



UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO

FACULTAD DE INGENIERÍA

“IMPLEMENTACIÓN Y
AUTOMATIZACIÓN DE LA RED
INALÁMBRICA EN LAS
BIBLIOTECAS DE LA
FACULTAD DE INGENIERÍA”

T E S I S
QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN PRESENTAN:

HERNANDEZ MORENO ENRIQUE
ROMERO BARRANCO ADRIAN
TREJO CRUZ ULISES BERNARDO

DIRECTOR DE TESIS: ING. FILIBERTO MANZO
GONZÁLEZ



MÉXICO, D. F.

2011



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

*A Graciela Moreno Servín, mujer
de una increíble experiencia natural,
"Mamá de mil brazos y mil acciones".*

A todos mis hermanos, por haber crecido conmigo.

*A mis compañeros de Tesis Adrián y Ulises
por tener la paciencia para acabar este trabajo.*

Por los amigos.

Gracias:

*A todos y cada uno de ustedes
pues son tan importantes
e indispensables en mi vida cotidiana
es bueno saber que cuento con ustedes
con su apoyo, comprensión, y consejo.*

*Por eso y muchas cosas más,
les brindo este logro con mucho cariño.*

*"Si no sabes explicar algo de
manera sencilla,
es que no lo entiendes del todo".
Albert Einstein*

Enrique

*A mi familia la cual me
brindo la confianza y el
apoyo a lo largo de todo
este tiempo.*

*A mis tías Esther, Beatriz e
Irene, gracias por quererme
como a un hijo.*

A mi esposa Claudia Ríos, te amo.

*A mis amigos de la Facultad
de Ingeniería de los cuales
aprendí mucho y compartí momentos
inolvidables.*

*A mis profesores que fueron
ejemplo y guía durante la carrera.*

*A todos aquellos que estuvieron
y están conmigo y han sido
parte importante de este
proyecto de vida.*

*Gracias a la Universidad, estoy
orgulloso de ser parte de esta comunidad
Universitaria.*

Adrián

*Quiero dedicar este logro a mis
padres BERNARDO y MANUELA
ya que con sus enormes sacrificios
es que he podido realizar este sueño,
este éxito también es de ustedes,
los amo.*

*A mis hermanas y hermano
VIOLETA, AZUCENA, TANIA y NOE
por formar parte de mí vida, sé que
cuento con ustedes, esto también es
por ustedes.*

*A CRIS por estar conmigo a pesar de
todos mis defectos y apoyarme
siempre, te amo mi princess.*

*A mis AMIGOS que siempre me
brindaron una palabra de aliento
y superación.*

*A la UNAM y a la FACULTAD DE
INGENIERIA siempre tendré su
escudo en mí corazón.*

*Y a todas las personas que son
parte de mí vida y que siempre
y me han apoyado.*

Ulises

Índice

Contenido	Página
Introducción.....	1
Capítulo I	
Antecedentes.....	4
1.1 Conceptos de una red de datos.....	5
1.1.1 Red de computadoras.....	5
1.1.2 Medios de Transmisión.....	5
1.1.2.1 Coaxial.....	5
1.1.2.2 Fibra óptica.....	6
1.1.2.3 Par trenzado.....	11
1.1.3 Cableado estructurado.....	12
1.1.3.1 Subsistema de cableado estructurado.....	12
1.1.4 Topologías.....	16
1.1.4.1 Tipos de topologías.....	16
1.1.5 Servidores.....	18
1.1.5.1 Tipos de servidores.....	19
1.1.6 Modelo OSI.....	22
1.1.6.1 Historia.....	22
1.1.6.2 Modelo de referencia OSI.....	23
1.2 Redes inalámbricas.....	29
1.2.1 Concepto de red inalámbrica.....	29
1.2.2 Orígenes.....	31
1.3 Aplicaciones.....	32
1.4 Ventajas y desventajas de las redes inalámbricas.....	33
1.5 Access Point.....	35
1.6 Antenas.....	36
1.6.1 El radiador isotrópico.....	36
1.6.2 Patrón de irradiación de una antena.....	38
1.6.3 Impedancia, frecuencia resonante.....	39
1.6.3.1 Frecuencia resonante.....	40
1.6.3.2 Impedancia.....	40
1.6.4 Tipos de antenas.....	40
1.6.4.1 Antenas de Sector.....	41
1.6.4.2 Antenas de Panel.....	41
1.6.4.3 Antenas Yagi.....	42
1.6.4.4 Antenas Parabólicas.....	42
1.6.4.5 Antenas Dipolo.....	43
1.7 Estándares y protocolos de las redes inalámbricas.....	43
1.7.1 Protocolos.....	43
1.8 Canales y frecuencias.....	48
1.9 Tipo de redes inalámbricas.....	50
1.10 Topologías.....	55
1.10.1 AD-HOC.....	55
1.10.2 Infraestructura.....	56
1.11 Tipos de encriptación para punto de acceso en redes inalámbricas.....	57

1.11.1 WEP (Wired Equivalent Privacy).....	57
1.11.2 WPA (Wi-Fi Protected Access).....	58
1.11.3 WPA2.....	60
 Capítulo II	
Infraestructura de la Biblioteca.....	61
2.1 Marco histórico de la biblioteca Antonio Dovalí Jaime.....	62
2.2 Marco histórico de la biblioteca Enrique Rivero Borrell.....	63
2.3 Problemática de las Bibliotecas.....	66
2.4 Espacio Físico de la biblioteca.....	67
2.4.1 Primer nivel: sótano de biblioteca.....	68
2.4.2 Segundo nivel planta baja de la biblioteca.....	68
2.4.3 Tercer nivel primer piso de la biblioteca.....	69
2.4.4 Cuarto nivel segundo piso de la biblioteca.....	70
2.4.5 Quinto nivel tercer piso de la biblioteca.....	70
2.5 Red de datos de la biblioteca Enrique Rivero Borrell.....	71
2.5.1 Los subsistemas que componen el sistema de cableado de la Biblioteca.....	71
2.6 Croquis de red de la Biblioteca Enrique Rivero Borrell.....	74
 Capítulo III	
Análisis y diseño de la red inalámbrica.....	78
3.1 Análisis de la Biblioteca Enrique Rivero Borrell.....	79
3.1.1 Análisis de infraestructura.....	80
3.2 Necesidades actuales de la Biblioteca Enrique Rivero Borrell.....	88
3.2.1 Aplicaciones y servicio de red.....	90
3.2.2 Conectividad.....	93
3.2.3 Interoperabilidad.....	93
3.2.4 Capacidad de desempeño.....	93
3.2.5 Administración.....	94
3.2.6 Tolerancia a fallos.....	94
3.2.7 Flexibilidad topológica.....	94
3.2.8 Documentación.....	95
3.3 Diseño y solución.....	95
3.3.1 Arquitectura.....	99
3.3.1.1 Red inalámbrica para alumnos de la Facultad de Ingeniería.....	100
3.3.2 Mecanismos de acceso y filtrado.....	101
3.3.2.1 Bases para el diseño del firewall.....	101
3.3.2.2 Políticas del firewall.....	102
3.3.2.3 Política interna de la red inalámbrica.....	103
3.3.2.4 Componentes del acceso a la red.....	103
3.4 Administración de subredes y direcciones IP.....	104
3.4.1 NAT.....	104

3.4.2 DHCP.....	105
3.5 Administración de Contenido en páginas WEB.....	105
Capítulo IV	
Automatización del Registro para Acceder a la red Inalámbrica.....	106
4.1 Análisis.....	107
4.1.1. Requerimientos generales del sistema de registro.....	109
4.2 Configuración general de los servicios del sistema de registro.....	111
4.2.1 Ports o paquetes precompilados.....	114
4.3 Beneficios del sistema de registro vía Web.....	115
4.3.1 Pasos para la inscripción en línea.....	116
4.3.2 Diagrama de flujo del proceso de inscripción en línea.....	118
4.3.3 Pantallas de la página de inscripción en línea.....	122
Conclusiones.....	134
Anexos.....	138
Anexo 1 Implementación.....	139
Anexo 2 Instalación de OpenBSD 4.5.....	142
Anexo 3 Actualización de OpenBSD.....	155
Anexo 4 Configuración de las tarjetas de red y del servidor NAT en OpenBSD.....	158
Anexo 5 Configuración del Bridge y filtrado MAC.....	161
Anexo 6 Servidor DHCP en OpenBSD.....	163
Anexo 7 Servidor de correos.....	166
Anexo 8 Apache, PHP y MySQL en OpenBSD 4.5.....	168
Anexo 9 Instalación y configuración de phpMyAdmin.....	177
Anexo 10 Servidor Radius en OpenBSD.....	179
Anexo 11 Filtrado de contenido con Squid.....	187
Anexo 12 Políticas del servicio.....	190
Anexo 13 Base de datos.....	193
Ápndice.....	195
Glosario.....	198
Bibliografía.....	208

INTRODUCCIÓN

El mundo de las comunicaciones ha tenido una serie de cambios muy importantes en los últimos años, uno de estos cambios ha sido el de prescindir de cables para comunicar dos o más dispositivos, esto se logra a través de las redes inalámbricas. Los dispositivos que hasta hace algunos años tenían conexión a través de un medio físico cableado y que tenían una ubicación física determinada como un teléfono, una computadora o una impresora están pasando en un porcentaje elevado a ser definitivamente de conexión inalámbrica.

Las redes inalámbricas están ganando mucha popularidad debido a su facilidad de uso e implementación, bajo costo, rango de cobertura, cantidad de servicios que ofrecen y aplicaciones que se van descubriendo para ellas continuamente.

Con el uso de las redes inalámbricas eliminamos la necesidad de usar cables y establecemos nuevas aplicaciones añadiendo flexibilidad a la red incrementando la productividad y eficiencia en los lugares donde se encuentran instaladas. Hoy en día podemos estar conectados a una red de datos mediante un dispositivo móvil en nuestro lugar de trabajo, nuestro hogar, parques, hoteles, restaurantes y en lugares de difícil acceso donde antes era inconcebible pensar tener comunicación.

Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios e inclusive áreas metropolitanas con la misma eficiencia que una red convencional aparte de contar con una movilidad y una cobertura mayor.

En esta Tesis se presenta una propuesta de red inalámbrica para implementarla en la biblioteca Enrique Rivero Borrell de la facultad

de Ingeniería, esta red pretende incrementar la cobertura de los servicios de internet dentro de la biblioteca y así solventar algunas necesidades que se tienen en cuanto a comunicaciones y servicios. Con esto se pretende ofrecer una herramienta para la formación profesional de los alumnos de esta facultad.

También se busca integrar un sistema para el registro de los usuarios que deseen tener acceso al servicio de Biblioteca Digital, este sistema ayudará en la administración de la red inalámbrica y agilizará este registro que se podrá hacer vía web.

CAPÍTULO I

ANTECEDENTES

1.1 Conceptos de una red de datos.

1.1.1 Red de computadoras.

Una red de computadoras (también llamada red de datos) es un conjunto de computadoras y/o dispositivos conectados por enlaces, a través de medios físicos (medios guiados) o inalámbricos (medios no guiados) y que comparten información (archivos), recursos (CD-ROM, impresoras, etcétera.) y servicios (e-mail, chat, juegos), etcétera.

1.1.2 Medios de Transmisión.

Normalmente son utilizados tres tipos de cables en las redes locales:

1.1.2.1 Coaxial.

Tiene un gran ancho de banda. Tiene una baja sensibilidad a EMI (Electromagnetic Interference). Se pueden alcanzar longitudes moderadas (200 a 300 mts) y es de costo mediano.

Usa un conector tipo T para conectar los dispositivos al medio. También puede usar un transceiver para tener una entrada tipo AUI (Attachment Unit Interface). El transceiver tiene que ser compatible respecto a la frecuencia a la que trabaja la red.

Hay dos tipos de cable coaxial:

- Cable fino (Thinnet).
- Cable grueso (Thicknet).

El tipo de cable coaxial más apropiado depende de las necesidades de la red en particular.

El cable Thinnet es un cable coaxial flexible de unos 0,64 centímetros de grueso (0,25 pulgadas). Este tipo de cable se puede

utilizar para la mayoría de los tipos de instalaciones de redes, ya que es un cable flexible y fácil de manejar.

El cable coaxial Thinnet puede transportar una señal hasta una distancia aproximada de 185 metros (unos 607 pies) antes de que la señal comience a sufrir atenuación.

1.1.2.2 Fibra óptica.

En un cable de fibra óptica, la fibra óptica lleva las señales digitales (datos) en la forma de pulsos modulados de luz. Ésta es una forma relativamente segura de enviar datos ya que no hay impulsos eléctricos dentro del cable de fibra óptica. Esto significa que la fibra óptica no puede ser "espiada" y los datos robados, que sí se puede hacer con los cables de cobre que llevan los datos como señales electrónicas.

El cable de fibra óptica es bueno para transmisiones muy rápidas y de alta capacidad debido a su carencia de atenuación y a la fidelidad de la señal. La fibra óptica consiste en un cilindro de vidrio extremadamente delgado, llamado el núcleo, rodeado por una cubierta concéntrica de vidrio, conocida como cladding. A veces la fibra está hecha de plástico. El plástico es más fácil de instalar, pero no puede llevar los pulsos de luz tan lejos como el vidrio.

Cada fibra pasa las señales en sólo una dirección, así que el cable consiste de dos o más fibras en cubiertas separadas. Uno para recibir y otro para enviar. Una capa de plástico de refuerzo rodea cada fibra y le da flexibilidad. Por último una capa de kevlar le provee de fuerza.

Tipos de fibra óptica.

Básicamente, existen dos tipos de fibra óptica: multimodo y monomodo.

