 91
Fig. 6.23: Configuración de la contraseña de root 91
Fig. 6.24: Selección de paquetes a instalarse 92
Fig. 6.25: Progreso de la instalación 92
Fig. 6.26: Aviso de la instalación completada 93
Fig. 6.27: Esquema básico del sistema de autenticación 94
Fig. 6.28: Intento fallido de conexión segura 102
Fig. 6.29: Obtención del certificado 102
Fig. 6.30: Detalles del certificado 103
Fig. 6.31: Confirmación de excepción de seguridad y conexión realizada 103

Fig. 6.32: Configuración de IP 114
Fig. 6.33: SSID, estándar de trabajo y canal 114
Fig. 6.34: Seguridad inalámbrica 115
Fig. 6.35: Ingreso al AP-2 115
Fig. 6.36: Configuración de IP 116
Fig. 6.37: Modo de operación como repetidor 116
Fig. 6.38: Búsqueda y selección de la señal a repetirse 117
Fig. 6.39: Seguridad 117
Fig. 6.40: Ingreso al AP-3 118
Fig. 6.41: Configuración de IP 118
Fig. 6.42: Modo de operación como repetidor 119
Fig. 6.43: Búsqueda y selección de la señal a repetirse 119
Fig. 6.44: SSID, estándar de operación y canal 120
Fig. 6.45: Ingreso al AP-4 120
Fig. 6.46: Configuración de IP 121
Fig. 6.47: Modo de operación como repetidor 121
Fig. 6.48: Búsqueda y selección de la señal a repetirse 122
Fig. 6.49: SSID, estándar de operación y canal 122
Fig. 6.50: Ingreso al AP-5 123
Fig. 6.51: Configuración de IP 123
Fig. 6.52: Modo de trabajo como repetidor 124
Fig. 6.53: Búsqueda y selección de la señal a repetirse 124
Fig. 6.54: SSID, estándar de operación y canal 125
Fig. 6.55: Aviso de conexión segura 125
Fig. 6.56: Configuración de acceso por certificado 126
Fig. 6.57: Página de autenticación 126
Fig. 6.58: Acceso autorizado 127
Fig. 6.59: Arranque de Airmagnet Survey 136
Fig. 6.60: Pantalla de inicio de Airmagnet Survey 136
Fig. 6.61: Pantalla de trabajo con Airmagnet Planner 137
Fig. 6.62: Nuevo proyecto en Planner – Nombre y directorio 138
Fig. 6.63: Nuevo proyecto en Planner – Plano y dimensiones 139
Fig. 6.64: Nuevo proyecto en Planner – Ambiente señal y potencia 140
Fig. 6.65: Nuevo proyecto en Planner - Descripción 140
Fig. 6.66: Recalibración del plano 141
Fig. 6.67: Tipos de obstáculos y herramienta creación de paredes 142
Fig. 6.68: Creación de obstáculos – Paredes y puertas 143
Fig. 6.69: Mapa de señal inalámbrica 145
Fig. 6.70: Propiedades del punto de acceso 146
Fig. 6.71: Ingreso a Daloradius 147
Fig. 6.72: Página de bienvenida 148
Fig. 6.73: Management 149

Fig. 6.74: Atributos de usuario 150
Fig. 6.75: Creación de grupos de atributos 150
Fig. 6.76: Reports 151
Fig. 6.77: Accounting 152
Fig. 6.78: Billing 153
Fig. 6.79: Estadísticas de usuarios 153
Fig. 6.80: Configuración de la base de datos 154
Fig. 6.81: Ayuda 155

Índice de tablas

Tabla 3.1: Variable independiente 30
Tabla 3.2: Variable dependiente 31
Tabla 4.1: Tabulación – Pregunta 1 33
Tabla 4.2: Tabulación – Pregunta 2 35
Tabla 4.3: Tabulación – Pregunta 3 36
Tabla 4.4: Tabulación – Pregunta 4 37
Tabla 4.5: Tabulación – Pregunta 5 38
Tabla 4.6: Frecuencias observadas 40
Tabla 4.7: Frecuencias esperadas 40
Tabla 4.8: Valores críticos del chi-cuadrado 41
Tabla 4.9: Cálculo de chi-cuadrado 42
Tabla 6.1: Campos de una trama 802.11 55
Tabla 6.2: Canales y frecuencias en 802.11b/g/n 56
Tabla 6.3: Características de equipos inicialmente activos en la FISEI 67
Tabla 6.4: Tabla comparativa – Software de simulación 69
Tabla 6.5: Diseño lógico y físico 73
Tabla 6.6: Configuración de equipos 113
Tabla 6.7: Presupuesto 127
Tabla 6.6: Especificaciones router inalámbrico Linksys 156
Tabla 6.7: Especificaciones punto de acceso 3com 157
Tabla 6.8: Especificaciones punto de acceso Cisco WAP200E 160
Tabla 6.9: Especificaciones punto de accceso Cisco WAP4410N 162

Índice de Ecuaciones

Ecuación 4.1: Chi-cuadrado 39
Ecuación 6.1: Cálculo del número de APs 71
Ecuación 6.2: Cálculo del ancho de banda 72
Ecuación 6.3: Pérdidas de propagación en zona urbana semiabierta 80
Ecuación 6.4: Pérdidas de propagación en zona urbana densa 80
Ecuación 6.5: Balance de pérdidas y ganancias 80

Resumen Ejecutivo

El presente documento tiene como objetivo describir todo el proceso desarrollado para el diseño e implementación de una red WLAN (Wireless Local Area Network) segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI).

En el primer capítulo se define el problema, planteándolo desde el contexto en el que se encuentra, con el respectivo análisis de la situación en la FISEI y determinando los objetivos que guiarán a través del desarrollo de dicho problema.

En el segundo capítulo se describe toda la fundamentación teórica inicialmente concebida para el desarrollo del problema, definiendo los conceptos y argumentos técnicos en los que se basa el presente proyecto.

El capítulo tres define la forma de abordar el problema para determinar una solución que permita verificar la hipótesis, valiéndose de métodos estadísticos e instrumentos de recopilación de información que aportarán con datos significativos que ayudarán a determinar una alternativa viable para el problema.

En el cuarto capítulo se analizan e interpretan los resultados obtenidos con los métodos utilizados en el capítulo tres, determinando con los datos proveídos por los alumnos de la FISEI, si el proyecto es necesario y viable en beneficio de la facultad y sus integrantes.

El quinto capítulo contiene todos los resultados obtenidos de los cuatro primeros, en forma de conclusiones y recomendaciones relacionadas con todo el proceso realizado anteriormente.

Finalmente se desarrolla la propuesta al problema en el capítulo seis, involucrando todo lo que concierne a la solución implementada por el autor de este documento y registrando toda la fundamentación teórica en la que se sustenta dicha propuesta.

Introducción

Las redes inalámbricas de área local (WLAN) se han popularizado con increíble rapidez, debido a la flexibilidad y prestaciones de esta tecnología que han llamado la atención de un enorme mercado. Con la implementación de este sistema en hogares, establecimientos educativos y campus universitarios, ha sido posible complementar sus redes cableadas existentes y disponer de un sistema de comunicación versátil para compartir información y acceder a internet.

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial, parte de la Universidad Técnica de Ambato (UTA), ha visto en las redes WLAN una alternativa práctica para ofrecer acceso a internet a sus alumnos, facilitando así una herramienta poderosa para el mejor desarrollo de tareas académicas y la investigación.

Sin embargo, la FISEI ha experimentado un crecimiento en infraestructura que no ha ido a la par con el crecimiento de su red inalámbrica, generando inconvenientes de acceso a internet mediante equipos portátiles, a los alumnos que han adoptado las nuevas instalaciones de la facultad como aulas académicas.

Es así que, se ha visto la necesidad de ampliar la cobertura de la red inalámbrica actual de la FISEI, y extender la señal al nuevo edificio de la facultad, para brindar el acceso a internet a aquellos estudiantes de dichas instalaciones.

El presente proyecto pretende aportar a la FISEI con un sistema completo que permita a los estudiantes, docentes y personal, acceder a la red de redes a través de un sistema inalámbrico práctico y eficiente, para el mejor desempeño académico de todos quienes forman parte de la facultad.

CAPITULO I

EL PROBLEMA

1.1 Tema

Red WLAN segura para la interconexión de los edificios de la facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.2 Planteamiento del Problema

1.2.1 Contextualización

Las redes inalámbricas han surgido de la gran necesidad de dotar de conectividad a un costo reducido, en comparación con las redes cableadas, además de ofrecer un notable nivel práctico de instalación y uso para el acceso hacia la información contenida en una red y sus elementos. La gran expansión de las mismas, hablando geográficamente y en todo campo ocupacional, han cambiado la forma en que las personas pueden acceder a Internet y compartir información de una manera más rápida y sencilla.

Es inevitable ver avisos que ofrecen el servicio de "Wireless" para el acceso a Internet, no solamente en ciudades grandes e importantes, sino también en poblados pequeños y zonas menos habitadas. Todo esto pone al descubierto la utilidad y la familiaridad que ya tienen las personas con este tipo de tecnología, que ya no sólo se implementa por utilidad sino también por necesidad.

En el campo educativo, específicamente hablando de la FISEI, la infraestructura inalámbrica actual ha dispuesto la misma para el acceso de los estudiantes a

internet, brindándoles otra opción para que puedan hacer investigación y realizar sus tareas de mejor manera con el acceso gratuito a la web. Con la creación de un nuevo edificio, ha surgido la necesidad de expandir la red inalámbrica actual hacia la nueva construcción, para proveer también de internet inalámbrico a los estudiantes de ésta, además de permitir intercomunicar ambos edificios mediante un enlace inalámbrico de este tipo.

1.2.2 Análisis Crítico

La red inalámbrica de la FISEI ha proporcionado servicio de internet inalámbrico a sus estudiantes desde hace ya un par de años, y el mismo ha servido para que los alumnos puedan realizar sus tareas de mejor manera, investigando y beneficiándose de la vasta información existente en la web.

Con el crecimiento de la facultad en términos de infraestructura, se ha hecho latente la necesidad de expandir la señal de internet inalámbrico al nuevo edificio, para dotar de conectividad a los alumnos que recibirán clases en dicho edificio.

Son varias las causas por las que el edificio dos de la FISEI no dispone de servicio de internet. Una de ellas es el hecho de que el edificio dos es una construcción relativamente nueva. Por otro lado, no han existido los recursos necesarios para desarrollar este proyecto. Otro motivo es el cambio reciente de autoridades en la facultad y finalmente, quizá los estudiantes no han hecho eco suficiente para que se satisfaga esta necesidad.

Como resultado de esta situación actual, los alumnos del nuevo edificio no disponen de servicio de internet inalámbrico que les pueda brindar una herramienta adicional para investigar y ampliar más sus conocimientos impartidos en clase. No se hace uso de una tecnología que en la actualidad es muy común y necesaria. No se aprovecha al máximo el ancho de banda disponible para la facultad y, sin una interconexión entre ambos edificios, no hay un intercambio eficiente de recursos y centralización de la información.

1.2.3 Prognosis

Si no se crea una red WLAN segura que interconecte los edificios de la FISEI, el acceso a internet para todos los estudiantes estaría limitado, debido al alcance de la única red inalámbrica existente en la facultad, que solamente "cubre" el edificio principal (donde se encuentran las oficinas administrativas) de la misma. Se pretende entonces, extender la señal inalámbrica hacia el edificio "nuevo" (edificio dos de ahora en adelante) de la FISEI y centralizar la información de toda la red en un solo punto de administración.

1.3 Formulación del Problema

¿De qué manera incide una red WLAN en la interconexión de los edificios de la FISEI?

1.4 Preguntas Directrices

- ¿Cuáles son los requerimientos para el diseño de una red WLAN segura para la FISEI?
- ¿Cómo se interconectarán los edificios de la FISEI mediante la WLAN?
- ¿Qué características deberá cumplir la red WLAN para la interconexión de los edificios de la FISEI?

1.5 Delimitación del Problema

El desarrollo de la WLAN se realizará en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial (FISEI) de la Universidad Técnica de Ambato (UTA).

El período de tiempo para la realización de este proyecto es de seis meses, a partir de la fecha de aprobación por parte del Honorable Consejo Directivo de la FISEI.

1.6 Justificación

La necesidad de proporcionar acceso inalámbrico a internet a todos los estudiantes de la FISEI es la principal razón del desarrollo de este proyecto. Es importante

aumentar el alcance de la red inalámbrica existente para "alcanzar" al edificio dos, logrando así cubrir la necesidad de los alumnos que ocupan dichas aulas.

Es de resaltar la necesidad de acceso rápido y práctico a la web (mediante redes de este tipo) que tienen los estudiantes de ésta y cualquier universidad, por la exigencia en investigación que demanda una carrera universitaria, especialmente de ingeniería.

El número limitado de computadores de escritorio disponibles para que los estudiantes se conecten a internet, se convierte en otra de las razones para proveer de un servicio de este tipo. Los alumnos que disponen de portátiles acceden a internet a través de la red inalámbrica, y permiten a los alumnos que no disponen de estos equipos, el uso de los computadores de escritorio de la facultad.

La interconexión entre ambos edificios permitirá unificar la información de los usuarios en un solo punto, haciendo eficiente la administración de los datos de la red.

1.7 Objetivos de la investigación

1.7.1 Objetivo General

Diseñar e implementar una red WLAN segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.7.2 Objetivos específicos

- Analizar la situación actual del acceso inalámbrico a internet en la FISEI.
- Establecer los requerimientos de una red WLAN para la interconexión de los edificios de la FISEI.
- Determinar los tipos de enlace en el desarrollo de una red WLAN para la interconexión de los edificios de la FISEI.
- Implementar una red WLAN segura para la interconexión de los edificios de la FISEI.

CAPITULO II

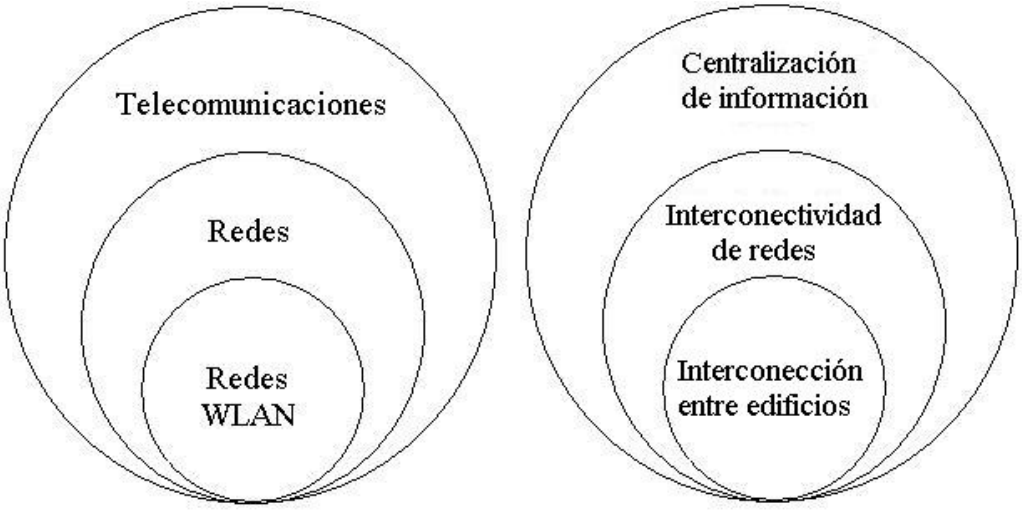
MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

Después de la revisión de la lista de tesis archivada en la biblioteca de la FISEI, no se ha encontrado información referente a diseño, implementación o creación de redes inalámbricas para la facultad, aunque cabe resaltar que existe una red de este tipo que provee de servicio de Internet en el edificio principal.

2.2 FUNDAMENTACIÓN

2.2.1 CATEGORÍAS FUNDAMENTALES



Variable Independiente Variable Dependiente

2.2.2 RED WLAN SEGURA

2.2.2.1 TELECOMUNICACIONES

La **telecomunicación** es una técnica que consiste en transmitir un mensaje desde un punto a otro, con la característica principal de ser bidireccional. El término *telecomunicación* cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras a nivel de enlace.

La base matemática sobre la que se desarrollan las telecomunicaciones fue desarrollada por el físico inglés James Clerk Maxwell. Maxwell introdujo el concepto de onda electromagnética, que permite una descripción matemática adecuada de la interacción entre electricidad y magnetismo mediante sus célebres ecuaciones que describen y cuantifican los campos de fuerzas.

Maxwell predijo que era posible propagar ondas por el espacio libre utilizando descargas eléctricas, hecho que corroboró Heinrich Hertz en 1887, ocho años después de la muerte de Maxwell, y que, posteriormente supuso el inicio de la era de la comunicación rápida a distancia. Hertz desarrolló el primer transmisor de radio generando radiofrecuencias entre 31 MHz y 1.25 GHz.

2.2.2.1.1 Características de un sistema de telecomunicación

Los elementos que componen un sistema de telecomunicación son un transmisor, un medio de transmisión y finalmente un receptor. El transmisor es el dispositivo que adecua los mensajes en forma de señales para poder enviarlas por el medio de transmisión. El medio de transmisión, por su naturaleza física, es posible que modifique o degrade la señal en su trayecto desde el transmisor al receptor debido a ruido o posibles interferencias. Por ello el receptor ha de tener un mecanismo de decodificación capaz de recuperar el mensaje dentro de ciertos límites de degradación de la señal.

La telecomunicación puede ser punto a punto, punto a multipunto o teledifusión, que es una forma particular de punto a multipunto que funciona solamente desde el transmisor a los receptores, siendo su versión más popular la radiodifusión.

2.2.2.1.2 Radiocomunicación

La **radiocomunicación** es un sistema de telecomunicación que se realiza a través de ondas de radio u ondas hertzianas, y que a su vez está caracterizado por el movimiento de los campos eléctricos y campos magnéticos. La comunicación vía radio se realiza a través del espectro radioeléctrico cuyas propiedades son diversas a lo largo de su gama: baja frecuencia, media frecuencia, alta frecuencia, muy alta frecuencia, ultra alta frecuencia, etc. En cada una de ellas, el comportamiento de las ondas es diferente.

2.2.2.1.3 Transmisión y recepción

Una onda de radio se origina cuando una partícula cargada se excita a una frecuencia situada en la zona de radiofrecuencia (RF) del espectro electromagnético.

Cuando la onda de radio actúa sobre un conductor eléctrico (la antena), induce en él un movimiento de la carga eléctrica (corriente eléctrica) que puede ser transformado en señales de audio u otro tipo de señales portadoras de información.

El emisor tiene como función producir una onda portadora, cuyas características son modificadas en función de las señales (audio o video) a transmitir. Propaga la onda portadora así modulada. El receptor capta la onda y la «demodula» para hacer llegar al espectador auditor tan solo la señal transmitida.

2.2.2.1.4 Sistemas AM y FM

Estos son los primeros sistemas de modulación que se utilizaron para transmitir a larga distancia y que aún se utilizan principalmente para transmisiones de

estaciones radiales. A continuación se muestra gráficamente como se realiza la modulación en amplitud (AM) y en frecuencia (FM):

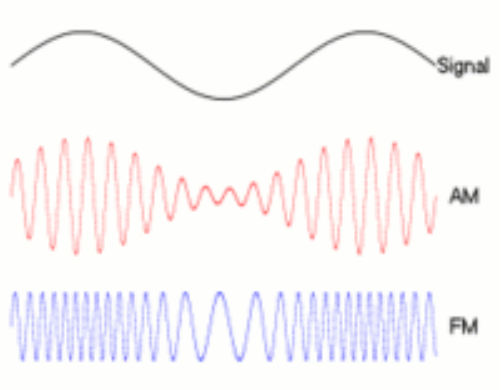


Fig. 2.1: Sistemas AM y FM

a. Amplitud Modulada

En el sistema de modulación de amplitud (AM), la señal (de baja frecuencia) se superpone a la amplitud de ondas hertzianas portadora (de alta frecuencia).

b. Frecuencia Modulada

En el sistema de modulación de frecuencia (FM), la amplitud de la onda portadora se mantiene constante, pero la frecuencia varia según la cadencia de las señales moduladoras. Este sistema permite eliminar señales parásitas e interferencias, y reproduce el sonido con mayor fidelidad.

2.2.2.2 REDES

Una red informática es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, recursos, servicios, etc.

Una red de comunicaciones es también un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, cable de fibra óptica, etc.).

Para simplificar la comunicación entre programas (aplicaciones) de distintos equipos, se definió el Modelo OSI, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

2.2.2.2.1 Clasificación

a. Por alcance:

- Red de área personal (*PAN*)
- Red de área local (*LAN*)
- Red de área de campus (*CAN*)
- Red de área metropolitana (*MAN*)
- Red de área amplia (*WAN*)

b. Por método de la conexión:

- Medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables.
- Medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas.

c. Por relación funcional:

- Cliente-servidor
- Igual-a-Igual (p2p)

d. Por Topología de red:

- Red en bus
- Red en estrella
- Red en anillo (o doble anillo)
- Red en malla (o totalmente conexa)
- Red en árbol

- Red mixta (cualquier combinación de las anteriores)

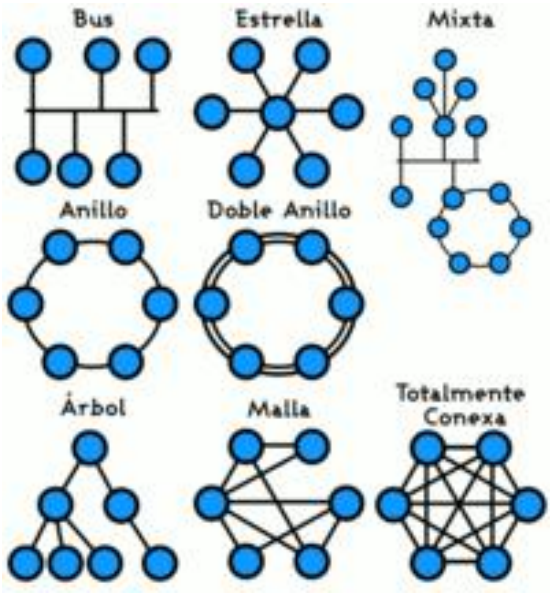


Fig. 2.2: Topologías de red

e. Por la direccionalidad de los datos (tipos de transmisión)

- *Simplex* (unidireccionales): un equipo terminal de datos transmite y otro recibe. (por ejemplo, streaming)
- *Half-Duplex* (bidireccionales): sólo un equipo transmite a la vez. También se llama *Semi-Duplex* (por ejemplo, una comunicación por equipos de radio, si los equipos no son *full dúplex*, uno no podría transmitir (hablar) si la otra persona está también transmitiendo (hablando) porque su equipo estaría recibiendo (escuchando) en ese momento).
- *Full-Duplex* (bidireccionales): ambos pueden transmitir y recibir a la vez una misma información. (por ejemplo, videoconferencia).

2.2.2.2.2 Redes fijas, inalámbricas, móviles y celulares

Otro parámetro que caracteriza las redes de comunicaciones y condiciona su diseño es el grado de movilidad y el uso de espectro radioélectrico de los extremos de la comunicación. Se tienen:

a) Redes fijas: los usuarios y los terminales están permanentemente fijos, conectados físicamente a las redes mediante un cable o mediante espectro radioeléctrico, pero sin poder desplazarse de ubicación.

b) Redes inalámbricas: utilizan espectro radioeléctrico para la comunicación

c) Redes de móviles: los usuarios están en movimiento dentro de las zonas de cobertura de la red, y los terminales proporcionan a la red las señales que permiten su seguimiento e identificación. Obsérvese que todas las redes de móviles son inalámbricas, pero no al revés.

d) Redes celulares: son redes inalámbricas que tienen divida la zona de cobertura en "células" o "celdas". Los sistemas de comunicaciones móviles son un ejemplo típico.

2.2.2.2.3 Protocolos de redes

Un protocolo de red es similar a un lenguaje, pero utilizado para la comunicación entre equipos. Son las reglas y procedimientos que se utilizan en una red para que los nodos de un sistema puedan comunicarse. Los protocolos gobiernan dos niveles de comunicaciones:

- Los protocolos de alto nivel: Estos definen la forma en que se comunican las aplicaciones.
- Los protocolos de bajo nivel: Estos definen la forma en que se transmiten las señales por cable.

Así como las computadoras están en constante cambio, también los protocolos están en continuo cambio. Actualmente, los protocolos más comúnmente utilizados en las redes son Ethernet, Token Ring y ARCNET. Cada uno de estos está diseñado para cierta clase de topología de red y tienen ciertas características estándar.

Ethernet

Actualmente es el protocolo más sencillo y es de bajo costo. Utiliza la topología de bus.

TokenRing

El protocolo de IBM es el Token ring, el cual se basa en la topología de anillo.

Arnet

Se basa en la topología de estrella o estrella distribuida, pero tiene una topología y protocolo propio.

2.2.2.2.4 Arquitectura de Redes

a. TCP/IP

El modelo de referencia TCP/IP (Transmision Control Protocol / Internet Protocol) es, de manera análoga al modelo de referencia OSI (Open System Interconnection), una abstracción de los protocolos empleados para comunicar distintas máquinas, primero en la red militar ARPANET (Advanced Research Projects Agency Network) y posteriormente en su sucesora, Internet. La arquitectura de referencia TCP/IP fue diseñada con el propósito de permitir la interconexión de redes con distintas naturalezas (satelitales, de radio, cableadas, etc.) y lo que es más importante, para garantizar que las comunicaciones se mantuvieran en caso de que cayera algún nodo, ya que una red con arquitectura TCP/IP debe ser capaz de encaminar la información por caminos alternativos.

b. Las capas del modelo TCP/IP

Al igual que el modelo OSI, TCP/IP está formado por capas, en cada una de las cuales se emplean protocolos de comunicación distintos. Pese a no ser idénticas, las capas del modelo TCP/IP guardan analogías con varias de las capas o niveles OSI.

Estas son las capas definidas en la arquitectura TCP/IP:

1. Nivel de enlace, equivalente a los niveles físico y de enlace de datos en OSI.

2. Nivel de red, equivalente al Nivel de red en OSI, en la que se define un formato de paquete y protocolo primario que se denomina IP.

3. Nivel de transporte, equivalente al de OSI.

4. Nivel de aplicación, también equivalente al del modelo OSI.

A continuación se muestra la similitud entre OSI y TCP/IP de forma gráfica.

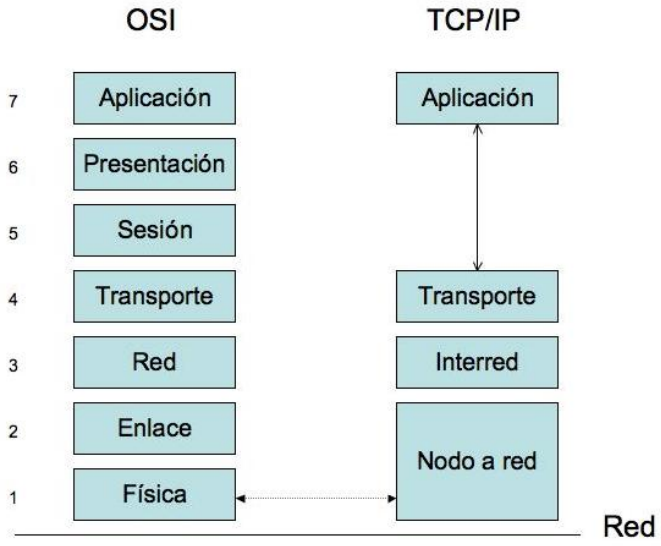


Fig. 2.3: Relación gráfica entre OSI y TCP/IP

c. Protocolos de nivel de transporte

En la capa de transporte se definen dos grandes protocolos que permiten la comunicación extremo a extremo entre dos máquinas. El primero de ellos, que da nombre a la arquitectura, es el protocolo TCP, sigla inglesa de Protocolo de Control de Transmisión. TCP es un protocolo confiable y orientado a conexión, lo que asegura la recepción sin errores de los paquetes de información en el destinatario y la correspondencia con el orden de envío. Las conexiones que quieren garantizar una calidad de servicio en Internet suelen emplear TCP como protocolo de transporte.

El otro gran protocolo es UDP, sigla inglesa de User Datagram Protocol. En contraste con TCP, UDP es un protocolo sin conexión, no confiable, idóneo para aplicaciones que no requieren un orden secuencial estricto de los paquetes ni un control del flujo de transmisión como el que ofrece TCP. Es el protocolo idóneo para aplicaciones en las que se da importancia a la velocidad de transmisión frente

a la corrección de errores, como por ejemplo para la transmisión de vídeo o voz sobre Internet.

2.2.2.3 REDES WLAN

"*WLAN* *(en inglés; Wireless Local Area Network) es un sistema inalámbrico flexible de comunicación de datos, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.*" [http://es.wikipedia.org/wiki/WLAN]

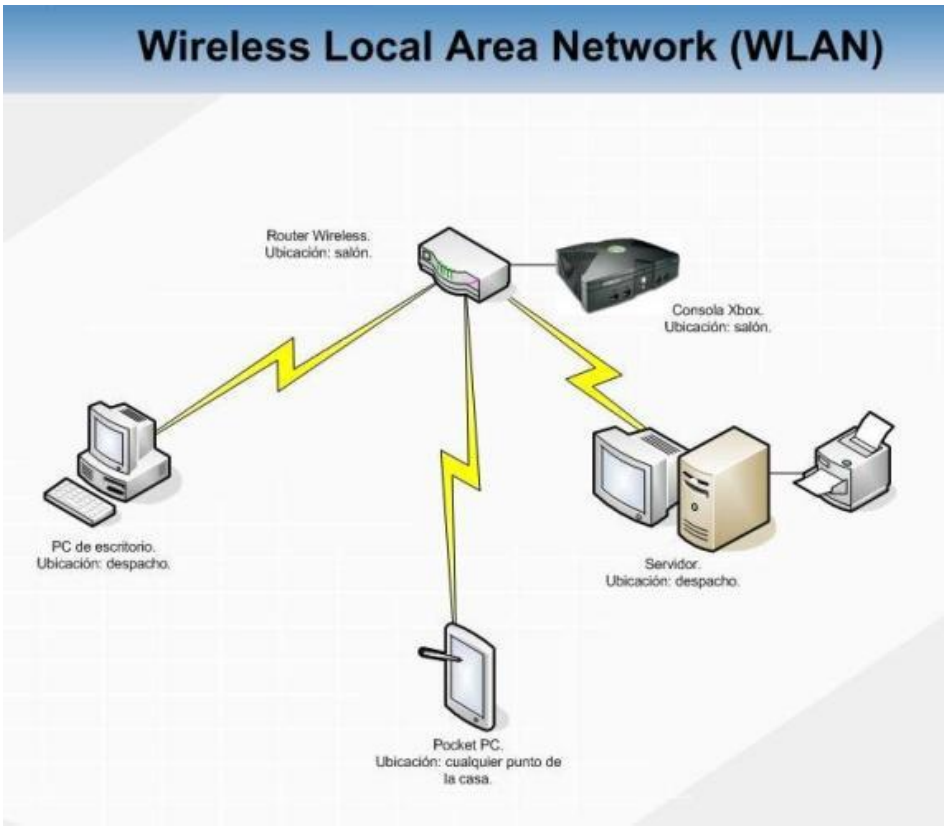


Fig. 2.4: Diagrama de una red WLAN

Cómo se puede apreciar en la Fig. 2.4, las WLAN son redes de conectividad simple y práctica donde distintos dispositivos con este soporte pueden intercambiar información con el punto de acceso, siempre y cuando ambos se puedan "escuchar" entre sí.

Estas redes al igual que las LAN cableadas están contempladas para áreas pequeñas tales como edificios, pequeñas áreas residenciales o campus universitarios.

2.2.2.3.1 Características

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso (AP) 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 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 puertosUSB de los equipos.

Para ser considerada como WLAN, la red debe tener una velocidad de transmisión de tipo medio (el mínimo establecido por el IEEE 802.11 es de 1 Mbps, aunque las actuales tienen una velocidad del orden de 2 Mbps), y además deben trabajar en el entorno de frecuencias de 2,45 GHz.

La principal ventaja de este tipo de redes (WLAN), que no necesitan licencia para su instalación, es 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 en todos los lugares por donde puedan estar trabajando. Además, a esto se añade la ventaja de que son mucho más sencillas de instalar que las redes cableadas y permiten la fácil reubicación de los terminales en caso necesario.

2.2.2.3.2 Funcionamiento

Se utilizan ondas de radio para llevar la información de un punto a otro sin necesidad de un medio físico guiado. Al hablar de ondas de radio se hace referencia normalmente a portadoras de radio, sobre las que va la información, ya que realizan la función de llevar la energía a un receptor remoto. Los datos a

transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final.

En una configuración típica de LAN sin cable, los puntos de acceso (transceivers) se conectan mediante cable normalizado con una "red principal" que comúnmente es una LAN. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente y las ondas, mediante una antena.

2.2.2.3.3 Estándares

- **IEEE 802.11**

El estándar **IEEE 802.11** define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

- **IEEE 802.11a**

Extensión del 802.11 que se aplica a redes inalámbricas LAN y provee una velocidad de hasta 54 Mbps en la banda de 5 GHz.

- **IEEE 802.11b**

También conocido como 802.11 High Rate o Wi-Fi. Extensión del 802.11, se aplica a redes inalámbricas LAN y provee una transmisión de 11 Mbps (con posibilidad de 5.5, 2 y 1 Mbps) en la banda de 2.4GHz. 802.11b utiliza solo DSSS. Fue una ratificación en 1999 al estándar 802.11 original, permitiendo una funcionalidad comparable al Ethernet.

- **IEEE 802.11g**

Extensión del 802.11 que se aplica a redes inalámbricas LAN. Provee más de 20 Mbps en la banda de 2.4 GHz.

- **IEEE 802.11n**

Es una propuesta de modificación al estándar IEEE 802.11 para mejorar significativamente el desempeño de la red, más allá de los estándares anteriores tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz dependiendo del entorno, esto puede transformarse a un desempeño visto por el usuario de 100Mbps.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009.

- **Hiperlan**

HIPERLAN (High Performance Radio LAN) es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz. Es similar a 802.11a (5 GHz) y es diferente de 802.11b/g (2,4 GHz).

- **Hiperlan 2**

Las especificaciones funcionales de HIPERLAN 2 se completaron en el mes de febrero de 2000. La versión 2 fue diseñada como una conexión inalámbrica rápida para muchos tipos de redes. Por ejemplo: red backbone UMTS, redes ATM e IP. También funciona como una red doméstica como HIPERLAN. HIPERLAN 2 usa la banda de 5 GHz y una velocidad de transmisión de hasta 54 Mbps.

Los servicios básicos son transmisión de datos, sonido, y vídeo. Se hace énfasis en la calidad de esos servicios (QoS).

Hiperlan: ¿tecnología obsoleta o futura?

Algunos creen que los estándares IEEE 802.11 ya han ocupado el nicho comercial para el que se diseñó HIPERLAN, aunque con menor rendimiento pero mayor penetración comercial, y que el efecto de la red instalada impedirá la adopción de HIPERLAN.

2.2.2.3.4 Seguridad

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP (Wired Equivalent Privacy), el WPA (Wi-Fi Protected Access), o el WPA2, que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- WEP: cifra los datos en su red con claves de 64 y 128 bits de forma que sólo el destinatario deseado pueda acceder a ellos. Este tipo de cifrado no es recomendado actualmente debido a las grandes vulnerabilidades que presenta, ya que cualquier cracker puede descifrar la clave en cuestión de minutos.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos sin restricción de longitud.
- WPA2 (estándar 802.11i): es una mejora relativa a WPA. En principio es el protocolo de seguridad más confiable para Wi-Fi en este momento. Sin embargo, requiere hardware y software compatibles ya que los antiguos no lo son.
- IPSEC (túneles IP): comúnmente utilizado en VPNs y el conjunto de estándares IEEE 802.1X, permitiendo la autenticación y autorización de usuarios.

- Filtrado MAC: sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- Ocultación del SSID: se puede ocultar el identificador de red de manera que sea invisible a los usuarios.

Es recomendable utilizar una o varias de estas protecciones.

2.2.2.3.5 WLAN - Hotspot

Un hotspot (‘punto caliente’) es una zona de cobertura Wi-Fi en el que un punto de acceso (*access point*) o varios, proveen servicios de red a través de un Proveedor de Servicios de Internet Inalámbrico (WISP). Los hotspots se encuentran en lugares públicos como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, etcétera. Este servicio permite mantenerse conectado a Internet en lugares públicos. Puede brindarse de manera gratuita o pagando una suma que depende del proveedor.

Los parámetros principales que se administran en una WLAN “Hotspot” son: ancho de banda, número de usuarios, autenticación de los mismos, tiempo de conexión, página de bienvenida, entre otros.

La implementación de una red inalámbrica con características de Hotspot es factible y sobre todo sencilla gracias a software especializado existente como por ejemplo, Antamedia Hotspot Software, Firstspot, Nocat (Linux), Aradial, Softvision Explorer o similares, que se encargan de brindar las funcionalidades requeridas de un servicio con los parámetros mencionados.

2.2.2.3.6 Diseño

Una red de área local inalámbrica (WLAN) debe cumplir los siguientes requerimientos básicos:

- Cobertura completa en el área determinada.
- Capacidad suficiente para soportar el tráfico.

Los requerimientos anteriores se cumplen a través de:

- Ubicación adecuada de los Access Point (AP)
- Asignación adecuada de canales

Barreras de Transmisión:

- Materiales como madera, plástico o vidrio, no son problema mientras que el concreto y ladrillos pueden ser barreras significativas.
- En un ambiente abierto se puede alcanzar 300m sin problema, pero sólo se puede alcanzar los 20 o 60 metros cuando hay obstrucciones de por medio.

Mediciones

- No existen reglas simples de cálculo. Es necesario medir, hacer pruebas exhaustivas y poner especial énfasis en aspectos de propagación para lograr cubrir el área de interés.
- Hay que tener un especial cuidado en el interior de un recinto ya que es un espacio tridimensional.
- Un AP podría cubrir dos pisos dependiendo de los materiales de construcción.

Interferencias entre canales

Las interferencias pueden ser:

- Co-canales: al transmitir simultáneamente sobre el mismo canal.
- Inter-canales: al transmitir sobre canales adyacentes

Tanto la interferencia de co-canales como inter-canales pueden limitar con severidad la capacidad de la WLAN.

Aspectos adicionales:

- Espaciar lo máximo posible los APs, asegurando cobertura completa del área. Este criterio ayuda a reducir la interferencia co-canal, costos de equipo e instalación.
- Para redes de un piso se deberían utilizar los canales 1, 6 y 11 para evitar toda interferencia inter-canal.

- Para redes de varios pisos se deberían utilizar los canales 1, 4, 7 y 11 para limitar la interferencia inter-canal. Además se usarán los mismos para evitar que canales adyacentes usen el mismo canal.

Densidad de Usuarios

- El diseño debe considerar áreas de servicio con distintas densidades de usuarios. Aunque generalmente las densidades son bajas, hay que considerar excepciones como una sala de clase.
- Si la densidad es alta se pueden utilizar hasta 3 AP con distintos canales para cubrir la misma área.

2.2.2.3.7 Implementación

Antes de implementar una WLAN hay algunos pasos preparatorios que se deben realizar:

- Elegir un proveedor de hardware que tenga en cuenta la seguridad. Cisco, Agere y otros proveedores usan en su hardware 802.1x y cambio de claves mediante Wired Equivalent Privacy (WEP) de 128 bits. Algunos proveedores puede que no ofrezcan estas características. De esta forma, antes de ponerse a comprar habrá que comprobar que el hardware que se adquirirá dispone de las características de seguridad que se desean.
- Decidir qué clase de cifrado y autenticación se pretende usar. Si es posible, utilizar 802.1x (seguridad realizada por un tercero).
- Decidir si la WLAN se integrará en gran medida con su LAN o no. ¿Se van a compartir ambas redes un espacio de direcciones común? Hay que analizar acerca de cómo desea asignar las direcciones IP para los clientes: ¿tiene cada punto de acceso su propio intervalo DHCP (Dinamic Host Configuration Protocol) o sería mejor usar un servidor DHCP centralizado?
- Realizar una inspección del lugar. Esta inspección puede ser compleja y cara (por ejemplo, si se va a proporcionar acceso de WLAN a todo un complejo de oficinas corporativas o al área metropolitana) o puede ser

sencilla (si se va a configurar un único punto de acceso, merodear por la zona para ver con qué fuerza llega la señal en diversas ubicaciones). No olvidar realizar esta comprobación fuera de los recintos donde se va a proporcionar el acceso para asegurarse de que la señal no llega demasiado lejos.

- Decidir cuántos usuarios de la red inalámbrica se desea que la utilicen simultáneamente. Si sólo hay unos pocos, no hay problema; si en cambio son más de 25, se necesitarán varios puntos de acceso incluso en un espacio relativamente pequeño. Lo interesante de las WLAN es que siempre puede agregar más puntos de acceso a medida que lo necesite para ampliar la red.
- Configurar un único punto de acceso y comprobar que la configuración de la autenticación y el cifrado funciona correctamente. Este paso es muy importante porque si una WLAN se configura de forma inapropiada, puede permitir a cualquier persona que pase cerca obtener una dirección en ella y utilizarla, posiblemente con fines no demasiado buenos.

2.2.3 INTERCONECCIÓN ENTRE LOS EDIFICIOS DE LA FISEI

2.2.3.1 CENTRALIZACIÓN DE LA INFORMACIÓN

El Internet y la posibilidad de disponer de banda ancha, siempre manteniendo una conexión permanente a la red de redes, invitan a revisar los conceptos bajo los cuales se determina la mejor opción entre centralizar y distribuir nuestro sistema de información.

Cuando se diseña la arquitectura de aplicaciones y la arquitectura de los datos, siempre hay que tener en cuenta el tema de la centralización y la distribución de los mismos.

Es necesario hacer un poco de historia porque, al parecer, se retorna a un punto donde ya se ha estado hace un par de décadas, pero con características un poco distintas.

Las primeras instalaciones de sistemas de información requerían de un servidor central donde se procesaba y almacenaba la información, y al cual se accedía mediante terminales conectados al mismo. La máxima distancia de un "terminal" era de aproximadamente 1,500 metros en las tecnologías de IBM con cable coaxial, o de 350 metros aproximadamente con cableado en estrella. No había mayores opciones ya que en los terminales no se tenía capacidad de procesamiento ni almacenamiento.

Con la aparición de los computadores personales (PCs) a principios de los años ochenta, y el desarrollo de las tecnologías de redes en aquella época, también se hizo posible tener equipos PC conectados al servidor, y utilizar la capacidad de almacenamiento del mismo para efectuar cálculos o presentación de las aplicaciones. No fue sino hasta la década de los noventa, con la aparición del concepto de cliente/servidor, que se pudo realmente hacer uso de esta funcionalidad.