Fibra óptica multimodo.

Este tipo de fibra fue el primero en fabricarse y comercializarse. Su nombre proviene del hecho de que transporta múltiples modos de forma simultánea, ya que este tipo de fibra se caracteriza por tener un diámetro del núcleo mucho mayor que las fibras monomodo.

El mayor diámetro del núcleo facilita el acoplamiento de la fibra, pero su principal inconveniente es que tiene un ancho de banda reducido como consecuencia de la dispersión modal. Los diámetros de núcleo y cubierta típicos de estas fibras son 50/125 y 62,5/125 mm.

La fibra óptica multimodo es adecuada para distancias cortas, como por ejemplo redes LAN o sistemas de video vigilancia.

Fibra óptica multimodo índice escalonado.

En este tipo de fibra óptica viajan varios rayos ópticos simultáneamente. Éstos se reflejan con diferentes ángulos sobre las paredes del núcleo, por lo que recorren diferentes distancias, y se desfasan en su viaje dentro de la fibra, razón por la cual la distancia de transmisión es corta.

Hay que destacar que hay un límite al ángulo de inserción del rayo luminoso dentro de la fibra óptica, si este límite se pasa el rayo de luz ya no se reflejará, sino que se refractará y no continuará el curso deseado (Figura 1.1).

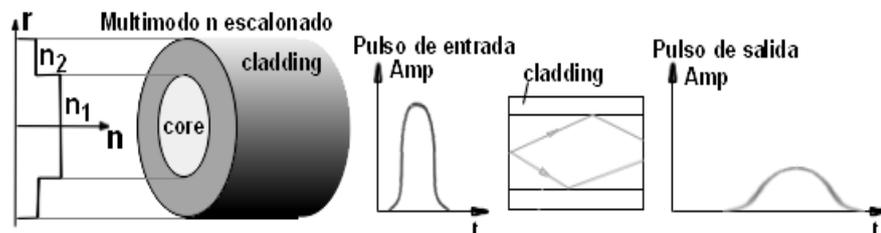


Figura 1.1 Fibra óptica multimodo índice escalonado.

Fibra óptica multimodo índice gradual.

En este tipo de fibra óptica, el núcleo está constituido de varias capas concéntricas de material óptico con diferentes índices de refracción, causando que el rayo de luz de refracte poco a poco mientras viaja por el núcleo.

En estas fibras el número de rayos ópticos diferentes que viajan es menor que en el caso de la fibra multimodo índice escalonado y por lo tanto, su distancia de propagación es mayor (Figura 1.2).

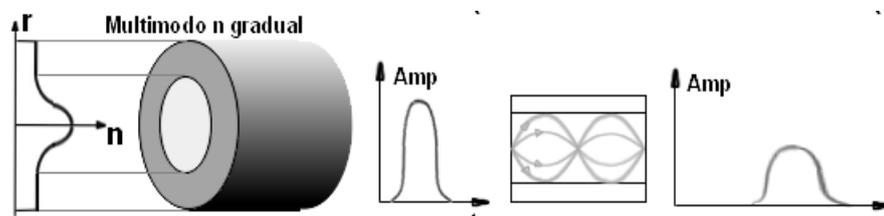


Figura 1.2 Fibra óptica multimodo índice gradual.

Fibra óptica monomodo.

Las fibras ópticas monomodo tienen un diámetro del núcleo mucho menor, lo que permite que se transmita un único modo y se evite la dispersión multimodal. Los diámetros de núcleo y cubierta típicos para estas fibras son de 9/125 mm.

Las fibras monomodo también se caracterizan por una menor atenuación que las fibras multimodo, aunque como desventaja resulta más complicado el acoplamiento de la luz y las tolerancias de los conectores y empalmes son más estrictas. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit, las cuales vienen limitadas principalmente por la dispersión cromática y los efectos no lineales.

Los diámetros de núcleo y cubierta típicos para estas fibras son de 9/125 mm.

La fibra óptica monomodo está diseñada para sistemas de comunicaciones ópticas de larga distancia (Figura 1.3).

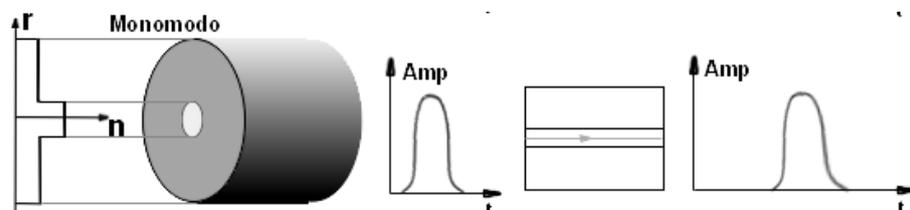


Figura 1.3 Fibra óptica monomodo.

Tipos de conectores para fibra óptica.

Éstos se encargan de conectar las líneas de fibra a un elemento, ya puede ser un transmisor o un receptor. Los tipos de conectores disponibles son muy variados, entre los que se pueden encontrar están los siguientes (Figura 1.4):

- FC, que se usa en la transmisión de datos y en las telecomunicaciones.
- FDDI, se usa para redes de fibra óptica.
- LC y MT-Array que se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC se usa en redes de edificios y en sistemas de seguridad.

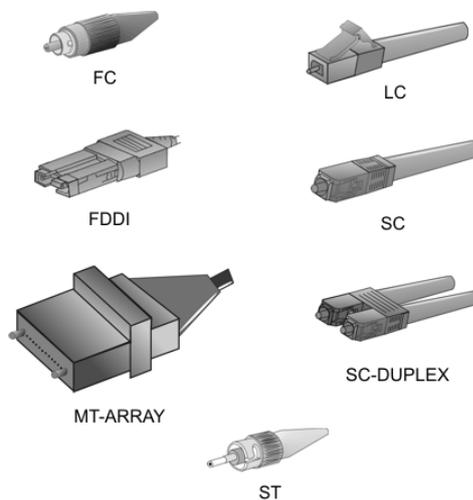


Figura 1.4 Tipos de conectores para fibra óptica.

1.1.2.3 Par trenzado.

Un cable de par trenzado es uno de los tipos de cables de pares compuesto por hilos, normalmente de cobre, trenzados entre sí. Hay cables de 2, 4, 25 o 100 pares de hilos e incluso de más. El trenzado mantiene estable las propiedades eléctricas a lo largo de toda la longitud del cable y reduce las interferencias creadas por los hilos adyacentes en los cables compuestos por varios pares.

Aún teniendo trenzado a veces es necesario apantallar estos cables con un recubrimiento metálico o incluso apantallar cada par trenzado dentro del cable completo para evitar interferencias entre éstos. Definimos 3 tipos básicos de pares trenzados según su recubrimiento:

- UTP: (Unshielded Twisted Pair) Sin ningún tipo de recubrimiento metálico.
- STP: (Shielded Twisted Pair) Recubrimiento metálico alrededor del cable completo.
- S/STP: (Screened STP) Recubrimiento metálico alrededor de cada par trenzado y del cable completo.

Categorías de UTP.

Las Categorías de UTP se muestran en la Tabla 1.1.

Tabla 1.1 Categorías de UTP.

Categoría	Características
1	Se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos, trabaja en una frecuencia de 4 MHz.
2	Puede transmitir datos a velocidades de hasta 4 Mbps, trabaja en una frecuencia de 5 MHz.
3	Se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps, trabaja en una frecuencia de 16 MHz.

4	Se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps, trabaja en una frecuencia de 20 MHz.
5	El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps, trabaja en una frecuencia de 100 MHz.
5e	Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque sí está diferenciada por los diferentes organismos.
6	Puede transmitir velocidades de hasta 1000 Mbps, trabaja en una frecuencia de 250 MHz.
7	Esta categoría no está estandarizada, se espera que cumpla los requisitos exigidos para el nuevo estándar 10GBaseT. Se supone que no utilizará el viejo conector RJ45, ya que la propuesta es utilizar un conector Nexans GG45 que es compatible con los RJ45. La novedad es que el nuevo conector tiene la apariencia de un RJ45 de 8 conectores al que se le han añadido 4 en la parte inferior.

1.1.3 Cableado estructurado.

Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. Las características e instalación de estos elementos se debe hacer en cumplimiento de estándares para que califiquen como cableado estructurado.

El propósito del cableado estructurado, es el de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

1.1.3.1 Subsistema de cableado estructurado.

Una solución de cableado estructurado se divide en una serie de subsistemas. Cada subsistema tiene una variedad de cables y productos diseñados para proporcionar una solución adecuada para cada caso (Figura 1.5).

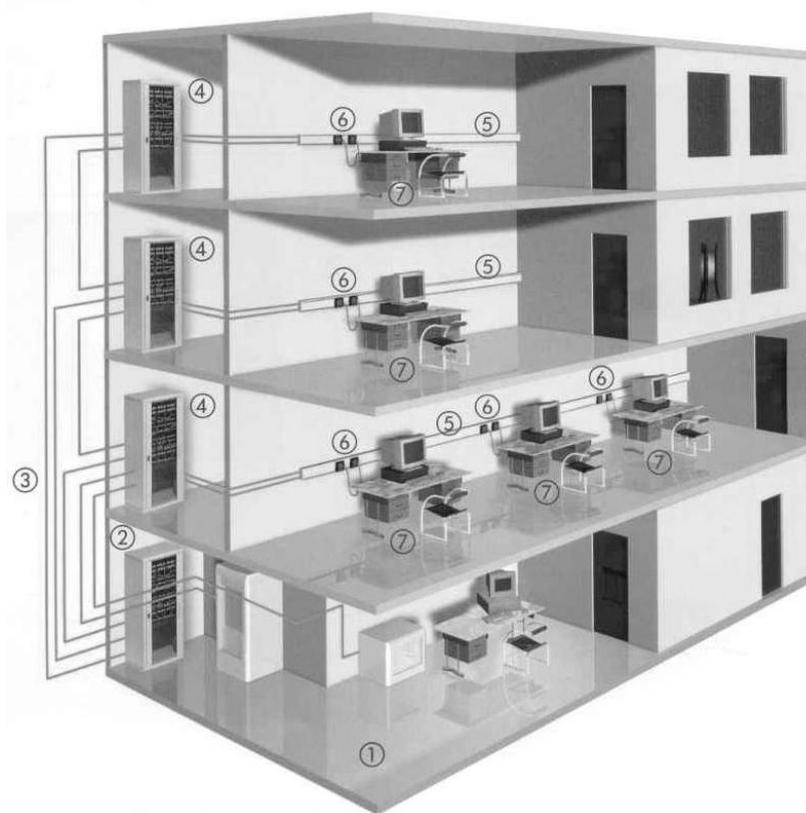


Figura 1.5 Subsistema de cableado estructurado.

1. Subsistema de administración.
2. Rack Principal.
3. Cableado horizontal.
4. Rack de planta.
5. Cableado vertical.
6. Tomas de usuario.
7. Área de trabajo.

1. Subsistema de administración.

En este subsistema se incluyen todos los componentes que se colocan dentro del cuarto de administración del piso y que permiten la conexión y administración de las distintas plantas que conforman el edificio o campus. Aquí encontramos los

bloques de conexión de diferentes tipos de cables y conectores por ejemplo, paneles de conexión tipo RJ45, las cajas terminales de acometida de fibra óptica con conectores adecuados, los armarios o rack's que sirven para la fijación de equipo de comunicación como podrían ser switch, hub, organizadores, patch panel, etcétera.

2. Rack principal.

En este rack o bastidor se aloja el equipo electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante. Se encuentran los dispositivos y equipos que alimentaran al edificio o campus, en este está instalada la acometida principal, que da acceso a internet.

3. Cableado horizontal.

Este subsistema comprende el conjunto de medios de transmisión (cables, fibras, coaxiales, etcétera.) que unen el rack de planta con el conector o conectores del área de trabajo, este cableado generalmente no debe ser mayor de 100 metros. Ésta es una de las partes más importantes a la hora del diseño debido a la distribución de los puntos de conexión o tomas de usuario.

En este subsistema se estudian y definen las rutas más adecuadas para distribuir la totalidad del cableado a lo largo de un piso. Estas rutas deben ajustarse a las distancias definidas por las normas. Igualmente se determina el tipo de elemento a utilizar para transportar el cable, de manera segura y confiable, con la capacidad suficiente y con el espacio requerido para crecimientos futuros. Entre los diferentes tipos de medios de transporte tenemos las bandejas de aluminio o de lámina, tuberías metálicas, ductos metálicos o en mampostería, canaletas perimetrales o por cielo raso, escalerillas, etcétera. En la instalación de estos

elementos, se deben cumplir diferentes aspectos de las normas respectivas, especialmente en lo relacionado con la capacidad de los mismos, materiales, curvaturas máximas, cantidad de cajas de paso, etcétera.

4. Rack de planta.

Este rack de planta ayuda a interconectar el rack principal con cada piso y de esta forma poder tener comunicación en cada piso del edificio o campus.

5. Cableado vertical.

Este subsistema está encargado de interconectar todos los subsistemas de cada piso a lo largo del edificio. Esta interconexión consiste en conectar los armarios de cada piso, con cables definidos para la aplicación diseñada.

Este subsistema puede estar compuesto por diferentes tipos de cables de acuerdo con el número de salidas de información que se tengan en cada piso. Generalmente se conectan siguiendo una topología en estrella estando el centro de la estrella en el cuarto principal de administración del sistema. En resumen, a través de estos cables (UTP, fibra o multipar) se llevan las señales de las aplicaciones definidas para el sistema (voz, datos, seguridad, video, etcétera.) desde el cuarto principal hasta dejarlas disponibles en cada piso.