Hoy hay muchas aplicaciones funcionando en este esquema, donde, parte del procesamiento y algunas validaciones se hacen en el PC del usuario. Estas posibilidades presentaban alternativas de distribución tanto de las aplicaciones (podrían estar en el servidor, en el PC, o en ambas) y la distribución de los datos. La disponibilidad del servicio dependería en gran parte de la posibilidad de conexión, posibilidad de por sí muy costosa, por lo que ni se pensaba en tener información fuera de los confines de la empresa.

Las tecnologías de Internet y sus posibilidades han impulsado también el desarrollo de otras tecnologías que permiten volver a considerar alternativas. El desarrollo en servidores, que ahora se concentra en grandes data centers, eliminan problemas de capacidad tanto de procesamiento como de espacio, problemas que eran factores de decisión y hoy no tienen peso. En estos mismos servidores separados en dos y hasta tres capas, se colocan hoy las aplicaciones, las reglas de negocio y los datos, permitiendo un buen desempeño y tiempo de respuesta de las mismas.

La misma centralización entonces, permite poder efectuar en un solo sitio copias de respaldo de los datos, de las aplicaciones y de sus resultados. Situaciones como el correo electrónico, cuando se maneja en el PC de cada usuario, genera un requerimiento de copias de respaldo bastante complejo y costoso de manejar. Al tener el correo almacenado en una entidad central, es fácil obtener el respaldo dentro del mismo procedimiento para respaldar el resto de la información.

El uso de un navegador de Internet en los dispositivos de acceso, utilizando la centralización de los datos y la aplicación (dejando el tema de la presentación de la información en el navegador), permite también manejar cualquier tipo de dispositivo, desde el común PC hasta los nuevos equipos celulares, y lo que se invente a futuro.

La centralización presenta una excelente oportunidad para la administración de la información, las aplicaciones y las reglas del negocio en forma ágil y segura, permitiendo que cualquier cambio en alguno de los tres elementos esté disponible en forma inmediata para cada uno de los usuarios que lo requiera. Esta funcionalidad requiere que el acceso a la misma sea de alta disponibilidad. Las líneas conmutadas y los servicios de conexión a través de Internet son relativamente buenos, y con el aparición de conexiones de banda ancha, esta disponibilidad se hace mejor y más rápida.

2.2.3.2 INTERCONECTIVIDAD DE REDES

Es el proceso de comunicación el cual ocurre entre dos o más redes que están conectadas entre sí de alguna manera.

¿Por qué es importante la interconectividad de redes?

- Compartir recursos
- Acceso instantáneo a bases de datos compartidas
- Insensibilidad a la distancia física y a la limitación en el número de nodos
- Administración centralizada de la red

¿Qué retos existen?

- Reducción de presupuestos (tiempo, dinero)
- Escasez de ingenieros especializados en redes
- Capacidad de planeación, administración y soporte
- Retos técnicos y retos de administración de redes

¿Qué retos técnicos existen?

- Equipos de diferentes fabricantes
- Arquitecturas, plataformas, sistemas operativos, protocolos, medios de comunicación diferentes
- Limitaciones en distancia y en tamaño de los paquetes
- Limitaciones en ancho de banda y potencia

¿Qué retos de administración de redes existen?

- Configuración
- Seguridad
- Confiabilidad
- Desempeño
- Localización, aislamiento, corrección y prevención de fallas
- Planeación hacia el futuro

El verdadero reto de la interconectividad es la transmisión de información entre redes LAN dispersas geográficamente.

2.2.3.2.1 Cómo se interconectan las redes

Las redes se conectan mediante equipos de telecomunicaciones conocidos como equipos de interconexión. Los equipos de interconexión de dos o más redes separadas, permiten intercambiar datos o recursos formando una intranet. Enlazar LANs en una intranet requiere de equipos que realicen ese propósito. Estos

dispositivos están diseñados para sobrellevar los obstáculos para la interconexión sin interrumpir el funcionamiento de las redes.

Existen equipos de interconexión a nivel de:
LAN: Hub, switch, router, repetidor, gateway, puente, punto de acceso (AP).
MAN (Metropolitan Area Network): Repetidor, switch capa 3, enrutador, multicanalizador, wireless bridges, puentes, módem analógico, módem ADSL (Asymmetric Digital Subscriber Line).
WAN (Wide Area Network): Enrutador, modem analógico, modem satelital.

2.2.3.3 INTERCONECCIÓN ENTRE EDIFICIOS

Dentro de una institución, el crecimiento de la misma en términos de infraestructura es inevitable. Por ejemplo, se puede construir un nuevo almacén, una empresa se traslada a un complejo compuesto por dos edificios que son visibles entre ellos, o incluso, varias empresas desean interconectarse para ahorrar costes de Internet y de infraestructura.

Debido a la existencia de varios edificios surge el problema de la interconexión de los mismos dentro en una sola red.

Para esto, o bien se extiende un cableado (muy caro debido a que para grandes distancias debemos optar por soluciones de Fibra óptica), o bien optamos por una solución inalámbrica que permita conectar edificios que pueden llegar a estar alejados una distancia considerable.

Para este tipo de solución son necesarios dos puntos de acceso que permitan la interconexión de ellos en configuraciones de puente (Bridge).

Una vez que se han instalado los puntos de tal forma que uno enlace con el otro, las redes conectadas a los puntos de acceso (las redes de los edificios) son automáticamente la misma red, pudiendo compartir información entre los distintos edificios sin ningún tipo de complicación.

2.3 Hipótesis

El diseño e implementación de una red WLAN segura permitirá la interconexiónentre los edificios de la FISEI.

2.4 Variables

2.4.1 Variable independiente

Red WLAN segura

2.4.2 Variable dependiente

Interconexión entre los edificios de la FISEI.

CAPITULO III

METODOLOGÍA

3.1 Enfoque

Este proyecto se basó en el enfoque cuali-cuantitativo pues éste busca la comprensión de los hechos. Este enfoque se visualiza desde un marco de referencia de los actores, le interesa la interpretación del problema en estudio, enfoque u objetivo.

3.2 Modalidad básica de la investigación

3.2.1 Investigación bibliográfica

Este proyecto estuvo sustentado bibliográficamente y las fuentes de información se indican en su respectiva sección.Se utilizaron fuentes de la web así como textos e información de tesis con temas afines.

3.3 Nivel o tipo de investigación

Este proyecto estuvo basado en un tipo de investigación exploratoria, descriptiva y explicativa. El desarrollo de la misma estuvo determinado por dichos niveles en ese orden, indagando sobre la situación del problema en primer lugar, para luego comprenderlo, explicarlo y finalmente proyectar y comprobar la hipótesis.

3.4 Población y muestra

3.4.1 Población

La población la integraron un total de 800 personas incluyendo estudiantes, docentes y personal administrativo.

3.4.2 Muestra

$$m = \frac{n}{\left(1 + \frac{n}{N}\right)}$$

Donde:

m = Tamaño de la muestra

n = Varianza de la muestra / Varianza de la población

N = Tamaño de la población

% Confianza = 95

Varianza de la muestra = (100 – % Confianza)/100 = 0.05

Varianza de la población (Constante) = 0.015^2 = 0.000225

$$n = \frac{0.05}{0.000225} = 222.22$$

$$m = \frac{222.22}{\left(1 + \frac{222.22}{800}\right)}$$

$$m = 174.97$$

El número de estudiantes encuestados fue de 180.

3.5 Operacionalización de variables

3.5.1 Variable independiente

<table>
<tr><th colspan="2">ABSTRACTO</th><th colspan="2">CONCRETO</th></tr>
<tr><th>Conceptualización</th><th>Categorías</th><th>Indicadores</th><th>Items</th></tr>
<tr><td rowspan="5">Red WLAN

Sistema de comunicación inalámbrico que utiliza energía de radiofrecuencia.</td><td rowspan="3">Sistema de comunicación inalámbrico</td><td>Transmisor</td><td rowspan="2">¿Qué es necesario para conectarse a la WLAN de la FISEI?

Un dispositivo WLAN compatible

Registro del dispositivo en la FISEI

Las dos anteriores</td></tr>
<tr><td>Receptor</td></tr>
<tr><td>Medio de transmisión</td><td>¿Al ser el medio de transmisión el aire, es importante la seguridad de la red?</td></tr>
<tr><td rowspan="3">Radiofrecuencia</td><td>Banda de frecuencia</td><td>¿Qué estándar 802.11 sería apropiado: a, b, g, n ?

a: 5.4GHz-54Mbps b: 2.4GHz-11Mbps g: 2.4GHz-54Mbps n:2.4GHz y 5.4GHz – 300Mbps</td></tr>
<tr><td>Atenuaciones</td><td>¿Las paredes del edificio presentan una atenuación considerable o despreciable?</td></tr>
<tr><td>Potencia</td><td>¿La señal inalámbrica debe cubrir solo el interior del edificio o extenderse unos metros afuera?</td></tr>
</table>

Tabla 3.1: Variable independiente

3.5.2 Variable dependiente

ABSTRACTO		CONCRETO	
Conceptualización	Categorías	Indicadores	Items
Interconexión de los edificios de la FISEI mediante la WLAN creada Comunicación entre dos o más redes para administrar eficientemente sus recursos	Comunicación entre redes	Enlaces	¿Qué tipo de enlace es el más apropiado para interconectar los edificios? Cableado o inalámbrico
		Compartir información	¿La interconexión entre ambos edificios permitirá el intercambio de información?
	Administrar recursos	Hardware	¿Al interconectar ambos edificios se logrará administrar eficientemente a los dispositivos de uno y otro edificio?
		Centralizar información	¿La interconexión permitirá organizar toda la información de la red en un solo punto?

Tabla 3.2: Variable dependiente

3.6 Recopilación de la información

- Estructuración de instrumentos

Se desarrolló una encuesta considerando que era la herramienta más adecuada para obtener información.

- Validación del instrumento

Se procedió a verificar el instrumento indicado (encuesta) para su posterior aprobación por parte del tutor de este proyecto, y su respectiva distribución.

- Aplicación del instrumento

La aplicación de la encuesta estuvo dirigida a los estudiantes de la FISEI dado que fueron los principales involucrados en este tema.

- Recopilación de la información

La encuesta con interrogantes técnicos referentes a redes y comunicaciones, estuvo dirigida a estudiantes de tercero a noveno nivel de las carreras de Ingeniería en Sistemas e Ingeniería en Electrónica y comunicaciones.

3.7 Procesamiento de la información

- Revisión de la información recogida

  Posterior al proceso de encuesta se verificó que los datos hayan sido llenados correctamente y que se hayan recopilado todas las copias del instrumento distribuido, resultando todo correcto.

- Tabulación de la información

  Los datos tabulados en el siguiente capítulo muestran la justificación por parte de los alumnos para la realización de este proyecto.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

A continuación se presenta la tabulación de los datos recogidos con la encuesta realizada y el análisis respectivo de cada pregunta de este instrumento.

1. ¿Es necesaria para usted la existencia de una red inalámbrica en el nuevo edificio?

Objetivo:

Conocer la necesidad y razón de acceso inalámbrico a internet en el edificio dos de la facultad.

Respuesta		Cantidad	Porcentaje (%)
No		0	0
Sí	Tareas	73	30.8
	Correo	57	24.05
	Redes Sociales	42	17.72
	Multimedia	43	18.14
	Otro	22	9.29
Total		237	100

Tabla 4.1: Tabulación – Pregunta 1

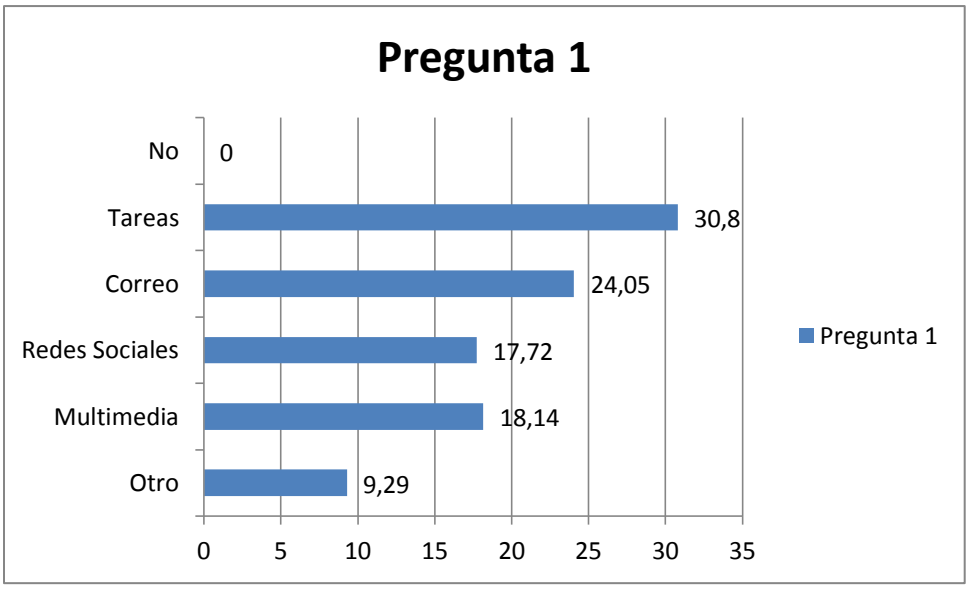


Fig. 4.1: Gráfico porcentual - Pregunta 1

Interpretación: Se puede apreciar que no existen alumnos de la FISEI que no esté de acuerdo con implementarse una red inalámbrica en el nuevo edificio de la facultad. Los alumnos explican cuáles son las principales actividades realizadas mediante la WLAN existente, tal y como se muestra en el gráfico porcentual.

Análisis: Se demuestra la necesidad de implementarse una red inalámbrica en el edificio dos de la FISEI.

2. **¿Dispone de un dispositivo compatible para acceder a la red inalámbrica de la FISEI?**

Objetivo:

Determinar el número de equipos que utilizan la red inalámbrica de la FISEI y el tiempo que pasan conectados a la misma.

Respuesta		Cantidad	Porcentaje
No		56	100
	Piensa adquirir uno?	42	75

Respuesta		Cantidad	Porcentaje
Sí (Tiempo que permanece conectado)	1 hora	18	14.52
	2 horas	38	30.64
	3 horas	21	16.94
	Más	47	37.9
Total		124	100

Tabla 4.2: Tabulación – Pregunta 2

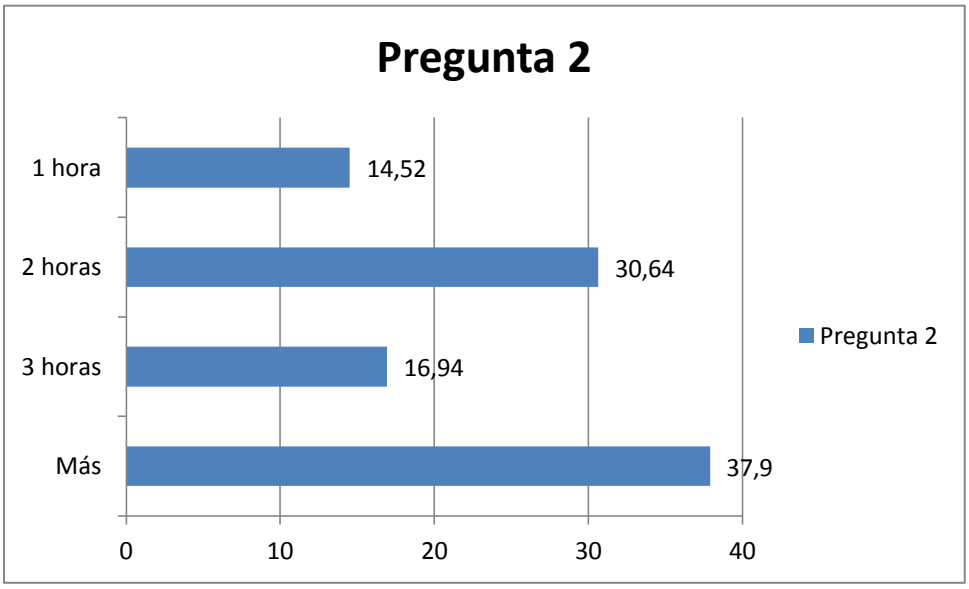


Fig. 4.2: Gráfico porcentual - Pregunta 2

Interpretación: La cantidad de alumnos que si disponen de equipos compatibles con la WLAN de la FISEI es superior a los alumnos que no disponen de ellos. Así mismo, de quienes no tienen equipos compatibles, el 75% piensa en adquirir uno a mediano plazo. En cuanto al tiempo de conexión, casi un 40% de alumnos utilizan la red más de 3 horas diariamente.

Análisis: El número de estudiantes que si pueden aprovechar la red inalámbrica de la FISEI es notablemente superior respecto al número de alumnos que no pueden hacerlo.

3. ¿Por qué es importante una seguridad eficiente en la red inalámbrica de la FISEI?

Objetivo:

Establecer por qué es necesario un sistema de seguridad para la red inalámbrica de la FISEI.

Respuesta	Cantidad	Porcentaje (%)
Evitar que se conecten personas ajenas a la facultad	80	35.71
Evitar ataques	88	39.29
Información sensible existente	56	25
No es importante	0	0
Total	224	100

Tabla 4.3: Tabulación – Pregunta 3

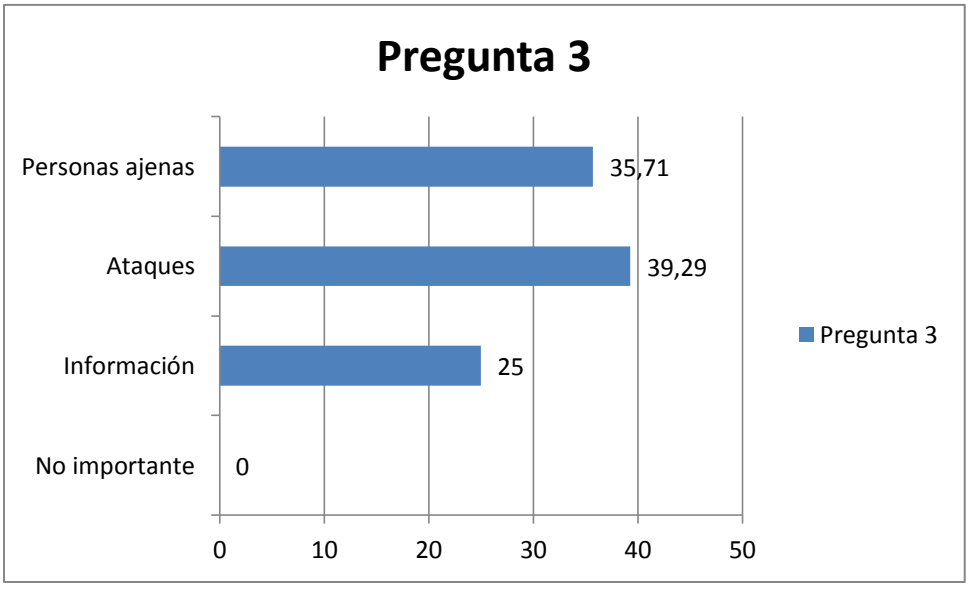


Fig. 4.3: Gráfico porcentual - Pregunta 3

Interpretación: El mayor porcentaje de respuestas muestra que los estudiantes están de acuerdo en que se implemente un sistema de seguridad eficiente para la red inalámbrica de la facultad ya sea por uno o varios factores de los indicados.

Análisis: Los alumnos de la facultad justifican la necesidad de implementar un sistema de seguridad eficiente para la WLAN de la FISEI.

4. ¿Por qué se debe elegir el estándar WIFI N (diseñado para redes inalámbricas de área local o WLAN) como tecnología para la red inalámbrica de la FISEI

Objetivo:

Definir la razón por la que se debería utilizar la tecnología WIFI N en la red inalámbrica de la facultad.

Respuesta	Cantidad	Porcentaje (%)
Mayor velocidad de transmisión	127	60.77
Mejor desempeño de la red	82	39.23
No se debe elegir WIFI N	0	0
Total	209	100

Tabla 4.4: Tabulación – Pregunta 4

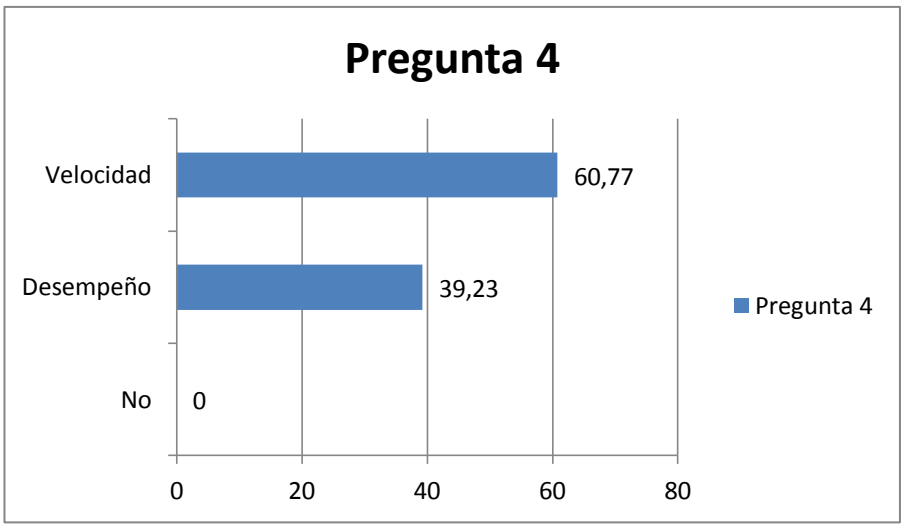


Fig. 4.4: Gráfico porcentual - Pregunta 4

Interpretación: La mayor velocidad y el mejor desempeño de la red son los factores que motivan la utilización del estándar 802.11n en la red inalámbrica de la FISEI, según los alumnos. Ninguno de ellos cree que no se debe elegir WIFI N como tecnología.

Análisis: En base a sus conocimientos técnicos, los alumnos de la facultad creen importante la implementación del estándar 802.11n como tecnología para la red inalámbrica de la FISEI.

5. La interconexión entre ambos edificios de la FISEI permitiría:

Objetivo:

Establecer las ventajas de interconectar ambos edificios de la FISEI mediante una red inalámbrica.

Respuesta	Cantidad	Porcentaje (%)
Administración eficiente de usuarios	75	32.47
Libre desplazamiento entre ambos edificios	156	67.53
No es necesario	0	0
Total	224	100

Tabla 4.5: Tabulación – Pregunta 5

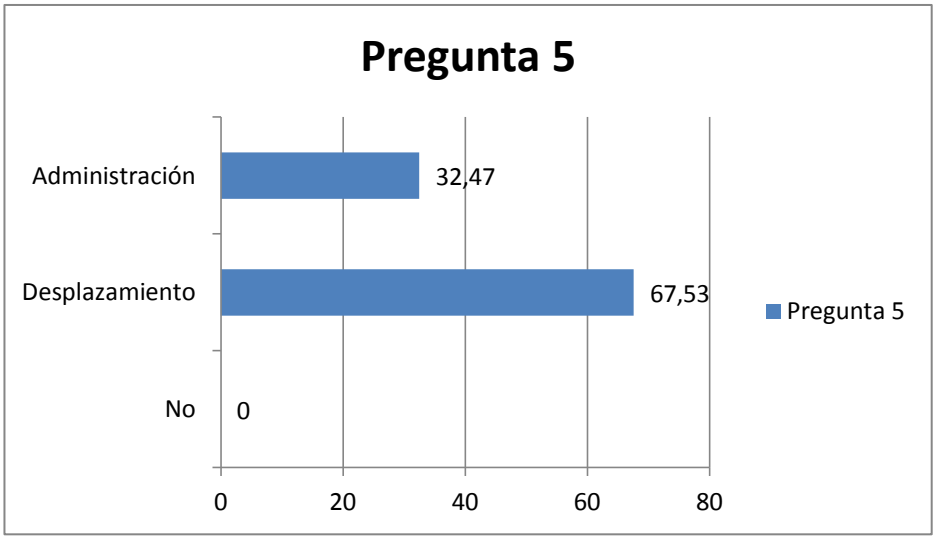


Fig. 4.5: Gráfico porcentual - Pregunta 5

Interpretación: Permanecer conectado a la red inalámbrica de la FISEI mientras los usuarios se desplazan entre uno u otro edificio es lo más importante para los alumnos, sin dejar de lado la administración eficiente de los mismos. No se cree que este punto sea innecesario.

Análisis: Se corrobora con esta opinión la importancia de interconectar ambos edificios inalámbricamente.

CONCLUSIÓN

La información recogida con la encuesta afirma la importancia y necesidad de conseguir los objetivos planteados para el desarrollo de este proyecto. Específicamente justifica los parámetros más importantes que debería tener la red inalámbrica de la FISEI, planteados en cada pregunta, tal como se concebía al inicio de este trabajo.

4.1 Verificación de la hipótesis

Posterior a la tabulación de datos, se procedió con la verificación de la hipótesis mediante el método estadístico Chi-cuadrado:

Chi-cuadrado

$$x^2 = \sum \left(\frac{(O - E)^2}{E} \right)$$

Ecuación 4.1: Chi-cuadrado

En donde**:**

x^2= Chi-cuadrado

$\sum$ = Sumatoria

O = Frecuencia Observada

E = Frecuencia esperada o técnica

4.1.1 Frecuencias Observadas

Nº	Pregunta	Muy Bueno	Bueno	Regular	Total
1	¿Es necesaria para usted la existencia de una red inalámbrica en el nuevo edificio?	75	60	45	180
2	¿Dispone de un equipo compatible para acceder a la red inalámbrica de la FISEI?	124	42	14	180
3	¿Por qué es importante una seguridad eficiente en la red inalámbrica de la FISEI?	65	73	42	180
5	¿La interconexión entre ambos edificios de la FISEI permitiría?	130	50	0	180
	TOTAL	394	225	101	720

Tabla 4.6: Frecuencias observadas

4.1.2 Frecuencias Esperadas

Nº	Pregunta	Muy Bueno	Bueno	Regular	Total
1	¿Es necesaria para usted la existencia de una red inalámbrica en el nuevo edificio?	98.5	56.25	25.25	180
2	¿Dispone de un equipo compatible para acceder a la red inalámbrica de la FISEI?	98.5	56.25	25.25	180
3	¿Por qué es importante una seguridad eficiente en la red inalámbrica de la FISEI?	98.5	56.25	25.25	180
5	¿La interconexión entre ambos edificios de la FISEI permitiría?	98.5	56.25	25.25	180
	TOTAL	394	225	101	720

Tabla 4.7: Frecuencias esperadas

4.1.3 Modelo lógico

Hipótesis alterna (Ha) = Hipótesis si

Hipótesis nula (Ho)= Hipótesis no

4.1.4 Nivel de significancia y regla de decisión

4.1.4.1 Grado de libertad

GL = (c-1)*(f-1)

GL = (4-1)*(3-1)

GL = 3 * 2

GL = 6

4.1.4.2 Grado de significancia

Nivel de significación (P): Denominado nivel de confianza, se refiere a la probabilidad de que los resultados observados se deban al azar. Este valor es fijado por el investigador (usualmente es el 5% o 10%), lo que indica que, si se toma P = 0.05, se está entendiendo que sólo en un 5% de las veces en que se realice la medición, el resultado obtenido podría deberse al azar. En el caso análogo, sería igual a decir que existe un nivel de confianza del 95%; el resultado es real y no debido a la casualidad.

Nivel de confiabilidad = 95%

Grado de significancia = 0.05

Valores críticos de chi-cuadrado

Esta tabla contiene los valores x^2 que corresponden a un área específica y a un número determinado de grados de libertad.

Grados libertad	**0,1**	**0,05**	**0,025**	**0,01**	**0,005**
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19

Tabla 4.8: Valores críticos del chi-cuadrado

$X_t^2(c-1)*(f-1)= 12.59$

4.1.5 Calculo del Chi-cuadrado

En donde:

O= Frecuencia observada

E= Frecuencia esperada

O-E= Frecuencias observadas – frecuencias esperadas

(O-E) ^{2}= Resultado de las frecuencias observadas y esperadas al cuadrado

(O-E) ^{2}/E = Resultado de las frecuencias observadas y esperadas al cuadrado dividido para las frecuencias esperadas.

O	**E**	**O-E**	**$(O-E)^2$**	**$(O-E)^2/E$**
75	98.5	-23.5	552.25	5.61
60	56.25	3.75	14.06	0.25
45	25.25	19.75	390.06	15.45
124	98.5	25.5	650.25	6.6
42	56.25	-14.25	203.06	3.62
14	25.25	-11.25	126.56	5.01
65	98.5	-33.5	1122.25	11.39
73	56.25	16.75	280.56	4.99
42	25.25	16.75	280.56	11.11
130	98.5	31.5	992.25	10.07
50	56.25	-6.25	39.06	0.69
0	25.25	-25.25	637.56	25.25
			TOTAL	**100.04**

Tabla 4.9: Cálculo de chi-cuadrado

$X^2 = 100.04$

Xt2(c-1)*(f-1) = 12.59

Criterio de decisión:

X2 < Xt2(c-1)*(f-1) → Acepta Ho.

Valores de decisión:

100.04 > 12.59→ Se rechaza Ho

Debido a que X2 es mayor a Xt2(c-1)*(f-1) se rechaza Ho y se acepta Ha.

Por lo tanto, se justifica la implementación de una Red WLAN segura para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El número de encuestados ha sido determinado según la muestra correspondiente de la población para evitar falsos resultados con un número menor de encuestados y evitar la pérdida de tiempo con un número mayor al necesario.

- El instrumento de recolección de datos, en este caso la encuesta, permitió saber la opinión de las personas involucradas en el presente proyecto y determinar si el desarrollo de este proyecto es necesario para la FISEI, y en este caso, lo es.

- Las preguntas de la encuesta fueron desarrolladas cuidadosamente, pensando en las personas a quienes se les iba a consultar. Las respuestas obtenidas fueron muy valiosas para determinar la factibilidad de este proyecto.

- Dado el número de preguntas y las alternativas para cada una de ellas, fue conveniente utilizar un método estadístico adecuado a este caso. El método del Chi-cuadrado fue el más idóneo para descubrir la hipótesis correcta.

5.2 Recomendaciones

- Es importante determinar el nivel de conocimiento de las personas a encuestarse antes de formular las preguntas. Esto brindará datos significativamente útiles para avanzar en un proyecto o cancelarlo. En este caso, las personas más idóneas para responder las preguntas formuladas fueron los alumnos de las carreras de Ingeniería en Electrónica e Ingeniería en Sistemas de tercero a noveno nivel.
- Antes que el proyecto empiece a tomar forma y se disponga de la adquisición de equipos y herramientas para el desarrollo del mismo, es importante definir antes si el proyecto es viable y tiene la aprobación de las personas involucradas, de lo contrario, serán gastos económicos y pérdida de tiempo irrecuperables.
- El número de preguntas formuladas en la encuesta está en estrecha relación con la confirmación o negación de la hipótesis, por lo tanto, es altamente recomendable que las preguntas tengan íntima concordancia con el tema a desarrollarse y definir un número razonable de éstas para un resultado correcto de la hipótesis formulada.
- La tabulación de los datos obtenidos con la encuesta es de vital importancia para definir los resultados. Es recomendable por ello, revisar que se recolecten todas las encuestas llenadas y que se contabilicen cuidadosamente cada una de las respuestas en ellas.

CAPITULO VI

PROPUESTA

6.1 Datos informativos

Tema: Red WLAN segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Ubicación:

Provincia: Tungurahua

Cantón: Ambato

Parroquia: Huachi Chico

Lugar: Universidad Técnica de Ambato – Campus Huachi – Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Tutor: Ing. Eduardo Chaso

Autor: Javier Seilema

6.2 Antecedentes de la propuesta

La idea de implementar una red WLAN segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, nace en primer lugar de la necesidad de acceso inalámbrico a internet en el edificio dos de la FISEI. Por supuesto, esta infraestructura y el edificio principal de la facultad no podían quedar aislados uno del otro y se concibió la conexión entre ambas edificaciones mediante enlace inalámbrico para que los alumnos puedan

desplazarse entre uno y otro edificio sin problemas de pérdida de conectividad a internet.

Por otro lado, debido a que una red inalámbrica está expuesta a ciertos riesgos por tratarse de un sistema que utiliza el aire como medio de transmisión, el desarrollo de un sistema de seguridad que sea eficiente, fue uno de los parámetros más importantes que no se podía pasar por alto y se integró en el presente proyecto.

6.3 Justificación

La necesidad de los alumnos de la FISEI en disponer de acceso inalámbrico hacia internet para la realización de tareas, temas de investigación entre otras actividades online, fue una de las razones más importantes para la implementación de una WLAN en el edificio dos de la facultad. Y aunque existía ya un sistema de este tipo en el edificio principal de la FISEI, con el desarrollo de este proyecto la seguridad y flexibilidad del mismo se vió ampliada ofreciendo ventajas para los usuarios y administradores.

6.4 Objetivos

6.4.1 Objetivo General

Diseñar e implementar una red WLAN segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

6.4.2 Objetivos Específicos:

- Analizar el diseño de la red inalámbrica existente en la FISEI.
- Definir los requerimientos para implementar la red inalámbrica en el edificio dos de la FISEI y la interconexión entre las dos infraestructuras de la Facultad.
- Establecer un sistema de seguridad eficiente para la WLAN propuesta.
- Implementar la red inalámbrica y el sistema de seguridad planteado.

6.5 Análisis de la factibilidad

6.5.1 Factibilidad técnica

Para la implementación de la red inalámbrica se requirió de puntos de acceso inalámbricos con función de repetidor, que cumplan con los estándares 802.11 b, g y n. Comercialmente, este tipo de equipos están disponibles en el mercado sin mayores problemas.

6.5.2 Factibilidad operativa

El software utilizado para la implementación del sistema de seguridad y la simulación de una red inalámbrica WLAN es gratuito y por lo tanto, no se requirió de un gasto económico extra para obtenerlo. Incluso la mayor parte del sofware en cuestión era libre.

6.5.3 Factibilidad económica

Los gastos contemplados para la realización del presente proyecto se encontraban dentro del presupuesto planificado, por lo tanto, fue factible la realización del mismo en cuanto a lo económico se refiere.

6.6 Fundamentación

6.6.1 Modelo OSI

OSI es un modelo de red y sus siglas significan Open Sistem Interconnection o interconexión de sistemas abiertos. Es utilizado para describir el proceso que existe entre la conexión física de red y la aplicación del usuario final. Consta de 7 capas o niveles descritos a continuación.

6.6.1.1 Capa física

Se encarga de las conexiones físicas de la computadora hacia la red. Por ejemplo, se encarga de definir el medio físico por el que se va mantener la comunicación: cable de par trenzado, coaxial, fibra óptica, etc.

6.6.1.2 Capa de enlace de datos

Define el formato de las tramas, sus cabeceras, etc. En este nivel se habla de direcciones MAC (Media Access Control) que son las que identifican a las tarjetas de red de forma única.

6.6.1.3 Capa de red

En esta capa se encuentra el protocolo IP. Esta capa es la encargada del enrutamiento y de dirigir los paquetes IP de una red a otra. Normalmente los "routers" se encuentran en esta capa.

6.6.1.4 Capa de transporte

En esta capa se encuentra el protocolo TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). Estos se encargan de dividir la información que envía el usuario en paquetes de tamaño aceptable por la capa inferior. La diferencia entre ambos es sencilla. En primer lugar, el TCP esta orientado a conexión, es decir la conexión se establece y se libera. Mientras dura una conexión hay un control de lo que se envía y por lo tanto se puede garantizar que los paquetes llegan y están ordenados.

El UDP no hace nada de lo anterior. Los paquetes se envían y el protocolo se despreocupa si estos llegan en buen estado o no. El UDP se usa para enviar datos pequeños, rápidamente, mientras que el TCP añade una sobrecarga al tener que controlar los aspectos de la conexión, aunque "garantiza" transmisiones libres de errores.

6.6.1.5 Capa de sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

6.6.1.6 Capa de presentación

Se encarga de "ordenar" los datos de una forma estándar. Define una forma común para todos, de tal forma que dos ordenadores de distinto tipo se entiendan.

6.6.1.7 Capa de aplicación

Aquí se encuentran los usuarios finales. Mail, FTP (File Transfer Protocol), Telnet, DNS (Domain Name Server), son distintas aplicaciones que se encuentran en esta capa.

6.6.2 TCP

TCP (Transmission Control Protocol) es un protocolo de comunicación orientado a conexión que se encuentra en la capa de transporte según OSI (Open Systems Interconnection) y garantiza conexiones fiables.

6.6.3 IP

Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados (unidades de transporte de información envíadas en una red de computadoras). Es un protocolo no fiable, es decir, de mejor entrega posible sin garantías.

6.6.4 Router

Interconecta redes en el nivel de red y encamina paquetes entre ellas.

Los routers son capaces de elegir las mejores rutas de transmisión así como tamaños óptimos para los paquetes. La función básica de encaminamiento está implementada en la capa IP. Por lo tanto, cualquier estación de trabajo que ejecute TCP/IP se puede usar como router.

6.6.5 Access Point

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un equipo que interconecta dispositivos de comunicación inalámbrica para formar una red de este tipo. Normalmente un WAP también puede conectarse a una red cableada y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos.

6.6.6 Switch

Un conmutador o switch es un dispositivo de redes de computadores que opera en la capa de enlace de datos del modelo OSI. Interconecta dos o más segmentos de red según la dirección MAC (Media Access Control) del destino de las tramas en la red.

6.6.7 Wi-Fi y sus Estándares

Wi-Fi (Wireless Fidelity) es una marca de la *Wi-Fi Alliance* (anteriormente la *WECA: Wireless Ethernet Compatibility Alliance*), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

WiFi nace tras la asociación de las empresas Nokia y Symbol Technologies para crear una tecnología inalámbrica que asegure la compatibilidad entre equipos con esta denominación.

El primer estándar WiFi para redes inalámbricas de área a local pasó a identificarse como 802.11b y de ahí en adelante han ido surgiendo otros estándares similares, aunque con mayores prestaciones que 802.11b para aumentar el rendimiento de las WLAN actuales.

6.6.8 802.11

El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

6.6.9 802.11g

Es una evolución del estándar 802.11b y dado que es retrocompatible, los dispositivos b y g pueden trabajar sin problemas en conjunto.

El estándar 802.11g utiliza la banda de los 2.4GHz al igual que la versión b pero con una velocidad teórica máxima de 54Mbps, rindiendo en términos reales 22 Mbps.

6.6.10 802.11n

IEEE 802.11n es una propuesta de modificación al estándar IEEE 802.11g para mejorar significativamente el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Una importante característica de 802.11n es que se trata de una tecnología retrocompatible que puede trabajar con b y g sin conflictos, aunque con ciertas limitaciones como la reducción de velocidad en un sistema híbrido como ese.

6.6.10.1 MIMO

MIMO es el acrónimo en inglés de Multiple-input Multiple-output (en español, Múltiple entrada múltiple salida) y es una tecnología incorporada en el estándar 802.11n para aumentar la eficiencia de un sistema inalámbrico.

MIMO se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas de dispositivos inalámbricos. En el formato de transmisión inalámbrica tradicional la señal se ve afectada por reflexiones, lo que ocasiona degradación o corrupción de la misma y por lo tanto pérdida de datos. MIMO aprovecha fenómenos físicos como la propagación multicamino para incrementar la tasa de transmisión y reducir la tasa de error. Para conseguirlo, MIMO hace uso de “Diversidad de espacio” y “Channel Bonding”.

La diversidad de espacio se refiere a la utilización de varias antenas para la transmisión/recepción de datos. En sistemas con una sola antena, la propagación multicamino ocasiona degradación de la señal y reduce la eficiencia del sistema.

La diversidad de espacio se aprovecha de la propagación multicamino para aumentar el rendimiento de la red al tomar en cuenta que, la probabilidad de que una misma señal transmitida llegue con errores a varias antenas de recepción, es menor que la probabilidad de que la misma señal llegue corrupta a una sola antena. De esta forma, el sistema de recepción utiliza todas las señales recibidas para interpretar correctamente la información transmitida, evitando la repetición de datos entre transmisor y receptor y consiguiendo eficiencia en el sistema. En la siguiente imagen se muestra un ejemplo de diversidad de espacio en el receptor.

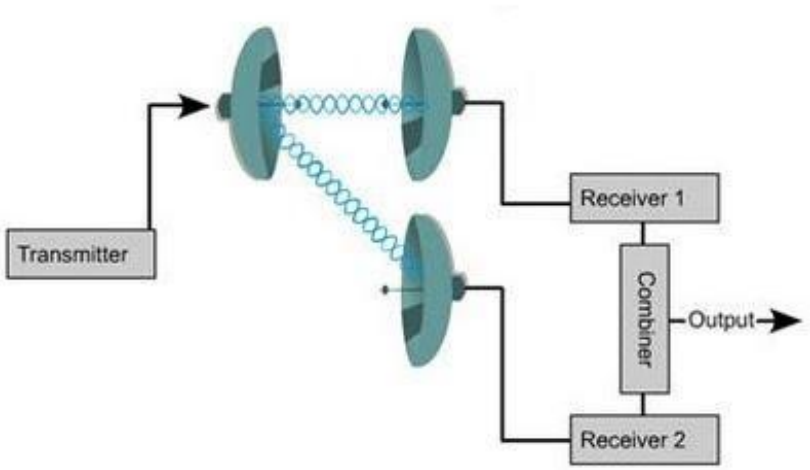


Fig. 6.1: Diversidad de espacio en el receptor

El Channel Bonding, también conocido como 40MHz o unión de interfaces de red, consiste en simular un dispositivo de red con gran ancho de banda uniendo varias tarjetas de red independientes, de manera que las aplicaciones vean una sóla interfaz de red. En 802.11n el Channel Bonding se basa en utilizar dos canales separados, que no se solapen, para transmitir datos simultáneamente. La unión de interfaces de red incrementa la cantidad de datos que pueden ser transmitidos. En el estándar n se utilizan dos bandas adyacentes de 20MHz cada una, por eso el nombre de 40MHz. A continuación se muestra un ejemplo de Channel Bonding basado en 4 canales.