Aquí se encuentra también todo lo relacionado con los ductos o espacios físicos con que la edificación cuenta para realizar esta distribución. Se tiene ductos o perforaciones en las placas, escalerillas metálicas, tuberías, etcétera.

6. Tomas de usuario.

En cada planta se instalan las rosetas (terminaciones de los cables) que sean necesarias en cada piso.

7. Áreas de trabajo.

El subsistema de área de trabajo, son las conexiones que se tienen dentro de la red desde la roseta hacia cualquier equipo ya sea una computadora, una cámara de seguridad, una impresora, una alarma, etcétera.

1.1.4 Topologías.

La topología de red es la disposición física en la que se conecta una red de computadoras.

1.1.4.1 Tipos de topologías.

Las principales topologías son:

- **Red en Bus.**

En una topología de bus (Figura.1.6), cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir, un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de la misma.

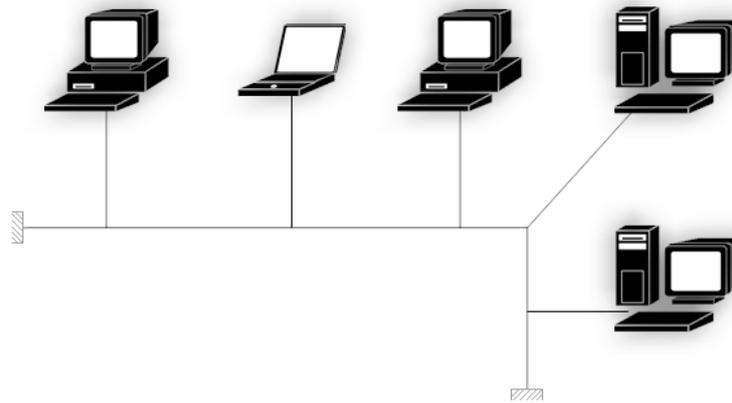


Figura 1.6 Topología de red bus.

- **Red en anillo.**

Una topología de anillo (Figura.1.7), consta de varios nodos unidos formando un círculo lógico. Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional, no obstante, sólo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como flecha o token.

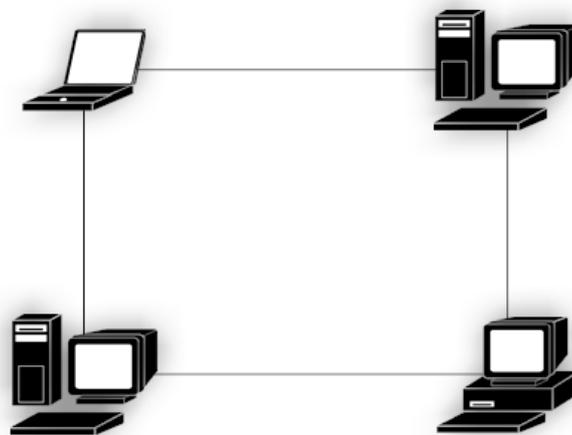


Figura 1.7 Topología de red anillo.

- **Red en estrella.**

Uno de los tipos más antiguos de topologías de redes es la estrella (Figura.1.8), la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico, ya que todos los mensajes de una topología LAN en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos.

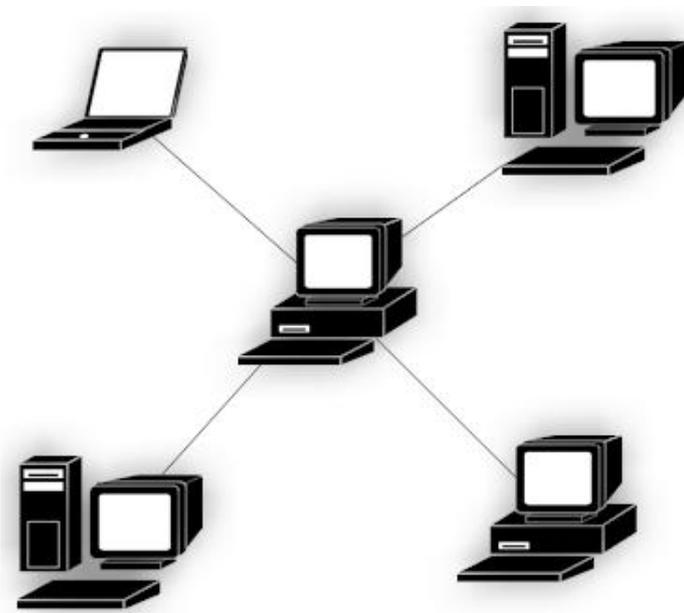


Figura 1.8 Topología de red estrella.

1.1.5 Servidores.

En una red de datos, un servidor es un equipo que pone ciertos recursos a disposición de otras computadoras (los clientes). Estos recursos pueden ser datos, aplicaciones, impresoras, etcétera.

Un servidor no es necesariamente una máquina de última generación grande y monstruosa, no es necesariamente un supercomputadora; un

servidor puede ser desde una computadora vieja, hasta una máquina sumamente potente.

1.1.5.1 Tipos de servidores.

Entre los servidores más conocidos se encuentran:

- **NAT.**

El NAT (Network Address Translation, en español Traducción de la dirección de red) es una aplicación no técnica y sencilla que determinado dispositivo o aplicación software es capaz de cambiar la dirección IP de origen o destino por otra dirección definida previamente. Se puede utilizar para dar salida a redes públicas a computadoras que se encuentran con direccionamiento privado o para proteger máquinas públicas.

- **Bridge.**

Un dispositivo que conecta dos o más redes físicas y sirve para transmitir paquetes entre ellas. Puede utilizarse también para filtrar los paquetes que entran o salen, selectivamente.

- **Proxy.**

La palabra proxy se usa en muchas situaciones en donde tiene sentido un *intermediario*.

El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

El servidor proxy de web (comúnmente conocido solamente como "proxy"). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etcétera.

- **DHCP.**

El DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Provee los parámetros de configuración a las computadoras conectadas a la red informática con el protocolo TCP/IP (Máscara de red, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- ✓ *Asignación manual o estática:* Asigna una dirección IP a una máquina determinada. Se suele utilizar cuando se quiere controlar la asignación de dirección IP a cada cliente, y evitar, también, que se conecten clientes no identificados.
- ✓ *Asignación automática:* Asigna una dirección IP de forma permanente a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado.

- ✓ *Asignación dinámica*: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

- **Servidor Web.**

Un servidor web es un programa que implementa el *protocolo HTTP* (*hypertext transfer protocol*). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (*hypertext markup language*): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

Un servidor web se encarga de mantenerse a la espera de *peticiones HTTP* llevada a cabo por un *cliente HTTP* que solemos conocer como *navegador*. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita.

- **Servidor de base de datos.**

Un servidor de base de datos es un equipo de cómputo que cuenta con una aplicación que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

- **Servidor Radius.**

Un servidor RADIUS centraliza una base de datos de usuarios y passwords y espera que equipos como access servers le pregunten si cierto usuario con cierto password tiene acceso. El servidor RADIUS recibe no solo usuario y password sino una multitud de atributos, como el puerto del access server a donde el usuario se está conectando, y debe responder si se le permite al usuario conectarse, junto con una serie de atributos que pueden ir desde la dirección IP a asignarle al usuario, protocolos a utilizar o reglas de filtrado de paquetes.

1.1.6 Modelo OSI.

1.1.6.1 Historia.

Al principio, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de trabajar en red, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban este tipo de tecnología de trabajo en red. Las tecnologías de trabajo en red que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional para la Estandarización (ISO) investigó modelos de trabajo

en red como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

1.1.6.2 Modelo de referencia OSI.

Siguiendo el esquema de este modelo se crearon numerosos protocolos, por ejemplo X.25, que durante muchos años ocuparon el centro de la escena de las comunicaciones informáticas. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo, sigue siendo muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones (sin importar su poca correspondencia con la realidad).

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

- **Capa Física (Capa 1).**

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (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); características del medio (por ejemplo tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etcétera.) y la forma en la que se transmite la información (codificación de señal, niveles de

tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etcétera).

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es unidireccional o bidireccional (símplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos, dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio.
 - Manejar las señales eléctricas/electromagnéticas.
 - Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etcétera.
 - Garantizar la conexión (aunque no la fiabilidad de ésta).
- **Capa de enlace de datos (Capa 2).**

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Se hace un direccionamiento de los datos en la red ya sea en la distribución adecuada desde un emisor a un receptor, la notificación de errores, de la topología de la red.

- **Capa de red (Capa 3).**

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan en español encaminadores, aunque es más

frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande).

El switch también puede trabajar en esta capa dependiendo de la función que se le asigne.

- **Capa de transporte (Capa 4).**

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a

3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Se puede definir a la capa de transporte como:

Capa encargada de efectuar el transporte de los datos de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando.

▪ **Capa de sesión (Capa 5).**

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.
- 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. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén trasmitiendo archivos.

- **Capa de presentación (Capa 6).**

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, se define a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

- **Capa de aplicación (Capa 7).**

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con

programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (HyperText Transfer Protocol).
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros.
- SMTP (Simple Mail Transfer Protocol), envío y distribución de correo electrónico.
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final.
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto.

1.2 Redes inalámbricas.

1.2.1 Concepto de red inalámbrica.

Una red de área local inalámbrica o WLAN (Wireless LAN) utiliza ondas electromagnéticas (radio o infrarrojo) para enlazar (mediante un adaptador) los equipos conectados a la red, en lugar de los cables coaxiales, cable UTP, fibra óptica, etcétera., que se utilizan en las LAN convencionales cableadas (Ethernet, Token Ring, etcétera.) como se aprecia en la Figura 1.9.

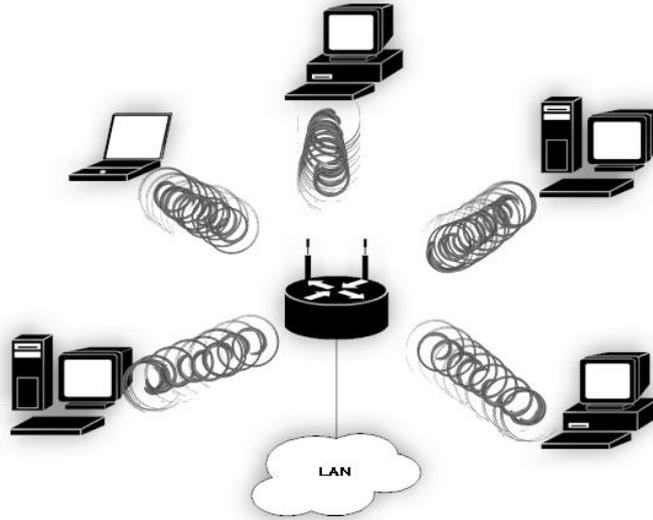


Figura 1.9 Red inalámbrica.

Las redes locales inalámbricas más que una sustitución de las LAN's convencionales son una extensión de las mismas, ya que permiten el intercambio de información entre los distintos medios en una forma transparente al usuario.

En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de infraestructura, enlazando los diferentes equipos y móviles asociados a la red.

Este hecho proporciona al usuario una gran movilidad sin perder conectividad. El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 10 y los 100 Mbps frente a los 10, 100 y hasta 1000 Mbps ofrecidos por una red de cableado estructurado.

Las redes inalámbricas, además de permitir extender las redes LAN existentes en las organizaciones, son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite o

cuando el tiempo por el cual se requiere contar con una red LAN es corto. En general las WLAN se utilizarán como complemento de las redes de cableado estructurado.

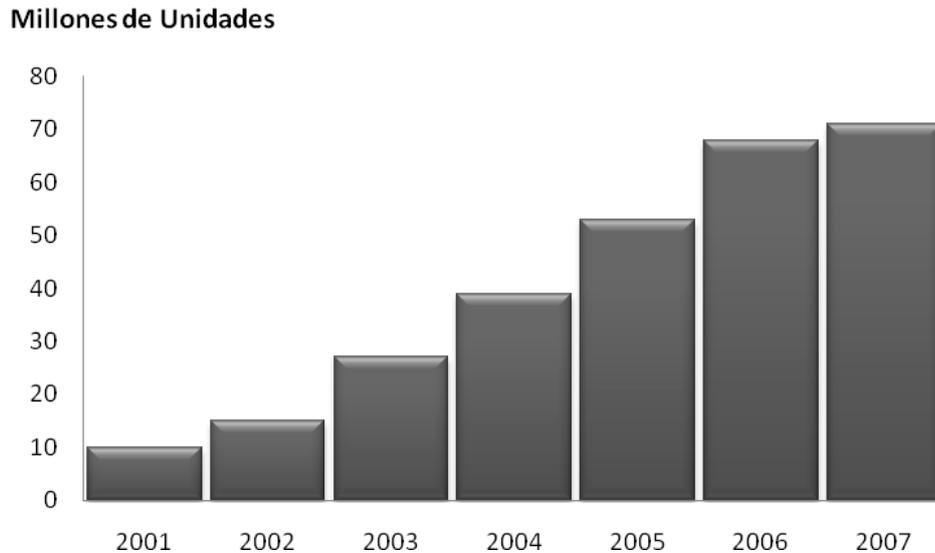
1.2.2 Orígenes.

El origen de las redes inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas. En mayo de 1985 la FCC (Federal Communications Commission) de Estados Unidos de América (EUA) asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en espectro disperso.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria, ese respaldo hizo que las WLAN empezaran a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y los precios elevados de una solución inalámbrica.



Fuente: In StatMDR www.instat.com

Figura 1.10 Crecimiento del mercado.

Sin embargo (ver Figura 1.10), se viene produciendo estos últimos años un crecimiento explosivo en este mercado. Y esto es debido a distintas razones:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles.
- La conclusión de la norma IEEE 802.11 para redes de área local inalámbricas que ha establecido un punto de referencia y ha mejorado en muchos aspectos estas redes.