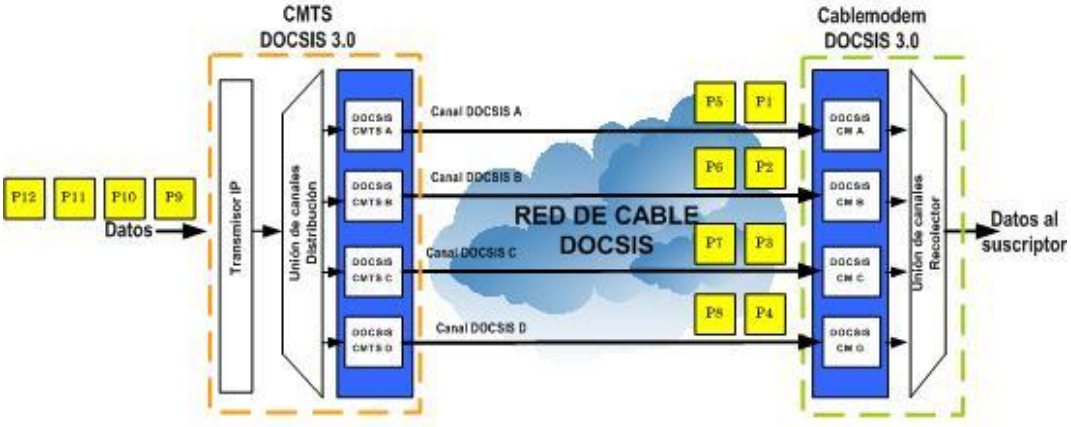


Fig. 6.2: Ejemplo de Channel Bonding

6.6.11 802.11g y 802.11n trabajando en conjunto

Al inicio de este proyecto se concebía como mejor alternativa la adopción del estándar 802.11n por las mejoras respecto a los anteriores estándares de la familia 802.11, tales como la velocidad de transmisión, su retro-compatibilidad con estándares anteriores y el mejor desempeño del sistema para manejar más información, sin aumentar por ello la tasa de error, gracias a la tecnología MIMO que utiliza varias antenas para la transmisión de información.

Sin embargo, el estándar 802.11n y las características mencionadas sólo podían ser aprovechadas cuando todo el sistema, incluyendo los puntos de acceso y los clientes inalámbricos trabajan con dicho estándar. Cuando no es así y dentro del sistema inalámbrico n se mezclan dispositivos de otros estándares, sean éstos b o g, la red no podrá optar por la mayor velocidad o el máximo desempeño, puesto que los equipos en versiones b/g no alcanzan a "comprender" la tecnología que 802.11n utiliza. Ello obliga a que la sistema completo trabaje a la velocidad del dispositivo más lento de la red, subutilizando las características que 802.11n ofrece.

Por tal razón y agregando que en la FISEI, además de equipos con tecnología n también existían puntos de acceso con tecnologías g, se decidió finalmente trabajar en base a ambos estándares para la implementación. Por un lado, los equipos con 802.11n ofrecen una mayor cobertura y rendimiento de la red gracias

a la tecnología MIMO, y por otra parte, la tecnología 802.11g con la que cuentan un par de equipos de la facultad que no pueden desaprovecharse dada la compatibilidad con 802.11n.

6.6.12 Arquitectura de red para el estándar 802.11

La arquitectura de la familia de estándares 802.11 está basada en la arquitectura celular, es decir, es un sistema subdividido en celdas (denominadas Basic Service Set o BSS en la nomenclatura de 802.11) donde cada una está controlada por una estación base (definida como Access Point o AP).

Aunque una red WLAN puede estar formada por una sola celda con un único AP, la mayoría de instalaciones se encuentran formadas por varias celdas, donde los Access Points están conectados a algún tipo de backbone (llamado Distribution System o DS) típicamente Ethernet.
El sistema completo incluyendo las diferentes celdas, sus respectivos APs y el DS, está definido en el estándar como Extended Service Set (ESS).
La siguiente figura define la arquitectura de 802.11 con los componentes descritos:

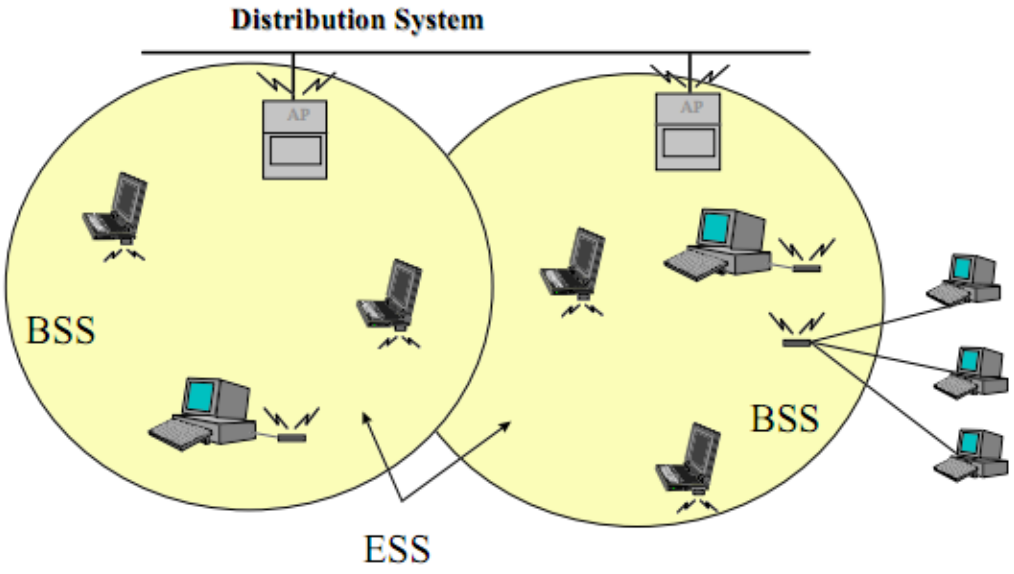


Fig. 6.3: Arquitectura de 802.11

Finalmente las estaciones de trabajo o clientes inalámbricos se definen como STA.

6.6.13 Formato de un paquete de datos (trama) en 802.11

En general, para la familia de estándares 802.11, el formato de un paquete de datos o trama es el siguiente:

Frame Control	Duration ID	Address1 (source)	Address2 (destination)	Address3 (rx node)	Sequence Control	Address4 (tx node)	Data	FCS
2	2	6	6	6	2	6	0 - 2,312	4

Fig. 6.4: Formato de una trama 802.11

Donde:

Campo	Octetos	Notes/Description
Frame Control	2	Información a nivel MAC
Duration ID	2	Duración de la trama
Address 1	6	Dirección del emisor
Address 2	6	Dirección del receptor
Address 3	6	Dirección de la estación receptora
Sequence Control	2	Control de tramas repetidas
Address 4	6	Dirección de la estación transmisora
FrameBody	0-2312	Datos
Checksum	4	CRC de 32 bits (verificación de trama)

Tabla 6.1: Campos de una trama 802.11

6.6.14 CSMA/CA

Es un protocolo utilizado por la familia 802.11 y significa Carrier Sense Multiple Access, Collision Avoidance (acceso múltiple por detección de portadora con evasión de colisiones). Este protocolo permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo, para evitar colisiones entre los paquetes de datos. Si el medio está libre, entonces puede transmitir, caso contrario, deberá esperar a que el medio se encuentre disponible.

6.6.15 Canales/Frecuencias utilizados por 802.11b/g/n en la banda de 2.4GHz

Canal	Frecuencia central	Ancho de banda
1	2412 MHz	2401 - 2423 MHz
2	2417 MHz	2406 - 2428 MHz
3	2422 MHz	2411 - 2433 MHz
4	2427 MHz	2416 - 2438 MHz
5	2432 MHz	2421 - 2443 MHz
6	2437 MHz	2426 - 2448 MHz
7	2442 MHz	2431 - 2453 MHz
8	2447 MHz	2436 - 2458 MHz
9	2452 MHz	2441 - 2463 MHz
10	2457 MHz	2446 - 2468 MHz
11	2462 MHz	2451 - 2473 MHz
12	2467 MHz	2456 - 2478 MHz
13	2472 MHz	2461 - 2483 MHz

Tabla 6.2: Canales y frecuencias en 802.11b/g/n

De los canales mostrados en la tabla 6.2, del 1 al 11 están legalmente disponibles para su utilización en América. Sin embargo, estos 11 canales no son completamente independientes (canales contiguos se superponen y se producen interferencias tal como se muestra en la Fig. 6.5). El ancho de banda de la señal (22MHz) es superior a la separación entre canales consecutivos (5MHz), por eso se hace necesaria una separación de al menos 5 canales con el fin de evitar interferencias entre celdas adyacentes. Tradicionalmente se utilizan los canales 1, 6 y 11. La configuración de canal solamente es realizada en el punto de acceso puesto que los clientes inalámbricos detectan automáticamente el canal.

En la Fig. 6.5 se muestra la distribución gráfica de los canales utilizados en 802.11.

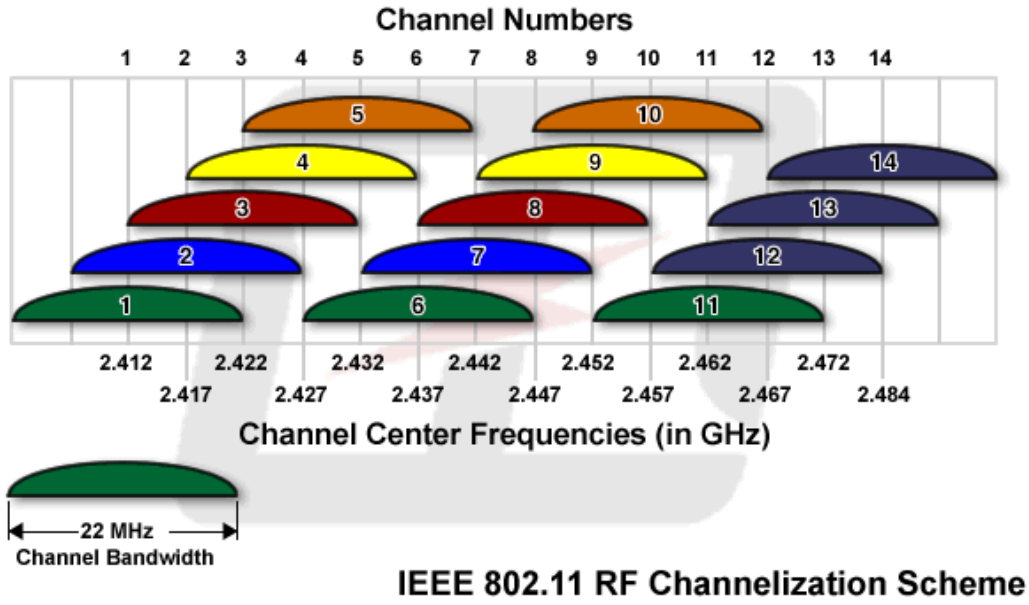


Fig. 6.5: Distribución de canales en 802.11

6.6.16 Roaming entre Access points

Los Puntos de Acceso Inalámbricos tienen un radio de cobertura aproximado de 100m, aunque esto varía bastante en la práctica entre un modelo y otro y según las condiciones ambientales y físicas del lugar (obstáculos, interferencias, etc).

Si interesa permitir la itinerancia (roaming, en inglés) o movilidad de los usuarios, es necesario colocar los Access Point de tal manera que haya "overlapping" o superposición entre los radios de cobertura.

6.6.16.1 Los Beacons y cómo funciona el Roaming entre APs.

Los Puntos de Acceso Inalámbricos emiten intermitentemente “señales”, de forma similar a los faros, para anunciar su presencia y que todas las estaciones que estén en el rango de cobertura sepan que el AP está disponible. Estas señales son paquetes denominados Beacons que contienen varios parámetros, entre ellos, el SSID. Cuando una estación se aleja demasiado de un Access Point, "pierde la señal", es decir que deja de percibir estos Beacons que le indican la presencia del Access Point.

Cuando existe superposición, se comienzan a captar los Beacons del otro Access Point, hacia el cual se está dirigiendo, a la vez que se van perdiendo gradualmente los del anterior.

6.6.16.2 La Problemática del Roaming

El estándar 802.11 no contiene instrucciones detalladas sobre el tema del roaming, por lo tanto, cada fabricante diseña el algoritmo de decisión según su criterio y con los parámetros que estima convenientes. Por esta razón pueden existir problemas, sobre todo en grandes ambientes donde se mezclan Puntos de Acceso de diferentes fabricantes o Puntos de Acceso de un fabricante con dispositivos móviles de otras marcas. Cada uno tendrá otro algoritmo de decisión y pueden producirse "desavenencias" en el roaming.

6.6.17 Técnicas de transmisión de datos en 802.11g/n

6.6.17.1 Modulación

La modulación es una técnica utilizada en comunicaciones para transmitir información a través de un medio no guiado como el aire. Dado que una señal de información por sí sola es incapaz de viajar a través de este medio de transmisión, se requiere de una señal que sí logre “llevar” esta información a través del aire. Técnicamente es el proceso de “montar” la señal de información (moduladora) sobre una “señal de transporte” (portadora) para tener una transmisión adecuada o eficiente. La señal resultante se denomina modulada y es formada en el transmisor (circuito modulador).

6.6.17.2 Multiplexación

En telecomunicaciones, la multiplexación es la combinación de dos o más canales de información en un solo medio de transmisión, usando un dispositivo llamado multiplexor.

6.6.17.3 OFDM

La Multiplexación por División de Frecuencias Ortogonales u Orthogonal Frequency Division Multiplexing (OFDM) es la técnica de transmisión utilizada por 802.11g/n y consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información. Posteriormente se modula la información en PSK (Phase Shift Keying) y QAM (Quadrature Amplitude Modulation).

OFDM ofrece una alta tasa de transmisión al dividir el flujo de datos en varios canales paralelos como se puede observar en la siguiente imagen.

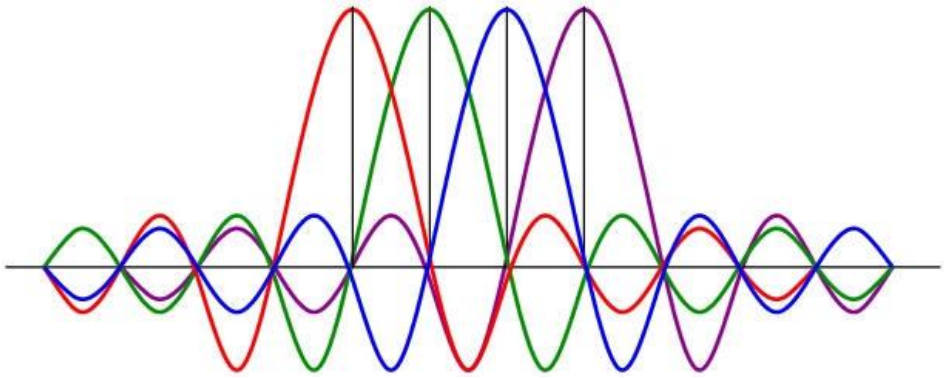


Fig. 6.6: Representación gráfica de OFDM

6.6.17.4 PSK

Es una técnica de modulación digital que consiste en hacer variar la fase de la portadora mientras la frecuencia y amplitud se mantienen constantes.

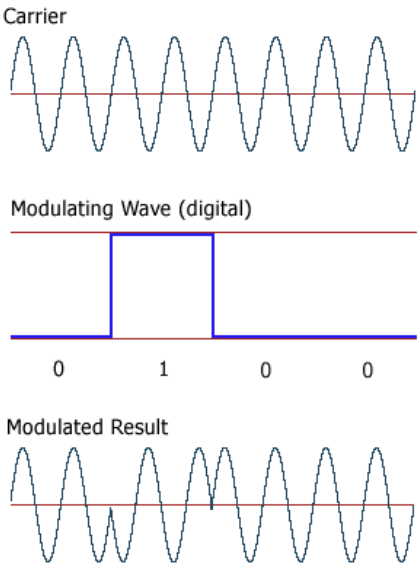


Fig. 6.7: Modulación PSK

6.6.17.5 QAM

Técnica de modulación en la que la señal portadora varía tanto en amplitud (ASK) como en fase. A continuación se muestra la modulación 8QAM (una variación de QAM) en la que se varía la amplitud y fase de la señal moduladora con 3 bits.

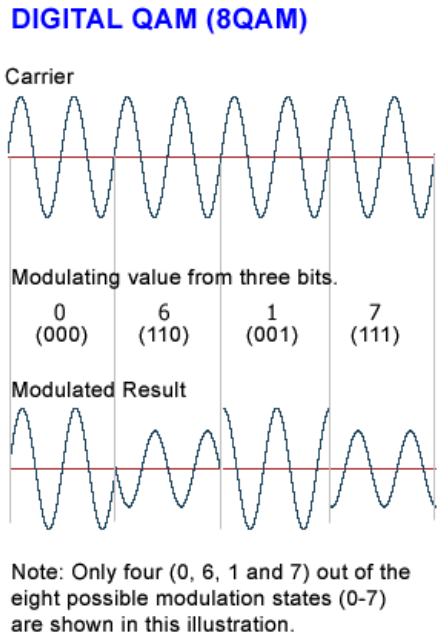


Fig. 6.8: Modulación QAM

6.6.17.6 QoS

QoS o Calidad de Servicio (*Quality of Service,* en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

6.6.18 Servidor de Autenticación

6.6.18.1 Servidor

Un servidor simplemente es una computadora que, formando parte de una red, provee servicios a otros computadores denominados clientes. No necesariamente es un equipo con características impresionantes. Ello dependerá del uso que quiera dársele.

Existen un sinnúmero de tipos de servidores, cada uno diseñado para realizar determinada tarea. Existen por ejemplo servidores web, servidores de bases de datos, de archivos, correo, proxy, etc.

Eso en cuanto al tipo de servicio que ofrecen. Ahora, también se los puede definir en base a las tareas que realizan de la siguiente forma:

- **Servidor dedicado:** son aquellos que le dedican toda su potencia a administrar los recursos de la red, es decir, a atender las solicitudes de procesamiento de los clientes.
- **Servidor no dedicado:** son aquellos que no dedican toda su potencia a los clientes, sino también pueden jugar el rol de estaciones de trabajo.

6.6.18.2 Radius

Radius es un acrónimo que viene de ***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**erver*. Es un protocolo que permite gestionar la autenticación, autorización y registro de usuarios remotos sobre un determinado recurso. Mediante este protocolo que utiliza el puerto 1812 UDP (User datagram protocol) se transmiten todas las peticiones de los clientes hacia el servidor radius para que este conceda o niegue

el acceso a cierto servicio. Las palabras auntenticación, autorización y registro son, en conjunto, más conocidas con el acrónimo AAA.

- **Autenticación:**

Individualmente, la palabra autenticación hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. Este paso consta de la presentación de credenciales (usuario y contraseña comúnmente) por parte del usuario que demanda acceso.

- **Autorización**

Se refiere a conceder servicios específicos a un determinado usuario (o la negación de éstos) en base a las credenciales presentadas por el mismo.

- **Registro**

Como su nombre lo indica, en este proceso se realiza un registro del consumo de recursos que tienen los usuarios.

6.6.18.3 Servidor Radius

Un servidor Radius es un sistema que realiza la autenticación, autorización y registro de clientes que desean acceder a determinado servicio. Para implementar un servidor de este tipo se requieren de varios paquetes que permitan su funcionamiento. Es necesario de un servidor web con soporte SSL, una base de datos y su respectivo sistema de gestión para almacenar información de los clientes y también, un sistema que haga de intermediario entre el servidor radius y el cliente, como Chillispot.

6.6.18.4 Servidor Web

Un servidor web es un programa que se ejecuta en un ordenador, manteniéndose a la espera de peticiones por parte de un cliente (navegador web) y que responde a

estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún inconveniente.

6.6.18.5 SSL

La misión del protocolo SSL (Secure Sockets Layer o Capa de conexión segura) es permitir que se establezca una conexión segura entre el servidor web y el visitante que accede al mismo mediante un navegador de internet, encriptando los datos entre ambos de forma que, lo datos que viajan entre ellos no sean legibles por terceros si fueran interceptados.

Se puede verificar que se tiene una conexión SSL observando en la barra de direcciones del navegador web el prefijo https (Hipertext transfer protocol secure).

6.6.18.6 Base de datos

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

6.6.18.7 Sofware Libre

Aunque suele confundirse comúnmente con gratuito y generalmente es así, no necesariamente el software libre carece de costo. El término libre más bien hace referencia a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, modificar el software y distribuirlo modificado.

6.6.18.8 Licencia GPL

Una de las más utilizadas en el software libre es la *Licencia Pública General de GNU* (GNU GPL). El autor conserva los derechos de autor (copyright) y permite la redistribución y modificación, bajo políticas específicas, para asegurarse de que todas las versiones modificadas del software permanezcan bajo los términos más restrictivos de la propia GNU GPL. Esto hace que sea imposible crear un producto con partes no licenciadas GPL: el conjunto tiene que ser GPL.

6.6.18.9 GNU/Linux

GNU/Linux es uno de los sistemas operativos más utilizados a nivel global. Comúnmente es nombrado como Linux simplemente. GNU/Linux es una combinación entre "herramientas" del sistema operativo GNU, y un núcleo o kernel denominado Linux, creado a comienzos de los años 90 por un estudiante finlandés de nombre Linus Torvalds.

GNU/Linux es uno de los ejemplos más representativos de software libre actualmente, entendiéndose por software libre a todo aquel que pueda ser ejecutado, estudiado-modificado, copiado y distribuido, generalmente bajo licencia GPL.

Gracias a este tipo de licencia que posee GNU/Linux, se han creado innumerables versiones modificadas de este sistema operativo denominadas distribuciones o "distros". Podemos resaltar algunas como Red Hat Enterprise, Slackware, Arch, Debian, Gentoo, CentOS, Fedora, Ubuntu, etc.

- **CentOS**

CentOS (Community ENTerprise Operating System) es un clon de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Además de proveer el sistema usable a suscriptores de pago, Red Hat también publica el código fuente de esta distribución Linux, el mismo que es utilizado por la comunidad CentOS para generar su propia versión, aunque ésta no es mantenida ni asistida por RedHat.

- **Apache**

El servidor HTTP Apache, es un servidor web de código abierto para plataformas como GNU/Linux, Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP y la noción de sitio virtual.

En windows, Apache se ejecuta normalmente como un servicio mientras que en GNU/Linux lo hace como demonio o "daemon" denominado httpd.

- **Freeradius**

Es uno de los servidores Radius más populares bajo licencia GPL y sin ningún costo. Freeradius es el paquete núcleo del servidor Radius propuesto, que se encarga de realizar el proceso de autenticación, autorización y registro de usuarios. Además de ser gratuito y simple, tiene las prestaciones necesarias para desarrollar un robusto servidor radius. Es compatible con los protocolos de autenticación más comunes y además, incorpora una interfaz de administración web para una gestión más sencilla de los clientes.

- **MySQL**

MySQL es un sistema de gestión de base de datos multiusuario que se ofrece tanto con licencia GPL como con otro tipo de licencias con costo. Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y el copyright del código está en poder del autor individual, MySQL es patrocinado por una empresa privada, que posee el copyright de la mayor parte del código.

- **Chillispot**

Es un portal cautivo de código abierto, o definido también como un controlador de un punto de accceso WLAN. Entiéndase por portal cautivo a la técnica utilizada para forzar a un cliente HTTP a ver una página determinada. Es uno de los paquetes más importantes para la autenticación de clientes inalámbricos cuando se trata de un servidor radius. Es gratuito y su código se encuentra bajo licencia GPL.

- **DaloRADIUS**

Es una aplicación para la administración web de clientes Radius. Está diseñada para la gestión de recursos y cuenta con características como administración de usuarios, registro e incluso un sistema de facturación. Dispone de cuatro idiomas: inglés, ruso, húngaro e italiano.

6.7 Metodología

Para el desarrollo de este proyecto, la ubicación más conveniente de los puntos de acceso en ambos edificios fue una de los puntos más importantes a ser considerado. Además de hacerlo en base a un mapa de señal (generado por un software de simulación) para lograr cubrir las áreas destinadas, fue imprescindible buscar los lugares más propicios para que los APs permanezcan seguros y que se pueda acceder a estos en el momento en que se requiera realizar ajustes.

De forma paralela a la implementación se intentó evitar inconvenientes a los usuarios, manteniendo activa la anterior red inalámbrica mientras se iba desarrollando este proyecto. En primer lugar se procedió a levantar el servidor radius. A continuación se realizó la reubicación e instalación de los puntos de acceso, y sólo después de haber preparado ambas partes, se integró todo el sistema y se realizaron las pruebas respectivas.

6.8 Modelo operativo

6.8.1 Análisis del sistema

La Facultad de Ingeniería en Sistemas, Electrónica e Industrial, cuenta con un ancho de banda hacia internet de 2.5 Mbps, de los cuales, 1 Mbps está destinado para el acceso inalámbrico a la web.

Actualmente existen 300 usuarios registrados y autorizados para el acceso a internet mediante la WLAN actual. El número promedio de usuarios conectados simultáneamente a diario es de 10 a 15, alcanzando pocas veces picos de 30

usuarios. El pico más alto de usuarios conectados al mismo tiempo hacia dicha red ha sido de 100, según los datos proporcionados por el departamento de administración de redes de la FISEI.

La red inalámbrica mencionada se encontraba operativa y proveía de acceso a internet sólo en el edificio principal de la facultad. Dicha red contaba con un router inalámbrico y un punto de acceso que funcionaba como repetidor del primero, ambos ubicados estratégicamente para que la señal llegara "adecuadamente" a todos los pisos del edificio y los estudiantes y docentes puedan acceder a internet.

Las características del router inalámbrico y puntos de acceso se describen a continuación.

Datos	**Router inalámbrico**	**Punto de acceso**
Marca	Linksys	3com
Modelo	WRT300N	7760
Estándares	b/g/n	a/b/g
Firmware	V1.1	AP software 1.6.40
MAC	00:1D:7E:3D:8C:48	00:1A:C1:86:F6:40
IP	192.168.124.2	192.168.124.3
DHCP Server	Enabled	Disabled
AP Mode	No aplicable	Repeater
SSID	FISEI	FISEI
Canal	6	6

Tabla 6.3: Características de equipos inicialmente activos en la FISEI

El router inalámbrico se encontraba en la oficina de administración de redes de la FISEI, la cual está ubicada en el segundo piso del edificio, mientras que, el punto de acceso se encontraba justo al frente de esa ubicación, al otro lado del ágora de la FISEI.

En cuanto a la administración de usuarios, los mismos se agregaban al sistema mediante autenticación MAC, sean éstos alumnos, docentes u otras personas de distinto título.

Debido a la política del personal de administración de redes de la FISEI, sólo son admitidos computadores portátiles para el acceso a la WLAN. No son aceptados por ningún motivo teléfonos inteligentes o dispositivos similares como tabletas.

La red inalámbrica de la FISEI se encontraba operando en perfecto estado desde el 2008.

Respecto al segundo edificio, desde su construcción no se había establecido ningún tipo de acceso inalámbrico hacia internet para los estudiantes en esta infraestructura. Sin embargo, la facultad ya había realizado la adquisición de puntos de acceso para la implementación de este sistema en esta construcción. Los datos de estos equipos se muestran en la sección de configuración de equipos al final de la implementación del servidor radius.

6.8.2 Requerimientos

6.8.2.1 Software

6.8.2.1.1 Software de diseño de la red inalámbrica

Para la implementación de la red inalámbrica se utilizó el software de diseño AirMagnet Planner, parte del kit AirMagnet Survey, de Fluke Networks, que se puede encontrar en la página web http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Survey. La versión demo gratuita de este software fue suficiente para realizar el diseño de la red WLAN de la FISEI.

Aunque existen otras soluciones en el mercado para el diseño de redes, que incluso son mucho más profesionales que AirMagnet Planner, la mayoría de ellas no ofrecían lo necesario para el desarrollo de este proyecto en sus versiones gratuitas, y el costo para adquirirlas era considerable. Un ejemplo de ese tipo de

software es RF3D WiFi Planner, una herramienta muy potente para el diseño de redes inalámbricas, que incluso ofrece la posibilidad de trabajar en ambientes 3D, aunque su costo por la versión profesional es prohibitivo. Su versión demo que sólo permite experimentar con el manejo del programa y no permite la creación de nuevos proyectos puede ser adquirida en esta página web http://www.psiber.com/en/home/products/wifi-simulation/rf3d-wifiplanner2.html.

Un cuadro comparativo sobre los dos programas mencionados se muestra a continuación.

	AirMagnet Planner	**RF3D WiFi Planner**
Estándares 802.11 soportados	a/b/g	a/b/g/n
Ambientes	Interior/Exterior	Interior/Exterior
Ubicación automática de APs	Impreciso	Óptimo
Soporta ambientes 3D	No	Sí
Versión Demo Gratuita	Sí	Sí, sólo manejo
Costo versión PRO	150 dólares	300 dólares

Tabla 6.4: Tabla comparativa – Software de simulación

Como se indicó, RF3D WiFi Planner no ofrecía la posibilidad de trabajar sobre un nuevo proyecto, razón suficiente para haber optado por AirMagnet Planner, un software que, si bien no ofrece la posibilidad de trabajar en 3D, sí fue muy útil en el momento de ayudar a determinar la ubicación más correcta de los puntos de acceso en los edificios de la FISEI.

6.8.2.1.2 Servidor radius

Para la implementación del servidor radius, se utilizó CentOS como sistema operativo, puesto que es una distribución Linux gratuita en todo sentido. Además, se trata de software libre y es un sistema operativo muy popular en servidores por su seguridad y estabilidad. Los sólidos conocimientos adquiridos sobre esta plataforma por parte del autor de este proyecto, fue otra de las razones para seleccionar CentOS como la distribución más propicia.

Si bien es cierto existía la posibilidad de crear el servidor Radius sobre un sistema Windows, era la opción menos indicada por el costo que tiene la licencia para la utilización de este sistema operativo.

Así mismo, todos los paquetes utilizados en CentOS para levantar el servidor Radius, fueron soluciones libres sin costo alguno.

Para la administración de los clientes del sistema inalámbrico se utilizó el paquete DaloRadius. Es un software gratuito y libre que puede ser adquirido en esta página web: http://sourceforge.net/projects/daloradius/files/.

6.8.2.2 Hardware

Anteriormente, la red inalámbrica de la FISEI disponía de dos puntos de acceso para cubrir el edificio principal de la facultad. Sin embargo, la cobertura que ofrecía ese par de puntos de acceso era insuficiente para abastecer de señal a toda la infraestructura, especialmente el tercer piso del edificio. Con la adquisición de dos puntos de acceso por parte de las autoridades de la facultad, se logró cubrir satisfactoriamente dicho edificio con uno de ellos, y extender la señal hacia el edificio dos con el restante. Dado que, un único punto de acceso en esta construcción no lograba cubrirla de señal satisfactoriamente, se optó por adquirir un punto de acceso adicional para proveer de acceso inalámbrico a los alumnos de esta infraestructura.

Considerando la tecnología n que utiliza el punto de acceso ubicado en este edificio, fue necesario adquirir otro equipo que incorpore la misma tecnología, y que, por supuesto, no tenga problemas en repetir la señal de dicho AP. Para este último requerimiento, fue preciso que el equipo sea de la misma marca y modelo que el punto de acceso ubicado en este edificio, para evitar problemas de compatibilidad al funcionar como repetidor. Obviamente las especificaciones son las mismas para ambos equipos y se muestran en el anexo 4 de este documento. Así mismo el costo del equipo se muestra en la sección de 6.9 que detalla el presupuesto de este proyecto.

6.8.3 Diseño de la red inalámbrica

Definir la ubicación más adecuada de los puntos de acceso fue el aspecto más importante en el diseño de la red inalámbrica. Al ser dos edificios de grandes dimensiones, la ubicación de los AP fue crucial para lograr una cobertura adecuada en ambas infraestructuras. El software de simulación permitió variar las posiciones de los puntos de acceso y observar los alcances de la señal en cada una de ellas para seleccionar la posición más correcta de los equipos y lograr una cobertura óptima.

6.8.3.1 Calidad de servicio o QoS

La calidad de servicio de la red inalámbrica está en íntima relación con el número de puntos de acceso. Del número de usuarios por AP dependerá el troughput (rendimiento) de la red. Por tal razón, a continuación se presenta el cálculo del número de puntos de acceso necesarios para mantener un rendimiento aceptable de la red. La fórmula utilizada estima este cálculo en base al ancho de banda deseado para cada usuario, el número total de usuarios, el porcentaje de uso de la red y la velocidad estimada de la misma.

Cálculo del número de APs en una Red WLAN 802.11:

$$Número\ de\ APs = \frac{AB * Número\ de\ usuarios * Porcentaje\ de\ uso}{Velocidad}$$

Ecuación 6.1: Cálculo del número de APs

- AB: Ancho de Banda que se desea para cada usuario= 2 Mbps
  AB aceptable para la transmisión de datos entre AP y cliente.
- Número de usuarios= 30
  Dato proporcionado por el departamento de redes de la FISEI
- Porcentaje promedio de uso de la red= 50%
  Considerando la información obtenida con la pregunta dos de la encuesta realizada, el tiempo máximo que la mayoría de usuarios pasa conectado a la

red de la FISEI es de 3 horas. Si se toma en cuenta el horario matutino y vespertino que existe en la facultad, el tiempo se duplica a 6 horas, por lo cual se concluye que el uso de la red es alrededor de un 50% a lo largo del día.

- Velocidad: 5.5 Mbps

  Se trata de un valor óptimo para la transmisión de datos en una red inalámbrica, considerando que, con una velocidad de 5.5Mbps no existe inconvenientes para trabajar con aplicaciones exigentes como el streaming de vídeo.

$$Número\ de\ APs = \frac{2Mbps * 30 * 0.5}{5.5Mbps}$$

$$\boldsymbol{Número\ de\ APs = 5.45} \approx 5$$

6.8.3.2 Cálculo del ancho de banda

Se consideró para este cálculo el ancho de banda disponible y el número de usuarios simultáneos máximo que se encuentran conectados a la red inalámbrica.

$$Ancho\ de\ banda\ por\ cada\ usuario = \frac{Ancho\ de\ Banda\ disponible}{Número\ de\ usuarios}$$

Ecuación 6.2: Cálculo del ancho de banda

$$Ancho\ de\ banda\ por\ cada\ usuario = \frac{1Mbps}{30}$$

$$Ancho\ de\ banda\ por\ cada\ usuario = 33.33Kbps$$

El resultado demuestra que, un ancho de banda total de 1 Mbps genera un valor bajo de AB para que cada cliente navegue en internet. Sin embargo, se trata de un resultado obtenido en base a un número pico de usuarios. Si se tiene en cuenta que el número promedio de usuarios conectados a la red es de 10 a 15, entonces el ancho de banda para cada uno se ve duplicado respecto al resultado obtenido, es decir 66 Kbps, un valor estimado aceptable para navegar en internet.

6.8.3.3 Diseño lógico y físico

Para comprender mejor como se encuentra estructurada la red inalámbrica implementada de la FISEI, se presenta el siguiente diagrama y tabla mostrando el diseño físico y lógico de la red. El edificio principal al que se hace mención, es aquel donde se encuentran las oficinas administrativas de la FISEI.

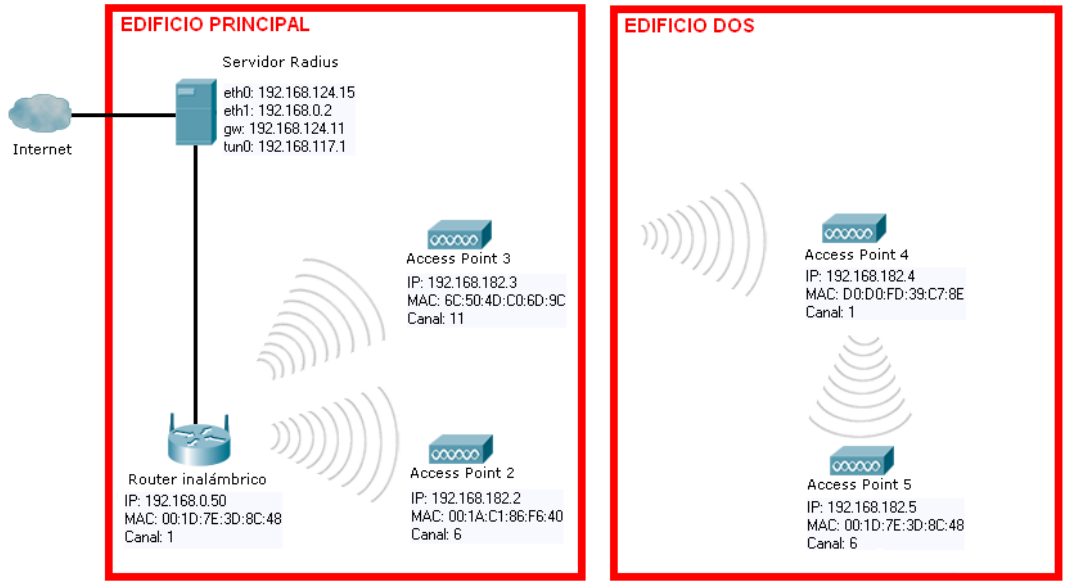


Fig. 6.9: Diagrama de la red inalámbrica

Equipo	Ubicación	Dirección IP	MAC	Canal
Servidor Radius	E. Principal	192.168.0.2	00:19:5B:89:BF:06	X
Router inalámbrico	E. Principal	192.168.0.50	00:1D:7E:3D:8C:48	1
Access Point 2	E. Principal	192.168.182.2	00:1A:C1:86:F6:40	6
Acccess Point 3	E. Principal	192.168.182.3	6C:50:4D:C0:6D:9C	11
Access Point 4	E. Dos	192.168.182.4	D0:D0:FD:39:C7:8E	1
Access Point 5	E. Dos	192.168.182.5	50:3D:E5:30:FB:14	6

Tabla 6.5: Diseño lógico y físico

6.8.3.4 Ubicación de los puntos de acceso en el edificio principal

A continuación se muestra la ubicación más adecuada para el router inalámbrico y los puntos de acceso en este edificio, utilizando el sofware de simulación Airmagnet Planner, mostrando un mapa de cobertura con una frontera de -70 dbm en intensidad de señal. Los parámetros tomados en cuenta para la ubicación de los equipos fueron: el área de cobertura, la seguridad, y la compatibilidad entre uno y otro para trabajar como repetidores y permitir el roaming entre todos ellos. El router inalámbrico de la Fig. 6.9 se encuentra representado por el AP-1 en la siguiente imagen.

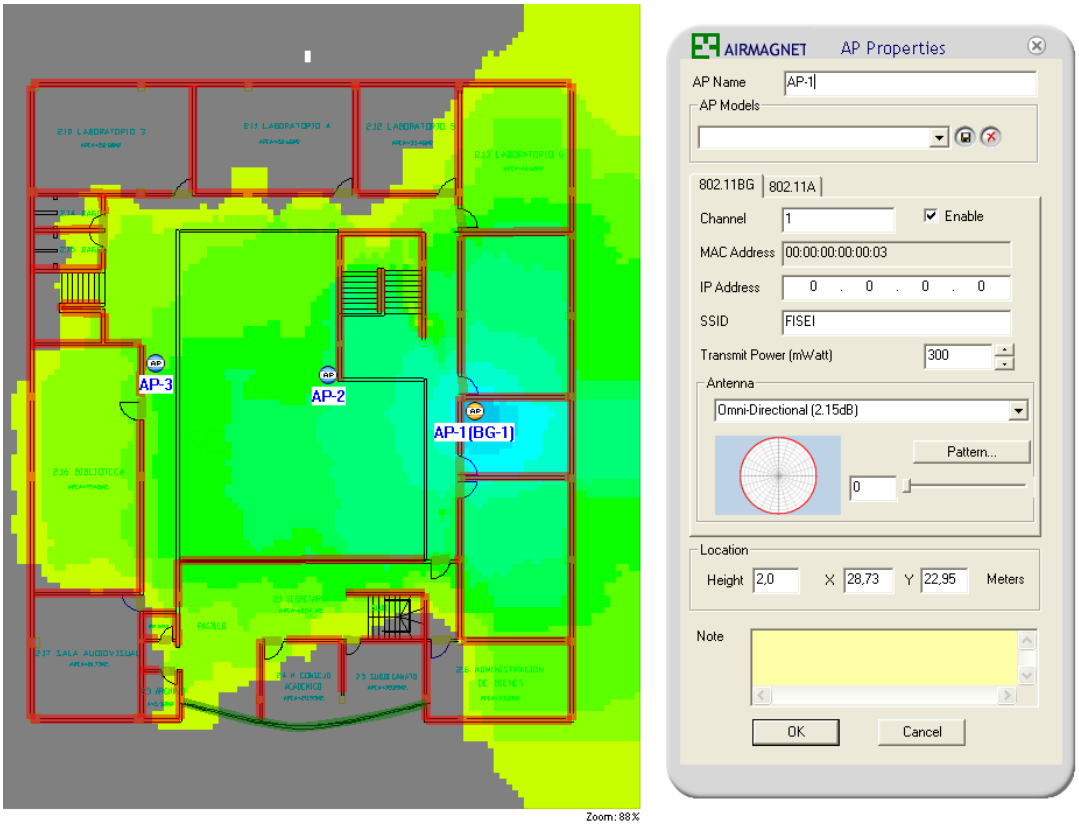


Fig. 6.10: Cobertura del AP-1 en edificio principal de la FISEI

Como se aprecia en la Fig. 6.10, el AP-1, que en realidad se trata de un router inalámbrico Linksys, y se encuentra a la derecha en la imagen superior, es el "punto base" de la red inalámbrica puesto que está conectado con cable al servidor radius y es el que genera la señal inalámbrica principal. Está ubicado en la oficina de administración de redes de la FISEI, puesto que ahí también se encuentra el servidor radius y porque se requería controlar de cerca su funcionamiento dado que es el generador "maestro" de la señal inalámbrica de ambas infraestructuras de la facultad.

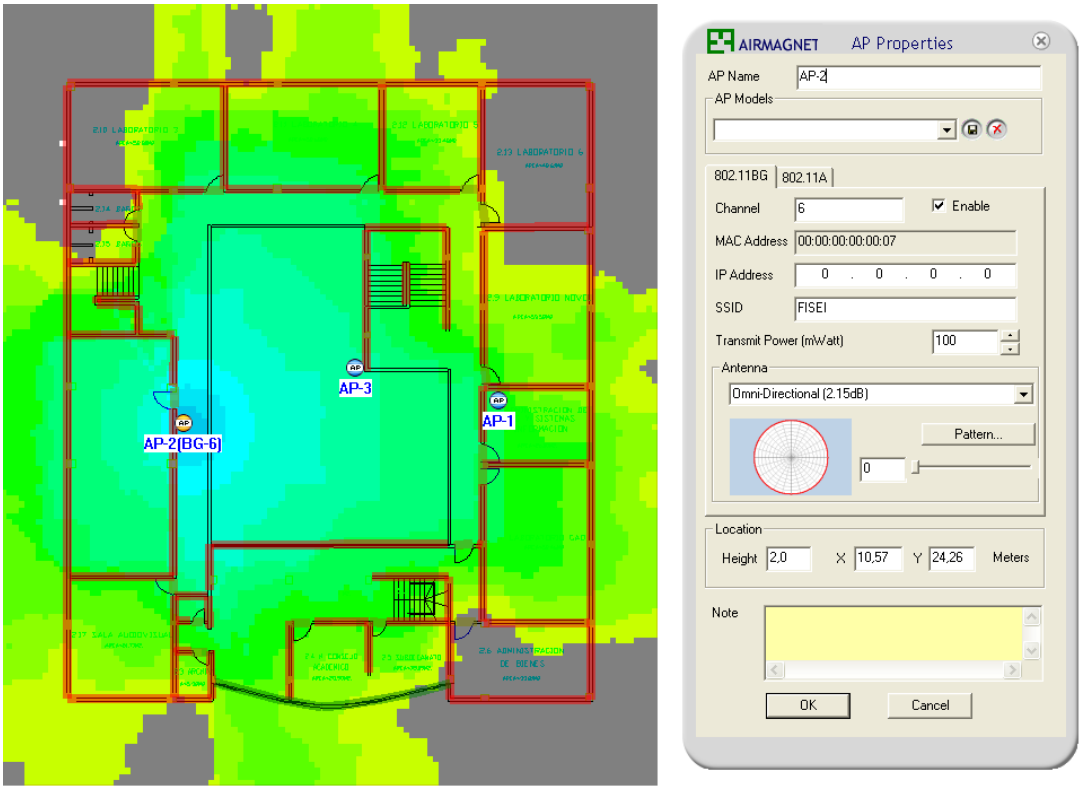


Fig. 6.11: Cobertura del AP-2 en edificio principal de la FISEI

En la Fig. 6.11, el AP-2, marca 3com, está ubicado en la parte izquierda de la imagen y se colocó en ese lugar para cubrir eficientemente toda la biblioteca de la facultad, área muy importante puesto que la mayoría de estudiantes trabajan con sus equipos portátiles allí. Las pruebas prácticas demostraron la necesidad de colocar un repetidor en esa zona para abarcarla completamente.

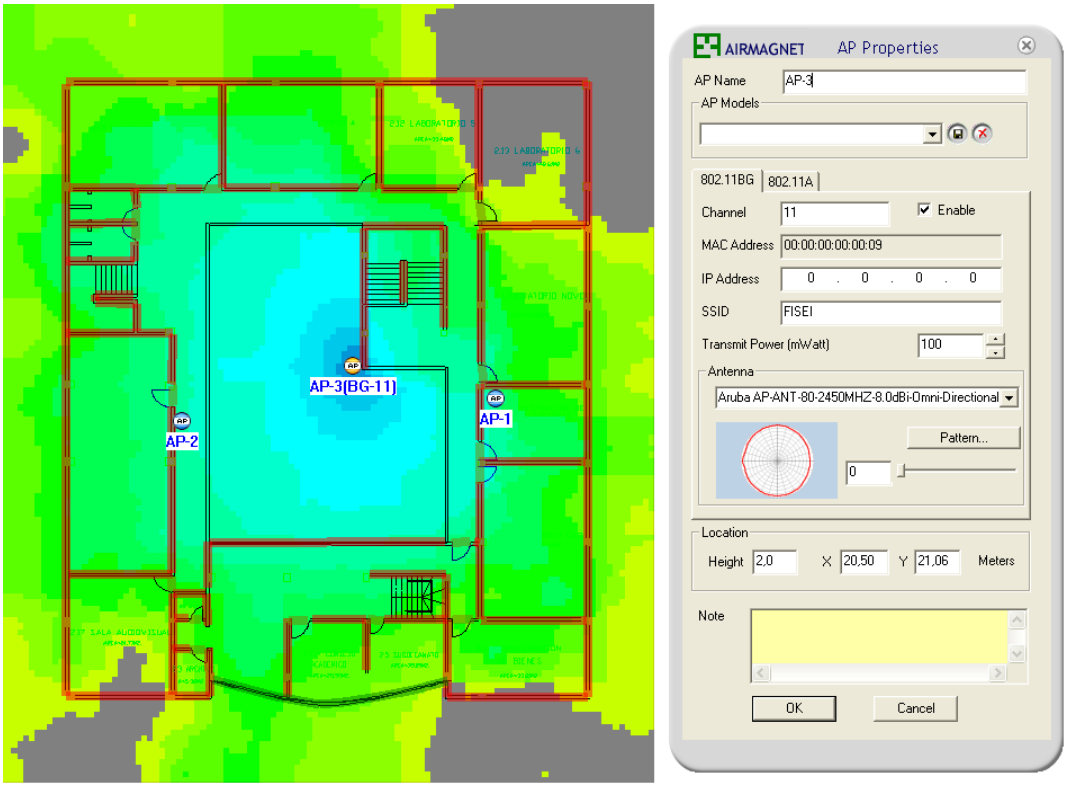


Fig. 6.12: Cobertura del AP-3 en edificio principal de la FISEI

En la Fig. 6.12, el AP-3 se trata de un punto de acceso Cisco con tecnología b/g, y está ubicado en esa posición con el objetivo de proyectar la señal inalámbrica hacia el edificio dos, a través de una antena exterior de 9dBi de ganancia. Además de estar colocado estratégicamente en ese lugar para recibir una señal coherente

del router inalámbrico, ayuda a cubrir el tercer piso ya que allí la señal era insuficiente según las pruebas prácticas realizadas.

Finalmente se muestra el mapa de cobertura de los tres equipos activados al mismo tiempo:

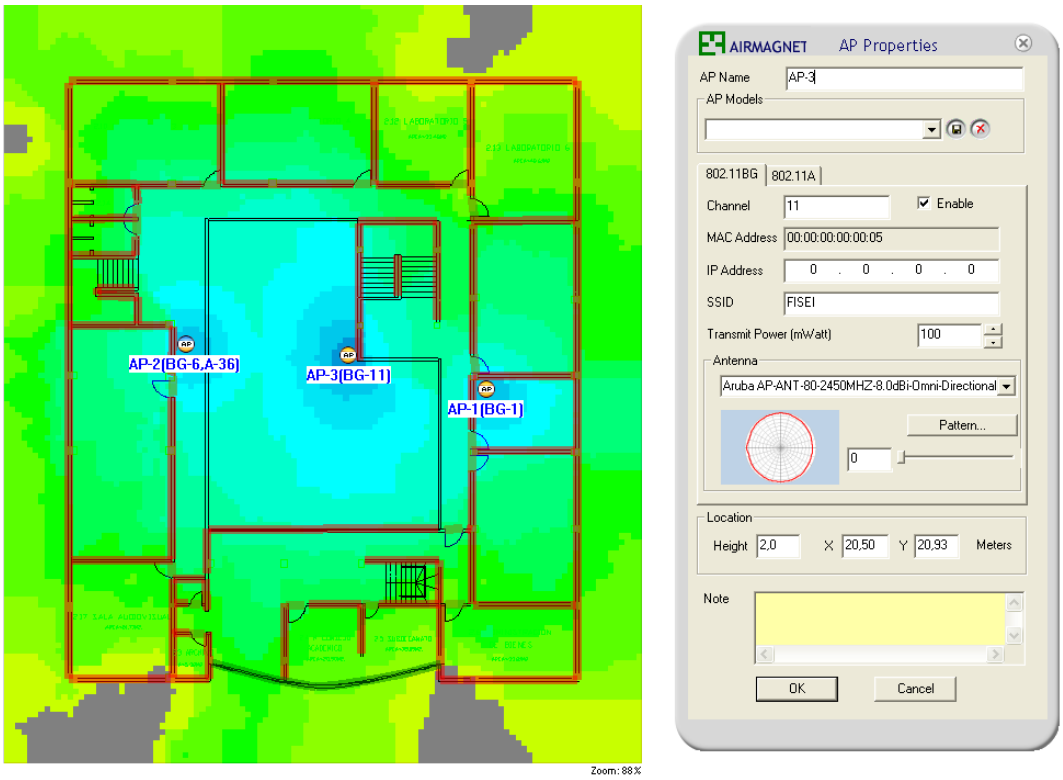


Fig. 6.13: Cobertura del AP-1, AP-2 y AP-3 en edificio principal de la FISEI

6.8.3.5 Ubicación de los puntos de acceso en el edificio dos

De la misma forma que en el edificio principal, a continuación se puede observar las imágenes del área de cobertura de los dos puntos de acceso restantes en el edificio dos de la FISEI.

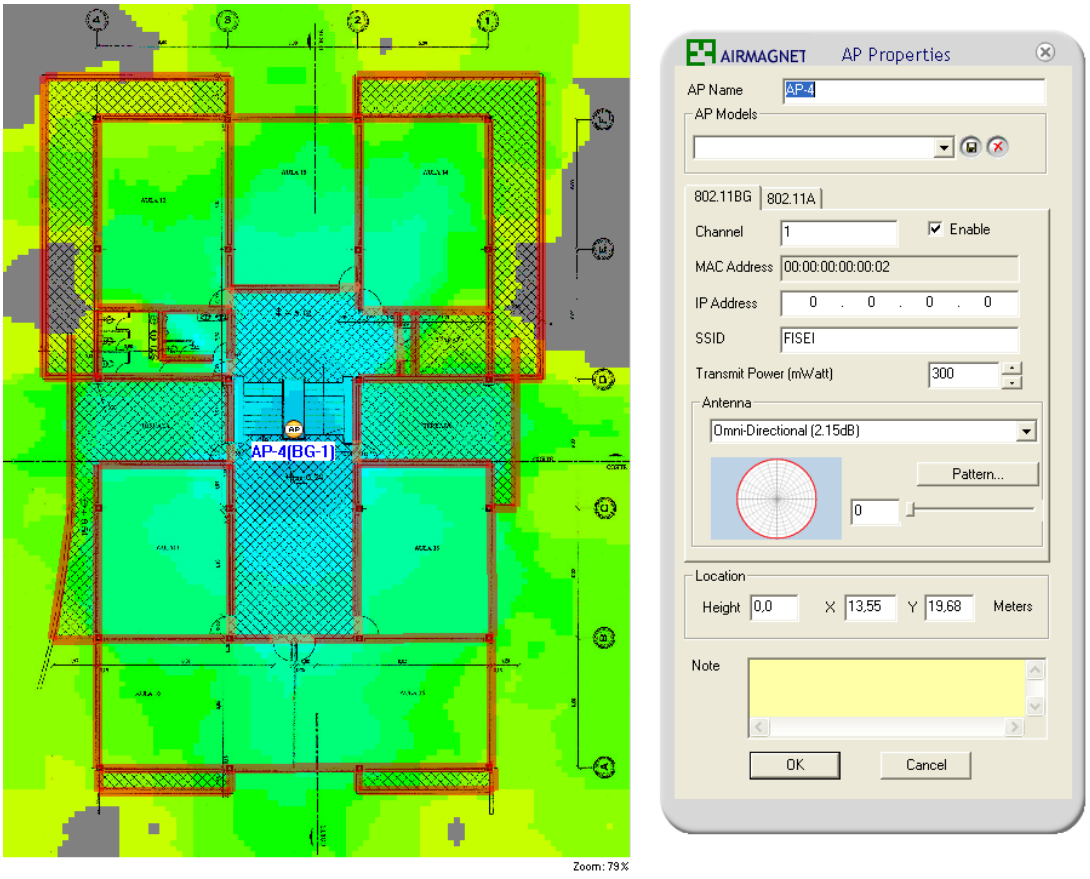


Fig. 6.14: Cobertura del AP-4 en edificio dos de la FISEI

Debido a la naturaleza de esta construcción y la relativa facilidad para la instalación de los puntos de acceso en el centro del edificio, en la Fig. 6.14 se puede apreciar una cobertura eficiente a nivel horizontal de esta infraestructura, con un punto de acceso Cisco con tecnología n. Puesto que se trata de un edificio de varias plantas de altura, era imprescindible la colocación de otro AP para cubrir las plantas bajas de esta construcción.

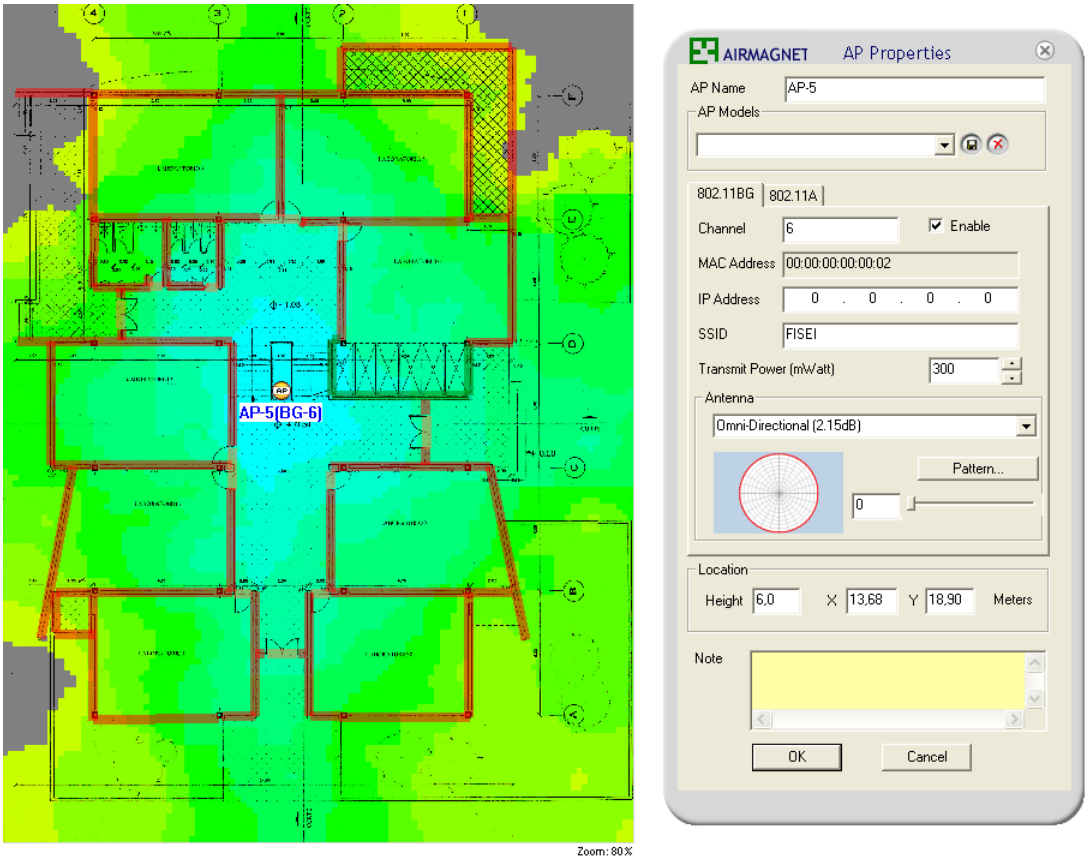


Fig. 6.15: Cobertura del AP-5 en edificio dos de la FISEI

De la misma forma, un segundo punto de acceso Cisco con tecnología n es utilizado para cubrir eficientemente la mitad inferior de la construcción como se puede observar en la Fig. 6.15.

6.8.3.6 Cálculos de cobertura realizados con el modelo Okumura-Hata

La cobertura real de un punto de acceso queda determinada por las condiciones reales de propagación, características de potencia y sensibilidad de los extremos terminales del enlace (puntos de acceso y clientes inalámbricos). Para determinar las pérdidas del enlace inalámbrico se utilizó el método de Okumura-Hata, por medio del cual se puede predecir las pérdidas de propagación en ambientes urbanos, suburbanos y rurales.

Para el edificio principal de la FISEI se utilizó la siguiente ecuación para zonas semiabiertas, por la estructura que presenta esta construcción:

$$L_p = 69.55 + 26.16 \log f - 13.82 \log h + [44.9 - 6.55 \log h] \log d - \left\{2\left[\log\left(\frac{f}{28}\right)\right]^2 + 5.4\right\}$$

Ecuación 6.3: Pérdidas de propagación en zona urbana semiabierta

La siguiente ecuación define las pérdidas para zonas urbanas densas y fue la más apropiada para utilizarse en el edificio dos de la FISEI, por su cantidad y variedad de obstrucciones:

$$L_p = 69.55 + 26.16 \log f - 13.82 \log h + [44.9 - 6.55 \log h] \log d$$

Ecuación 6.4: Pérdidas de propagación en zona urbana densa

También fue necesario determinar el balance de pérdidas y ganancias del enlace mediante la siguiente ecuación:

$$L_p = P_{TX} - S_{RX} - L_C + G_{TX} + G_{RX}$$

Ecuación 6.5: Balance de pérdidas y ganancias

Finalmente se presenta la sensibilidad de recepción de algunas tarjetas de red Wi-Fi (presentados por los fabricantes) utilizadas en equipos portátiles; información necesaria para los cálculos de los enlaces:

Tarjetas Orinocco PCMCIA Silver/Gold: 11Mbps → -82 dBm; 5.5Mbps → -87 dBm; 2Mbps → -91 dBm; 1Mbps → -94 dBm.
Tarjetas CISCO Aironet 350: 11Mbps → -85 dBm; 5.5 Mbps → -89 dBm; 2 Mbps → -91 dBm; 1 Mbps → -94 dBm.
Tarjeta ProximSymphony ISA: 1.6 Mbps → -77 dBm; 0.8 Mbps → -85 dBm.

Las antenas que vienen en los equipos WLAN generalmente no tienen mucha ganancia (2 dBi). Muchos de los adaptadores PCI o USB para desktops entran en este apartado. Dichas tarjetas vienen con antenas de no más de 2.5 pulgadas, como por ejemplo la DWL-510 de D-Link o la WUSB11.

Área de cobertura del router inalámbrico Linksys (tecnología n) en el edificio principal

Datos:

f= 2412 MHz (canal 1)
h =4 m
d = 35 m
GTX = 6 dBi
PTX = 60 dBm
Área: Semiabierta
Tipo de antena: Omnidireccional

Ubicación: Segundo Piso Edificio principal FISEI

Pérdidas de propagación

$$L_p = 69.55 + 26.16\log f - \ 13.82\log h + \ [44.9 - 6.55\log h]\log d - \left\{2\left[\log\left(\frac{f}{28}\right)\right]^2 + 5.4\right\}$$

$$L_p = 69.55 + 26.16\log(2412) - \ 13.82\log(4) + \ [44.9 - 6.55\log(4)]\log(0.035) - \left\{2\left[\log\left(\frac{2412}{28}\right)\right]^2 + 5.4\right\}$$

$$L_p = 69.55 + 88.48 - \ 8.32 + \ [41](-1.46) - 12.89$$

$$L_p = 76.96 \text{ dB}$$

Balance de pérdidas y nivel de señal recibida

$$L_p = P_{TX} - S_{RX} - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = P_{TX} - L_p - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = 60dBm - 76.96dB - 0.4dB + 8dBi$$

$$S_{RX} = -8.15dBm$$

El nivel de señal recibida es mayor que el umbral de recepción de las tarjetas inalámbricas WLAN más comunes, por lo tanto, según el modelo de Okumura Hata, el enlace entre el cliente inalámbrico, ubicado en cualquier punto del edificio principal de la FISEI (en el plano horizontal y en la planta baja), y el router Linksys, es viable.

Área de cobertura del punto de acceso 3com (tecnología b/g) en el edificio principal

Datos:

f= 2437 MHz (canal 6)

h =4 m

d = 35 m

GTX = 2 dBi

PTX = 20 dBm

Área: Semiabierta

Tipo de antena: Omnidireccional

Ubicación: Segundo Piso Edificio principal FISEI

Pérdidas de propagación

$$L_p = 69.55 + 26.16 \log f - 13.82 \log h + [44.9 - 6.55 \log h] \log d - \left\{2\left[\log\left(\frac{f}{28}\right)\right]^2 + 5.4\right\}$$

$$L_p = 69.55 + 26.16 \log(2437) - 13.82 \log(4) + [44.9 - 6.55 \log(4)] \log(0.035) - \left\{2\left[\log\left(\frac{2437}{28}\right)\right]^2 + 5.4\right\}$$

$$L_p = 69.55 + 88.48 - 8.32 + [41](-1.46) - 12.89$$

$$L_p = 75.75 \text{ dB}$$

Balance de pérdidas y nivel de señal recibida

$$L_p = P_{TX} - S_{RX} - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = P_{TX} - L_p - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = 20dBm - 75.75dB - 0.4dB + 4dBi$$

$$S_{RX} = -52.15dBm$$

De igual forma que con el router Linksys, el enlace entre cliente inalámbrico y el punto de acceso 3com es viable en el edificio principal de la FISEI, según el modelo de Okumura Hata.

Área de cobertura del punto de Cisco (tecnología b/g) en el edificio principal

Datos:

f= 2462 MHz (canal 11)
h =5 m
d = 35 m

GTX = 9 dBi

PTX = 20 dBm

Área: Semiabierta

Tipo de antena: Omnidireccional

Ubicación: Segundo Piso Edificio principal FISEI

Pérdidas de propagación

$$L_p = 69.55 + 26.16 \log f - 13.82 \log h + [44.9 - 6.55 \log h] \log d - \left\{2\left[\log\left(\frac{f}{28}\right)\right]^2 + 5.4\right\}$$

$$L_p = 69.55 + 26.16 \log(2462) - 13.82 \log(5) + [44.9 - 6.55 \log(5)] \log(0.035) - \left\{2\left[\log\left(\frac{2462}{28}\right)\right]^2 + 5.4\right\}$$

$$L_p = 69.55 + 88.48 - 9.66 + [40.32](-1.46) - 12.89$$

$$L_p = 76.61 \text{ dB}$$

Balance de pérdidas y nivel de señal recibida

$$L_p = P_{TX} - S_{RX} - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = P_{TX} - L_p - L_C - L_{Ca} + G_{TX} + G_{RX}$$

$$S_{RX} = 20dBm - 76.61dB - 0.4dB - 0.8dB(3) + 11dBi$$

$$S_{RX} = -48.41dBm$$

Con este cálculo se comprobó que el alcance de la señal de este punto de acceso logra llegar hacia el AP-4 en el edificio dos.

Área de cobertura del punto de acceso Cisco (tecnología n) en el edificio dos

Datos:

f= 2412 MHz (canal 1)
h = 4 m
d = 20 m
GTX = 6 dBi
PTX = 60 dBm
Área: Densa
Tipo de antena: Omnidireccional

Ubicación: Cuarto piso del edificio dos

Pérdidas de propagación

$$L_p = 69.55 + 26.16 \log f - 13.82 \log h + [44.9 - 6.55 \log h] \log d$$

$$L_p = 69.55 + 26.16 \log(2412) - 13.82 \log(4) + [44.9 - 6.55 \log(4)] \log(0.02)$$

$$L_p = 69.55 + 88.48 - 8.32 + [40.96](-1.69)$$

$$L_p = 69.55 + 88.48 - 8.32 - 69.22$$

$$L_p = 80.49dB$$

Balance de pérdidas y nivel de señal recibida

$$L_p = P_{TX} - S_{RX} - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = P_{TX} - L_p - L_C + G_{TX} + G_{RX}$$

$$S_{RX} = 60dBm - 80.49dB - 0.4dB + 8dBi$$

$$S_{RX} = -42.89dBm$$

El nivel de señal recibida es mayor que la sensibilidad de recepción de los clientes inalámbricos, por lo tanto, se confirma la viabilidad del enlace en el edificio dos de la FISEI.

6.8.3.7 Sistema de respaldo de comunicación

Un sistema de respaldo para una red inalámbrica WLAN puede evitar ciertos inconvenientes con la caída de los enlaces y de esta forma, convertirla en una red robusta frente a determinados tipos de interferencia. Sin embargo, el costo de un sistema así, específico para estas redes o para enlaces de este tipo, podría significar un considerable costo económico para la empresa que lo implementa. La FISEI no disponía de suficientes recursos económicos para implementar este tipo de soluciones demasiado "sofisticadas". Por tal razón, se determinó la utilización de un cableado ethernet como una solución de respaldo para la red WLAN implementada. El cable se extiende desde el router inalámbrico hacia el AP-4. El objetivo es que este sistema pueda ser utilizado en caso de que el enlace entre el punto de acceso 3 del edificio principal y el punto de acceso 4 del edificio dos falle en determinado momento. De esta forma, el acceso a internet en el edificio dos se podrá mantener en caso de caída de este enlace, previa una reconfiguración del AP-4 para que, en vez de repetir la señal del AP-3, repita la señal del router inalámbrico. Sabiendo que estos dos AP son los equipos que tienen una mayor distancia entre sí y que el enlace pasa por una zona vulnerable a los cambios de clima, esta solución de respaldo proporcionará una mayor fiabilidad del sistema.

6.8.4 Sistema de autenticación para la WLAN

Para proveer de seguridad a la red inalámbrica de la facultad, se implementó un sistema de autenticación basado en un servidor Radius. Este se encarga de procesar todas las peticiones provenientes de los clientes inalámbricos, concediendo el acceso a internet a todos aquellos que se encuentren registrados en la base de datos del servidor y negando las solicitudes de los que no lo estén.

6.8.4.1 Instalación del sistema operativo Linux

La seguridad, flexibilidad y estabilidad que Linux ofrece como sistema operativo determinaron su elección como la plataforma adecuada en este proyecto.

Existen cientos de distribuciones Linux para elegir, sin embargo, CentOS fue la opción más adecuada por ser una distro totalmente libre y sin exigentes requerimientos de hardware.

Las características de hardware del equipo se describen a continuación:

Procesador: Intel Pentium IV

Memoria: 1 GB

Disco Duro: 150 GB

Número de interfaces de red: 2

Instalación de CentOS 5.4

Las siguientes imágenes muestran la instalación del Sistema Operativo CentOS 5.4. Desde la Fig. 6.16 hasta la Fig. 6.26 se detalla el proceso de instalación a través de las capturas de pantalla tomadas de este procedimiento. Se inicia con la pantalla de bienvenida que guía a través del proceso de instalación (Fig. 6.16), continuando con la comprobación del CD de CentOS (Fig. 6.17) y luego las capturas de pantalla que muestran la instalación en modo gráfico (Fig. 6.18). Existen varios pasos a seguirse en este punto: la partición del disco duro (Fig. 6.19), configuración de IP (Fig. 6.21), selección de región (Fig. 6.22), configuración de contraseña (Fig. 6.23) y la selección de paquetes a instalarse (Fig. 6.24). Se puede apreciar finalmente la barra de progreso de la instalación (Fig. 6.25) y el proceso completado (Fig. 6.26).

Fig. 6.16: Arranque desde el CD de instalación

Fig. 6.17: Comprobación del estado del CD de instalación

Fig. 6.18: Inicio de la instalación en modo gráfico

Fig. 6.19: Partición del disco duro

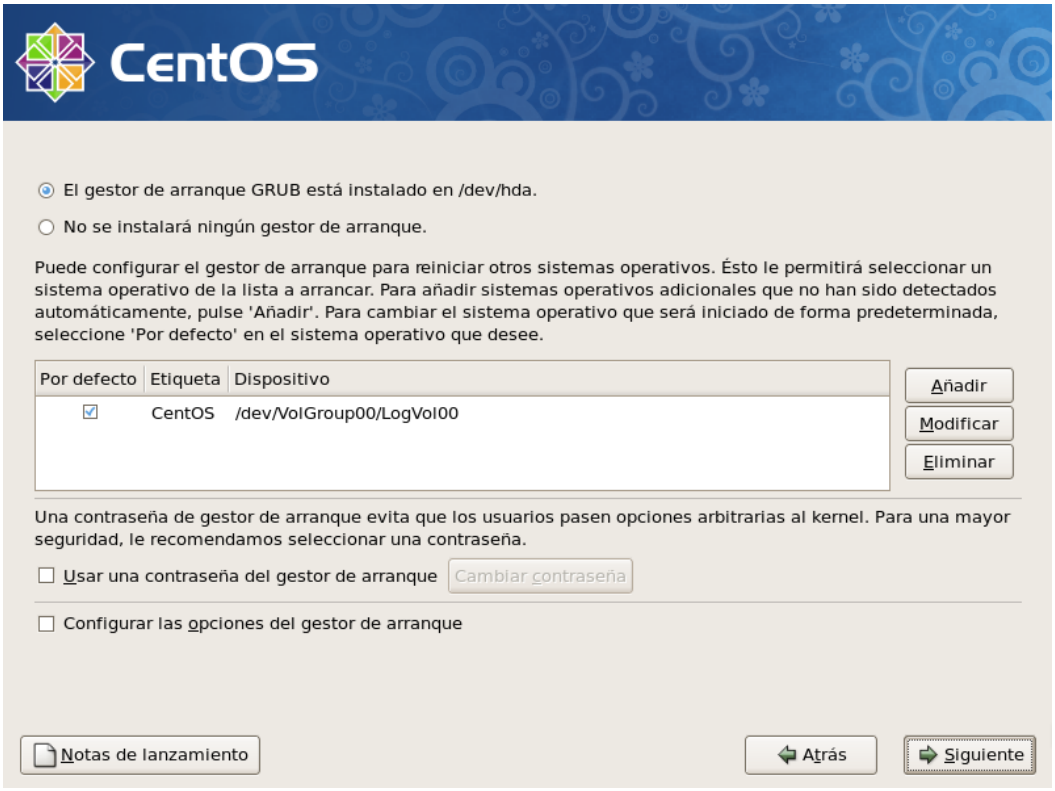


Fig. 6.20: Configuración del gestor de arranque

Fig. 6.21: Configuración del direccionamiento IP del servidor

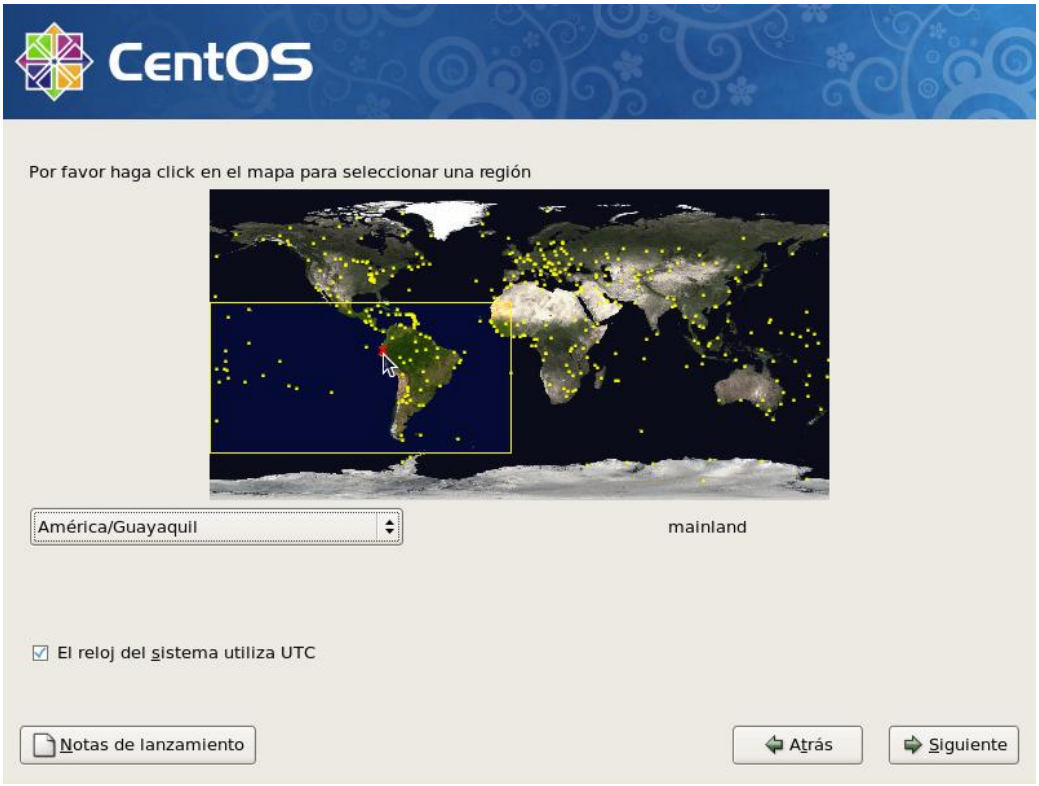


Fig. 6.22: Selección de la región

Fig. 6.23: Configuración de la contraseña de root

Fig. 6.24: Selección de paquetes a instalarse

Fig. 6.25: Progreso de la instalación

Fig. 6.26: Aviso de la instalación completada

6.8.4.2 Configuración de servicios y aplicaciones necesarias

A continuación se procedió a instalar/configurar los servicios necesarios para levantar el servidor radius. Los mismos se listan a continuación:

- Servidor Web Apache con soporte SSL
- Servidor Radius Freeradius
- Servidor Mysql
- Chillispot
- Configuración de los Access Points

Se verificó que el direccionamiento IP sea correcto en ambas interfaces de red del equipo (eth0 y eth1), además de la conexión con internet. A continuación se muestra un diagrama básico del sistema de autenticación para comprenderlo mejor.

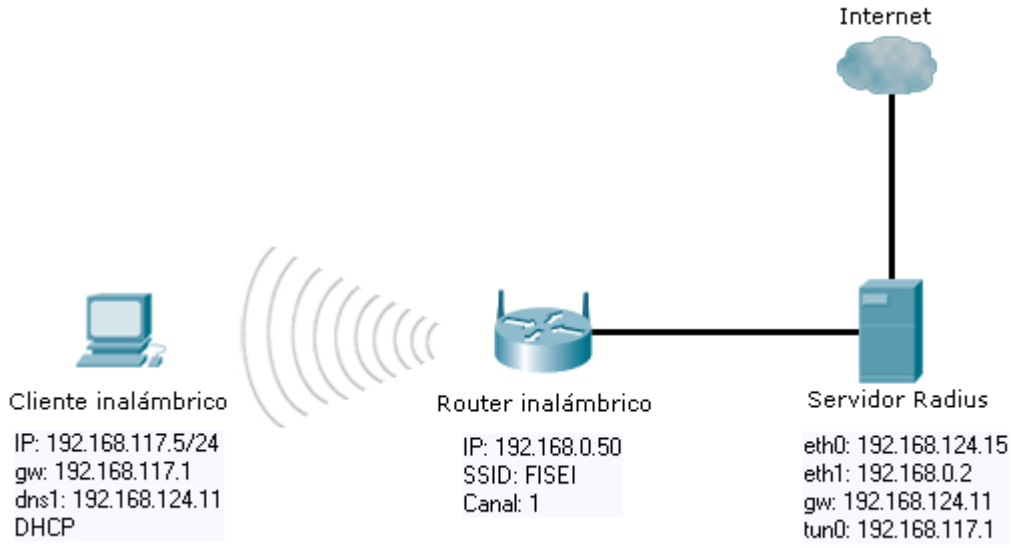


Fig. 6.27: Esquema básico del sistema de autenticación

Se chequeó el estado de las interfaces de red de la siguiente forma:

```
[root@fisei ~]# ifconfig
eth0    Link encap:EthernetHWaddr 00:19:D1:A7:F4:D3
        inet addr:192.168.124.15  Bcast:192.168.124.255
         Mask:255.255.255.0
        inet6 addr: fe80::219:d1ff:fea7:f4d3/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:75911 errors:0 dropped:0 overruns:0 frame:0
        TX packets:63201 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:68633136 (65.4 MiB)  TX bytes:7115996 (6.7 MiB)
        Interrupt:50 Base address:0xc000

eth1    Link encap:EthernetHWaddr 00:19:5B:89:BF:06
        inet addr:192.168.0.2  Bcast:192.168.0.255  Mask:255.255.255.0
        UP BROADCAST  MTU:1500  Metric:1
        RX packets:37 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2220 (2.1 KiB)  TX bytes:180 (180.0 b)
        Interrupt:58 Base address:0xe000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:11630 errors:0 dropped:0 overruns:0 frame:0
        TX packets:11630 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:6760566 (6.4 MiB)  TX bytes:6760566 (6.4 MiB)
```

Las interfaces eth0 y eth1 se encuentran activas y correctamente configuradas.

Si en cualquier momento se requiere cambiar cualquier información sobre el direccionamiento ip de las interfaces, se puede fácilmente modificar sus archivos de configuración:

```
[root@fisei ~]# cd /etc/sysconfig/network-scripts

[root@fisei ~]# vi ifcfg-eth0

# Realtek Semiconductor Co., Ltd. RTL8111/8168B PCI Express Gigabit
Ethernet controller
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:19:d1:a7:f4:d3
IPV6INIT=yes
IPV6_AUTOCONF=yes
ONBOOT=yes
TYPE=Ethernet
PEERDNS=yes
USERCTL=yes
NETMASK=255.255.255.0
IPADDR=192.168.124.15
GATEWAY=192.168.124.1

[root@fisei ~]# vi ifcfg-eth1

# VIA Technologies, Inc. VT6105/VT6106S [Rhine-III]
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:19:5b:89:bf:06
NETMASK=255.255.255.0
IPADDR=192.168.0.2
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
PEERDNS=yes
```

Como requisito para el correcto funcionamiento de Chillispot, también se debió verificar que el sistema disponga del módulo de kernel TUN, que permite crear un puente virtual de red y un enrutamiento para la conexión entre el cliente inalámbrico y el servidor. Se procedió de la siguiente manera:

```
[root@fisei ~]# lsmod
Module                  Size  Usedby
vfat                    15937  1
fat                     51165  1 vfat
i915                    24001  3
drm                     65365  4 i915
ipt_MASQUERADE          7617  1
ipt_REJECT              9665  1
xt_tcpudp               7105  6
xt_state                6209  1
iptable_mangle          6849  0
iptable_nat             11077  1
ip_nat                  21101  2
iptable_filter          7105  1
ip_tables               17029  3
tun                     21441  2
autofs4                 29253  3
hidp                    23105  2
rfcomm                  42457  0
l2cap                   29505  10 hidp,rfcomm
```

Al mostrarse tun en la lista significa que si se dispone de este módulo. En CentOS este soporte viene habilitado por defecto. En el caso de no estar habilitado, es indispensable actualizar el kernel pero como se indica, en esta distribución no es necesario.

Se procedió entonces a habilitar el reenvío de paquetes entre ambas interfaces de red con el objetivo de que el sistema trabaje como un router. El comando utilizado es el siguiente:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Este comando se debe digitar cada vez que se reinicie el servidor. Se puede automatizar este proceso para que arranque solo, cada vez que el sistema inicie, agregando la línea anterior dentro del archivo /etc/rc.d/rc.local

Una segunda forma de hacer dicha tarea es habilitar el ip_forward dentro del archivo /etc/sysctl.conf cambiándolo de cero a uno. Se detalla el contenido de ese archivo a continuación.

```
vi /etc/sysctl.conf

# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
```

A continuación se instalaron los paquetes necesarios para levantar el servidor radius.

6.8.4.2.1 Servidor Web Apache

Apache puede ya estar instalado dentro del sistema. Todo depende de si este paquete fue agregado durante la instalación de CentOS. Se puede comprobar si esta instalado con el siguiente comando:

```
rpm –q  httpd
```

Si se indica que el paquete no esta instalado, se puede instalarlo desde el CD de instalación o desde internet. Para la primera forma, después del montaje del CD y de ubicarse en el directorio de paquetes, se digita el siguiente comando:

```
rpm –ivh httpd-2.2.3-22.el5.centos.i386.rpm
```

Desde internet se puede instalar con el comando yum, así:

```
yum install httpd
```

A continuación se realizó la configuración de Apache, modificando el fichero httpd.conf que se encuentra en el directorio /etc/httpd/conf. Se cambió la línea "ServerName", ingresando la ip de la interfaz eth0:

```
ServerName 192.168.124.15:80
```

Se levanta el servicio:

```
service httpd start
```

Para que el servicio arranque automáticamente cuando inicia el servidor:

```
chkconfig httpd on
```

Finalmente se comprueba que Apache funciona correctamente digitando la IP anterior en el navegador:

http://192.168.124.15

Un correcto funcionamiento del servicio mostrará una página web diseñada por Apache.

- **Soporte SSL/TLS en el Servidor Web Apache**

Después de instalar Apache se debió verificar que tenga soporte para conexiones seguras mediante SSL. Se chequea esto observando que exista el archivo ssl.conf dentro del directorio /etc/httpd/conf.d:

```
[root@fisei ~]# ls /etc/httpd/conf.d
fisei.conf   perl.conf    python.conf     ssl.conf
fisei.conf.respaldo       php.conf        README       webalizer.conf
manual.conf               proxy_ajp.conf  squid.conf   welcome.conf
```

Existe el soporte. Después se verificó que CentOS disponga de OpenSSL y mod_ssl, paquetes que permiten correr una conexión cifrada entre servidor y cliente mediante el protocolo SSL/TLS (Secure Sockets Layer o Protocolo de capa de conexión segura) / (TransportLayer Security o Seguridad de la capa de transporte).

```
rpm –q openssl

openssl-0.9.8e-12.el5_4.6

rpm –q mod_ssl

mod_ssl-2.2.3-31.el5.centos
```

Si estos paquetes no están instalados, se puede utilizar yum para su instalación:

```
yum install openssl mod_ssl
```

Para establecer una conexión encriptada SSL entre cliente y servidor, es imprescindible que el segundo se autentique utilizando un certificado digital firmado.

Se procedió entonces con la creación del certificado, generando previamente un directorio para almacenarlos. Es recomendable por aspectos de seguridad, que dicho directorio sólo sea accesible por el super-usuario root:

```
mkdir –m 700 –p /etc/ssl/fisei.edu.ec
```

Dentro de fisei.edu.ec se creó una clave pública RSA (Rivest, Shamir, Adleman) de 1024 octetos. En base a esa clave se creó el certificado y se auto-firmó. Se procedió de la siguiente manera:

```
cd /etc/ssl/fisei.edu.ec
```

Creación de la clave pública RSA:

```
opensslgenrsa -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.............++++++
.....................................++++++
e is 65537 (0x10001)
```

Creación del certificado:

```
opensslreq -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]:Tungurahua
Locality Name (eg, city) [Newbury]:Ambato
Organization Name (eg, company) [My Company Ltd]:UTA
Organizational Unit Name (eg, section) []:FISEI
Common Name (eg, your name or your server's hostname) []:Santiago
Email Address []:santya6o@hotmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234567890

An optional company name []:www.unazonageek.com
```

Firma del certificado:

```
openssl x509 -req -days 730 -in server.csr \
> -signkeyserver.key -out server.crt
Signature ok
subject=/C=EC/ST=Tungurahua/L=Ambato/O=UTA/OU=FISEI/CN=Santiago/emailAdd
ress=santya6o@hotmail.com
Getting Private key
```

Se ha firmado el certificado por un período de 730 días.