1.3 Aplicaciones.

Las aplicaciones más típicas de las WLAN que podemos encontrar actualmente son las siguientes:

- En edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.

- Donde se requiere reconfigurar la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- En redes locales para situaciones de emergencia o congestión de la red cableada.
- En hospitales, fábricas, almacenes y cualquier sitio donde el usuario requiera tener acceso a la información mientras el usuario se encuentra en movimiento.
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada, ya que la solución inalámbrica es más viable para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales, este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de áreas locales cableadas situadas en dos edificios distintos.

1.4 Ventajas y desventajas de las redes inalámbricas.

En la tabla 1.2 se muestran las ventajas y desventajas tanto de las redes inalámbricas como de las redes de cableado estructurado.

Tabla 1.2 Ventajas y desventajas redes inalámbricas.

	Cableado estructurado	Redes inalámbricas
Ventajas.	<ul style="list-style-type: none"> • Tecnología madura. • Altas velocidades de transmisión. • Confiabilidad. • Cumple con estándares de la industria. 	<ul style="list-style-type: none"> • Buenas características de desempeño. • Resistencia a las interferencias externas. • Seguridad física. • Facilidad de instalación. • Facilidad de mantenimiento. • Facilidad de detección de fallos. • Imprescindible en ciertas circunstancias geográficas. • Menor tiempo de instalación. • Buen nivel de integración con redes tradicionales existentes. • Mínima capacidad para la instalación y el soporte.

Desventajas.	<ul style="list-style-type: none"> • Reparaciones costosas. • El tiempo de reparación es mayor. • Dificultad para el tendido del cableado o la reutilización de éste. • Mayor tiempo de instalación. 	<ul style="list-style-type: none"> • Potencia y distancias limitadas. • Velocidad de transmisión limitada. • Alto costo por unidad. • Es una tecnología relativamente nueva.
--------------	--	--

1.5 Access Point.

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Muchos WAP pueden conectarse entre sí para formar una red aún mayor. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Los AP siempre están a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada (Figura 1.11).

Un único AP puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.



Figura 1.11 Access Point.

1.6 Antenas.

Una antena es un conductor de longitud definida que se coloca al final de la línea de transmisión, y que se encarga de transmitir al ambiente, o irradiar, la señal suministrada por el equipo. La antena posee el comportamiento menos predecible, esto debido a que interacciona fuertemente con todo lo que lo rodea y solo se puede saber su comportamiento real hasta que se pone a prueba.

1.6.1 El radiador isotrópico.

El radiador isotrópico es una antena perfectamente omnidireccional, con cero decibeles de ganancia, que irradia la señal en forma de esfera perfectamente uniforme, con la misma intensidad en todas las direcciones (Figura 1.12). Ésta es una antena imaginaria, que no puede fabricarse porque cualquier antena, sin importar qué tan perfectamente esté construida, tiene una ganancia dada en alguna dirección. Esa ganancia puede ser de tan solo unas fracciones de dB, pero ahí está presente siempre.



Figura 1.12 Radiador isotrópico.

La ganancia de una antena es una medida de su tendencia a concentrar la señal en una dirección específica. Una antena con alta ganancia es altamente direccional, mientras que una antena con baja ganancia es omnidireccional. La unidad para medir la ganancia es el decibel (dB). El decibel, en antenas, es una relación logarítmica entre voltajes, que se utiliza principalmente para medir ganancia, esta puede ser positiva o negativa.

También podemos dar la medida en dBd. Si hablamos de 10 dBd estamos diciendo que la antena posee 10 dB de ganancia más que el dipolo ideal. O sea, poniendo ambas antenas lado a lado, el dipolo ideal daría una ganancia de 2.15 dB, mientras que nuestra antena daría 10 dB más, o sea, 12.15 dB.

Para convertir de dBi a dBd (y viceversa) se emplea la siguiente fórmula:

$$\text{dBi} = \text{dBd} - 2.15$$

En el mercado es común ver ganancias expresadas en dBi, principalmente por el efecto de "impacto" que tiene el ver un número más grande. Para un fabricante que busca vender antenas resulta muy cómodo el dBi, pero para un comprador que quiere saber cómo se

comporta una antena tiene poca utilidad porque se compara la antena a una antena no existente, que nunca ha existido y de cuyo funcionamiento no se tiene mayor idea. Para nosotros lo mejor sería expresar la ganancia en dBd, dando una idea más realista de su funcionamiento.

1.6.2 Patrón de irradiación de una antena.

Cada antena tiene su propia forma de irradiar una señal. Hay antenas que irradian más en una dirección que en otra, hay otras que tienden a irradiar casi por igual en todas las direcciones, y hay antenas que irradian sólo en ciertas direcciones.

La forma característica que tiene una antena de emitir la señal es lo que se conoce como su patrón de irradiación.

En un patrón de irradiación hay direcciones en las que se emite mucha energía, y direcciones en donde no se emite energía del todo, a estas se les conocen como direcciones "sordas" de las antenas, en donde prácticamente no se reciben señales.

Los patrones de irradiación de una antena por lo general son brindados por el fabricante en las especificaciones.

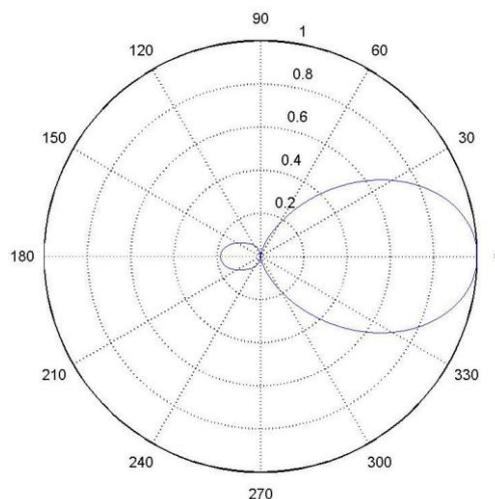


Figura 1.13 Patrón Azimutal.

En la Figura. 1.13 se muestra el llamado patrón azimutal, que sería la forma de irradiar de la antena si se estuviera observando desde arriba. Los puntos donde la curva (la elipse) se aleja más del centro del gráfico son las direcciones que tienen mayor ganancia, mientras que los puntos donde la curva toca el centro son direcciones de cero irradiación.

Dependiendo de la zona a la que se le quiera ofrecer el servicio es la antena que se debe escoger por ejemplo, las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal extensa en los alrededores. Las antenas sectoriales se suelen utilizar cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa (Figura 1.14).

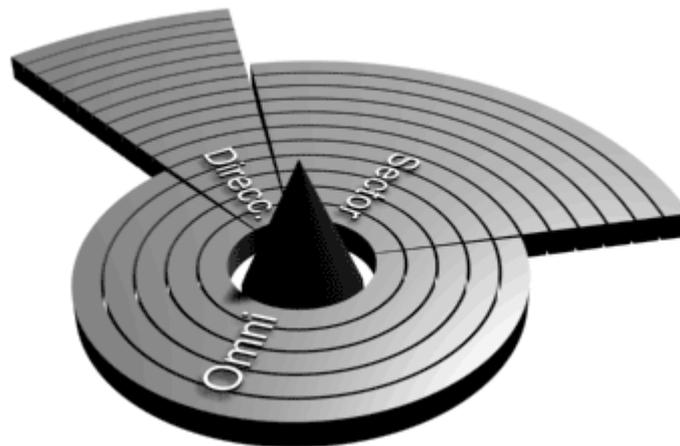


Figura 1.14 Zona de cobertura en los tipos de antenas.

1.6.3 Impedancia, frecuencia resonante.

Existen dos características importantes de una antena que se deben tener presentes en todo momento, las cuales son su frecuencia resonante y su impedancia.

1.6.3.1 Frecuencia resonante.

Es la frecuencia a la cual la antena se vuelve eléctricamente resonante, y en la cual existe una cancelación interna mínima de la señal de radio. A esta frecuencia resonante la antena irradia el 100% de la señal que se le proporciona.

1.6.3.2 Impedancia.

La impedancia de una antena es una especie de resistencia que posee toda antena, y de hecho todo sistema eléctrico, y que se deriva del efecto combinado de resistencia de los elementos, reactancias capacitivas y reactancias inductivas. La impedancia afecta la transferencia de energía entre las diferentes partes de un sistema de radio. En cuanto a impedancia, la regla general es que para lograr una máxima transferencia de energía a la antena, la impedancia de la antena debe ser igual a la impedancia de la línea de transmisión, la cual debe ser igual a la impedancia del equipo de radio.

1.6.4 Tipos de antenas.

Existen muchos tipos diferentes de antenas disponibles en el mercado. Cada antena tiene sus características propias de funcionamiento y sus requerimientos en cuanto a altura, alimentación, etcétera.

Una antena que irradia básicamente por igual en todas direcciones se llama antena omnidireccional. La antena que concentra la señal hacia una dirección específica se llama antena direccional.

1.6.4.1 Antenas de Sector.

Al igual que las antenas omnidireccionales, su uso es para conexiones punto a multipunto. Éstas, sin embargo, sólo emiten en una dirección Su radio de cobertura está entre los 60 y los 180 grados (figura 1.15). La ganancia de estas antenas es mejor que las omnidireccionales (aproximadamente 22 dBi), y permiten orientarlas hacia la dirección que mas interesa (incluso hacia arriba y hacia abajo).



Figura 1.15 Antena de sector.

1.6.4.2 Antenas de Panel.

Se utilizan para conexiones punto a punto enfocadas. Son como pequeñas cajas planas y tienen una ganancia de hasta 22 dBi (figura 1.16).



Figura 1.16 Antena de panel.

1.6.4.3 Antenas Yagi.

Las antenas yagi, (o direccionales) tienen forma de tubo. En su interior tienen unas barras de metal que cruzan el interior de ese tubo. La señal que emiten es direccional y proporciona una ganancia que oscila entre los 15 y los 21 dBi. Hay que enfocarla directamente al lugar con el que se quiere enlazar (figura 1.17).



Figura 1.17 Antena Yagi.

1.6.4.4 Antenas Parabólicas.

Las antenas parabólicas son las más potentes que se pueden adquirir (hasta 27 dBi), por lo que son las más indicadas para cubrir largas distancias entre emisor y receptor. Cuanta mayor ganancia tienen, mayor diámetro de rejilla (figura 1.18).



Figura 1.18 Antena Parabólica.

1.6.4.5 Antenas Dipolo.

Este tipo de antenas, están más indicadas para lugares pequeños, y más concretamente para uso de Access Points. La ganancia de esas antenas oscila entre los 2 y los 5 dBi (figura 1.19).



Figura 1.19 Antena dipolo.

1.7 Estándares y protocolos de las redes inalámbricas.

El estándar 802.11 es un estándar de protocolo de comunicaciones que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

El estándar 802.11 fue desarrollado por el instituto de Ingenieros Eléctricos y Electrónicos (IEEE), para las redes inalámbricas.

1.7.1 Protocolos.

- *802.11 legacy.*

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la

banda 2.4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

- *802.11b.*

La revisión 802.11b del estándar original fue ratificada en 1999. El protocolo 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

- *802.11a.*

El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. El protocolo 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede íter

operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso, esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

- *802.11h.*

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE y que se hizo público en octubre de 2003. El protocolo 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélite.

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU (International Telecommunication Union) que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares.

Con el fin de respetar estos requerimientos, el estándar 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

- *802.11g.*

En Junio de 2003, se ratificó un tercer estándar de modulación el 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

- *802.11n.*

En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO (Multiple Input – Multiple Output), que permite utilizar

varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto. No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo esté implantado).

- *802.11e.*

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access.
- (HCCA) Controlled Access.

- *802.11i.*

Esta dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado).

- 802.11 Super G (protocolo propietario).

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz, alcanza una velocidad de transferencia de 108 Mbps. Esto es proporcionado por el chipset Atheros.

1.8 Canales y frecuencias.

- IEEE 802.11 b.

Los identificadores de canales, frecuencias de canales centrales, y dominios reguladores de cada canal de IEEE 802.11b 22-MHz-de-par-a-par (tabla 1.3).

Tabla 1.3 Canal y frecuencia IEEE 802.11b para 22 Mhz.

Id del Canal	Frecuencia en MHz	Dominios Reguladores				
		América	EMEA	Israel	China	Japón
1	2412	X	X		X	X
2	2417	X	X		X	X
3	2422	X	X	X	X	X
4	2427	X	X	X	X	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	X	X
10	2457	X	X		X	X
11	2462	X	X		X	X
12	2467		X			X
13	2472		X			X
14	2484					X

- IEEE 802.11a

Los identificadores de canales, frecuencias de canales centrales, y dominios reguladores de cada canal de IEEE 802.11a 20-MHz-de-par-a-par (tabla 1.4).

Tabla 1.4 Canal y frecuencia IEEE 802.11a para 20 MHz.

Id del canal	Frecuencia en MHz	Dominios Reguladores			
		América	EMEA	Israel	Japón
34	5170		X		
36	5180	X		X	
38	5190		X		
40	5200	X		X	
42	5210		X		
44	5220	X		X	
46	5230		X		
48	5240	X		X	
52	5260	X			X
56	5280	X			X
60	5300	X			X
64	5320	X			X
149	5745				
153	5765				
157	5785				
161	5805				

1.9 Tipo de redes inalámbricas.

- *Wireless WAN (Wide Area Network).*

Una WAN es una red de computadores que abarca una área geográfica relativamente extensa, típicamente permiten a múltiples organismos como oficinas de gobierno, universidades y otras instituciones conectarse en una misma red.