A continuación se asegura que todos estos archivos sean sólo accesibles por root:

```
chmod 400  server.*
```

Se creó la estructura de directorios para el sitio que será creado como virtual en el servidor web.

```
mkdir –p /var/www/fisei.edu.ec/{cgi-bin,html,logs,etc,var}
```

También se creó el archivo fisei.conf en el directorio /etc/httpd/conf.d, con el siguiente contenido:

```
NameVirtualHost 192.168.124.15:80
       <VirtualHost 192.168.124.15:80>
              ServerAdmin webmaster@fisei.edu.ec
              DocumentRoot /var/www/fisei.edu.ec/html
              ServerName www.fisei.edu.ec
              ServerAlias fisei.edu.ec
              Redirect 301 / https://www.fisei.edu.ec/
              CustomLog /var/www/fisei.edu.ec/logs/access_log combined
              Errorlog /var/www/fisei.edu.ec/logs/error_log
       </VirtualHost>
NameVirtualHost 192.168.124.15:443
       <VirtualHost 192.168.124.15:443>
              ServerAdmin webmaster@fisei.edu.ec
              DocumentRoot /var/www/fisei.edu.ec/html
              ServerName www.fisei.edu.ec
              ScriptAlias /cgi-bin/ /var/www/fisei.edu.ec/cgi-bin/
              SSLEngine on
              SSLCertificatefile /etc/ssl/fisei.edu.ec/server.crt
              SSLCertificateKeyfile/etc/ssl/fisei.edu.ec/server.key
              SetEnvIf User-Agent ".*MSIE.*" nokeepalivessl-unclear-
              shutdown
              CustomLog /var/www/fisei.edu.ec/logs/ssl_request_log \"%t
              %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
              CustomLog /var/www/fisei.edu.ec/logs/ssl_access
              combined
              Errorlog /var/www/fisei.edu.ec/logs/ssl_error_log
       </VirtualHost>
```

Para finalizar se reinicia el servidor web apache y se comprueba su funcionamiento mediante un navegador:

```
service httpd restart
```

A continuación se muestran las capturas de pantalla donde se puede apreciar el correcto funcionamiento del servidor web Apache, trabajando con conexión segura sobre https. Se muestra también la obtención del certificado de seguridad y sus detalles.

Fig. 6.28: Intento fallido de conexión segura

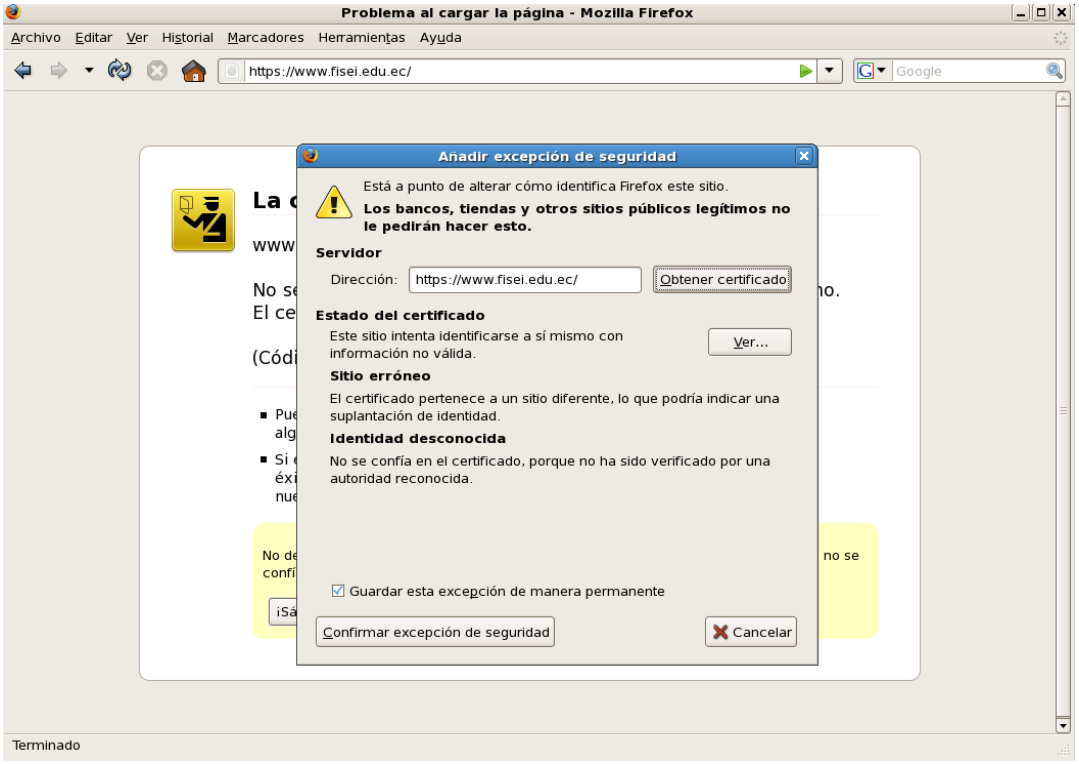


Fig. 6.29: Obtención del certificado

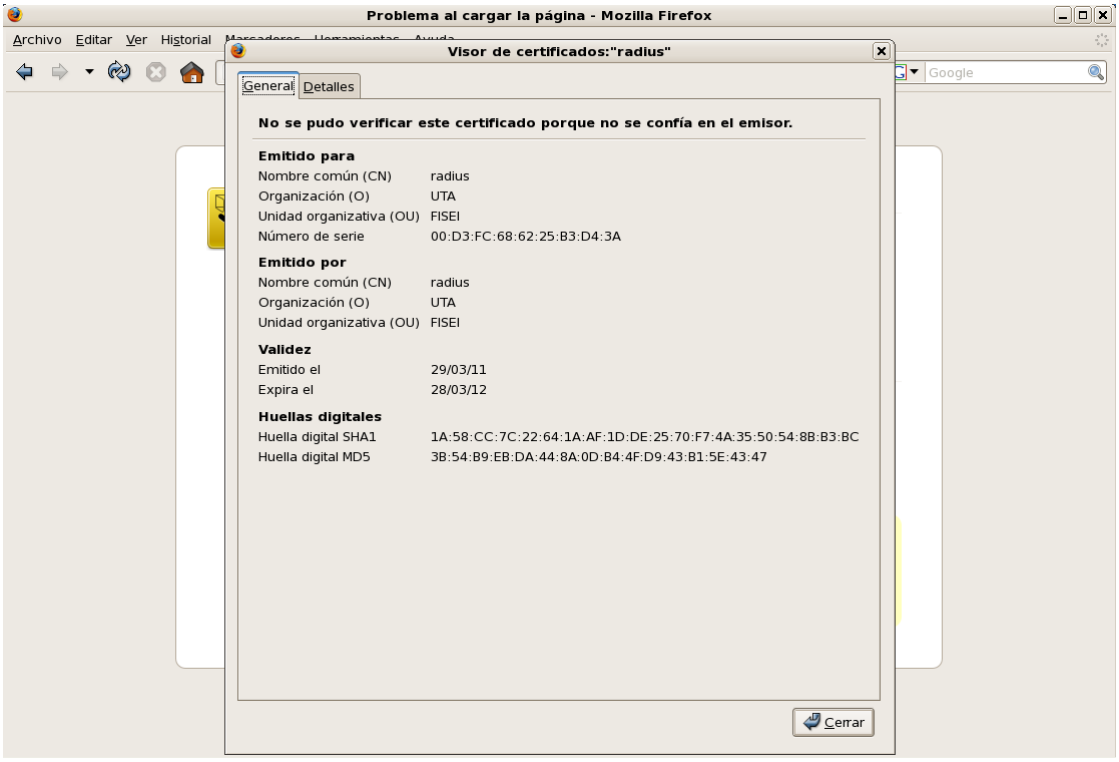


Fig. 6.30: Detalles del certificado

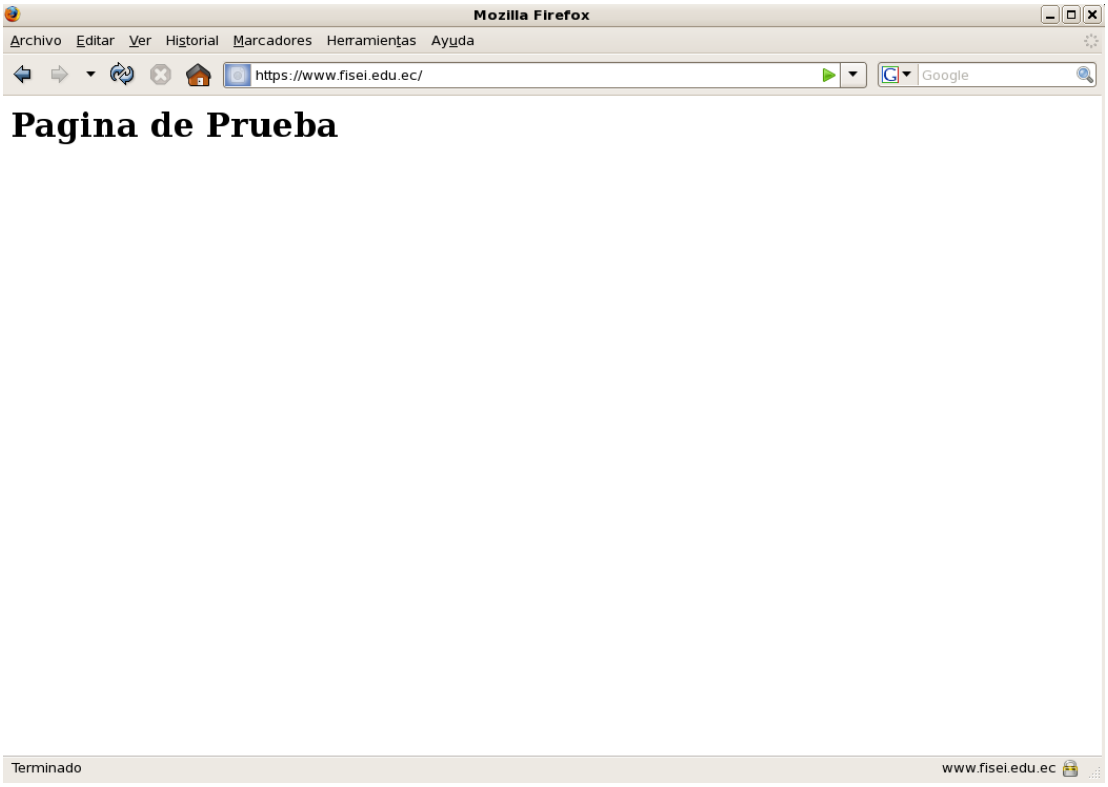


Fig. 6.31: Confirmación de excepción de seguridad y conexión realizada

6.8.4.2.2 Servidor Radius Freeradius

Debido a la necesidad de usar opciones adicionales, freeradius no se instaló a partir de archivos rpm. Fue necesario descargar el paquete desde su fuente y compilarlo e instalarlo manualmente, de la siguiente forma:

```
wget ftp://ftp.freeradius.org/pub/radius/freeradius-server-2.1.9.tar.bz2
```

A continuación:

```
tar xvjf freeradius-server-2.1.9.tar.bz2

cd freeradius-server-2.1.9

./configure

make

make install

cp ./raddb/dictionary /usr/local/etc/raddb/dictionary

cd /usr/local/etc/raddb
```

Luego de haberse instalado freeradius se modificó el archivo principal de configuración denominado radiusd.conf. Se modificaron las líneas necesarias para que freeradius se conecte con Mysql y Chillispot, servicios instalados más adelante.

```
vi radiusd.conf
```

Se busca la línea $INCLUDE ${confdir}/modules/
Bajo ella se agrega lo siguiente:

```
$INCLUDE sql.conf
sqlcounternoresetcounter {
        driver = "rlm_sqlcounter"
        counter-name = Max-All-Session-Time
        check-name = "Max-All-Session"
sqlmod-inst = sql
        key = User-Name
        reset = never
        query = "SELECT SUM(AcctSessionTime) FROM radacct WHERE
      UserName='%{%k}'"
}
```

Este código habilita lo necesario para controlar el tiempo de conexión de los usuarios.

Se chequea/modifica la sección “instantiate” del mismo archivo radiusd.conf, verificando que tenga los parámetros mostrados a continuación. Luego se guardan los cambios.

```
instantiate {

exec

expr

noresetcounter

}
```

En el archivo “default” localizado en el directorio /usr/local/etc/raddb/sites-available, se chequean/modifican también las secciones “authorize”, “authentication”, “preaccounting”, “accounting” y “session”:

```
cd /usr/local/etc/raddb/sites-available

vi default
```

Sección Authorize

```
authorize {

preprocess

chap

mschap

suffix

sql

noresetcounter

}
```

Sección Authenticate

```
authenticate {
Auth-Type PAP {
pap
}
Auth-Type CHAP {
chap
}
Auth-Type MS-CHAP {
mschap
}
}
```

Sección PreAccounting

```
preacct {
preprocess
suffix
}
```

Sección Accounting

```
accounting {
acct_unique
detail
unix
sql
}
```

Sección Session

```
session  {

sql

}
```

Se modificó el archivo sql.conf ubicado en /usr/local/etc/raddb:

```
sql {
        driver = "rlm_sql_mysql"
        server = "localhost"
        login = "freeradius"
        password = "12345"
         radius_db = "radius"
        acct_table1 = "radacct"
         acct_table2 = "radacct"
```

En el archivo “dictionary” se agrega la siguiente línea que habilitará el soporte Wispr para controlar parámetros de ancho de banda y finalización de conexiones:

```
$INCLUDE /usr/local/share/freeradius/dictionary.wispr
```

Por último se modifica el archivo clients.conf

```
client 127.0.0.1 {

       secret = testing123

       shortname = localhost
```

Se configura el servicio para que arranque cuando el servidor se encienda:

```
echo 'radiusd'>> /etc/rc.d/rc.local
```

6.8.4.2.3 Servidor Mysql

Si la instalación del servidor Mysql no se ha realizado durante el proceso de instalación de CentOS, se puede instalarlo desde internet utilizando yum, tal como los servicios anteriores:

```
yum install mysql mysql-server php-mysql
```

Se arranca el servicio y se configuran ciertos parámetros para darle seguridad:

```
service mysqld start

mysql –u root –p

> use mysql;

> update user set Password=PASSWORD('nuevopassword') where user='root';
```

Se configura el servicio para que arranque automáticamente:

```
chkconfig mysqld on
```

Puesto que freeradius y mysql deben conectarse para intercambiar información, el servidor de base de datos debe estar configurado y sincronizado correctamente con freeradius. Se procedió de la siguiente manera:

```
mysql –u root –p

> CREATE DATABASE radius;

> GRANT ALL PRIVILEGES ON radius.* to 'freeradius'@'localhost'
IDENTIFIED BY 'clave';

> FLUSH PRIVILEGES;

>exit

cd /usr/local/share/doc/freeradius/examples

mysql –u root –p radius<postgresql_update_raddact_group_trigger.sql
```

Se creó un usuario en la base de datos para las pruebas posteriores de conexión entre mysql y freeradius:

```
mysql –u root –p

> use radius;

> INSERT INTO radcheck (UserName, Attribute, Value) VALUES
('usuario','Password','contraseña');

>exit
```

6.8.4.2.4 Chillispot

Este servicio es muy importante para auntenticar a los usuarios de una red inalámbrica. Se encarga de establecer la conexión con los clientes a través del access point y envía las credenciales de autenticación al servidor radius para que valide a los usuarios en base a los registros de la base de datos.

En primer lugar se descargó chillispot desde su fuente:

```
wget http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm
```

Instalación:

```
rpm –ivh chillispot-1.1.0.i386.rpm
```

Se configura el archivo chilli.conf

```
vi /etc/chilli.conf
```

```
#Etiqueta que asigna direcciones IP a los clientes inalámbricos:
net 192.168.117.0/24

#Para asignar las direcciones IP dinámicamente:
dynip 192.168.117.0/24

#Servidor DNS que utilizarán los clientes:
dns1 192.168.124.15

#Dominio a utilizar por los clientes:
domain fisei.uta.ec

ipup /etc/chilli.ipup

ipdown /etc/chilli.ipdown

#Dirección del servidor radius
radiuslisten 127.0.0.1

radiusserver1 127.0.0.1

#Puertos UDP del servidor radius
radiusauthport 1812

radiusacctport 1813
```

```
#Contraseña compartida con el servidor radius
radiussecret testing123

# Interfaz de red a utilizar.
dhcpif eth1

# Dirección que manejará la autenticación
uamserver https://www.fisei.edu.ec/cgi-bin/hotspotlogin.cgi

# Contraseña compartida con el script de autenticación
uamsecret ht2eb8ej6s4et3rg1ulp

#Dirección permitida sin necesidad de autenticación
uamallowed 192.168.117.1
```

Se copian los archivos adicionales para su funcionamiento:

```
cp /usr/share/doc/chillispot-1.1.0/firewall.iptables /etc/rc.d

cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi
/var/www/fisei.edu.ec/cgi-bin/
```

Se configura el inicio automático del primero:

```
cd /etc/rc.d

echo "firewall.iptables">> /etc/rc.d/rc.local
```

Hotspotlogin.cgi contiene la página de autenticación de chillispot y se la puede personalizar de acuerdo a la necesidad.

Se levanta y configura el arranque automático del servicio:

```
service chilli start

chkconfig chilli on
```

6.8.4.2.5 Daloradius

Mediante esta interfaz web se administrará a los usuarios de la red inalámbrica y se controlará el registro de los mismos, parámetros de ancho de banda, y caducidad de conexiones.

Antes de trabajar con esta aplicación fue necesario tener funcionando correctamente Apache, Mysql e instalado el módulo de Php. Para verificar que php está instalado:

```
rpm –q php
```

Si no existe, tal como los servicios anteriores, se instala mediante yum y conectado a internet.

```
yum install php
```

Se descarga daloradius:

```
wget http://ufpr.dl.sourceforge.net/project/daloradius/daloradius/daloradius-0.9-8/daloradius-0.9-8.tar.gz
```

Luego:

```
tar xvfz daloradius-0.9-8.tar.gz
```

Puesto que daloradius es una interfaz web y como tal se la maneja, se trasladaron todos sus archivos al directorio web del servidor:

```
mv daloradius-0.9-8 /var/www/html/daloradius
```

A continuación se copian las tablas que daloradius necesita para trabajar, en la base de datos del servidor radius:

```
cd /var/www/html/daloradius/contrib/db

mysql –u root –p radius <mysql-daloradius.sql
```

```
mysql –u root –p radius < fr1-mysql-freeradius.sql
```

Se edita el archivo principal de configuración de daloradius, con los datos correctos para que pueda acceder a la base de datos del servidor radius:

```
cd /var/www/html/daloradius/library
vi daloradius.conf.php

$configValues['FREERADIUS_VERSION'] = '2';

$configValues['CONFIG_DB_ENGINE'] = 'mysql';

$configValues['CONFIG_DB_HOST'] = '127.0.0.1';

$configValues['CONFIG_DB_USER'] = 'root';

$configValues['CONFIG_DB_PASS'] = 'radius';

$configValues['CONFIG_DB_NAME'] = 'radius';

$configValues['CONFIG_MAINT_TEST_USER_RADIUSSERVER'] = '127.0.0.1';

$configValues['CONFIG_MAINT_TEST_USER_RADIUSPORT'] = '1812';

$configValues['CONFIG_MAINT_TEST_USER_RADIUSSECRET'] = 'testing123';
```

Finalmente se puede acceder la interfaz de administración daloradius mediante un navegador web:

http://127.0.0.1/daloradius

Para el ingreso, los datos por defecto son:

Username: administrator
Password: radius

6.8.4.3 Configuración de Equipos

Se presenta la tabla con los parámetros configurados en todos los equipos, y a continuación, las imágenes del proceso en cada uno de ellos.

Datos	**Router Inalámbrico**	**AP - 2**	**AP - 3**	**AP - 4**	**AP - 5**
Marca	Linksys	3com	Cisco	Cisco	Cisco
Modelo	WRT300N	7760	WAP200E	WAP4410N	WAP4410N
Estándares	b/g/n	a/b/g	b/g	b/g/n	b/g/n
Versión Firmware	V1.1	AP software 1.6.40	2.0.0.27	2.0.1.0	2.0.1.0
MAC	00:1D:7E:3D:8C:48	00:1A:C1:86:F6:40	6C:50:4D:C0:6D:9C	D0:D0:FD:39:C7:8E	50:3D:E5:30:FB:14
IP	192.168.0.50	192.168.182.2	192.168.182.3	192.168.182.4	192.168.182.5
Máscara	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
DHCP	Disabled	Disabled	Disabled	Disabled	Disabled
Encryption	Disabled	Disabled	Disabled	Disabled	Disabled
AP Mode	No aplicable	Repeater	Repeater	Repeater	Repeater
SSID	FISEI	FISEI	FISEI	FISEI	FISEI
Canal	1	6	11	1	6

Tabla 6.6: Configuración de equipos

6.8.4.3.1 Configuración del Router inalámbrico:

A continuación se muestra en imágenes el proceso de configuración de este equipo, incluyendo el direccionamiento IP (Fig.6.32), SSID (Fig. 6.33) y seguridad inalámbrica (Fig. 6.34).

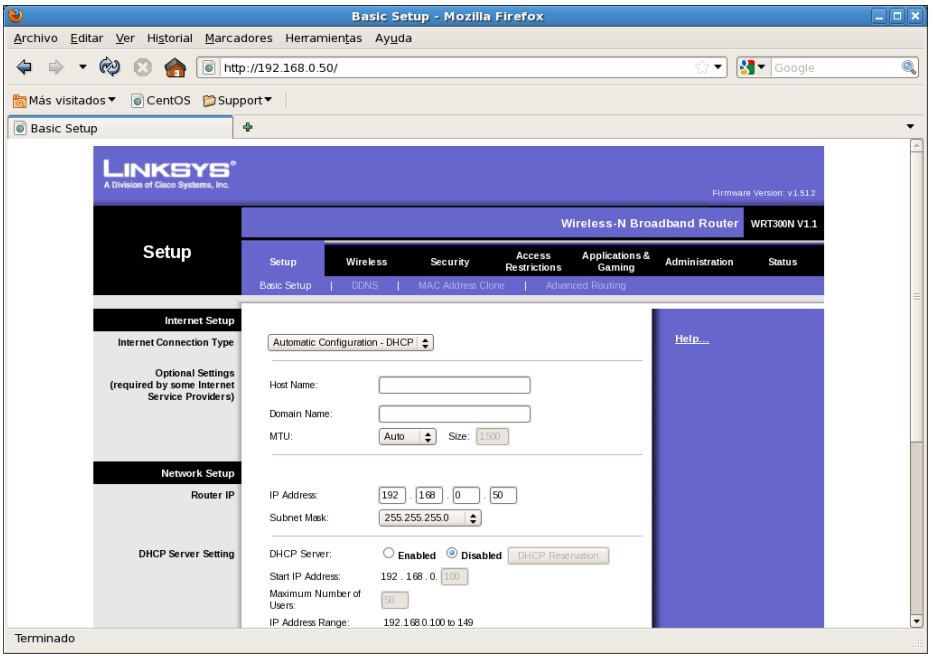


Fig. 6.32: Configuración de IP

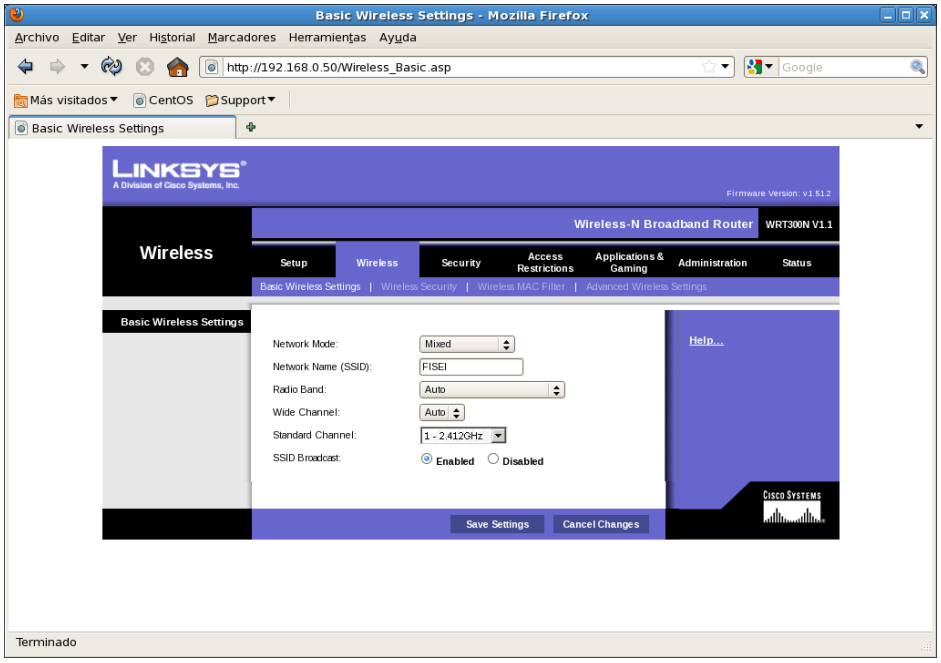


Fig. 6.33: SSID, estándar de trabajo y canal

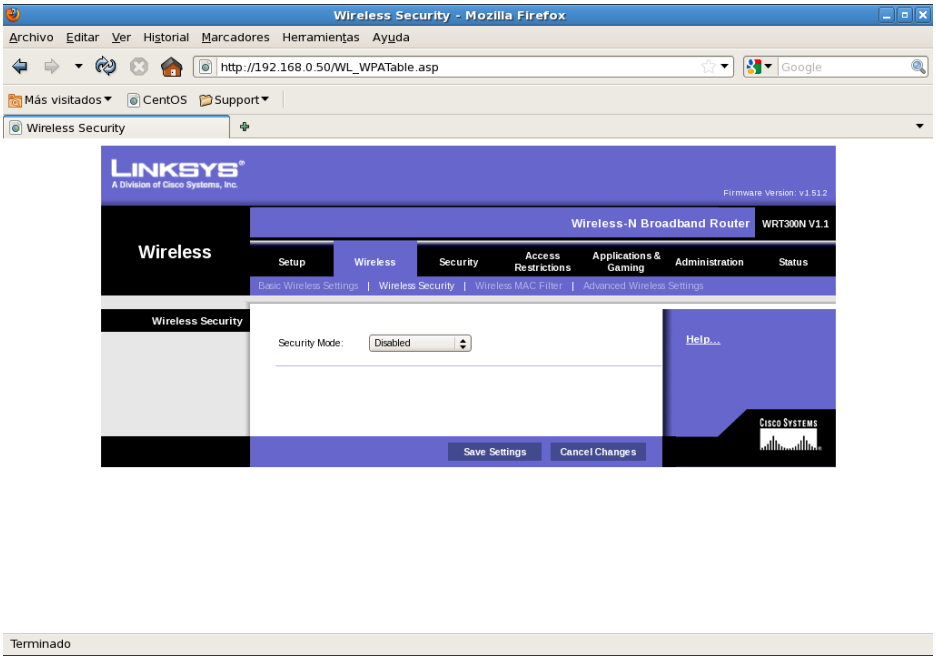


Fig. 6.34: Seguridad inalámbrica

6.8.4.3.2 Configuración del AP – 2

Como se detalló en la tabla 6.6, el AP-2 es un punto de acceso 3com, modelo 7760, y las capturas de pantalla de su configuración se plasman a continuación (desde Fig. 6.35 hasta Fig. 6.39)

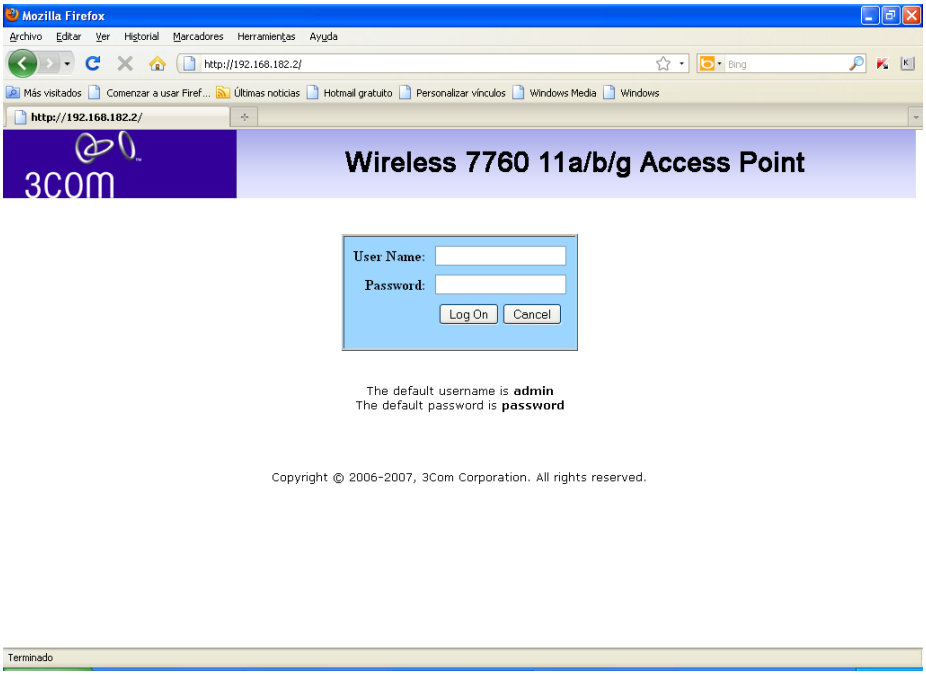


Fig. 6.35: Ingreso al AP-2

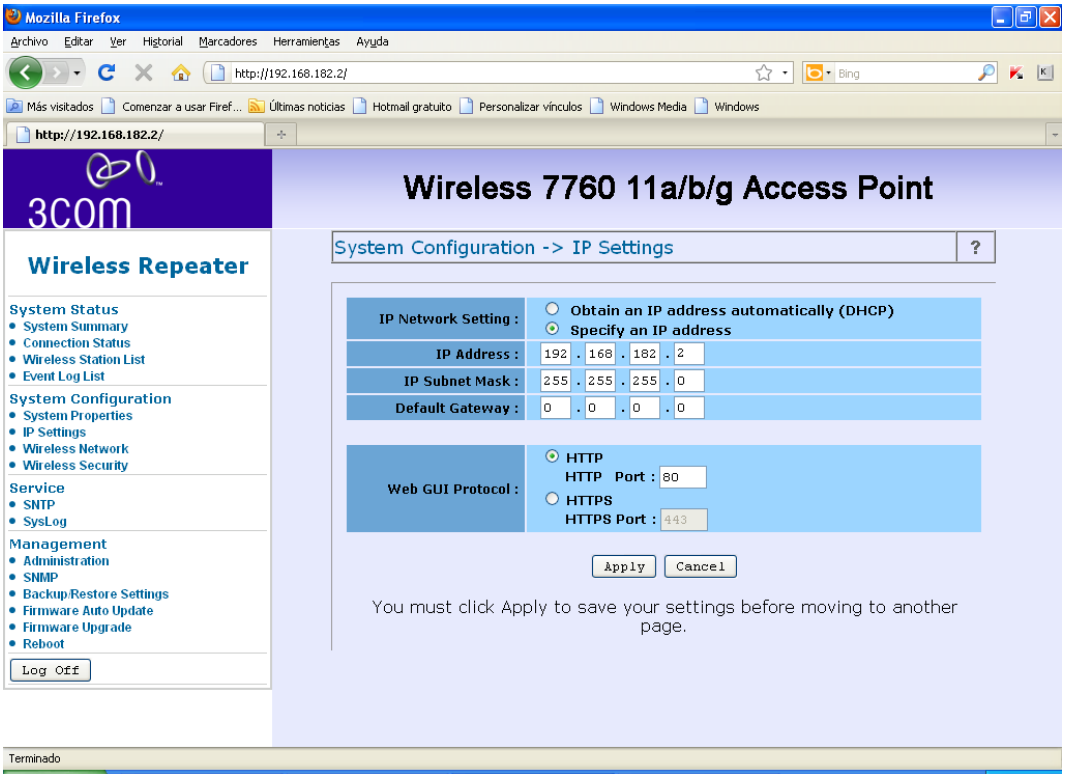


Fig. 6.36: Configuración de IP

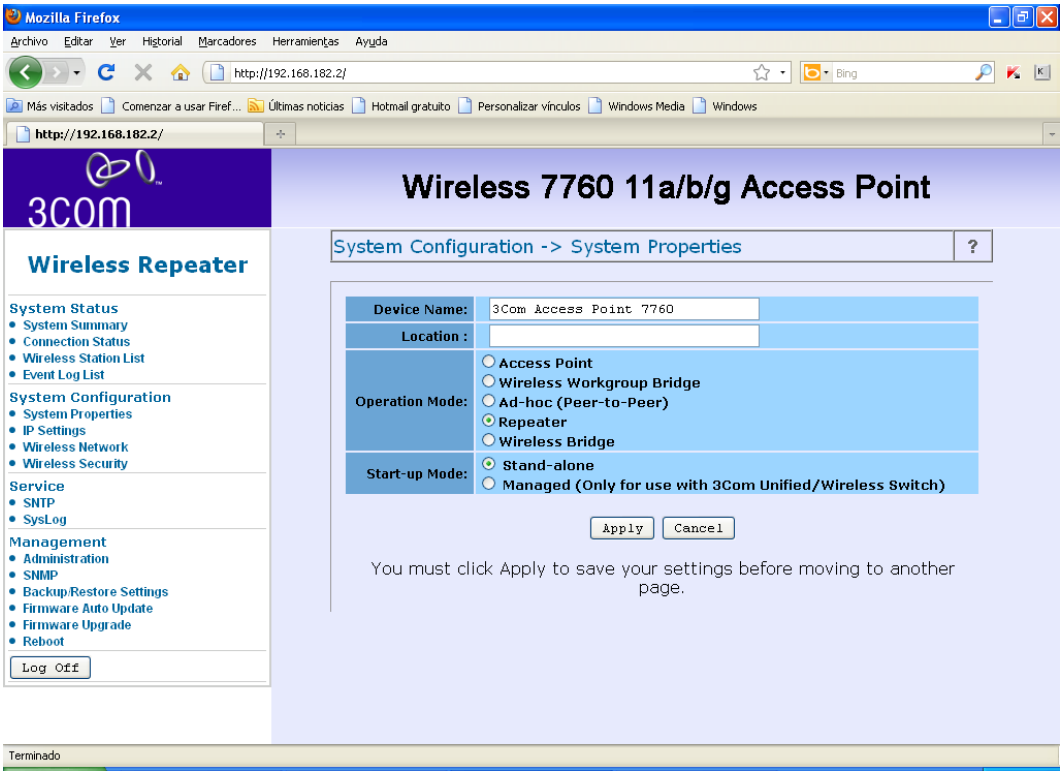


Fig. 6.37: Modo de operación como repetidor

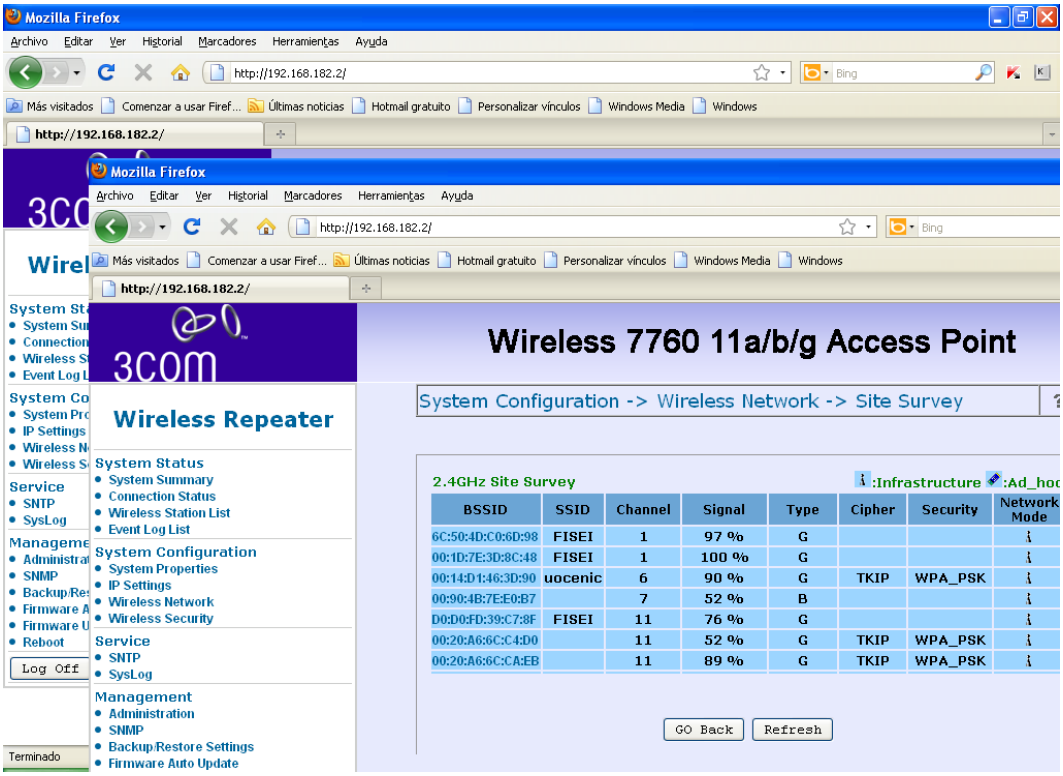


Fig. 6.38: Búsqueda y selección de la señal a repetirse

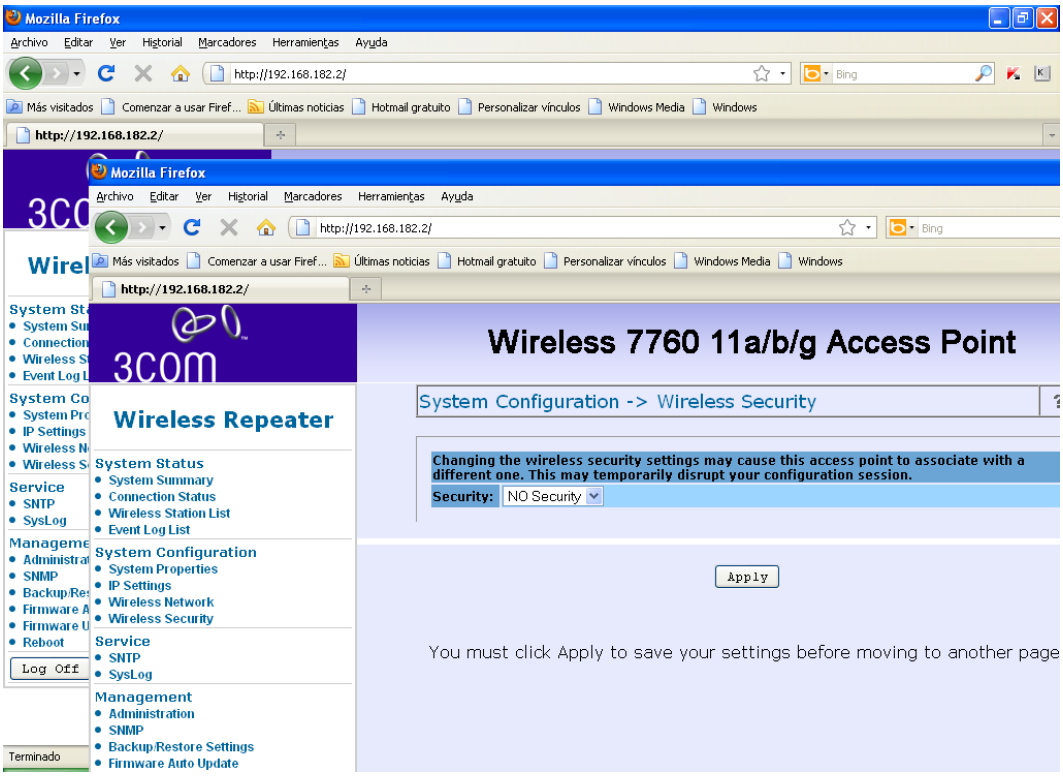


Fig. 6.39: Seguridad

6.8.4.3.3 Configuración del AP – 3

Se trata de un punto de acceso Cisco, modelo WAP200E, y de la misma forma que los equipos anteriores, también se detalla su configuración mediante las siguientes figuras (desde Fig. 6.40 hasta Fig. 6.44).