Por medio de una WAN Inalámbrica se pueden conectar las diferentes localidades utilizando conexiones satelitales, o por antenas de radio microondas. Estas redes son mucho más flexibles, económicas y fáciles de instalar.

En sí la forma más común de implantación de una red WAN es por medio de Satélites, los cuales enlazan una o mas estaciones bases, para la emisión y recepción, conocidas como estaciones terrestres. Los satélites utilizan una banda de frecuencias para recibir la información, luego amplifican y repiten la señal para enviarla en otra frecuencia.

Para que la comunicación satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en tierra los perderían de vista. Para mantenerse estacionario, el satélite debe tener un periodo de rotación igual que el de la tierra, y esto sucede cuando el satélite se encuentra a una altura de 35,784 Km.

Por el advenimiento de nuevas tecnologías celulares como 2.5G y 3G, se podría predecir, que el nacimiento de nuevas redes WAN basadas en PDA's y teléfonos celulares está por venir. Comunidades de usuarios con intereses comunes, instituciones y empresas, se verán beneficiadas por la conectividad que ofrecerán las redes celulares de datos de la próxima

generación.

Nuevos productos, servicios, y actividades derivadas de estas tecnologías impulsarán cambios radicales en la manera en que se trabaja hoy en día, nuevos negocios basados en estas tecnologías saldrán al mercado, y se verá de una vez por todas las utilidades de tener Internet en cualquier lugar en cualquier momento.

- LMDS.

LMDS (Local Multipoint Distribution Service) es una tecnología inalámbrica vía radio para comunicación entre puntos fijos. El rango de frecuencias utilizado varia entre 2 y 40 GHz dependiendo de la regulación del país en el que se utilice.

LMDS utiliza un transmisor central emitiendo su señal sobre un radio de hasta 5 Km. Las antenas de los receptores se sitúan generalmente en los tejados de los edificios para procurar una visibilidad directa con el transmisor central.

Un inconveniente de los sistemas LMDS es que no existe un estándar que asegure la compatibilidad de los equipos de distintos fabricantes.

- WiMAX.

WiMAX (Worlwide Interoperability for Microwave Access) es una organización sin ánimo de lucro creada en abril de 2002 por fabricantes y suministradores de equipos inalámbricos. El objetivo de WiMAX es promover el uso de las tecnologías IEEE 802.16^a la cual permite crear redes inalámbricas metropolitanas de banda ancha.

Desde el punto de vista de la cobertura una estación base típica WiMAX tiene un alcance de hasta 50 Km. Aunque la cobertura típica suele ser

menor 10 Km. Por otro lado desde el punto de vista del servicio una estación base puede ofrecer servicio a más de 60 empresas (a 2 Mbps) y cientos de hogares (a 256 Kbps) simultáneamente.

- *Wireless LAN (Local Area Network).*

La Wireless LAN permite conectar una red de computadores en una localidad geográfica, de manera inalámbrica para compartir archivos, servicios, impresoras, y otros recursos. Usualmente utilizan señales de radio, las cuales son captadas por PC-Cards, o tarjetas PCMCIA conectadas a laptops, o a slots PCI para PCMCIA de PCs de escritorio. Estas redes en general, soportan tasas de transmisión entre los 11Mbps y 54Mbps (mega bits por segundo) y tienen un rango de entre 30 a 300 metros, con señales capaces de atravesar paredes.

Estas tecnologías son de gran uso en bibliotecas, unidades móviles como ambulancias para los hospitales, etcétera.

En los Estados Unidos, muchas bibliotecas han implantado con éxito Wireless LAN a costos mucho más bajos de lo que saldría implantar redes físicas, y además les permiten acceso a la red en cualquier lugar de la biblioteca a todos sus usuarios.

- WI-FI.

Wi-Fi (Wireless-Fidelity) es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11. Fue creado para ser utilizado en redes locales inalámbricas; con el sistema WI-FI se pueden establecer comunicaciones a una velocidad máxima de 11 Mbps, alcanzando distancias de hasta varios cientos de metros. No obstante, versiones mas recientes de esta tecnología permiten alcanzar los 22, 54 y hasta 100 Mbps.

- HomeRF.

En 1998 se creó un grupo de trabajo bajo el nombre HomeRF (Home Radio Frequency) con el objetivo de desarrollar y promover un sistema de red inalámbrica para el hogar a principios de 1999 HomeRF sacó la versión 1.0 de su protocolo SWAP (Shared Wireless Access Protocol) el cual permite transmitir datos a 1.6 Mbps y mantener hasta cuatro comunicaciones duplex de voz. Tiene un alcance de unos 50 metros y una potencia de transmisión de 100mW.

- *Wireless PAN (Personal Area Network).*

Permite interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información. El líder en esta área es el estándar Bluetooth, una tecnología de radio de corto alcance (2.4 GHz) que simplifica las comunicaciones entre dispositivos de red y otras computadoras. Debido a que no fue diseñada para soportar grandes cargas de tráfico, no es una buena alternativa para sustituir redes locales o amplias.

- Bluetooth.

Bluetooth fue desarrollado en 1994 por la empresa sueca Ericsson con el objetivo de conseguir un sistema de comunicación de los teléfonos móviles con sus accesorios (auriculares, computadoras, etcétera).

Las comunicaciones de Bluetooth se llevan a cabo mediante el modelo maestro/esclavo. Un Terminal maestro puede comunicarse hasta con siete esclavos simultáneamente.

Bluetooth utiliza la técnica FHSS (Frequency Hopping Spread Spectrum, Espectro Expandido por Salto de Frecuencia) en la banda de frecuencias de

2.4 GHz. Puede establecer comunicaciones asimétricas donde la velocidad máxima en una dirección es de 721 Kbps y 57.6 Kbps en la otra o comunicaciones simétricas de 432.6 Kbps en ambas direcciones. Por otro lado, puede transmitir tanto voz como datos.

- Infrarrojo.

La luz infrarroja es un tipo de radiación electromagnética invisible para el ojo humano. Los sistemas de comunicaciones con infrarrojo se basan en la emisión y recepción de haces de luz infrarroja.

Los sistemas de comunicaciones de infrarrojo pueden ser divididos en dos categorías:

Infrarrojo de haz directo. Esta comunicación necesita una visibilidad directa sin obstáculos entre ambos terminales.

Infrarrojo de haz difuso. En este caso el haz tiene suficiente potencia como para alcanzar el destino mediante múltiples reflexiones en los obstáculos intermedios. En este caso no se necesita visibilidad directa entre terminales. Las ventajas que ofrecen las comunicaciones de infrarrojo es que no están reguladas, son de bajo coste e inmunes a interferencias de los sistemas de radio de alta frecuencia. Sus principales inconvenientes son su corto alcance, el hecho de que no puedan traspasar objetos y que no son utilizables en el exterior debido a que agentes naturales como la lluvia o la niebla les producen interferencias.

IrDA (Infrared Data Association) es una asociación que tiene como objetivo crear y promover el uso de sistemas de comunicaciones por infrarrojo. Actualmente tiene creados dos estándares:

IrDA-Control. Es un protocolo de baja velocidad optimizado para ser utilizado en los dispositivos de control remoto inalámbricos.

IrDA-Data. Es un protocolo orientado a crear redes de datos de corto alcance. Está diseñado para trabajar a distancias menores de 1 metro y a velocidades que van desde los 9.6 Kbps hasta los 16 Mbps.

1.10 Topologías.

1.10.1 AD-HOC.

En una topología AD-HOC (Figura.1.20), los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas AD-HOC serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

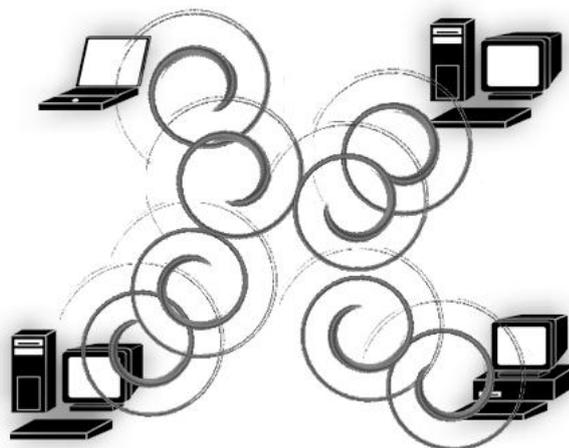


Figura. 1.20 Topología AD-HOC.

1.10.2 Infraestructura.

Una topología de infraestructura (Figura. 1.20) es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

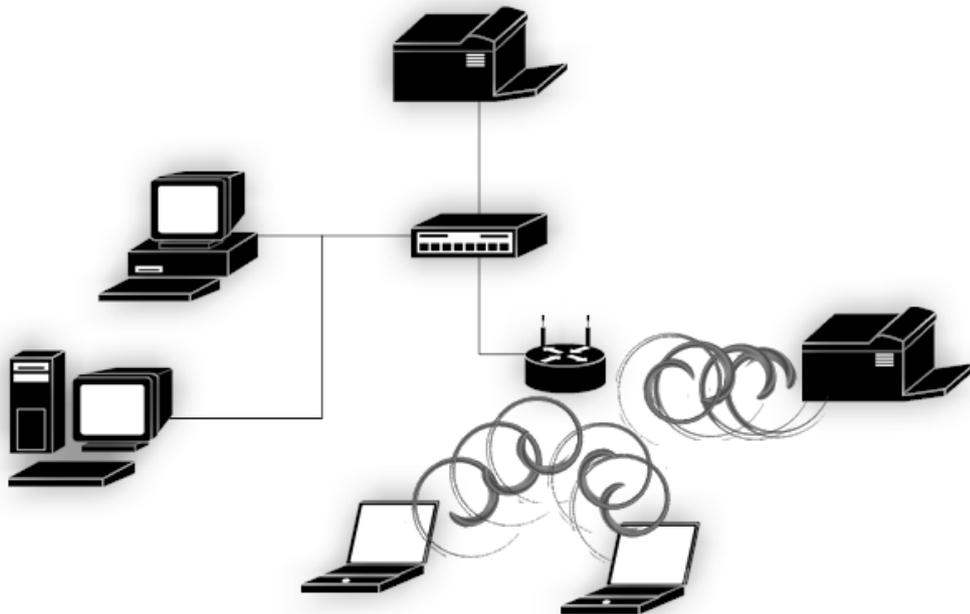


Figura. 1.21 Topología infraestructura.

1.11 Tipos de encriptación para punto de acceso en redes inalámbricas.

La función de la encriptación en un punto de acceso, es la de poder administrar quien puede conectarse a este punto acceso y poder utilizar los recursos de la red inalámbrica, así como la de mantener privados los datos que consultan nuestros usuarios.

1.11.1 WEP (*Wired Equivalent Privacy*).

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación *IV*) o de 128 bits (104 bits más 24 bits del *IV*).

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de verificación de integridad CRC.

RC4 es un algoritmo de cifrado de flujo. Es decir, funciona expandiendo una semilla para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación (*IV*) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo).

El principal problema con la implementación de este algoritmo es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para descifrarlo.

Para atacar una red Wireless se suelen utilizar los llamados Packet sniffers y los *WEP Crackers*. Para llevar a cabo este ataque, se captura una cantidad de paquetes necesaria (dependerá del número de bits de cifrado) mediante la utilización de un Packet sniffer y luego mediante un WEP cracker o key cracker se trata de “romper” el cifrado de la red.

Un key cracker es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP. Crackear una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario.

1.11.2 WPA (*Wi-Fi Protected Access*).

Es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo WEP. El método de encriptación WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. El método de encriptación WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida ([PSK] - Pre-Shared Key) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.

Dos de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Autenticación de los usuarios mediante EAP (Extensible Authentication Protocol), Este sistema permite controlar a todos y cada uno de los usuarios que se conectan a la red.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. El método WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan durante 60 segundos al detectar dos intentos de ataque durante 1 minuto.

1.11.3 WPA2.

Está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

El estándar 802.11i fue ratificado en Junio de 2004.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de EUA - FIPS140-2. El método WPA2 está idealmente pensado para empresas tanto del sector privado como del público. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i.

CAPÍTULO II

Infraestructura

de la Biblioteca

2.1 Marco histórico de la biblioteca Antonio Dovalí Jaime.

El Ing. Antonio Dovalí fue director de la Facultad de Ingeniería de 1959 a 1966, La biblioteca fue nombrada en su honor al poco tiempo de su deceso. Los primeros años de la biblioteca transcurren entre la década de los sesentas, incrementando su acervo de manera importante para los alumnos de la Facultad.

En 1990 se realizan grandes cambios en la biblioteca Antonio Dovalí Jaime pues se cierra el área de procesos técnicos que posteriormente pasaría a ser parte de la imprenta dejando la biblioteca con la distribución actual y por primera vez se abre la estantería a los alumnos, dejando atrás el servicio por ventanilla. Además se implementa el primer sistema automatizado para la consulta de libros que se llama circula el cual se utilizaba a la par con el tradicional catálogo de fichas.

Bajo la coordinación del Ing. Juan Manuel Hernández Osnaya, se realiza la petición a la Dirección General de Bibliotecas de la UNAM para la instalación del catálogo automatizado de bibliotecas LIBRUNAM. Quedando el módulo CIRCULA, como base para el préstamo de materiales en la biblioteca Antonio Dovalí Jaime. Dicho sistema permitió agilizar el préstamo de libros sin la necesidad de tarjetas personales a cada usuario.

En 1997, el Lic. Alejandro Fernández Silva continúa con los cambios realizando remodelaciones a la entrada que ya contaba con el sistema seguridad SENSORMATIC y el área de mezzanine, además de cambio de mobiliario, la biblioteca obtuvo una apariencia mas moderna y atractiva.