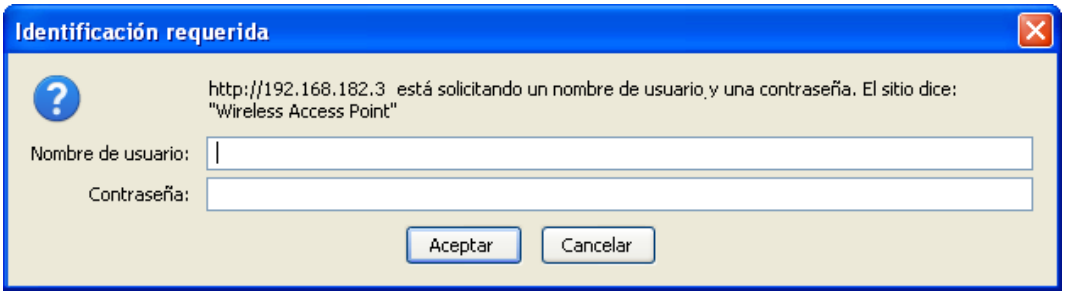


Fig. 6.40: Ingreso al AP-3

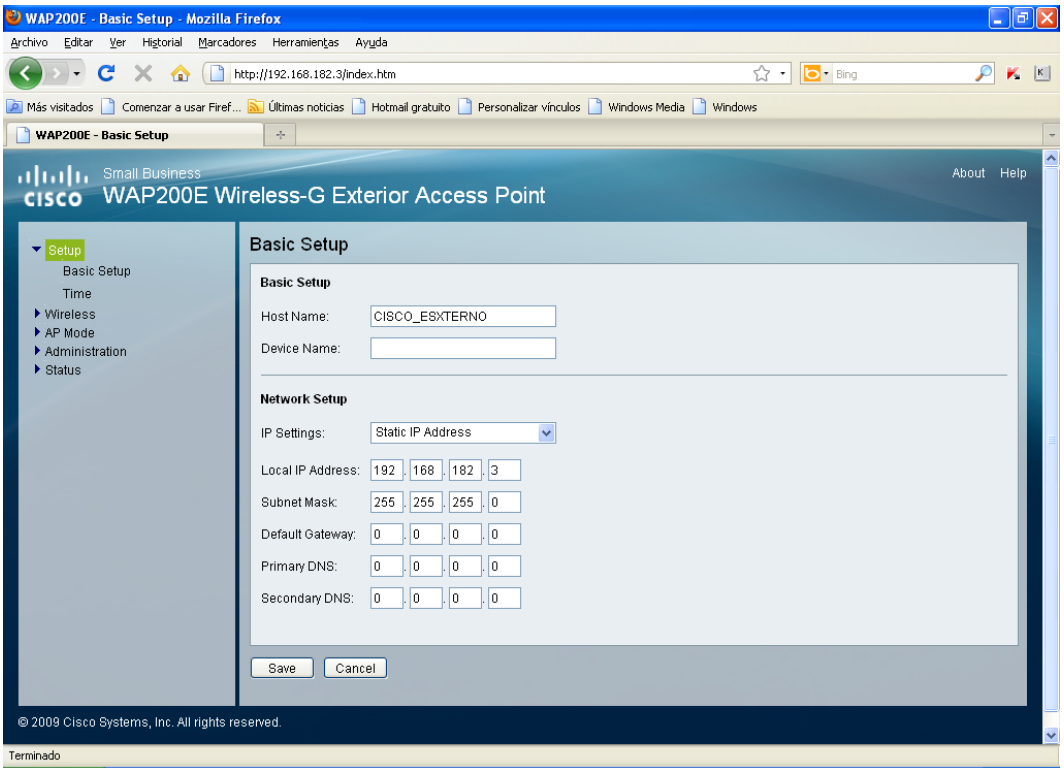


Fig. 6.41: Configuración de IP

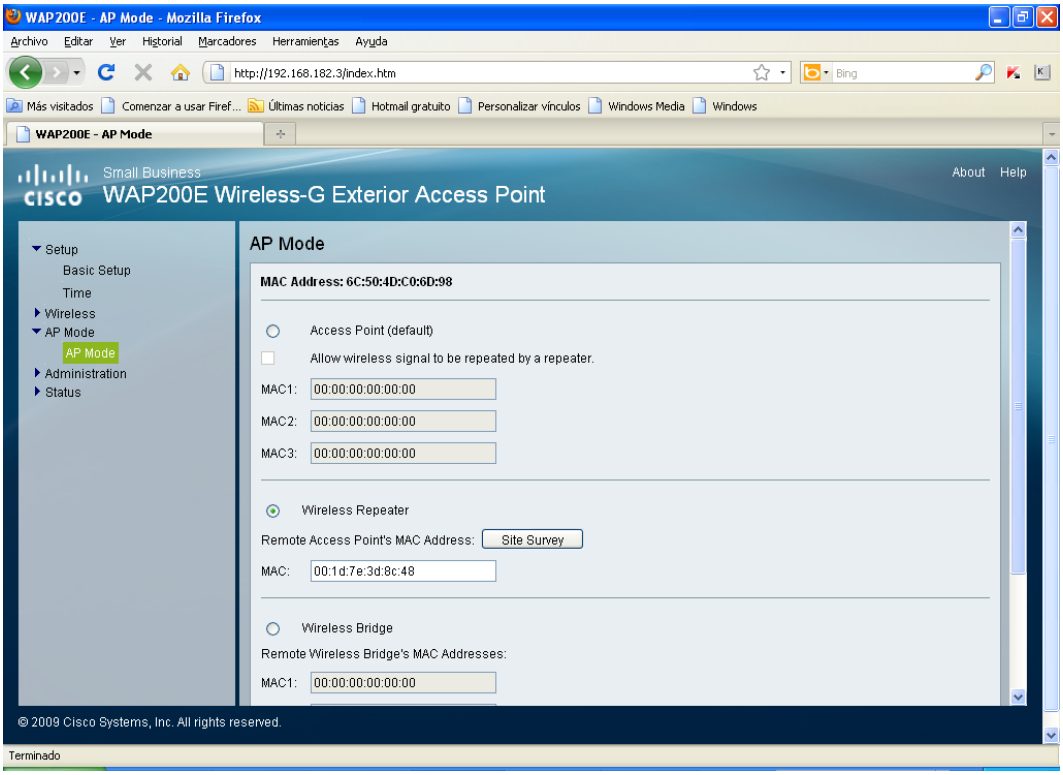


Fig. 6.42: Modo de operación como repetidor

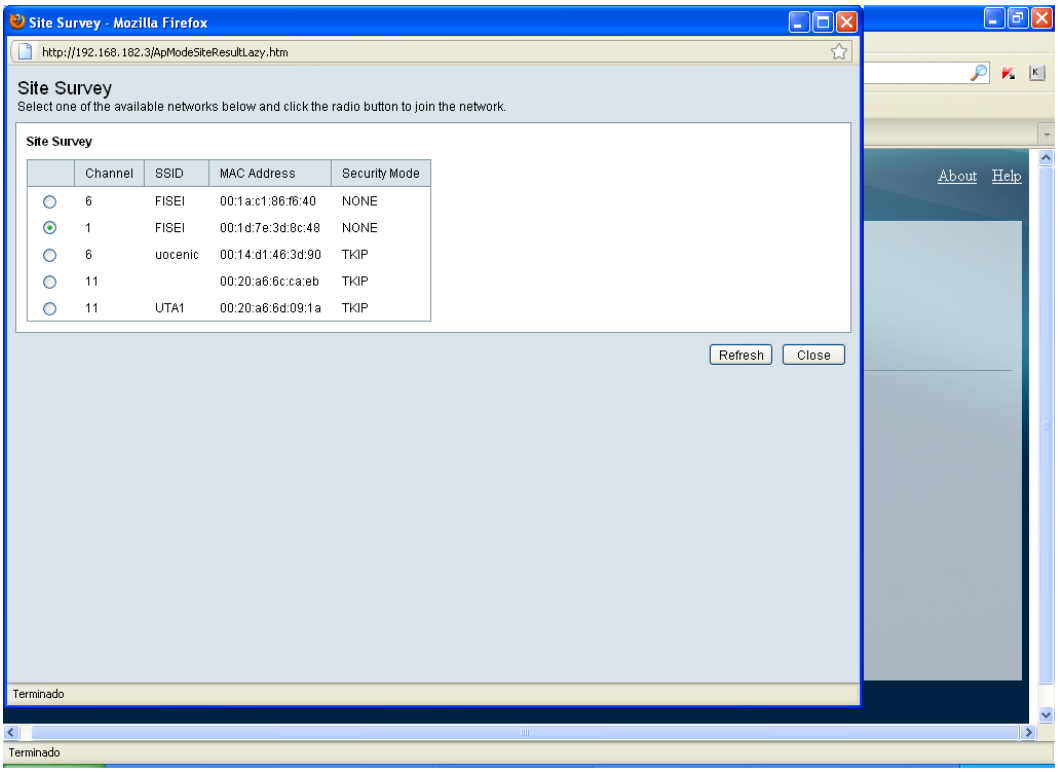


Fig. 6.43: Búsqueda y selección de la señal a repetirse

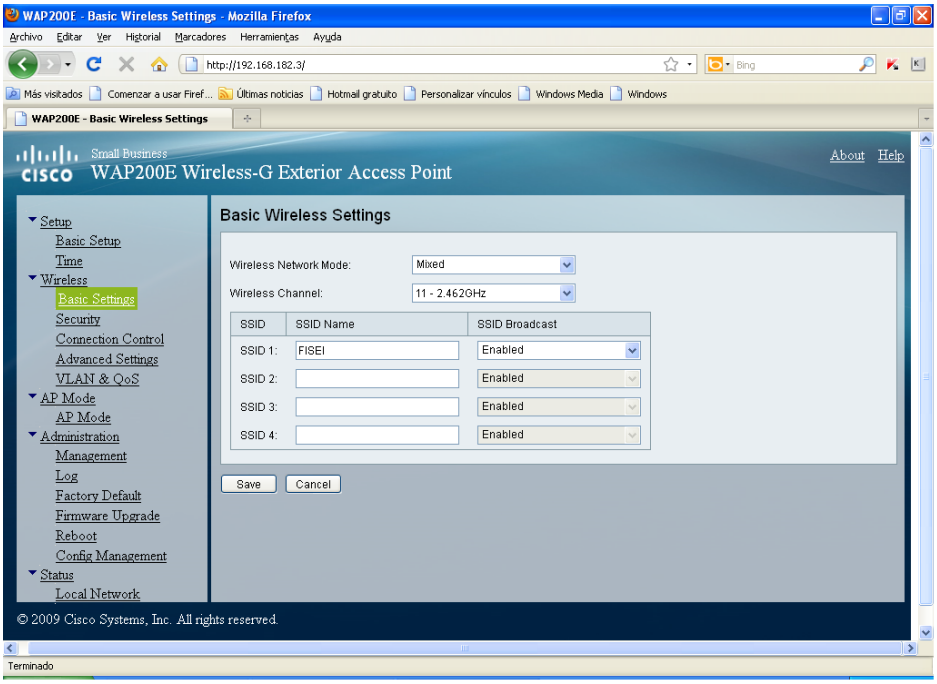


Fig. 6.44: SSID, estándar de operación y canal

6.8.4.3.4 Configuración del AP – 4

Es un punto de acceso Cisco, modelo WAP4410N. Los parámetros de configuración tales como la dirección IP, el SSID, el canal y otros datos se muestran en las figuras a continuación (desde Fig. 6.45 hasta Fig. 6.49).

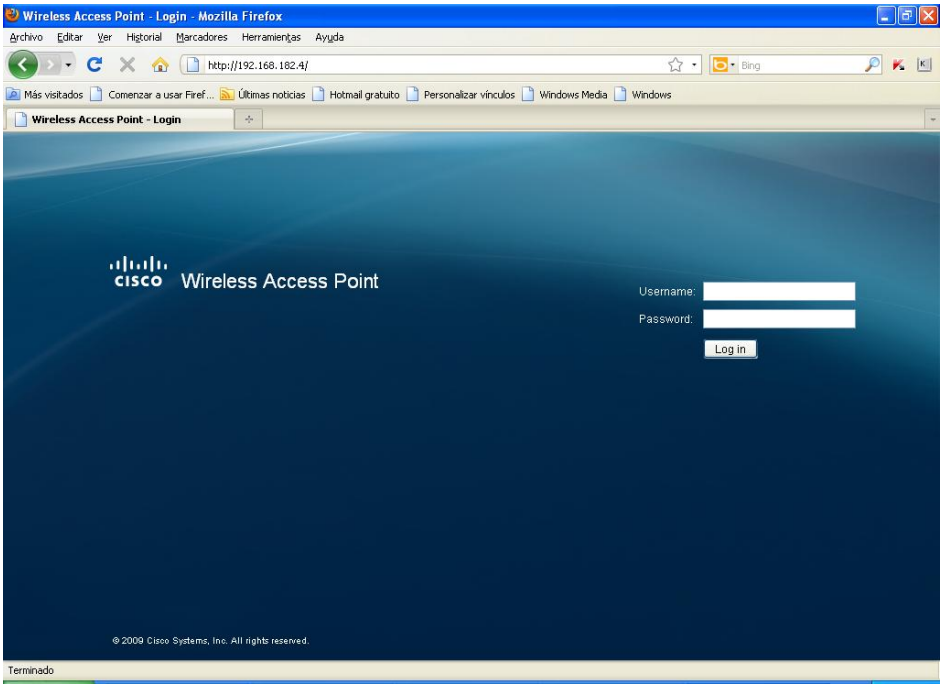


Fig. 6.45: Ingreso al AP-4

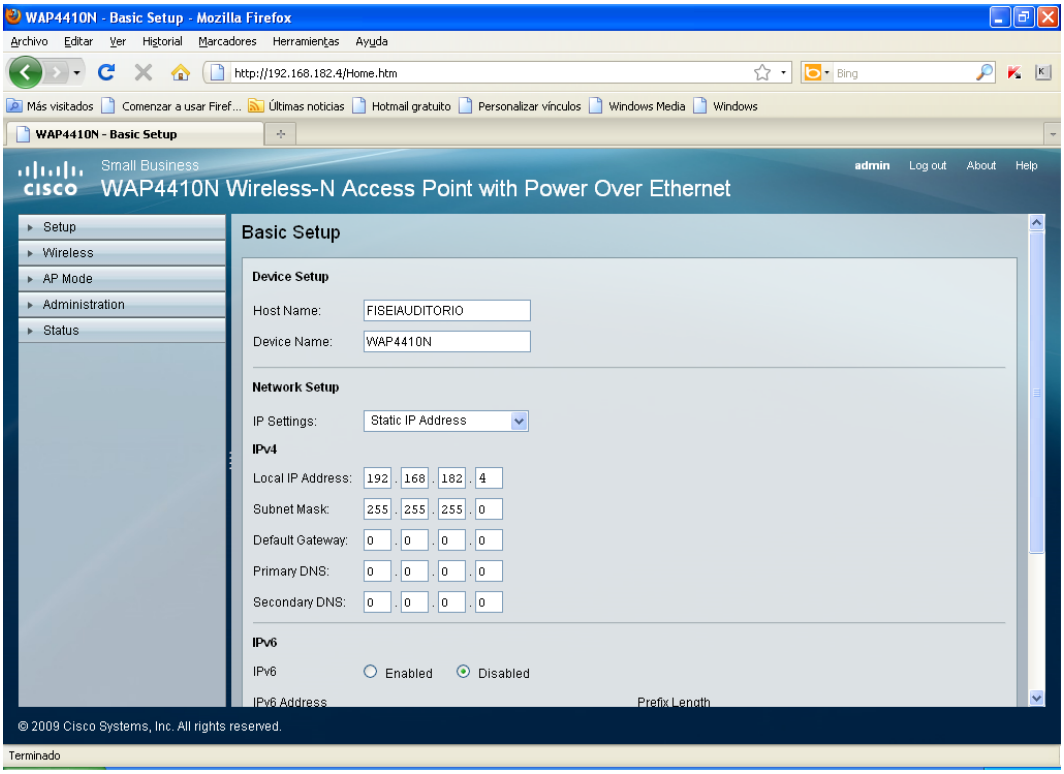


Fig. 6.46: Configuración de IP

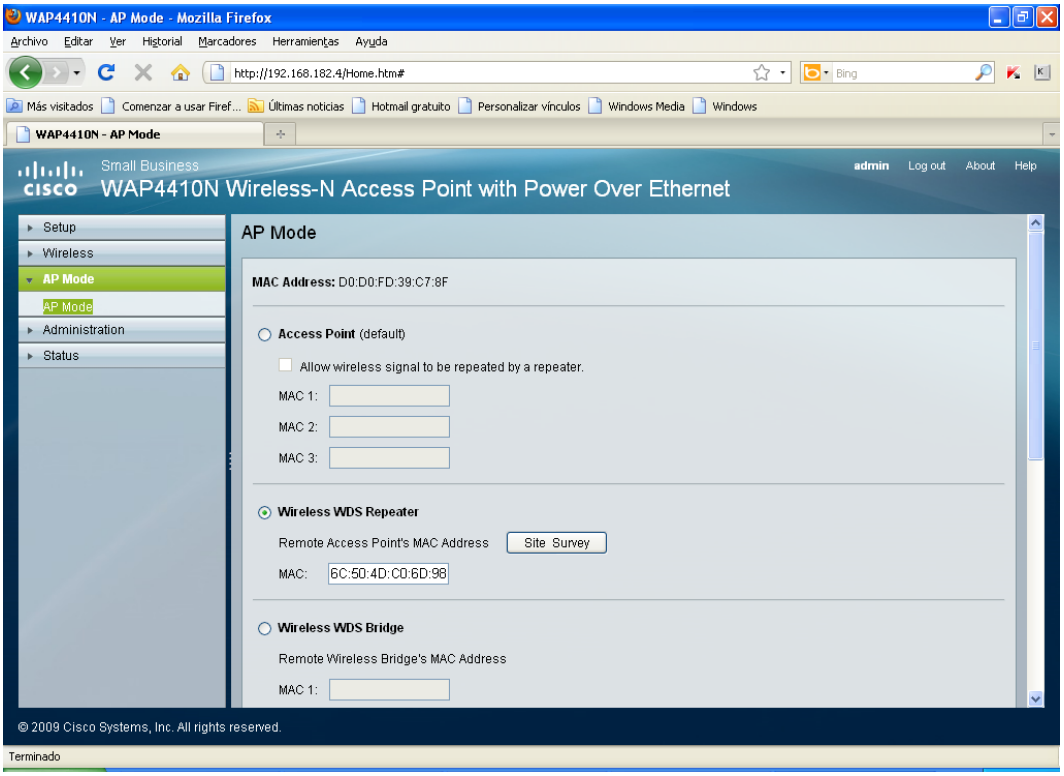


Fig. 6.47: Modo de operación como repetidor

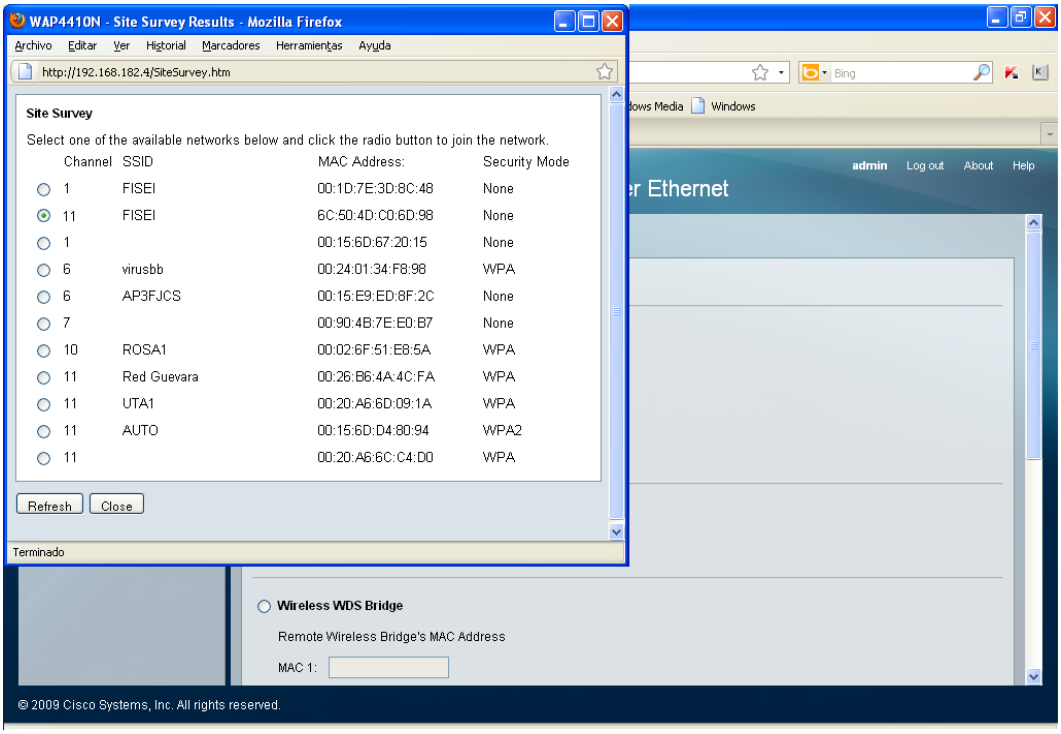


Fig. 6.48: Búsqueda y selección de la señal a repetirse

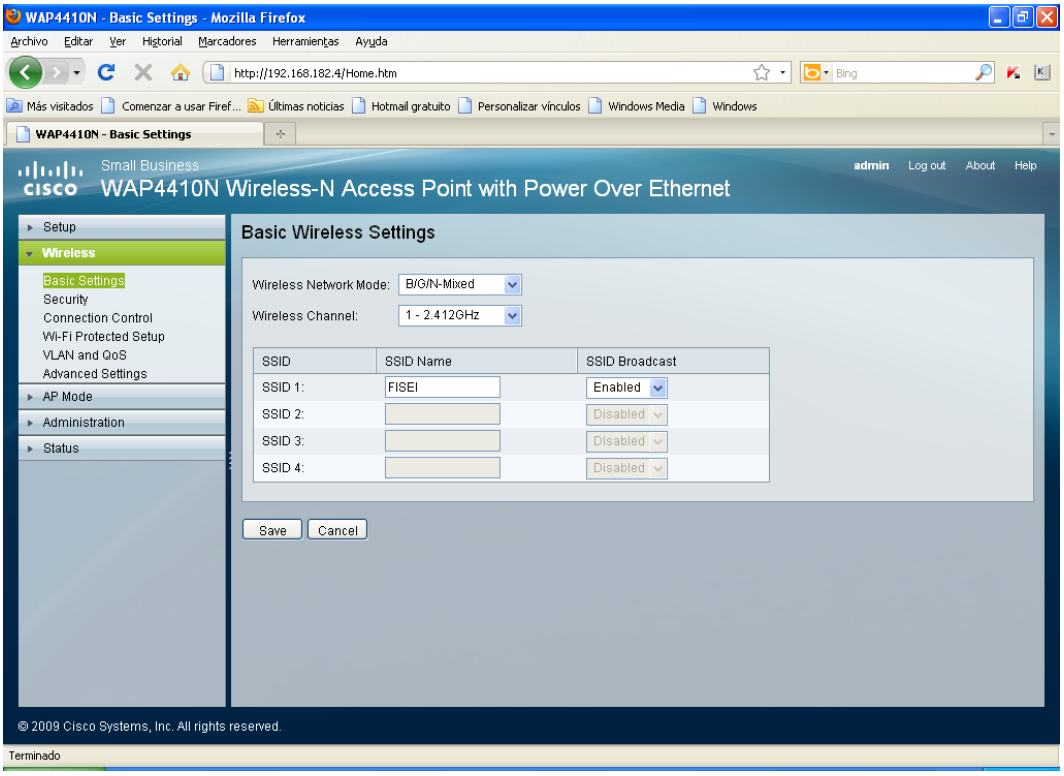


Fig. 6.49: SSID, estándar de operación y canal

6.8.4.3.5 Configuración del AP – 5

Es el segundo punto de acceso Cisco, modelo WAP4410N. Sus parámetros de configuración se describen mediante las siguientes imágenes (desde Fig. 6.50 hasta Fig. 6.54).

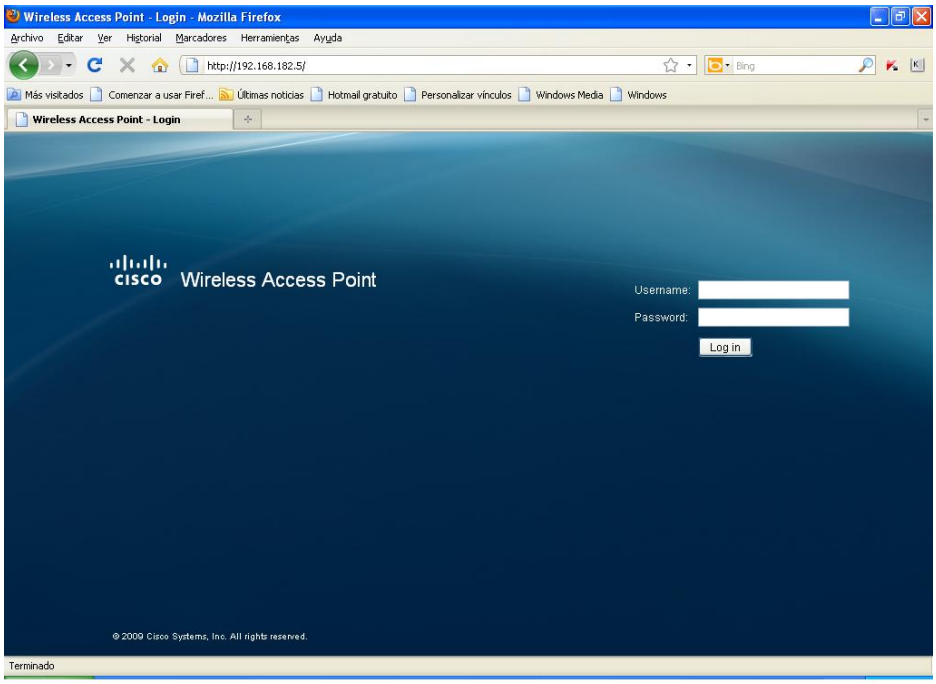


Fig. 6.50: Ingreso al AP-5

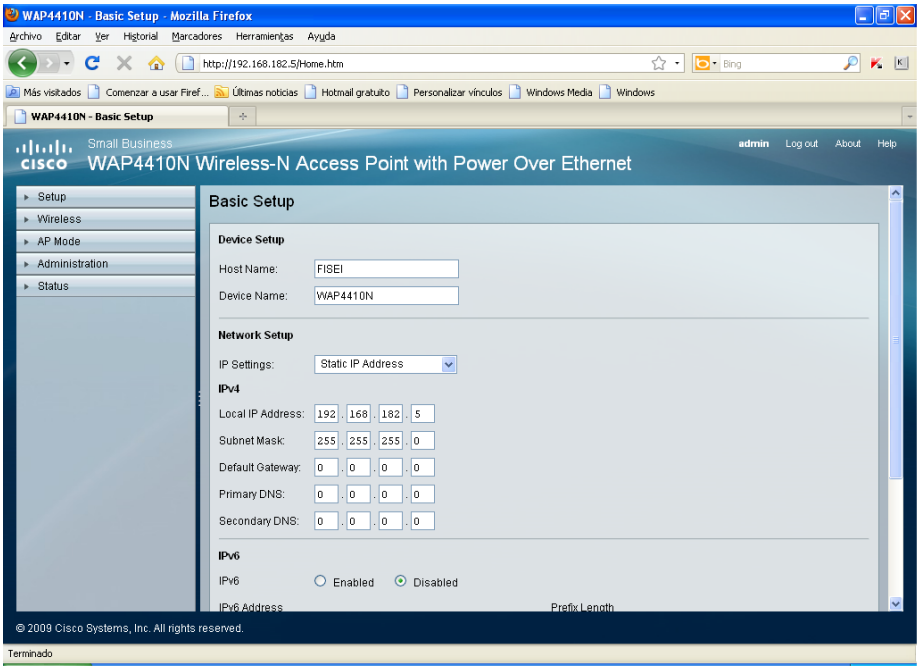


Fig. 6.51: Configuración de IP

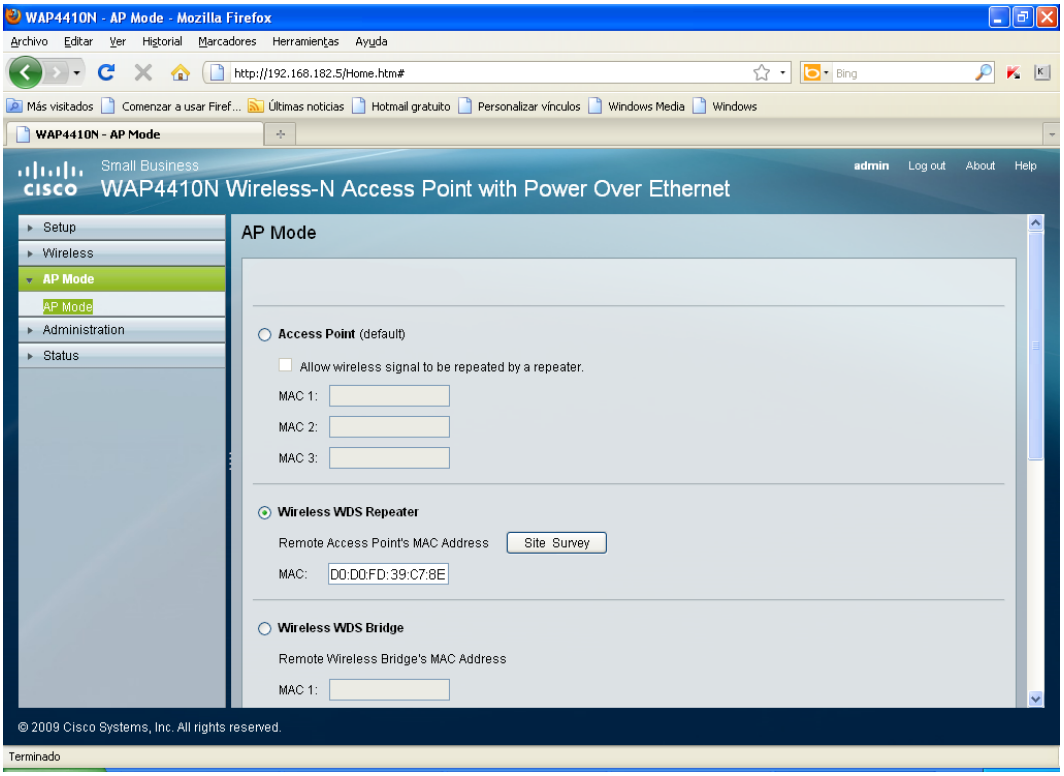


Fig. 6.52: Modo de trabajo como repetidor

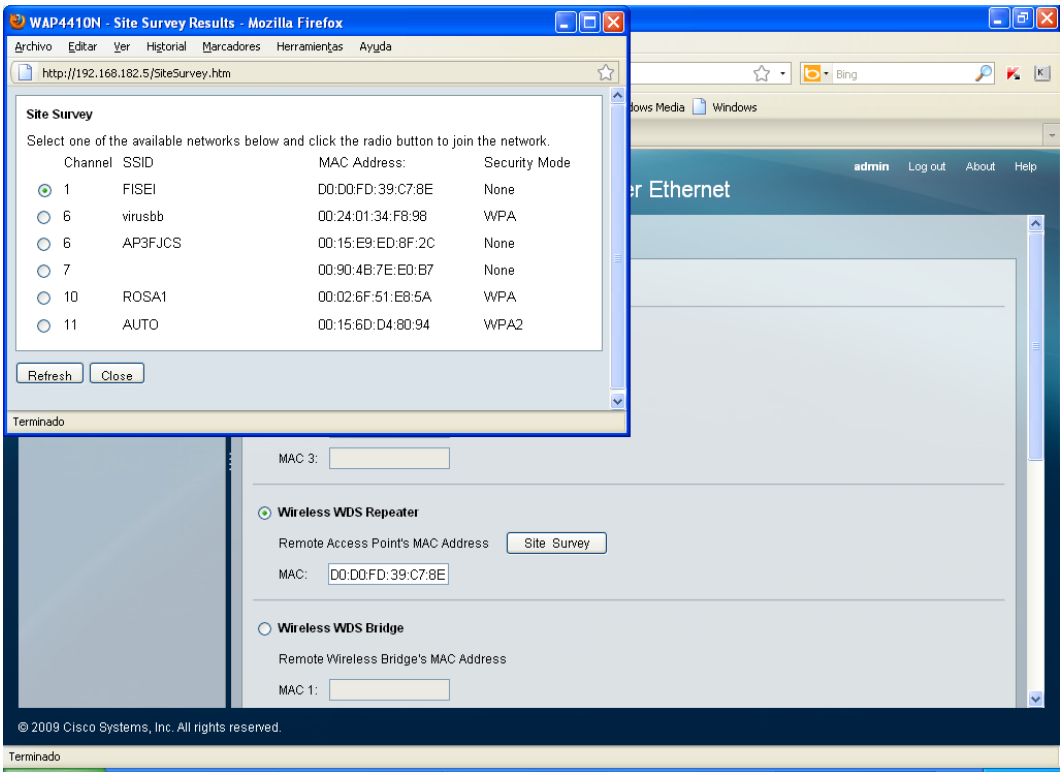


Fig. 6.53: Búsqueda y selección de la señal a repetirse

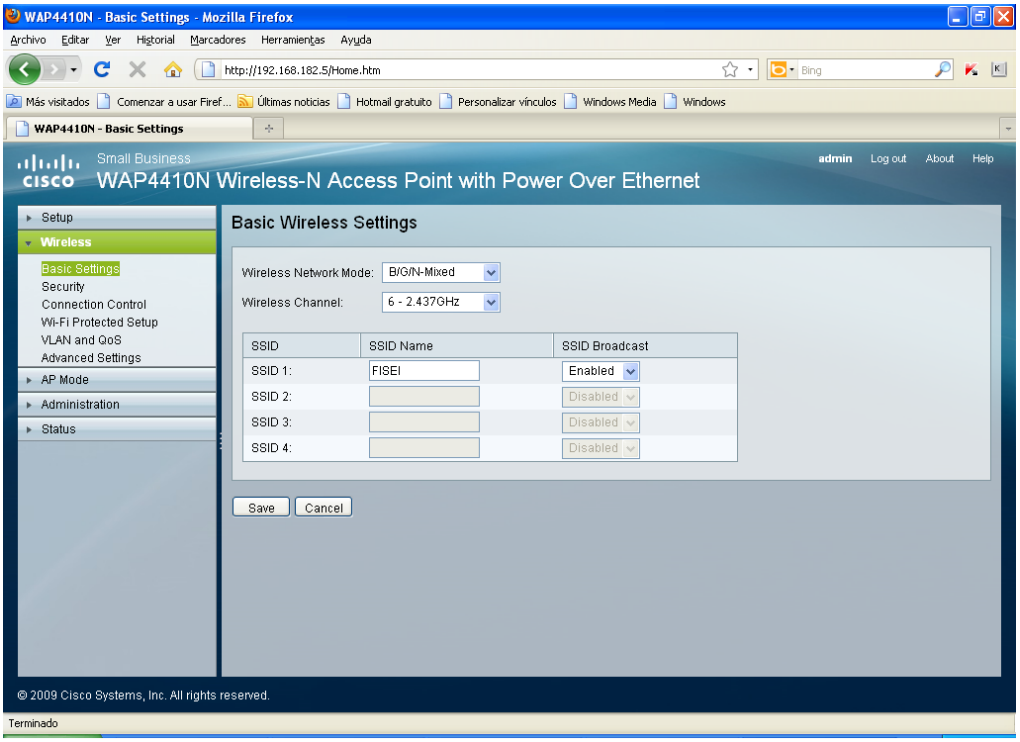


Fig. 6.54: SSID, estándar de operación y canal

6.8.5 Pruebas de Acceso

Ya con los puntos de acceso configurados se verificó que el servidor radius funcione correctamente. Para ello se estableció conexión con la red inalámbrica mediante un computador portátil compatible:

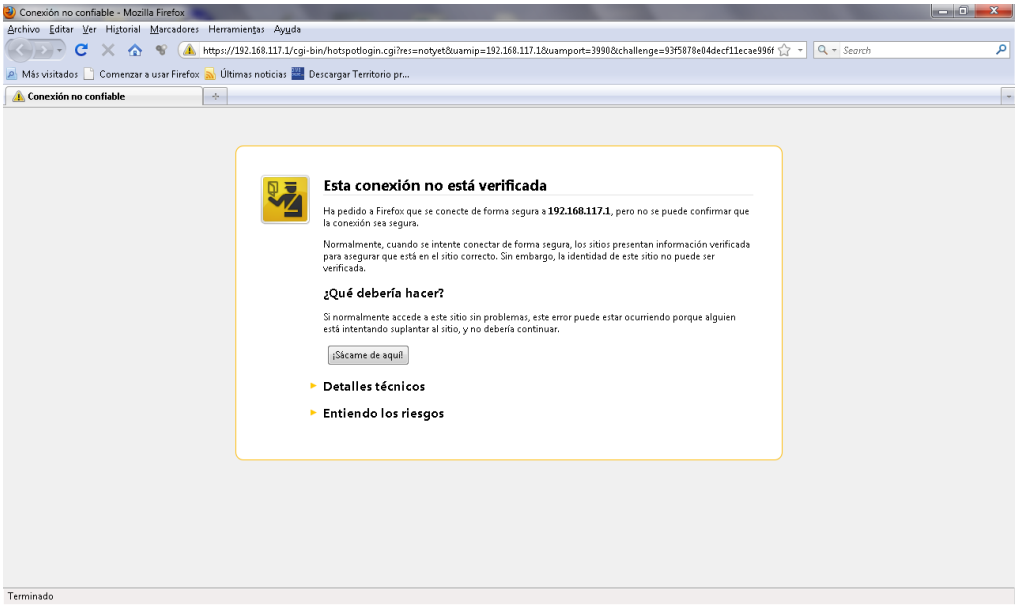


Fig. 6.55: Aviso de conexión segura

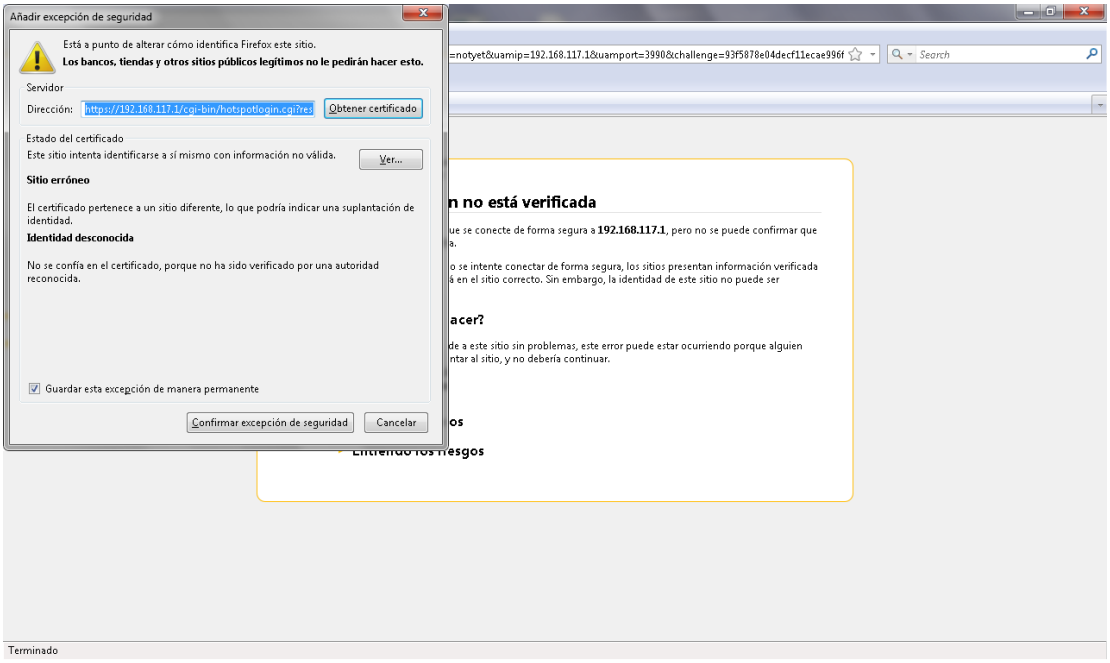


Fig. 6.56: Configuración de acceso por certificado

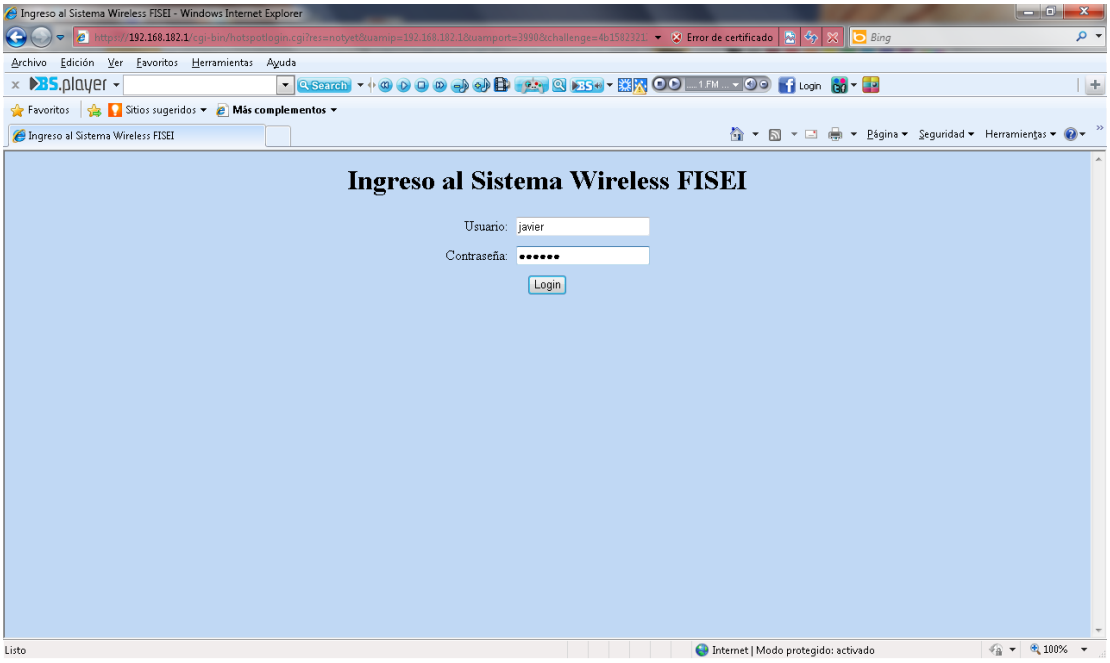


Fig. 6.57: Página de autenticación

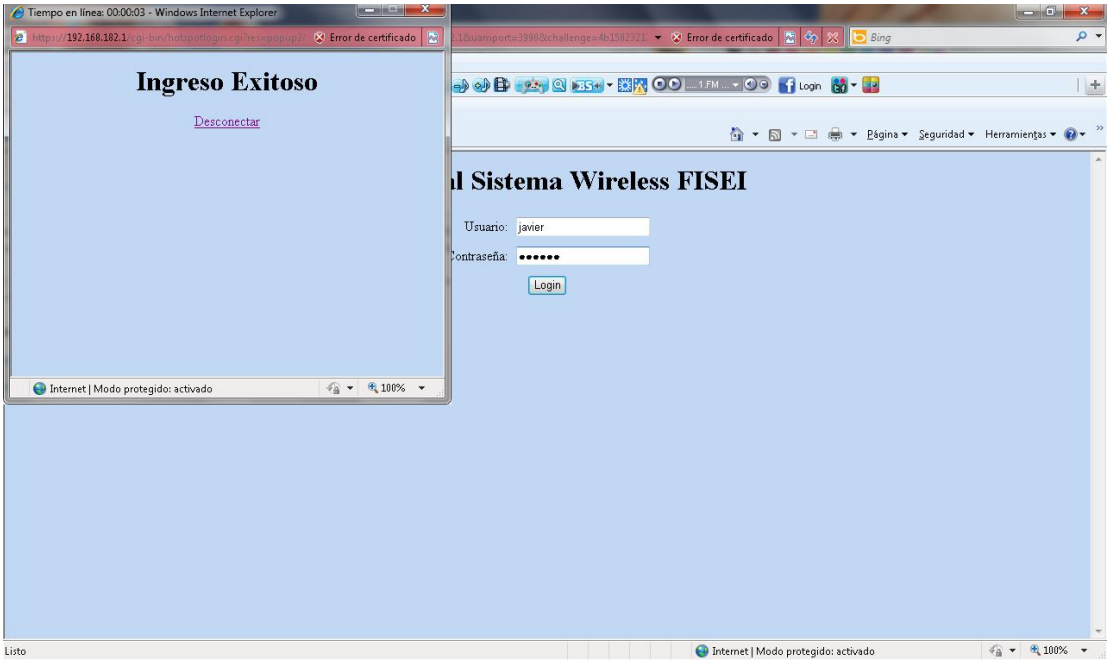


Fig. 6.58: Acceso autorizado

6.9 Presupuesto

Debido a que la cobertura en el edificio dos de la FISEI fue insuficiente con la utilización de un punto de acceso con tecnología n, se realizó la compra de otro equipo idéntico a dicho AP para alcanzar a cubrir eficientemente toda la infraestructura. En la siguiente tabla se especifíca el costo de este equipo y su instalación en conjunto con el otro AP restante en el edificio dos de la facultad.