En 2005, la Lic. Ma. Del Consuelo Tuñón Rodríguez, realiza un cambio fundamental al adquirir las plataformas de libros electrónicos (Overdrive, Safari, etc.) adentrándose en las tecnologías de la información.

2.2 Marco histórico de la biblioteca Enrique Rivero Borrell.

La Facultad de Ingeniería ante la clara percepción de las necesidades futuras de su proyecto académico, ha desarrollado un plan maestro, que norma el crecimiento, la adecuación y optimización del espacio físico. Dentro de este plan maestro se contemplaron trece acciones por ejecutar, una de las cuales es la biblioteca Enrique Rivera Borrell.

Una biblioteca, en el umbral del siglo XXI, no se concibe únicamente como un espacio donde se tienen ordenados los libros para su lectura y consulta, representa además, un espacio de estudio, reflexión y creación. Sus espacios deben ser flexibles para adecuarse a las situaciones que la tecnología vaya requiriendo.

El estudio actualmente no requiere necesariamente de un libro, ya que existen nuevas tecnologías como lo son: la computadora y los sistemas audiovisuales (multimedia) que marcan el inicio de un camino nuevo para el aprendizaje y esto sirva para que los alumnos puedan hacer uso de estas tecnologías para su formación profesional.

La construcción de esta trascendental obra se inició el 23 enero de 1995 y fue encargada a la constructora Estudios Profesionales en Construcción, S.A. de C.V. (EPC), y estuvo dirigida por el Ing. Jaime Torres Herrera, director general de la obra, quien además se encargó de los trabajos de coordinación del grupo de ingenieros

egresados de esta Facultad y que participaron en los trabajos de dirección de la obra.

Dicha obra tuvo una duración de año y medio, y fue inaugurada el 20 de septiembre del 1996, por lo que este día será recordado como una fecha importante para la Facultad de Ingeniería.

La concepción arquitectónica está fundamentada en la arquitectura emocional de los espacios, de los cuales hablaba el maestro Mathias Goeritz. La biblioteca pretende proporcionar un ambiente confortable que permita la concentración y al mismo tiempo mantenga el espacio vital de cada persona.

El edificio se ubica entre los ejes del puente de acceso al edificio de Ciencias Básicas de la Facultad de Ingeniería. El diseño de la obra es de los arquitectos Francisco Serrano, Fernando Pineda y Luís Mc Gregor y el eje de la escultura del maestro Sebastián (figura 2.1).



Figura 2.1 Biblioteca Enrique Rivero Borrel.

El cruce de estos dos ejes genera un patio en el centro de la biblioteca, este espacio jerárquicamente resulta el más importante y en él se ubica la escultura del maestro Sebastián, bañada de luz a través de los vitrales del maestro Narcissus Quagliata.

Esta escultura y los vitrales, más que elementos decorativos enriquecen y embellecen el espacio arquitectónico, que motiva a los lectores a la concentración.

Para esta obra se realizó un análisis minucioso de las bibliotecas existentes de la Universidad y de las que estaban en proceso de realización. Además se hizo una encuesta a diez mil estudiantes de la Facultad de Ingeniería y se llevó a cabo una investigación sobre avances y tendencias de algunas bibliotecas recién terminadas o en proceso de construcción que se visitaron en San Diego, Los Ángeles y California. De esta visita se obtuvo información importantísima sobre la prospectiva de este interesante género de edificios.

La conclusión más importante fue que la biblioteca debe ser la columna vertebral del proceso enseñanza - aprendizaje en el futuro, ya que una biblioteca en el umbral del siglo XXI no se concibe como un espacio donde se guardan los libros para su lectura y consulta, sino que debe ser un espacio donde se cuente con toda la información, donde se logre el estudio, la reflexión y la creación.

Se pensó en sistemas constructivos en los que predominara la mano de obra y permitieran extender la derrama económica de la obra en beneficio social durante momentos críticos del país. En la obra se utilizaron materiales nacionales sin descuidar la calidad.

Se instalaron equipos ahorradores de agua, de energía y se separaron las aguas pluviales de las negras para alimentar mantos acuíferos y que se descargaran en la planta de tratamiento de C.U. respectivamente.

La biblioteca cubre una superficie construida de 3,990.48 m². Tiene capacidad de préstamos a domicilio de 10,360 ejemplares, de

estantería abierta de 49,912, de procesos técnicos y bodega de 12,500, para obtener una capacidad de acervos de 77,772.

Actualmente la biblioteca cuenta con 56 cubículos de estudio, 10 para consulta de video, 12 de consulta de CD-ROM, 15 para consulta de Internet y 100 para área de consulta lo que representa una capacidad de usuario de 466 cubículos. Además tiene espacios para gobierno, servicios educativos, auxiliares, culturales y sanitarios.

2.3 Problemática de las Bibliotecas.

La biblioteca Enrique Rivero Borrell es uno de los centros de consulta de información más importante para la comunidad estudiantil, académica y de investigación de la Facultad de Ingeniería, es por esto que busca estar a la vanguardia en la información que la comunidad científica va generando, esta información en ocasiones tarda mucho en llegar a la biblioteca de una manera impresa, con pocos ejemplares y a veces esta información ya es obsoleta, en cambio a través de los medios electrónicos se puede encontrar esta información casi a la par en cuanto se publica. Se puede acceder a ella desde diferentes medios de comunicación electrónica, en diferentes fuentes donde se encuentra y se puede consultar cuantas veces se desee y por diferentes usuarios al mismo tiempo.

En la actualidad, las bibliotecas de la Facultad de Ingeniería ofrecen servicios de consulta y préstamos de libros, cuentan con una sala de proyecciones donde se ofrece un catálogo de cintas y videos de corte científico, dispone con un centro de enseñanza autodidacta para el idioma inglés, ofrece asesorías personalizadas a los alumnos, etcétera.

Una de las finalidades de las bibliotecas es ofrecer un mejor servicio a los alumnos, y siguiendo con esta ideología se busca una manera de implementar el servicio de Internet para que la comunidad de la facultad de Ingeniería puedan realizar consultas a libros electrónicos, videoconferencias, consultas a bibliotecas externas, etcétera. con la finalidad de que esto sea una herramienta más para la formación profesional de los estudiantes.

Para esto la biblioteca ha puesto a disposición de los estudiantes una sala de cómputo para esta finalidad, pero la cantidad de equipos ha sido rebasada por el número de usuarios que requieren de este servicio.

Ante esta situación la biblioteca a tratado de adquirir más equipos de computo para tratar de subsanar este problema, pero se han dado cuenta que esto no solucionaría el problema totalmente ya que se tendría que invertir gran parte del presupuesto que se les asigna y aún así no se cubriría la demanda de la comunidad, además de que el espacio físico de la biblioteca se vería afectado por la colocación de los equipos de computo para el servicio de los alumnos.

Al observar todas estas problemáticas la biblioteca de la facultad de Ingeniería busca alguna solución que pueda cubrir los requerimientos del servicio para ofrecerlos a los alumnos pero tratando de reducir costos lo mas posible.

2.4 Espacio Físico de la biblioteca.

La biblioteca Enrique Rivero Borrell se encuentra constituido por cinco niveles en este capitulo presentaremos una breve descripción de los mismos además de los servicios que ofrecen.

2.4.1 Primer nivel: sótano de biblioteca.

En el sótano de la biblioteca está dividido por dos habitaciones el más amplio alberga material de lectura que será dado de baja por encontrarse mutilado, no cumple con el requerimiento de la biblioteca, o es material viejo.

El cuarto adjunto es el cuarto de comunicaciones aquí se encuentra las conexiones de fibra óptica además de los concentradores, patch panel y la salida del cableado estructurado para la biblioteca como se muestra en la figura 2.2.

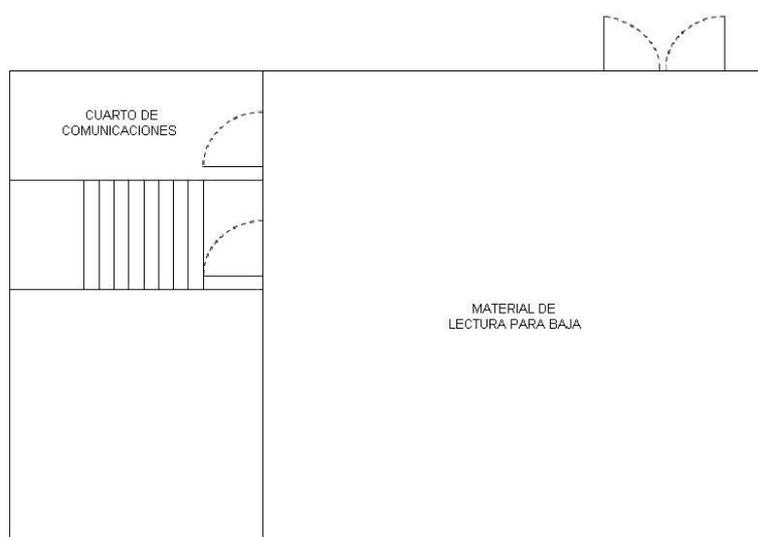


Figura 2.2 Sótano de la biblioteca.

2.4.2 Segundo nivel planta baja de la biblioteca.

La planta baja de la biblioteca presenta la entrada principal de la biblioteca así como la sala de exposiciones y el cuarto principal de procesos técnico como se muestra en la figura 2.3.

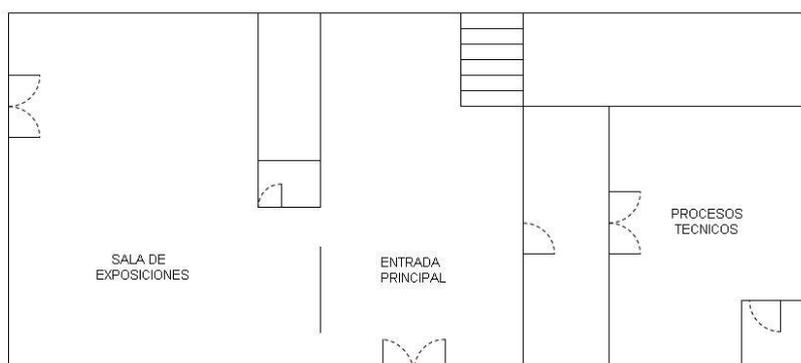


Figura 2.3 Planta baja de la biblioteca.

2.4.3 Tercer nivel primer piso de la biblioteca.

El primer piso de de la biblioteca está constituido por el área de préstamo de libros, la hemeroteca, el Centro de Aprendizaje Autodirigido de la Facultad de Ingeniería (CAALFI que en la actualidad ya no existe), una sala de consulta general, el área de préstamos interbibliotecarios, cubículos de asesoría y estudio grupal y una sala de audiovisuales como se muestra en la figura 2.4.

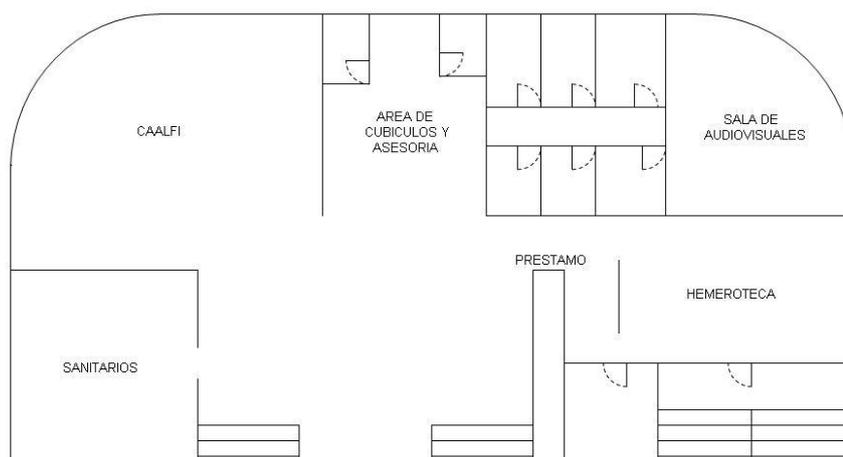


Figura 2.4 Primer piso de la biblioteca.

2.4.4 Cuarto nivel segundo piso de la biblioteca.

El segundo piso de de la biblioteca esta dividida por la sala de consulta digital, un área de lectura común, un área de estantes donde se encuentran dispuestos los libros, una zona de fotocopias y un cuarto de procesos técnicos como se muestra en la figura 2.5.

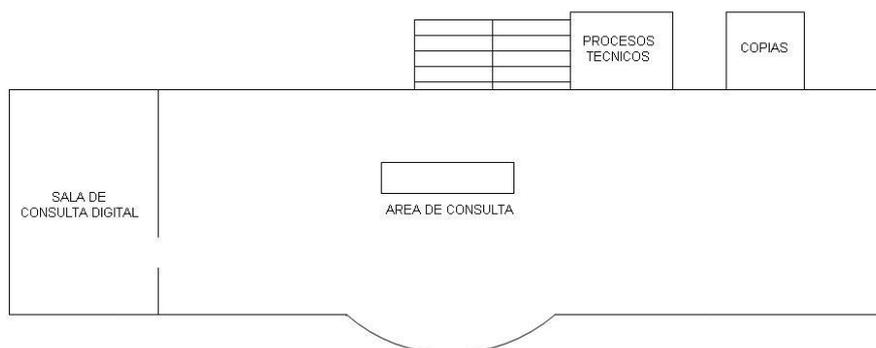


Figura 2.5 Segundo piso de la biblioteca.