Item	Cantidad	Valor unitario	Subtotal
AP Cisco WAP 4410N	1	$ 280	$ 280
Instalación de AP	2	$ 10	$20
Total			**$ 300**

Tabla 6.7: Presupuesto

6.10 Administración

La administración de la red inalámbrica implementada estará a cargo del departamento de redes de la FISEI. El servidor radius instalado en un equipo propio de la facultad, estará ubicado en dicho departamento y los laboratoristas con su director, serán los responsables del mantenimiento y administración del mismo.

La aplicación Daloradius utilizada para la administración de los usuarios en el servidor radius, cuenta con su respectivo manual en la sección de anexos del presente documento, e indica todo lo necesario para el manejo de los clientes inalámbricos de la red.

6.11 Conclusiones y Recomendaciones

6.11.1 Conclusiones

- Para la implementación del servidor radius se utilizó software libre, no solamente por las características que lo distingue del software privativo, sino también por las prestaciones que ofrece y que son comparables con las de software profesional con costo.

- Aunque el paquete freeradius incorpora una solución web para la administración de los clientes inalámbricos, denominada "Dialupadmin", no disponía de características como la manipulación de parámetros de conexión de usuarios ni autenticación por MAC, características que si son ofrecidas por daloradius y son necesarias.

- Se utilizaron puntos de acceso en vez de otro tipo de equipos (routers inalámbricos, por ejemplo) porque son los únicos dispositivos capaces de repetir señales en una WLAN. El único router inalámbrico utilizado no puede funcionar como repetidor y esa es otra de las razones para estar conectado directamente al servidor radius.

- El software de simulación Airmagnet Planner, utilizado para el diseño de la red inalámbrica, fue una herramienta de gran ayuda en este proceso, ya que, ayudó a definir la ubicación más adecuada de los puntos de acceso. Aunque no determinaba automáticamente la posición más correcta de los AP, la ubicación manual de ellos fue simple y se pudieron determinar las mismas en base al mapa de señal que genera este software.

6.11.2 Recomendaciones

- Aunque en la actualidad se dispone de sistemas operativos Windows específicos para trabajo en servidores, Linux es la plataforma líder en este campo y a diferencia de sistemas Windows, dispone de distribuciones completamente gratuitas; una razón poderosa para recomendar Linux como la primera alternativa cuando se trata de la implementación de servidores.
- La inestabilidad e inseguridad de los sistemas Windows es otra de las razones para sugerir a Linux como la plataforma indicada en proyectos de este tipo. Su superioridad frente al sistema operativo de Microsoft es notable sin lugar a dudas.
- Para la instalación de los servicios y la configuración de todos ellos en pos de levantar el servidor radius, es recomendable adquirir un nivel de conocimiento medio en el manejo de comandos dentro de la consola de la distribución Linux correspondiente, en este caso, CentOS. En este mismo punto, al adentrarse por primera vez y de forma práctica en el mundo Linux, se sugiere comenzar a experimentar como usuario normal y no como superusuario.
- Es completamente manejable la administración de usuarios del servidor radius mediante el manejo de comandos en Linux, sin embargo, la tarea puede volverse compleja cuando no se dominan bases de datos como mysql o en general, habilidad dentro de la consola. Por tal razón, es recomendable disponer de un sistema o interfaz de administración que facilite esta tarea a

los administradores. En este proyecto por ejemplo, se ha utilizado daloradius como alternativa.

- Para el diseño de redes inalámbricas WLAN, es recomendable hacer uso de un software como AirMagnet Planner que ayude a definir la ubicación de los puntos de acceso. Esta es una herramienta poderosa y muy útil para definir en menor tiempo y con mayor precisión, el lugar estratégico para los APs. La complejidad del diseño se verá multiplicada con un número mayor de puntos de acceso y la utilización de software de este tipo es bastante útil en esos casos.

6.12 BIBLIOGRAFÍA

Tesis de Maestría – Ms. David Guevara: Autenticación de redes inalámbricas usando software libre.

6.12.1 LINKOGRAFÍA

- http://www.alcancelibre.org/staticpages/index.php/como-centos5-grafico
- http://www.linuxparatodos.net/portal/staticpages/index.php?page=instalacion-grafico-centos5
- http://www.tribulinux.com/tutoriales-como-configurar-red-centos-fedora-redhat.html
- http://rm-rf.es/como-configurar-tarjetas-de-red-en-red-hat-enterprise-centos-y-fedora-core/
- http://www.linuxparatodos.net/portal/staticpages/index.php?page=08-parametros-red
- http://systemadmin.es/2008/12/configuracion-de-interfaces-de-red-virtuales-en-redhat
- http://rm-rf.es/como-configurar-tarjetas-de-red-en-red-hat-enterprise-centos-y-fedora-core/
- http://www.ipaiw.com/?p=220

- http://es.wikipedia.org/wiki/Anexo:Comandos_linux
- http://mundogeek.net/archivos/2007/05/10/descomprimir-archivos-en-linux-desde-la-consola/
- http://cacorrea.wordpress.com/2009/09/19/servidor-radius/
- http://fruizondre.wordpress.com/2009/11/02/hotspot-con-chillispot/#comment-44
- http://daloradius.com/
- http://147.52.159.12/mirrors/ftp.freeradius.org/
- http://www.pumawifi.org/?q=node/52/15
- http://tldp.org/HOWTO/8021X-HOWTO/freeradius.html
- http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=como-mysql-quickstart
- http://blogdrake.net/blog/peratu/como-instalar-servidor-apache-php-y-ssl
- http://www.pchardware.org/redes/redes_osi.php
- http://www.cyber-cafe-software.com/spa/Hotspot/Instalaci%C3%B3n-Configuraci%C3%B3n-Hotspot.asp
- http://www.monografias.com/trabajos55/implementacion-red-wifi/implementacion-red-wifi2.shtml
- http://www.appinformatica.com/routers.htm
- http://www.slideshare.net/deicyarias1/redes-inalambricas-2
- http://www.wificlub.org/featured/alcance-de-redes-wifi/
- http://www.guatewireless.org/hardware/dbm-y-potencia/
- http://docente.ucol.mx/al940435/public_html/CSMA.htm
- http://www.paramowifix.net/antenas/calculoenlacewlan.html
- http://es.wikipedia.org/wiki/Modelo_OSI
- http://encyclopedia2.thefreedictionary.com/PSK
- http://fondosdibujosanimados.com.es/wallpaper/Ofdm/
- http://tic-enreda2.blogspot.com/2008/11/clculo-de-usuarios-por-access-points.html
- http://www.broadcom.com/collateral/wp/802_11n-WP100-R.pdf

- http://homecommunity.cisco.com/t5/Wireless-Routers/Roaming-with-Multiple-Access-Points/td-p/44873
- http://www.slideshare.net/albinogoncalves/la-situacin-de-las-tecnologas-wlan
- http://wifitech.wordpress.com/acerca-de/
- http://www.wificlub.org/featured/alcance-de-redes-wifi/
- http://sumanual.com/instrucciones-guia-manual/LINKSYS/WRT300N-_E
- http://www.compunoa.com/access-point-cisco-wap200e-exterior-p-1214.html
- http://www.newtekuy.com/catalog/router-inalambrico-80211g-cisco-wap4410n-300mbps-mimo-vlan-qos-poe-linux-p-4027.html
- http://www.audiodesignguide.com/HomeNetwork/dua0045-4aaa01rev01.pdf
- http://www.flukenetworks.com/enterprise-network/wlan-security-and-analysis
- http://www.psiber.com/rf3d/rf3d.html

ANEXOS

6.13.1 ANEXO 1: Encuesta realizada a los alumnos de la FISEI

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

ENCUESTA DIRIGIDA A LOS ESTUDIANTES DE LA FISEI

La presente encuesta tiene como fin la recolección de datos para el desarrollo de una red inalámbrica segura que interconecte los edificios de la FISEI.

El manejo de la información resultante será estrictamente confidencial. Marque una "X" en el paréntesis respectivo que decida:

1. ¿Es necesaria para usted la existencia de una red inalámbrica en el **nuevo** edificio?

   No ( ) En caso contrario, ¿Por qué motivo? (Uno o varios indicadores):

   Tareas ( ) Correo ( ) Redes Sociales ( ) Multimedia ( ) Otro:

……..…….……

2. ¿Dispone de un dispositivo compatible para acceder a la red inalámbrica de la FISEI?
   - No ( ) → ¿Piensa a mediano plazo adquirir alguno? ( )
   - Si ( ) → ¿Cuánto tiempo está conectado a dicha red inalámbrica?

     1 hora ( ) 2 horas ( ) 3 horas ( ) más tiempo ( )

3. ¿Por qué es importante una seguridad eficiente en la red inalámbrica de la FISEI?

   - Para evitar que personas ajenas a la facultad se conecten a la misma ( )
   - Para evitar posibles ataques e inyección de virus en la red ( )
   - Por la información sensible existente en las portátiles conectadas ( )
   - No es importante. Explique por qué motivo:

     ……..……

4. ¿Por qué se debe elegir el estándar *WIFI **N*** (diseñado para redes inalámbricas de área local o WLAN) como tecnología para la red inalámbrica de la FISEI?

   - Porque permite mayor velocidad de transmisión y es compatible con estándares WIFI anteriores ( )
   - Porque provee un mejor desempeño de la red inalámbrica ( )
   - Si no se debe elegir 802.11**n**, explique por qué razón:

     ……

5. La interconexión entre ambos edificios de la FISEI permitiría:

- Administrar eficientemente los usuarios de la red inalámbrica de uno u otro edificio ( )
- Que los alumnos puedan desplazarse libremente entre ambos edificios mientras navegan en internet ( )
- No serviría de nada porque…….

6.13.2 ANEXO 2: Manual del software de simulación AirMagnet Planner

Airmagnet Planner

Es un software que provee una solución para el diseño e implementación de redes WLAN.

Airmagnet Planner está integrado dentro Airmagnet Survey, un programa que ofrece diversas herramientas útiles para diseñar redes WLAN, por tal razón, necesariamente se instala Survey para disponer de Planner.

La instalación de Airmagnet Survey es idéntica a la instalación de cualquier otro programa de ordenador para Windows. Luego de la instalación se arranca el sofware, presentándose entonces una pantalla de bienvenida como la que se muestra en la imagen a continuación.

Fig. 6.59: Arranque de Airmagnet Survey

Después de terminar el arranque del programa se mostrará la pantalla de la interfaz del sofware, de forma similar a la imagen presentada a continuación.

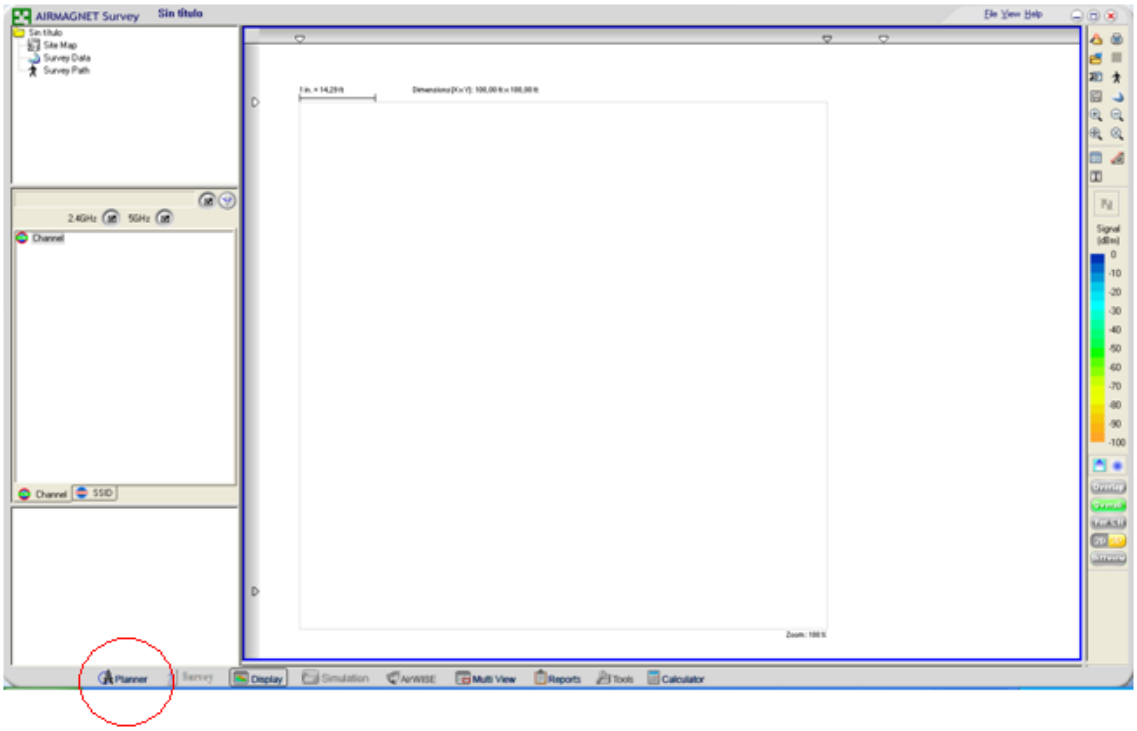


Fig. 6.60: Pantalla de inicio de Airmagnet Survey

Al hacer clic en la opción indicada con el círculo rojo “Planner” tendremos una pantalla similar a la anterior, donde se iniciará el trabajo del diseño. Para una idea general, se indica a continuación los detalles más relevantes de la pantalla de Planner.

Fig. 6.61: Pantalla de trabajo con Airmagnet Planner

Para iniciar inmediatamente con el diseño, en la barra de menú (parte superior derecha) se seleccionará **File → New Project**. Se mostrará el asistente para el inicio de un nuevo proyecto, requiriendo que se escriba el nombre del proyecto y el directorio donde se guardará.

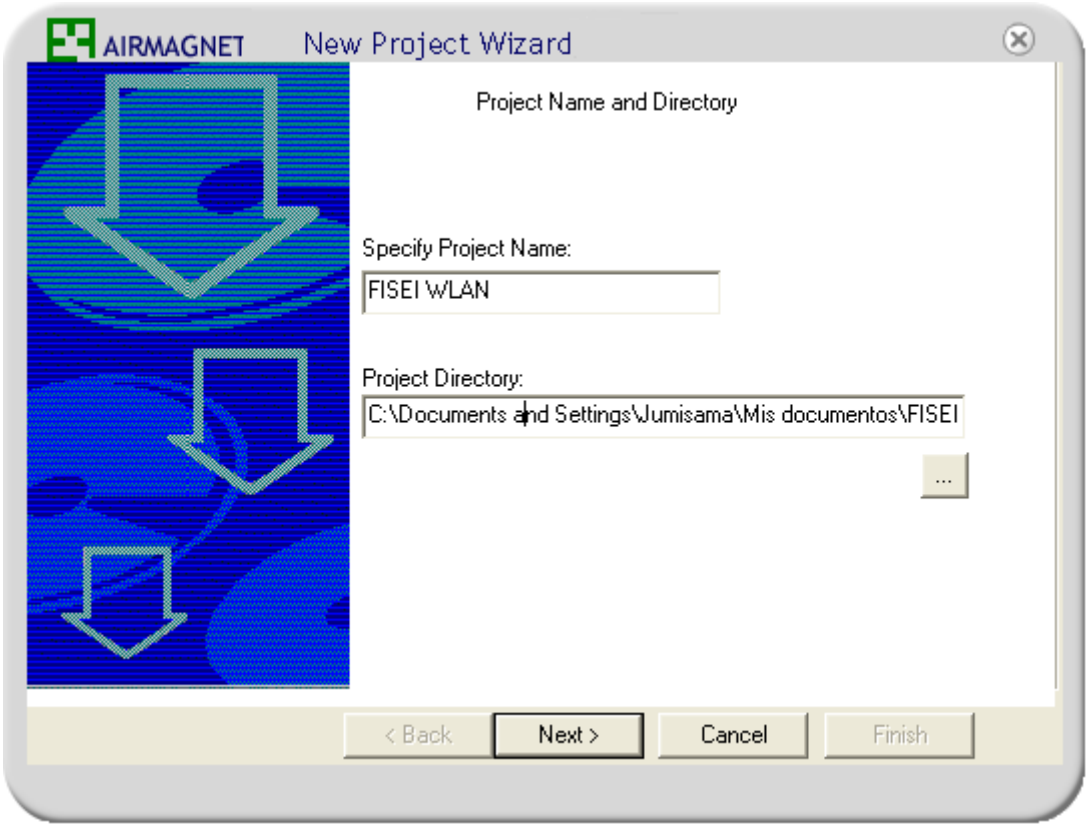


Fig. 6.62: Nuevo proyecto en Planner – Nombre y directorio

Después de dar clic en **Next** habrá que ingresar el plano del área donde se implementará la WLAN. En este caso, se iniciará con el plano de la planta baja del nuevo edificio. Se eligirá la primera opción, tal como se muestra en la imagen, y se seleccionará el plano desde una ubicación del disco duro. Los formatos aceptados para los planos son los siguientes: dxf, dwg, jpg, bmp, dib, gif, emf, wmf, vdx, vsd.

La unidad de medida será la indica por defecto, es decir, **Meters**. En la sección ***Floor Plan Dimensions*** se dejará en blanco los dos campos mostrados. Dicha sección permite ingresar el ancho y largo del plano, pero es recomendable no hacerlo. Se dimensionará el plano con la herramienta de calibración del programa para una mayor exactitud y confiabilidad.

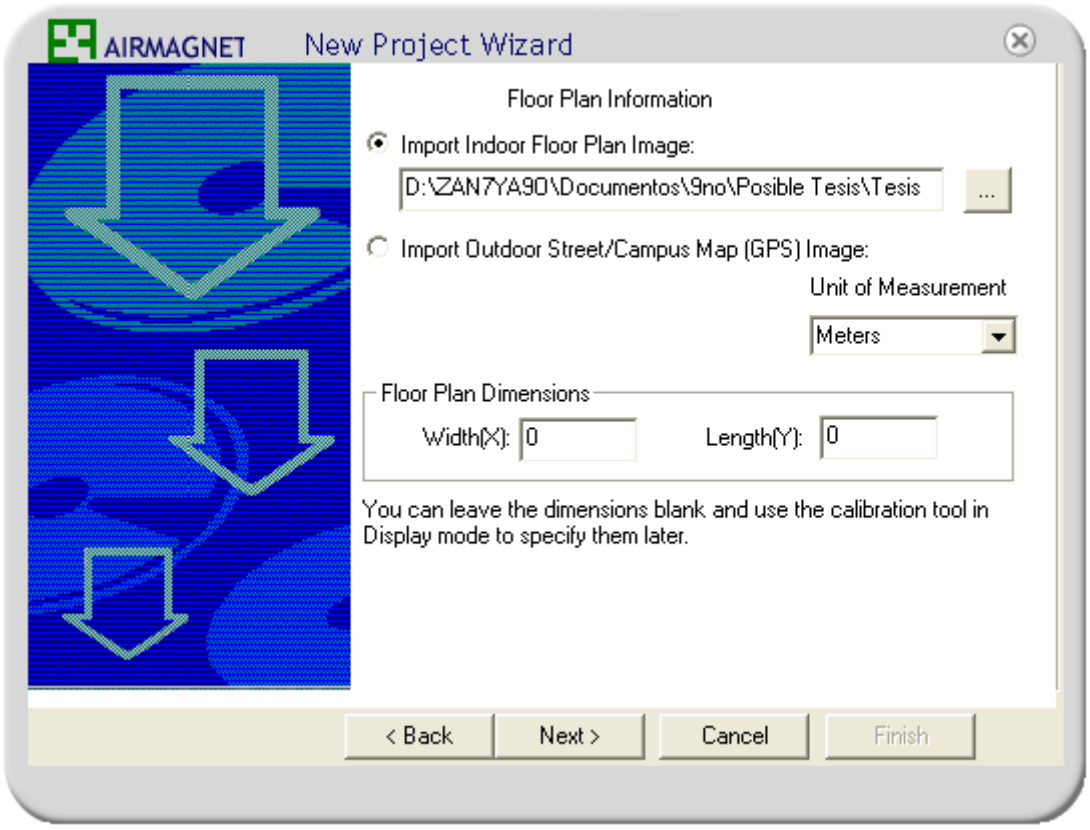


Fig. 6.63: Nuevo proyecto en Planner – Plano y dimensiones

A continuación clic en **Next** y habrá que indicar el ambiente de trabajo. Se eligirá la opción observada en la imagen que es la adecuada para un Hotel, o una oficina con densa cantidad de paredes.

El parámetro *Signal Propagation Assessment* indica la cantidad de metros que la señal puede viajar antes de encontrarse con un obstáculo.

El último campo permite digitar la potencia por defecto del punto de acceso en el orden de los milivatios.

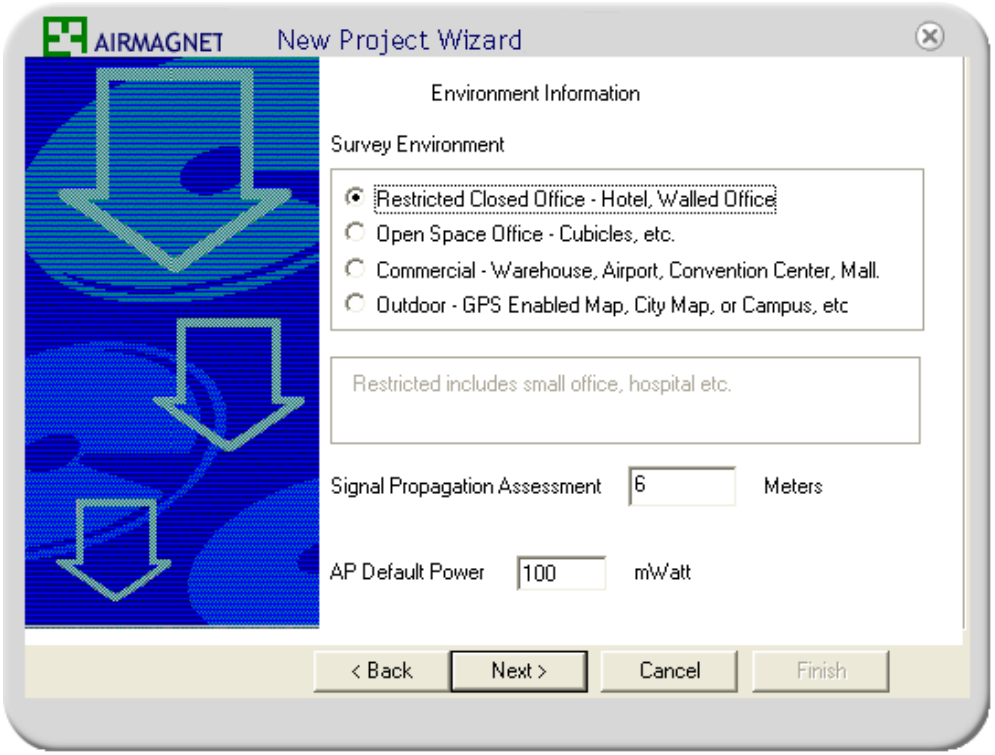


Fig. 6.64: Nuevo proyecto en Planner – Ambiente señal y potencia

Por último se puede agregar una descripción al proyecto.

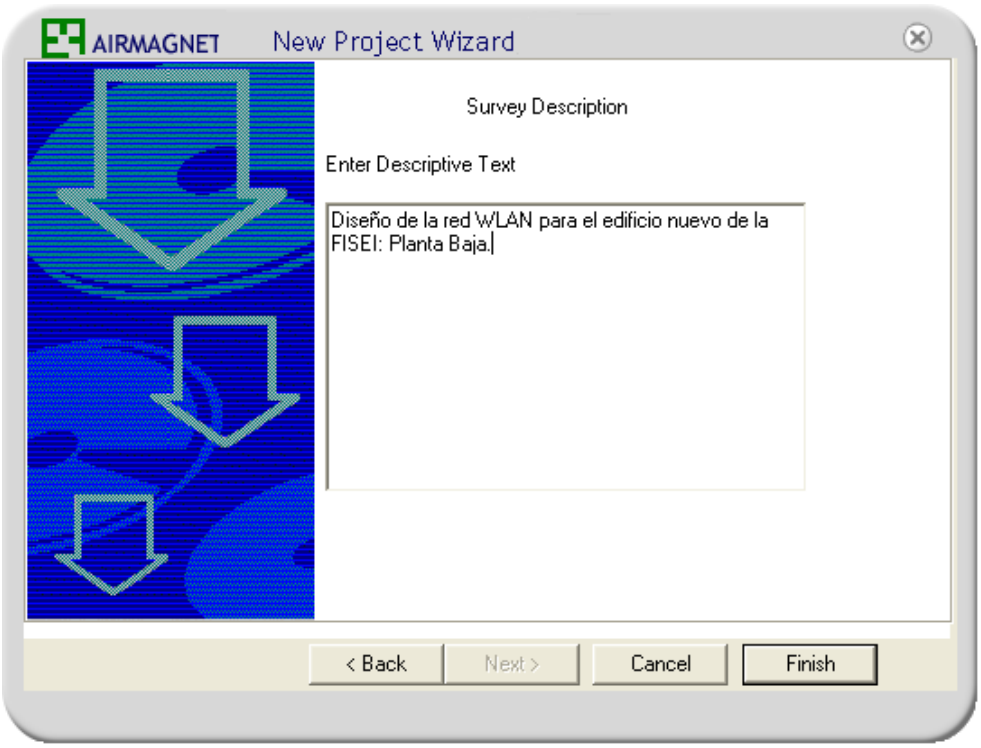


Fig. 6.65: Nuevo proyecto en Planner - Descripción

Al finalizar aparecerá en el área de trabajo el plano que, en primer lugar, se redimensionará con la herramienta de medida que se encuentra en la sección de herramientas. Es un icono que tiene la forma de una escuadra y al posar el ratón sobre éste mostrará "Measure Mode". Después de dar clic en el icono se mostrará una advertencia en inglés indicando si se desea recalibrar el plano después de realizar la medición. Clic en **Sí**.

Se mostrará un puntero similar a una *tachuela*. Con éste se toma el primer punto de referencia en el plano y luego de hacer clic, se prosigue con el siguiente punto y así mismo se hará otro clic. Aparecerá el siguiente cuadro de diálogo (ver imagen inferior) donde se habrá de indicar la **distancia real** entre ambos puntos y a continuación se dará clic en "Recalibrate", seguido de **OK**. Se mostrará la imagen redimensionada completamente.

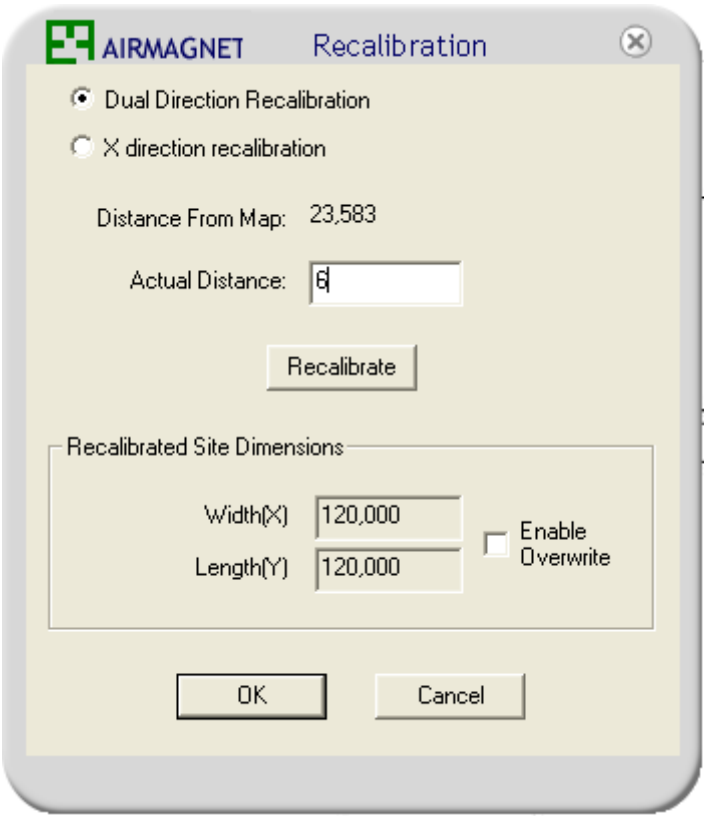


Fig. 6.66: Recalibración del plano

Para ir indicando el tipo de obstrucciones en el plano habrá que seleccionarse la herramienta para creación de paredes indicada en la siguiente imagen. En el cuadro superior se tiene disponibles varios tipos de obstrucciones con su respectiva pérdida en dB tanto para paredes como para puertas y ventanas.

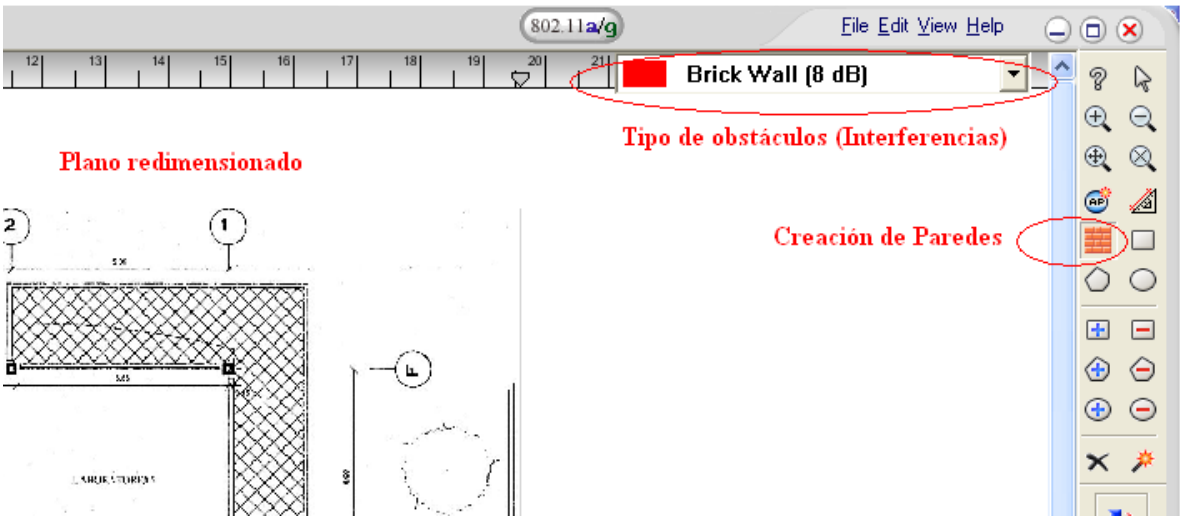


Fig. 6.67: Tipos de obstáculos y herramienta creación de paredes

Para ir indicando las obstrucciones, con el puntero habrá que ir repasando las paredes, puertas (vidrio o madera), siempre seleccionando el tipo de obstáculo respectivo en la pestaña superior derecha, tal como se muestra en la Fig. 6.68.

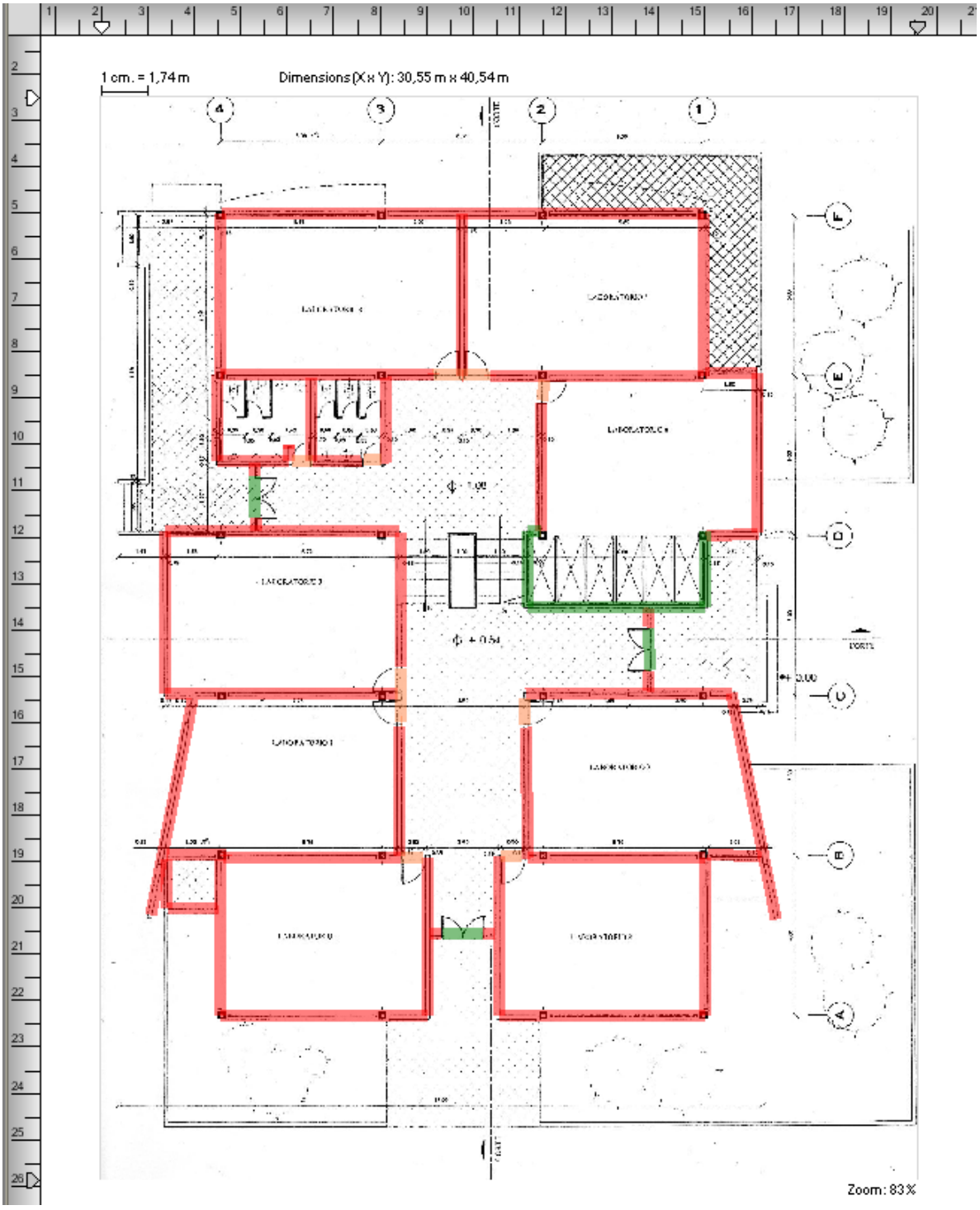


Fig. 6.68: Creación de obstáculos – Paredes y puertas

Con un clic izquierdo se inicia el recorrido a través de cada pared y cuando se desee terminar se hará clic derecho. Para cambios de dirección, en el *punto de quiebre* se hará otro clic izquierdo y se continuará con el recorrido. Es conveniente pulsar la tecla **Shift** para realizar rectas horizontales o verticales.

Posteriormente se colocan los puntos de acceso en el lugar que se considere adecuado. Aunque el programa puede indicar dónde y cuántos puntos de acceso colocar en el plano, lo hace de forma muy imprecisa.

Para colocar un AP, simplemente se selecciona el icono que está justo sobre el icono de la herramienta de creación de paredes y se hace clic en el plano, en el lugar que se desee. En la planta baja se consideró adecuado ubicarlo en el cubículo de vidrio, repasado de color verde en la anterior imágen. Se hizo de tal forma debido a que éste se encuentra aproximadamente en la mitad de la planta y porque al ubicarlo físicamente no se tendría mayores inconvenientes.

En la imágen inferior se muestra la ubicación del punto de acceso explicada anteriormente. Para generar el *mapa de señal* se hará clic en el icono que muestra dos flechas de color rojo y azul (Refrescar). El mapa de señal muestra la intensidad de la señal en dBs, con un código de colores que se traduce en la barra derecha. La misma barra derecha se puede desplazar hacia abajo o hacia arriba para variar el mínimo nivel de señal que se desea mostrar.

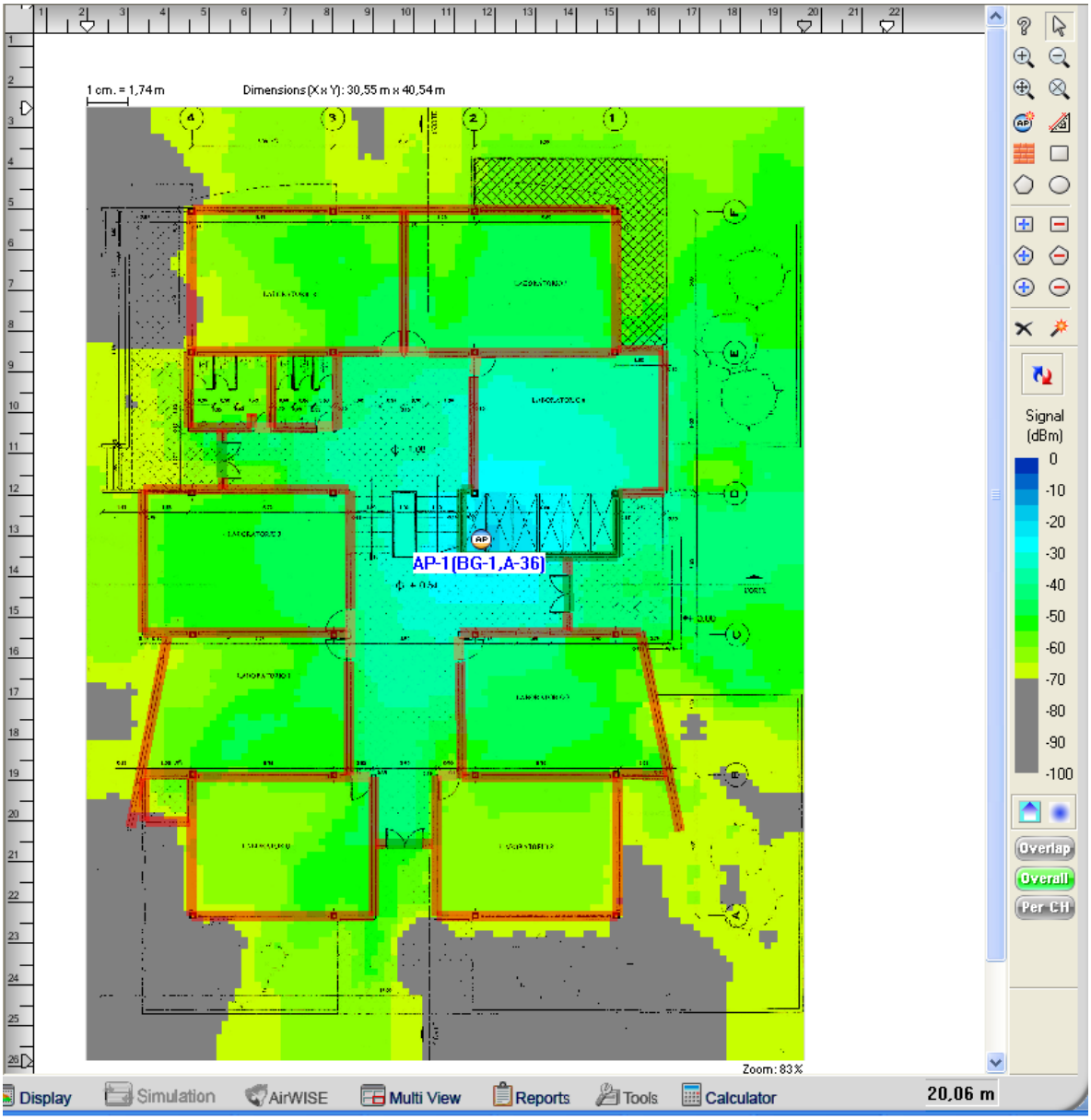


Fig. 6.69: Mapa de señal inalámbrica

Las características del punto de acceso como el tipo de antena y la potencia de transmisión, se pueden ajustar en la sección "Datos de Antenas", que se encuentra en la parte inferior izquierda de la pantalla de trabajo de Planner, mostrada en la Fig. 3. Además, para determinar los parámetros tales como el canal de transmisión, el modo de transmisión (A y BG), la dirección MAC, dirección IP, SSID, el patrón de la antena o la localización de la misma, se hará clic derecho en el punto de acceso, en la opción **Propiedades**.

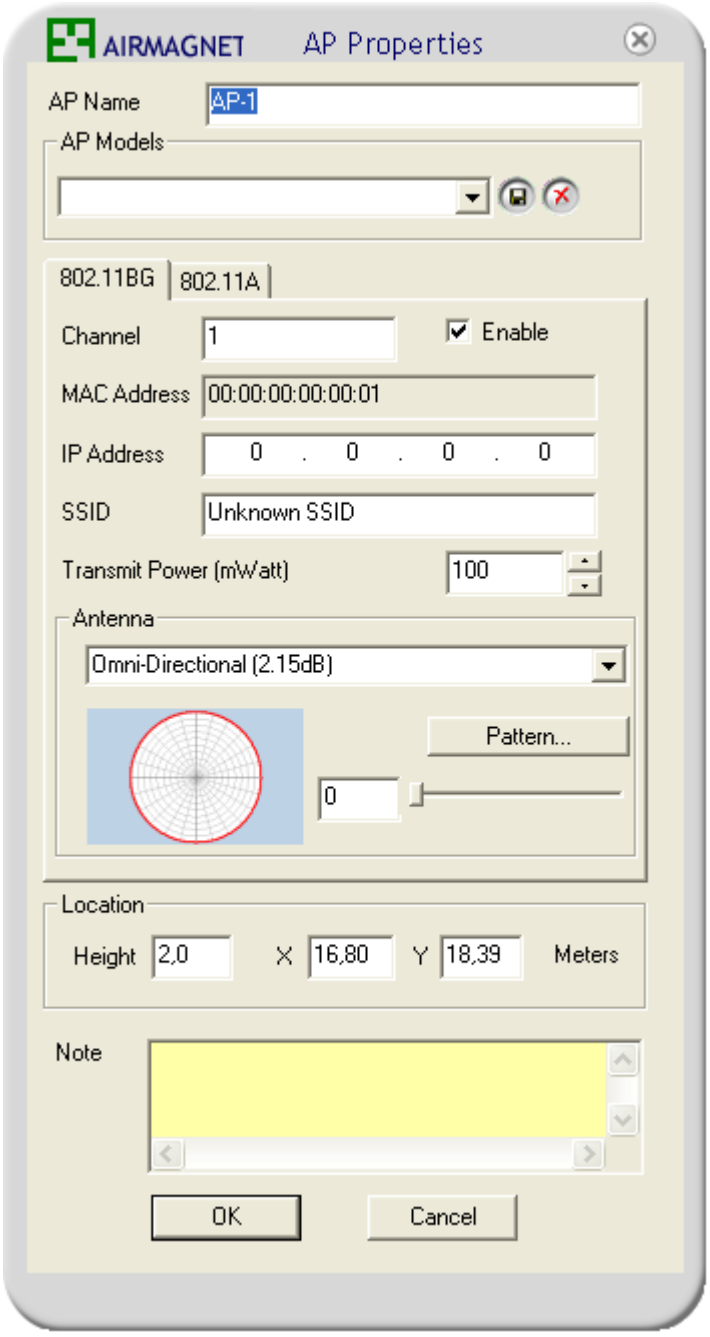


Fig. 6.70: Propiedades del punto de acceso

Este es el instructivo básico de manejo de Planner y con ello será posible determinar las ubicaciones más adecuadas de los puntos de acceso en las plantas del edificio y el alcance teórico de la señal.