2.4.5 Quinto nivel tercer piso de la biblioteca.

En el tercer piso de de la biblioteca se encuentra la coordinación de la biblioteca, un área de lectura común, zona de estantes con libros y un cuarto de procesos técnicos como se muestra en la figura 2.6.

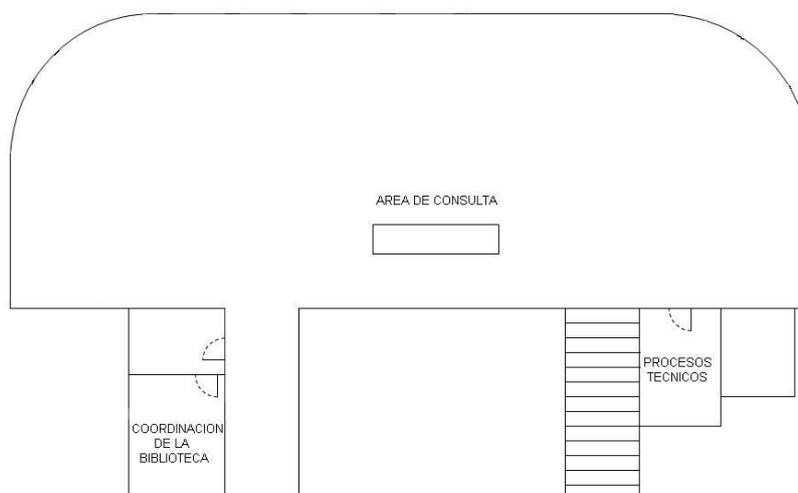


Figura 2.6 Tercer piso de la biblioteca.

2.5 Red de datos de la biblioteca Enrique Rivero Borrell.

La forma como se construye la red que soporte la comunicación entre los dispositivos de comunicación de datos está representada por la topología de la red local.

La biblioteca Enrique Rivero Borrell tiene una topología tipo estrella. Esta topología se adopto porque la administración de esta es más sencilla ya que si por ejemplo se requiere colocar o remover algún equipo de cómputo en la biblioteca, basta con solo conectar o desconectar el cable y en caso de que se desconectara una computadora o se rompiera el cable, no se afecta la comunicación de la red si no que solo sería afectada la comunicación de este equipo.

El cableado estructurado está conformado por cable UTP categoría 5.

La acometida principal llega al sótano por medio de fibra óptica, aquí con la ayuda de un transceiver se pasa la señal de fibra óptica a impulsos eléctricos hacia un cable UTP y por medio de este se distribuye la información hacia los HUB`s y de esta forma distribuirla hacia la biblioteca. La velocidad de la acometida principal es de 10 MB.

2.5.1 Los subsistemas que componen el sistema de cableado de la Biblioteca.

8. Subsistema de administración.

Esta zona se encuentra ubicada en el sótano de la biblioteca, aquí se encuentra instalado el rack principal, la acometida

principal de fibra óptica, también se encuentran los bloques de conexiones 110 (figura 2.7), y se encuentra un UPS para evitar fallas en el suministro de energía y evitar posibles descargas que puedan dañar los equipos de comunicación.

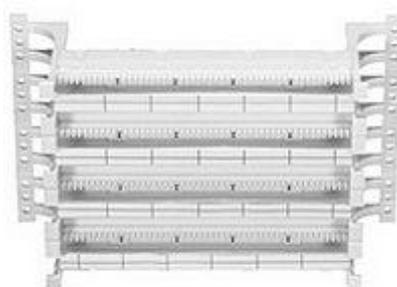


Figura 2.7.

9. Rack Principal.

El rack principal se encuentra instalado en el sótano, en este se encuentran montados los HUB`s de comunicación quedan acceso a la red y el transceiver aunque este último se encuentra sólo sobre puesto.

10. Cableado horizontal.

Éste se encuentra constituido por tuberías de metal que nos ayudan a conducir los cables UTP desde cada piso de la biblioteca hacia el subsistema de administración.

11. Rack de planta.

Este rack nos ayuda a conectar los nodos de un piso con el rack principal y de esta forma ahorra un poco de cable, pero este subsistema no se encuentra instalado en la biblioteca, si no que cada nodo fue llevado desde su ubicación en el área

de trabajo hasta el subsistema de administración y de esta forma se desperdicia mucho cable UTP y por lo tanto los costos aumentan.

12. Cableado vertical.

Este subsistema está constituido por canaletas metálicas que corren a ras de piso. Con la ayuda de estas es que se puede distribuir el cable UTP hacia cada nodo dentro de las áreas de trabajo en la biblioteca.

13. Tomas de usuario.

Éstas se encuentran colocadas sobre la canaleta metálica, están constituidas por cajas de registro data box y faceplates de plástico además de jack`s RJ45 categoría 5.

14. Área de trabajo.

Procesos técnicos:

En esta área se realiza el procesamiento del material adquirido como por ejemplo libros, folletos, materiales gráficos, periódicos, etcétera, se clasifican y catalogan.

Hemeroteca:

En esta sala es donde se guardan, ordenan, conservan diarios, revistas y otras publicaciones para su consulta por parte de alumnos y profesores.

Zona de préstamo:

Aquí con la ayuda del sistema circula se realiza el préstamo de material a los alumnos y profesores para su consulta fuera de la biblioteca.

Área de consulta:

Esta es la zona que mas extensión ocupa de la biblioteca ya que aquí es donde los alumnos pueden realizar las consultas del material bibliográfico.

Sala de consulta digital:

En esta sala, que se encuentra ubicada en el segundo piso de la biblioteca, se encuentran instaladas unas computadoras para que los alumnos puedan hacer consultas a libros electrónicos.

Coordinación de la biblioteca:

Aquí se encuentra ubicada la oficina de la coordinadora de la biblioteca junto con sus asistentes.

2.6 Croquis de red de la Biblioteca Enrique Rivero Borrell.

- **Sótano.**

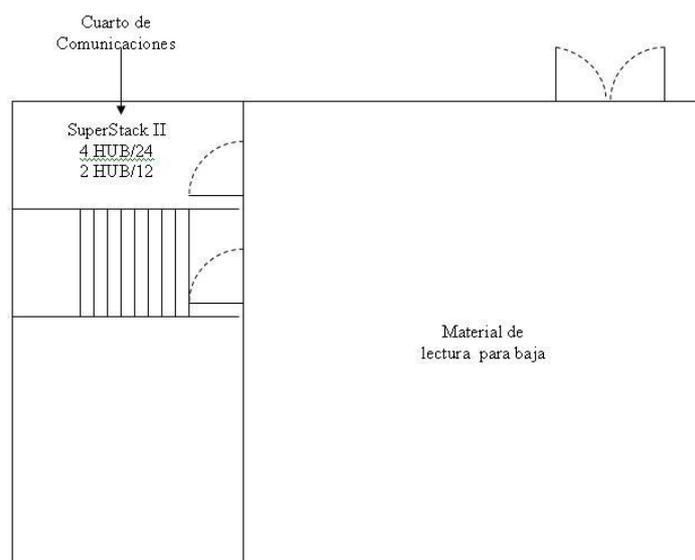


Figura 2.8 Croquis red sótano de la biblioteca.

- **Planta baja.**

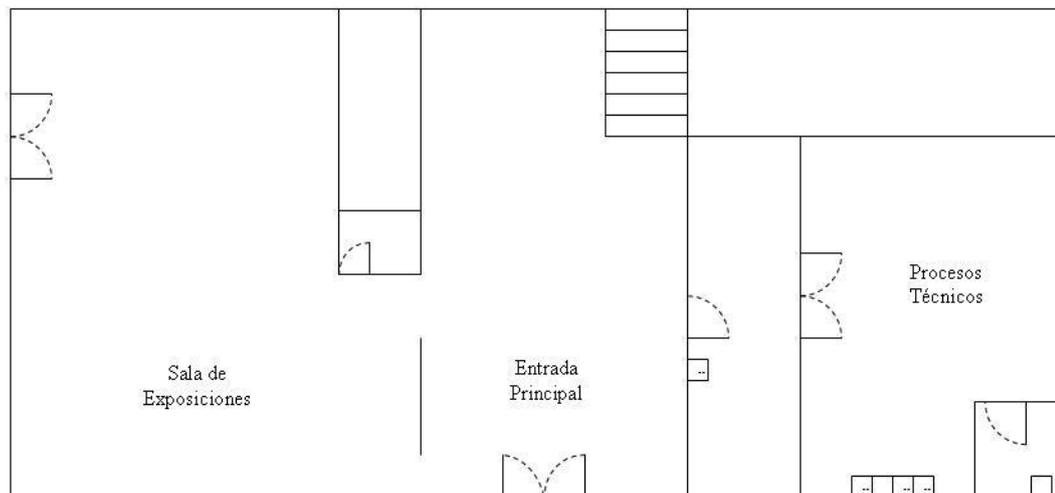


Figura 2.9 Croquis red planta baja de la biblioteca.

- **Primer piso.**

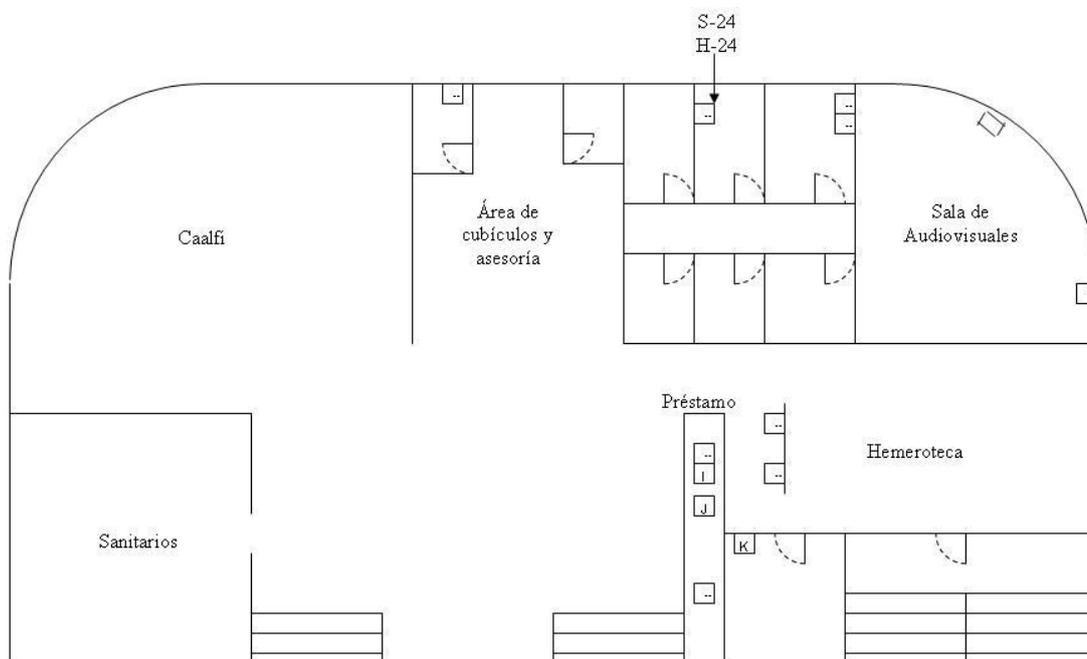


Figura 2.10 Croquis red primer piso de la biblioteca.

- **Segundo piso.**

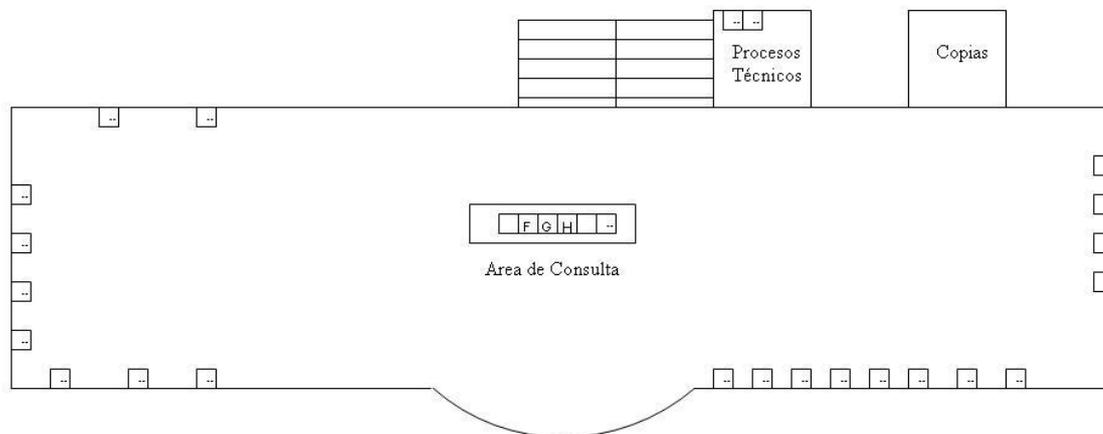


Figura 2.11 Croquis red segundo piso de la biblioteca.