El proceso que se ha indicado es el mismo a seguir para las otras plantas en las que se requiera ubicar puntos de acceso.

6.13.3 ANEXO 3: Manual de Daloradius

Daloradius provee el soporte necesario para la administración de usuarios, reportes de su actividad, contabilidad de datos, estadísticas y facturación. Esta última opción estará subutilizada en este caso.

Esta aplicación dispone de variadas opciones para el manejo de un servidor radius, pero dado que muchas de ellas no se aplican a este caso, no serán objeto de mención en este apartado para simplificar su manejo.

A continuación se muestra en la Fig. 6.71 y Fig. 6.72, la página de logueo de daloradius y la página de bienvenida respectivamente.

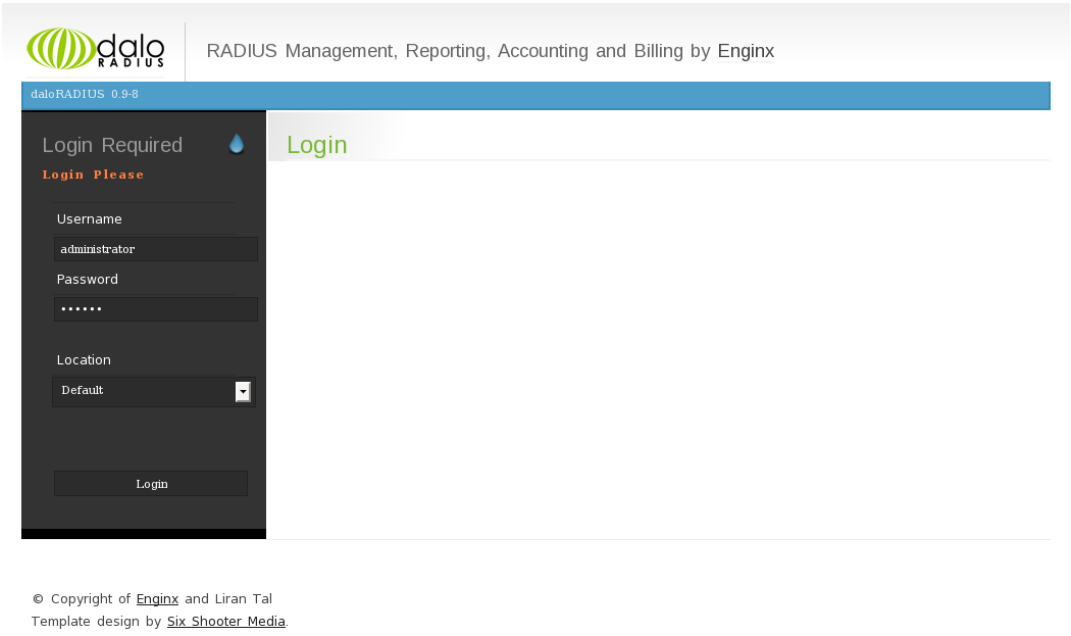


Fig. 6.71: Ingreso a Daloradius

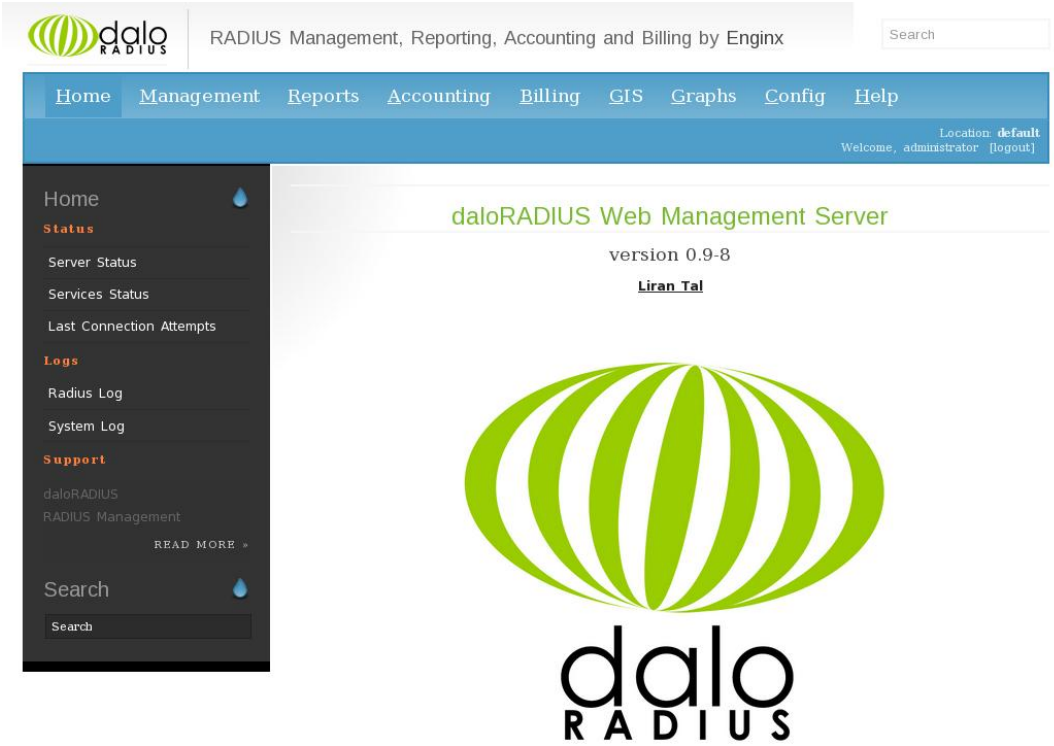


Fig. 6.72: Página de bienvenida

Management

- **Users**

  En este submenú se listan, agregan, buscan, editan y eliminan usuarios. Un usuario se puede agregar por nombre de usuario y contraseña, por MAC o por código PIN, aunque esta última opción no es soportada por Chillispot.

- **Attributes**

  Son parámetros para limitar aspectos de conexión de los usuarios. Por ejemplo, un atributo es el ancho de banda de bajada. Daloradius dispone de varios "Vendors" o "proveedores" de atributos pero en este caso, sólo se utilizan Chillispot y Wispr como vendors puesto que son los únicos para los que Chillispot dispone de soporte.

- **Groups**

  Se utiliza para crear grupos de atributos que posteriormente pueden ser asignados a los usuarios.

- **User-Groups**

  Con esta opción se puede listar a todos los usuarios de la base de datos y verificar el grupo de atributos que tiene asignado cada uno.

La Fig. 6.73 muestra la captura de pantalla de la sección “Management”. En la Fig. 6.74 y Fig. 6.75 se observa la pantalla de atributos y la creación de grupos de atributos respectivamente.

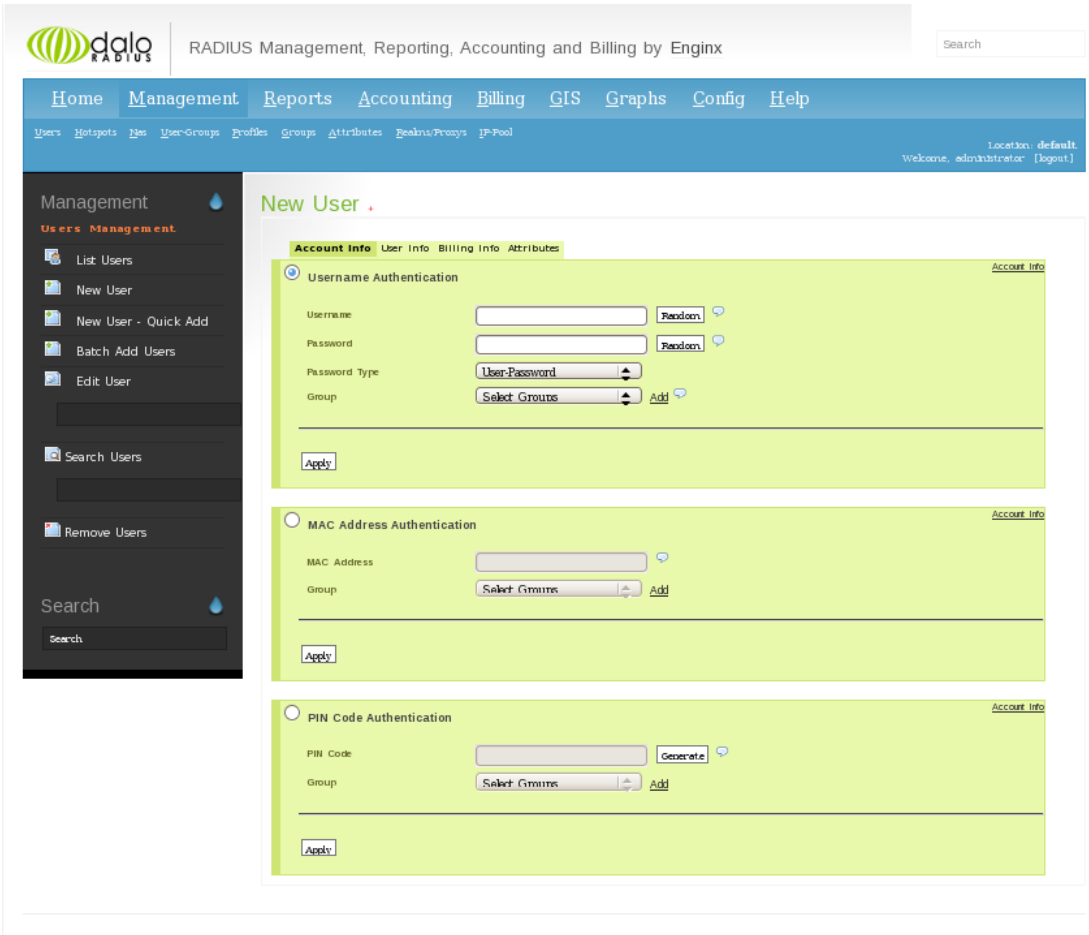


Fig. 6.73: Management

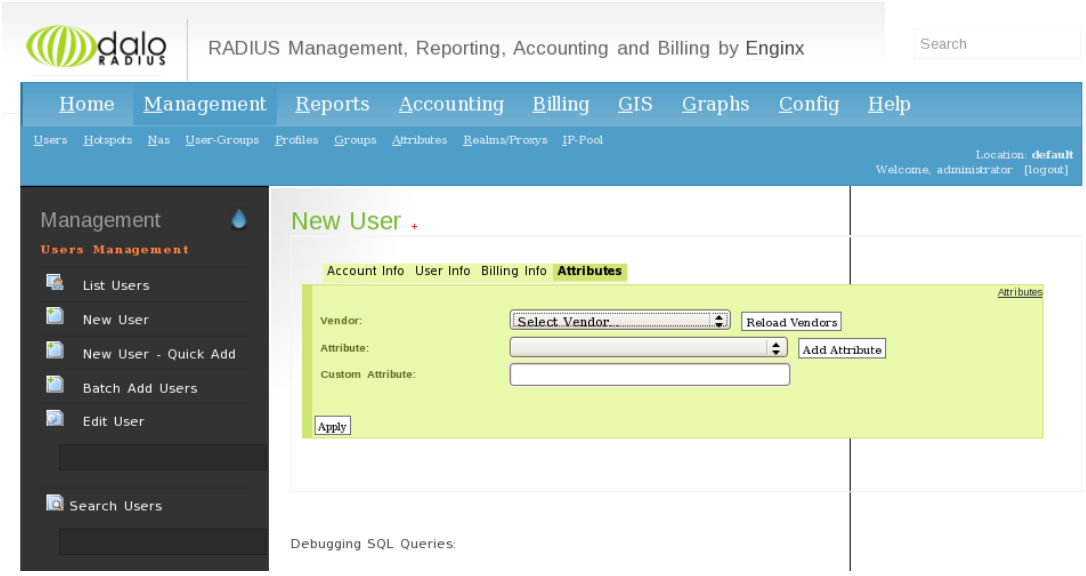


Fig. 6.74: Atributos de usuario

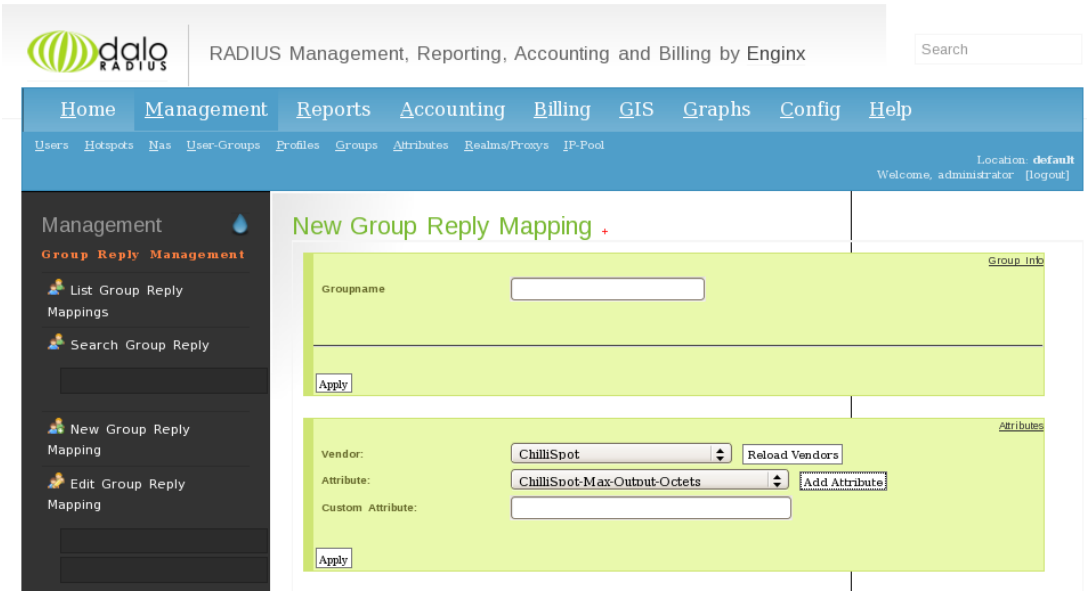


Fig. 6.75: Creación de grupos de atributos

Reports

- **General**

Aquí se puede listar los usuarios conectados en ese instante al servidor radius, los últimos intentos de conexión de determinado usuario, el "top usuarios" en

base a su ancho de banda o al tiempo de conexión, y el historial de modificación de datos hechos en daloradius.

- **Logs**

  En este apartado se tiene el detalle de las últimas actividades que ha realizado daloradius además de registros del sistema. Muy útil cuando se necesita corregir posibles errores.

- **Status**

  Muestra si el servicio radius y mysql se encuentran activos, además de proporcionar información del estado del servidor, incluyendo información de memoria y configuraciónes de las interfaces de red.

En la siguiente imagen se muestra una captura de pantalla de “Reports”:

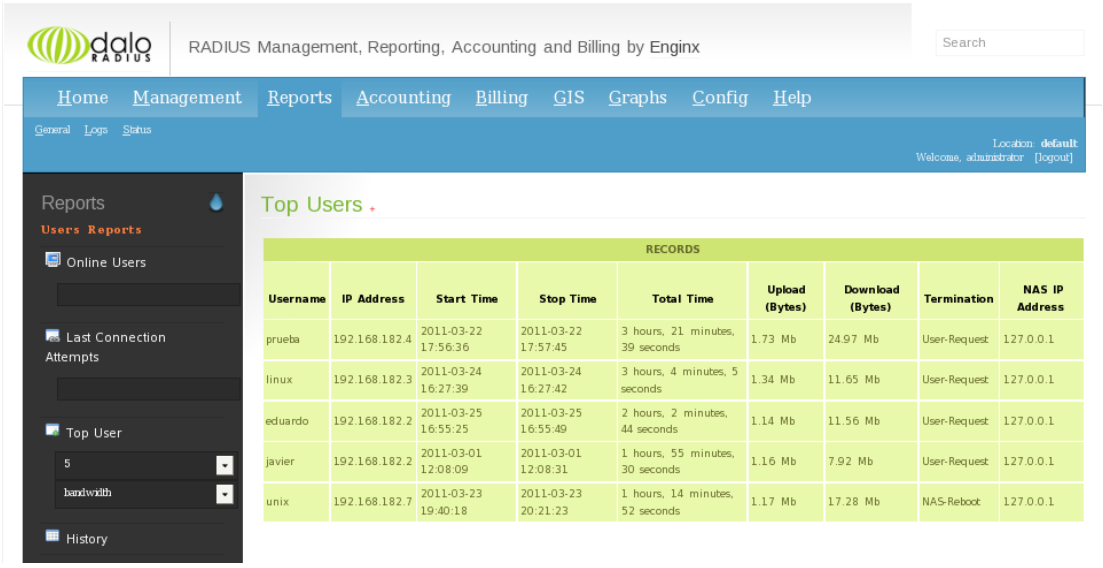


Fig. 6.76: Reports

Accounting

- **General**

  Menú donde se puede consultar registros sobre determinado usuario, que incluye información sobre su dirección IP, tiempos de conexión, y cantidad de datos transmitidos. Es posible hacer esta consulta en la base de datos mediante el nombre de usuario, la dirección IP, o en base a una fecha determinada.

- **Maintenance**

  Sección de mantenimiento que se utiliza para limpiar los registros de uno todos los usuarios en base a determinada fecha.

A continuación una captura de pantalla de la sección "Accounting":

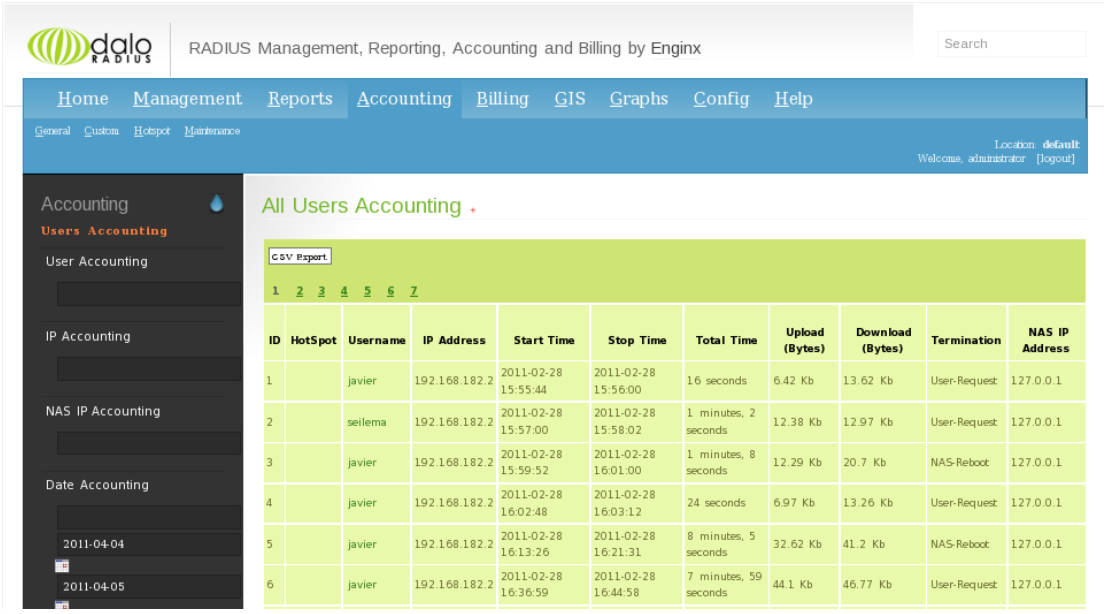


Fig. 6.77: Accounting

Billing

Puesto que daloradius es un software diseñado para hotspots comerciales, dispone de esta característica de facturación que en este caso no es aplicable y no se utiliza. En la Fig. 6.78 se muestra la sección Billing.

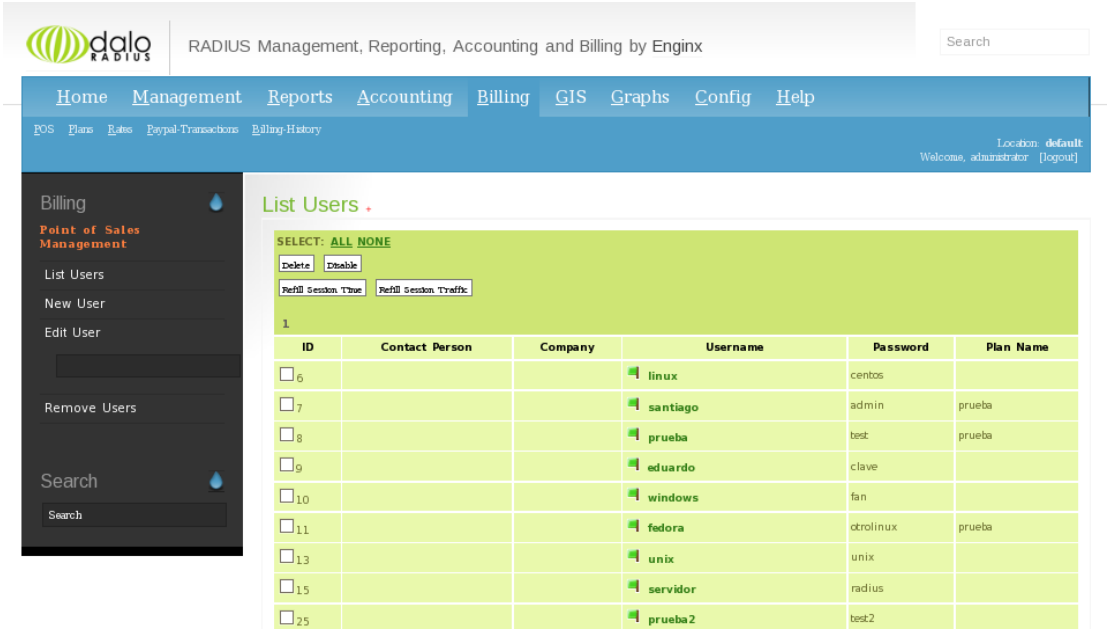


Fig. 6.78: Billing

Graphs

Muestra estadísticas de logueo de usuarios y tamaño de datos subidos y descargados diariamente. La Fig. 6.79 muestra una captura de pantalla de "Graphs".

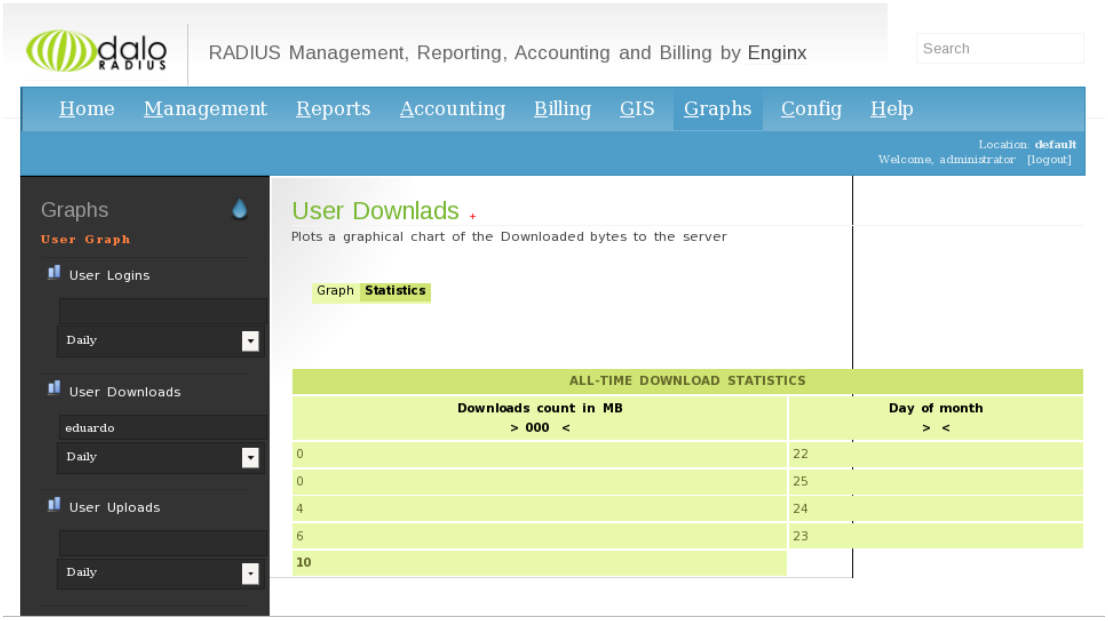


Fig. 6.79: Estadísticas de usuarios

Config

- **General**

  Configuraciones de la base de datos, lenguaje de la aplicación, anotaciones sobre lo que se realiza en daloradius y finalmente, configuración de la interface de la aplicación incluyendo auto-completar, número de resultados por página y ocultación de la contraseña de logueo.

- **Maintenance**

  Aquí se puede hacer pruebas de conectividad de un usuario para determinar si realmente es aceptado o rechazado por el servidor radius. Además se dispone de la opción para forzar la desconexión de algún cliente.

- **Operators**

  Menú que permite listar, crear, editar y eliminar usuarios que administran daloradius.

- **Backup**

  Para administrar y crear respaldos de las tablas del servidor radius y daloradius.

La Fig. 6.80 muestra la sección “Config” en una captura de pantalla.

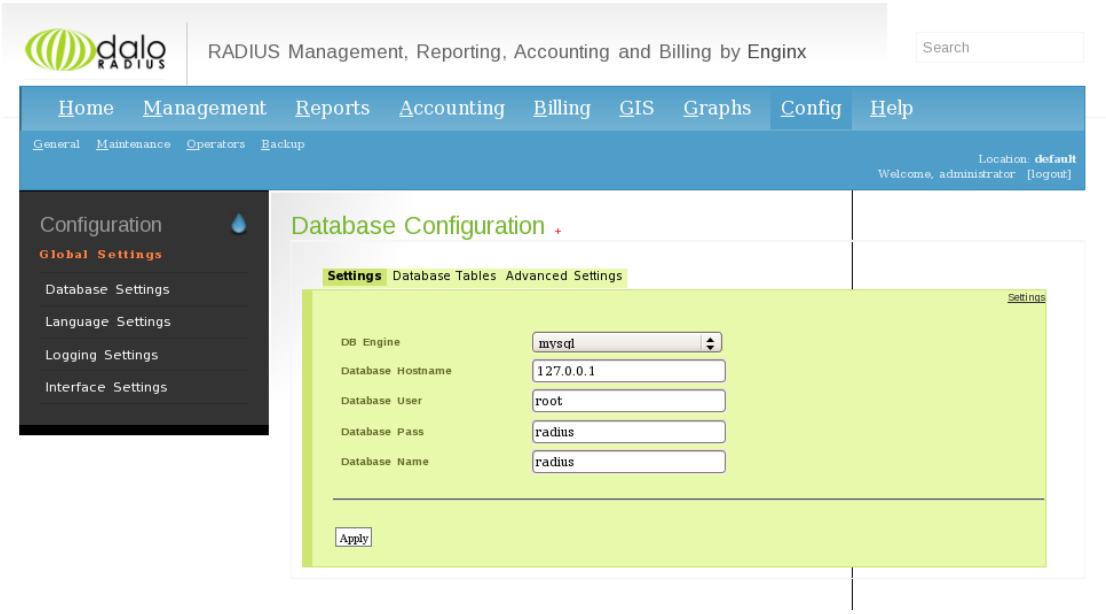


Fig. 6.80: Configuración de la base de datos

Help

El espacio web original de ayuda para daloradius aún se encuentra en construcción, sin embargo, es posible buscar información de soporte en la página web http://daloradius.wiki.sourceforge.net. A continuación una captura de pantalla de la sección “Help”.

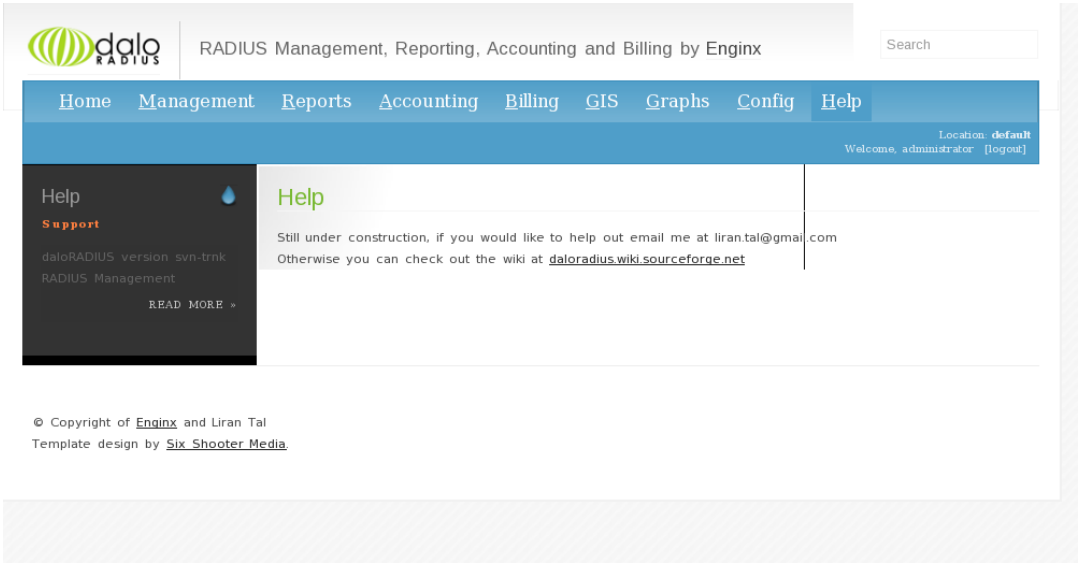


Fig. 6.81: Ayuda

6.13.4 ANEXO 4: Especificaciones del router y puntos de acceso

Especificaciones del router inalámbrico Linksys WRT300n

La siguiente tabla lista las especificaciones del equipo Linksys WRT300n:

Specifications	
Model	WRT300N
Standards	Draft 802.11n, 802.11g, 802.11b, 802.3, 802.3u
Ports	Power, Internet, Ethernet
Button	Reset
Cabling Type	CAT5
LEDs	Power, Internet, Ethernet (1-4), Wireless
Number of Antennas	3
Transmit Power	17 dBm
Antenna Gain	2 dBi
UPnP able/cert	able
Security Features	Up to 256-bit wireless encryption
Security Key Bits	64, 128, 256
Environmental	
Dimensions	7.40" x 1.57" x 6.93" (188 x 40 x 176 mm)
Weight	18.60 oz. (0.527 kg)
Power	12 V, 1 A
Certification	FCC, CE, IC-03
Operating Temp.	0° C to 40° C (32° F to 104° F)
Storage Temp.	-20° C to 70° C (-4° F to 158° F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Tabla 6.8: Especificaciones router inalámbrico Linksys

Especificaciones del punto de acceso 3com 7760

Las tres tablas siguientes listan las características del equipo 3com 7760.

Physical specifications

Feature	Description
Dimensions (H x W x D)	16.5 x 8.3 x 3.2 cm (6.5 x 3.25 x 1.25 in)
Weight	198.0 g (7.0 oz)

Power specifications

Feature	Description
Power consumption	6 W maximum (from PoE port)
Transmit power settings	• **802.11a** : ◦ 6 Mb/s: ≥ +18 dBm ◦ 9 Mb/s: ≥ +18 dBm ◦ 12 Mb/s: ≥ +18 dBm ◦ 18 Mb/s: ≥ +18 dBm ◦ 24 Mb/s: ≥ +18 dBm ◦ 36 Mb/s: ≥ +18 dBm ◦ 48 Mb/s: ≥ +16 dBm ◦ 54 Mb/s: ≥ +16 dBm • **802.11b/g** : ◦ 1 - 11 Mb/s: ≥ +18 dBm ◦ 12 Mb/s: ≥ +18 dBm ◦ 18 Mb/s: ≥ +18 dBm ◦ 24 Mb/s: ≥ +18 dBm ◦ 36 Mb/s: ≥ +18 dBm ◦ 48 Mb/s: ≥ +16 dBm ◦ 54 Mb/s: ≥ +16 dBm

Tabla 6.9: Especificaciones punto de acceso 3com

La tabla 6.7.1 muestra los detalles del ambiente de funcionamiento y más especificaciones técnicas del equipo 3com 7760.

Environmental specifications

Feature	Description
Operating temperature	-10° to 40°C (14° to 104°F)
Storage temperature	-40° to 70°C (-40° to 158°F)
Humidity	10% to 95% non-condensing

Technical specifications

Feature	Description
Media interfaces	• RJ-45, IEEE 802.11a, 802.11b, 802.11g
Data rates	• **802.11g/a** : 54, 48, 36, 24, 18, 12, 9, 6 Mb/s • **802.11b** : 11, 5.5, 2, 1 Mb/s
Frequency band	• **802.11a** : 5 GHz • **802.11b/g** : 2.4 GHz
Operating range	• **802.11a** : Up to 50 m (164 ft) transmit and receive • **802.11b/g** : Up to 100 m (328 ft) transmit and receive
Operating channels	Depends on local country regulations. Choose correct country of operation.
Modulation technique	Direct Sequence Spread Spectrum (DSSS), Orthogonal Frequency Division Multiplexing (OFDM)
Media access protocol	CSMA/CA
Antenna	2 removable 2 dB gain antennas with R-SMA connector

Tabla 6.7.1: Especificaciones del punto de acceso 3com

La tabla siguiente muestra las especificaciones técnicas restantes y sistemas de seguridad del AP 3com 7760.

LEDs	Power, 10/100 Mb/s, 802.11b/g activity, or 11g activity

Receive sensitivity	• **802.11a** :
	  ◦ 6 Mb/s: ≤ -87 dBm
	  ◦ 9 Mb/s: ≤ -86 dBm
	  ◦ 12 Mb/s: ≤ -84 dBm
	  ◦ 18 Mb/s: ≤ -82 dBm
	  ◦ 24 Mb/s: ≤ -79 dBm
	  ◦ 36 Mb/s: ≤ -75 dBm
	  ◦ 48 Mb/s: ≤ -72 dBm
	  ◦ 54 Mb/s: ≤ -71 dBm
	• **802.11b/g** :
	  ◦ 1 Mb/s: ≤ -95 dBm
	  ◦ 2 Mb/s: ≤ -92 dBm
	  ◦ 5.5 Mb/s: ≤ -91 dBm
	  ◦ 6 Mb/s: ≤ -89 dBm
	  ◦ 9 Mb/s: ≤ -88 dBm
	  ◦ 11 Mb/s: ≤ -88 dBm
	  ◦ 12 Mb/s: ≤ -86 dBm
	  ◦ 18 Mb/s: ≤ -84 dBm
	  ◦ 24 Mb/s: ≤ -81 dBm
	  ◦ 36 Mb/s: ≤ -77 dBm
	  ◦ 48 Mb/s: ≤ -73 dBm
	  ◦ 54 Mb/s: ≤ -72 dBm

Safety certifications and protocols

Feature	Description
Security	WPA2 AEs and TKIP encryption; 64/128/152-bit WEP encryption; 802.1X with EAP-TLS, EAP-TTLS, and PEAP; WPA-PSK authentication; MAC address authentication and filtering; 802.1Q VLAN; multiple SSID; RADIUS client authentication, authorization, and accounting
Networking protocols	TCP/IP, Bridging protocol, DHCP, HTTP, FTP

Tabla 6.7.2: Especificaciones del punto de acceso 3com

Especificaciones del punto de acceso Cisco WAP200E

Las tablas 6.8 y 6.8.1 listan las especificaciones del punto de acceso Cisco WAP200E, ubicado en el edificio principal de la FISEI.

Specifications	
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, IEEE 802.3af (PoE), 802.1p (QoS priority), 802.1Q (VLAN), 802.1X (security authentication), 802.11i ready (security WPA2)
Ports	1 Ethernet, 1 external antenna
Buttons	Reset
Cabling type	Unshielded twisted pair (UTP) Category 5
LEDs	Power, Ethernet, Wireless
Operating system	Linux
Setup/Configuration	
Web user interface	Built-in web user interface for easy browser-based configuration (HTTP/HTTPS)
Static IP	Yes
Dynamic Host Configuration Protocol (DHCP) client	Yes
Management	
Event logging	Yes
Web firmware upgrade	Yes
Operating Modes	
Access point	Access point mode, point-to-point bridge mode, point-to-multipoint bridge mode, repeater mode
Wireless	
Spec/modulation	802.11b/direct sequence spread spectrum (DSSS), 802.11g/orthogonal frequency division multiplexing (ODFM)
Data rates	802.11b: 1, 2, 5.5, 11 Mbps; 802.11g: 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Channels	11 North America, 13 Europe (ETSI and Japan) auto-channel selection
Number of internal antennas	2 at 6 dBi (directional)
Antenna connector type	Reverse polarity female N-type
Detachable antenna	Yes (sold separately)
RF power (Effective Isotropic Radiated Power [EIRP])	802.11g: typical 16.5 dBm, 802.11b: typical 17 dBm
Antenna gain	Internal antenna: 6 dBi
Adjustable power	Yes
Receiver sensitivity	802.11g: 54 Mbps at -65 dBm, 802.11b: 11 Mbps at -85 dBM

Tabla 6.10: Especificaciones punto de acceso Cisco WAP200E

La tabla 6.8.1 especifica las características de seguridad, parámetros físicos y de funcionamiento del equipo Cisco WAP200E.

Security	
WEP/WPA/WPA2	WEP, WPA-PSK, WPA2-PSK, WPA Enterprise, WPA2 Enterprise
Connection control	Wireless connection control: MAC based
SSID broadcast	SSID broadcast enable/disable
Web-based utility access control	HTTP/HTTPS, wireless client web GUI access control
Wireless Security	
WEP bits	64, 128
WPA bits and parameters	128 - Temporal Key Integrity Protocol (TKIP)/Advanced Encryption Standard (AES)
WPA2 bits and parameters	256 - AES
SSID broadcast on/off	Yes
Client isolation	Yes
MAC-based wireless connection control	Yes
Wireless web GUI access on/off	Yes
Environmental	
Dimensions **W x H x D**	6.42 x 8.07 x 2.17 in. (163 x 205 x 55 mm)
Unit weight	2.47 lb (1.121 kg)
Mounting options	Industrial-strength, weather-resistant housing, lightning protection for outdoor enclosure, ceiling or wall mountable
Power	• 48V DC • Maximum power draw: 4.8W
PoE in	Yes
Certification	FCC, IC,CE
Operating temperature	-4° to 140°F (-20° to 60°C)
Storage temperature	-4° to 140°F (-20° to 60°C)
Operating humidity	5% to 95%, noncondensing
Storage humidity	5% to 95%, noncondensing

Tabla 6.8.1: Especificaciones del punto de acceso Cisco WAP200E

Especificaciones del punto de acceso Cisco WAP4410N

A continuación se muestran las tablas 6.9 y 6.9.1 que listan las especificaciones técnicas de este equipo ubicado en el edificio dos de la FISEI. Cabe recalcar que existen dos equipos de este modelo en el edificio indicado.

WAP4410N Specifications

Model	WAP4410N
Standards	Draft IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power Over Ethernet), 802.1x (Security Authentication), 802.11i Security WPA/WPA2, WMM
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP Cat 5e or higher
LEDs	Power, Ethernet, Wireless, POE
Operating System	Linux
Web UI	Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
Event Logging	Email logging, Remote Syslog
Web F/W Upgrade	Firmware upgradeable through web-browser
DHCP	DHCP Client
WEP/WPA/WPA2	WEP 64bit/128bit, WPA-TKIP, WPA2-AES, WPA-Enterprise, and WPA2-Enterprise
Access Control	Wireless Connection Control: MAC-Based
SSID Broadcast	SSID Broadcast Enable/Disable
Radius Server	Up to 2 Radius Servers can be configured for redundancy purposes
WPS	Supports WPS (WiFi Protected Setup), which is a WIFI Alliance specification for simple and secure setup of a wireless network.

Tabla 6.11: Especificaciones punto de accceso Cisco WAP4410N

La tabla 6.9.1 especifíca parámetros de transmisión, recepción y características eléctricas del equipo Cisco WAP4410N.

QoS	4 queues, 802.1p VLAN priority, WMM Wireless priority, Mapping of 802.1p priority to WMM priority to maintain end-to-end QoS
Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 11g/OFDM, 11n/MIMO-OFDM
Channels	Operating Channels: 11 North America, 13 Most of Europe (ETSI and Japan)
Internal Antenna	None
External Antennas	3 (omni-directional)
Transmit Power	Transmit Power at Normal Temp Range for FCC: 11b - 16 dBm@1TX, 19 dBm@2TX, 20.5dbm@3TX; 11g - 13 dBm@1TX, 16 dBm@2TX, 19dbm@3TX 11n - 20 dBm@MCSO~4/8~12, 18dBm@MCS5/13, 14dBm@MCS6/14, 12dBm@MCS7/15 Transmit Power at Normal Temp Range for ETSI: 11b/g/n: 18.5dBm
Antenna Gain in dBi	2
Receiver Sensitivity	11.n: 300Mbps@ -69dBm, 11.g: 54Mbps@ -73dBm, 11.b: 11Mbps@ -88dBm
Device Dimensions	6.69X6.69X1.60 inches (170X170X40.7mm) 0.86 lbs. (0.39 kg)
Power	12V 1A DC input, and IEEE802.3af Compliant PoE. Maximum power draw is 10.1 Watts.

Tabla 6.9.1: Especificaciones del punto de acceso Cisco WAP4410N