- **Tercer piso.**

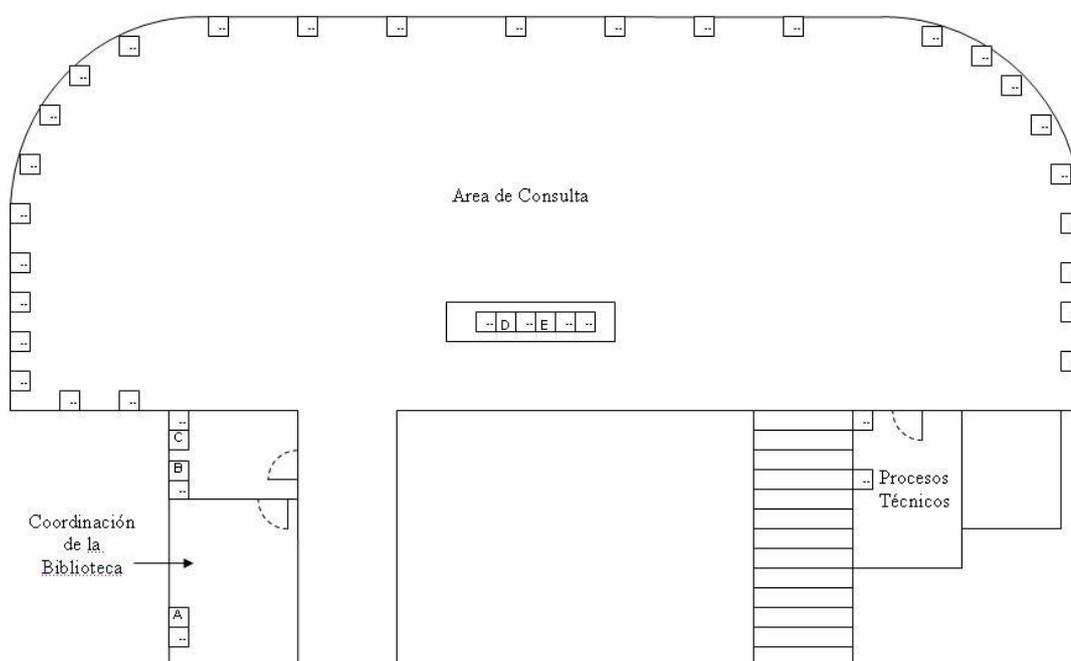


Figura 2.12 Croquis red tercer piso de la biblioteca.

Tabla 2.1. Nodos de red usados por la biblioteca.

Nodo	Dirección IP	Ubicación	Puerto concentrador	Descripción
A	192.168.206.101	Coordinación	HUB	PC
B	192.168.206.102	Coordinación	HUB	PC
C	192.168.206.103	Coordinación	HUB	PC
D	192.168.206.115	Consulta 3er piso	HUB	PC
E	132.248.139.217	Consulta 3er piso	HUB	PC
F	132.248.139.216	Consulta 2do piso	HUB	PC
G	192.168.206.104	Consulta 2do piso	HUB	PC
H	192.168.206.105	Consulta 2do piso	HUB	PC
I	192.168.206.106	Prestamos	HUB	PC
J	192.168.206.107	Prestamos	HUB	PC
K	192.168.206.108	Trabajadores	HUB	PC

Debido a que las conexiones hacia los Hubs no son por medio de UTP's, sino por conectores generales que contienen todos los cables, nos fue imposible detectar exactamente, a cuál de los concentradores se dirigía cada uno de los nodos.

CAPÍTULO III

Análisis y Diseño de la Red Inalámbrica

3.1 Análisis de la Biblioteca Enrique Rivero Borrell.

Las principales áreas que conforman la biblioteca Enrique Rivero Borrell son:

- Procesos técnicos.
- Cubículos.
- Áreas comunes.
- Estantes de libros.
- Cuarto de comunicaciones.
- CAALFI.

Para poder realizar una optima implementación de la red inalámbrica de la biblioteca Enrique Rivero Borrell se tomaron en cuenta las siguientes consideraciones:

- El rango de cobertura es inversamente proporcional a la velocidad de conexión de un cliente. El máximo rango de cobertura está unido a la mínima velocidad de conexión.
- La elección de una antena apropiada es un factor crítico en maximizar el rango de radio de cobertura.
- El ambiente físico es importante ya que las áreas abiertas dan una mejor cobertura que las áreas cerradas o con obstáculos físicos.
- Las obstrucciones físicas principalmente las metálicas pueden disminuir considerablemente el desempeño de los adaptadores de red inalámbricos.
- La penetración de las ondas electromagnéticas está influenciada por los materiales usados en la construcción.
- El Cableado eléctrico.

- Construcciones poco robustas permiten mayores rangos de cobertura que las construcciones de concreto. El metal como el acero es una barrera para la señal.

3.1.1 Análisis de infraestructura.

Este análisis se realiza ya que las antenas inalámbricas funcionan con ondas de radio que no recorren la misma distancia en todas las direcciones. Las paredes, las puertas, las personas y otros obstáculos suponen distintos grados de pérdida de señal (atenuación) que provocan que el patrón de la radiación de radiofrecuencia sea irregular e imprevisible.

Por estas razones la señal puede verse afectada y con ello el desempeño de la red inalámbrica. La biblioteca Enrique Rivero Borrel es un solo edificio, construido con diferentes materiales, dentro de los cuales destacan:

- Muros divisorios de cancelería (de aluminio y vidrio) fachada celosía.
- Muros prefabricados Spancret, tabla roca.
- Techo de concreto y plafón.
- Pisos de concreto.
- Muros de concreto y panel.
- Acabados de madera.
- Estantes de metal.
- Aplanados de yeso.
- Loseta.
- Muros cubiertos con pintura a base de agua.
- Columnas de concreto.
- Estructura metálica cubierta con pintura a base de aceite.

Al observar la infraestructura de la biblioteca Enrique Rivero Borrell se puede observar que es un espacio abierto en los niveles superiores que la conforman (segundo piso y tercer piso), y por esta razón existirá línea de vista directa, además de que en estas zonas es donde más afluencia de alumnos existe.

En la tabla 3.1 se muestran algunos de los materiales más comunes y su grado de atenuación:

Tabla 3.1 Grado de atenuación en algunos materiales.

<i>Obstáculo</i>	<i>Grado de Atenuación</i>
Espacio abierto	Ninguno
Madera	Bajo
Yeso	Bajo
Materiales sintéticos	Bajo
Bloque de hormigón	Bajo
Asbesto	Bajo
Cristal	Bajo
Malla de alambre en cristal	Medio
Cristal metálico tintado	Bajo
Cuerpo humano	Medio
Agua	Medio
Ladrillos	Medio
Mármol	Medio
Apilamiento de Papel	Alto
Hormigón	Alto
Cristal antibalas	Alto
Materiales plateados	Muy alto
Metal Muy	Alto

Otros factores que reducen el alcance y afectan al área de cobertura son los revestimientos de aluminio, las tuberías, el cableado eléctrico, los hornos microondas y los teléfonos inalámbricos.

Teniendo en cuenta los factores anteriores se efectuaron pruebas de ubicación y distribución del punto de acceso en cada piso de la biblioteca Enrique Rivero Borrell. Se observó la atenuación de la señal en cada piso de la biblioteca.

También se observó que el desempeño de la antena dependía de la altura a la que se encontraba y el canal en el cual transmite.

A continuación se detalla los pasos que seguimos para la realización de las pruebas:

1. Se colocó el access point (figura 3.1) en una ubicación donde considerábamos que abarcaría la mayor área de cobertura (Figura 3.2) posible tratando de evitar los obstáculos más posibles.

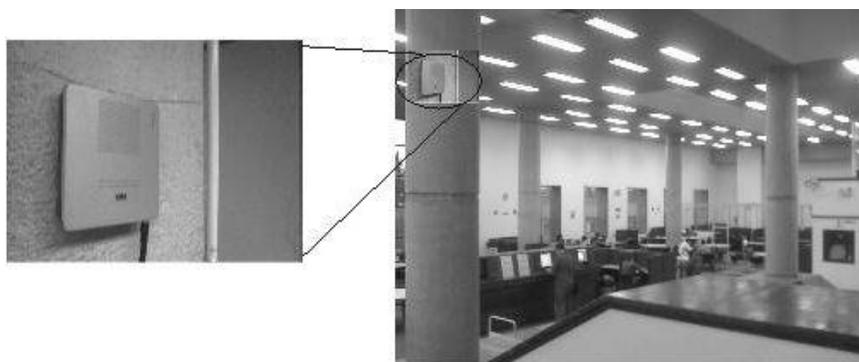


Figura 3.1 Ubicación access point segundo piso.

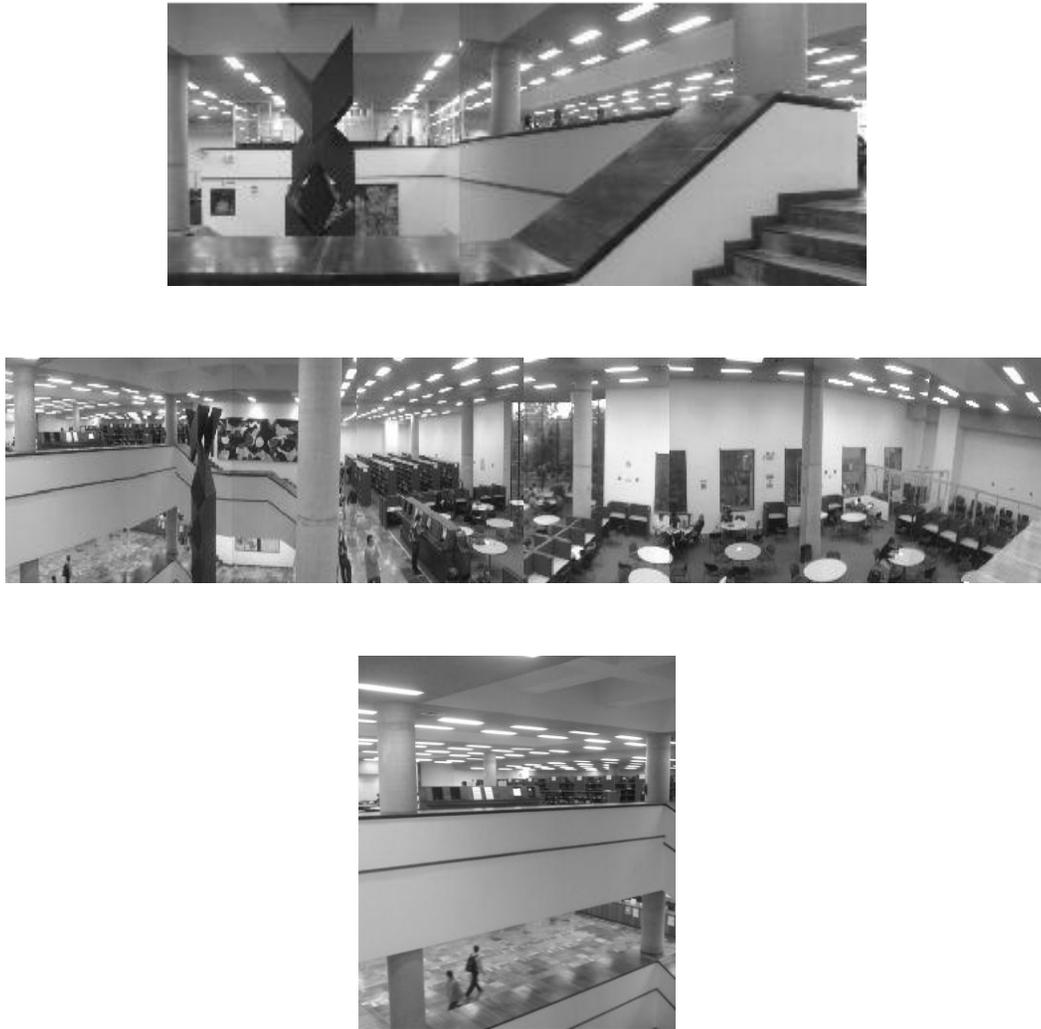
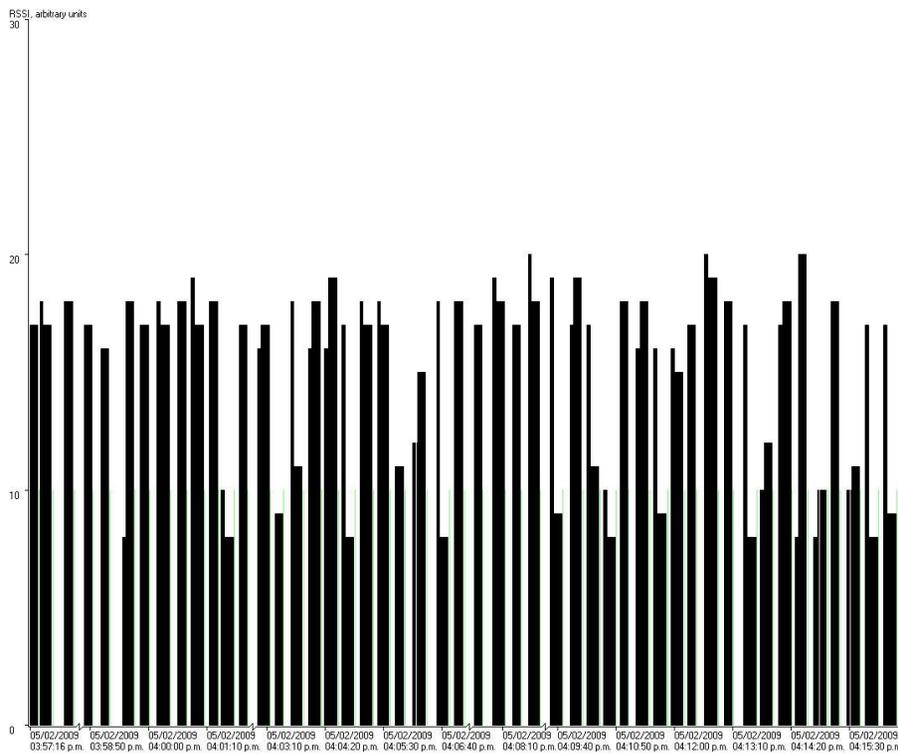


Figura 3.2 Áreas de cobertura.

2. Se fueron registrando las lecturas de conexión en una laptop en Mbps en cada uno de los pisos de la biblioteca para poder observar el nivel en de pérdida de señal que se iba generando.



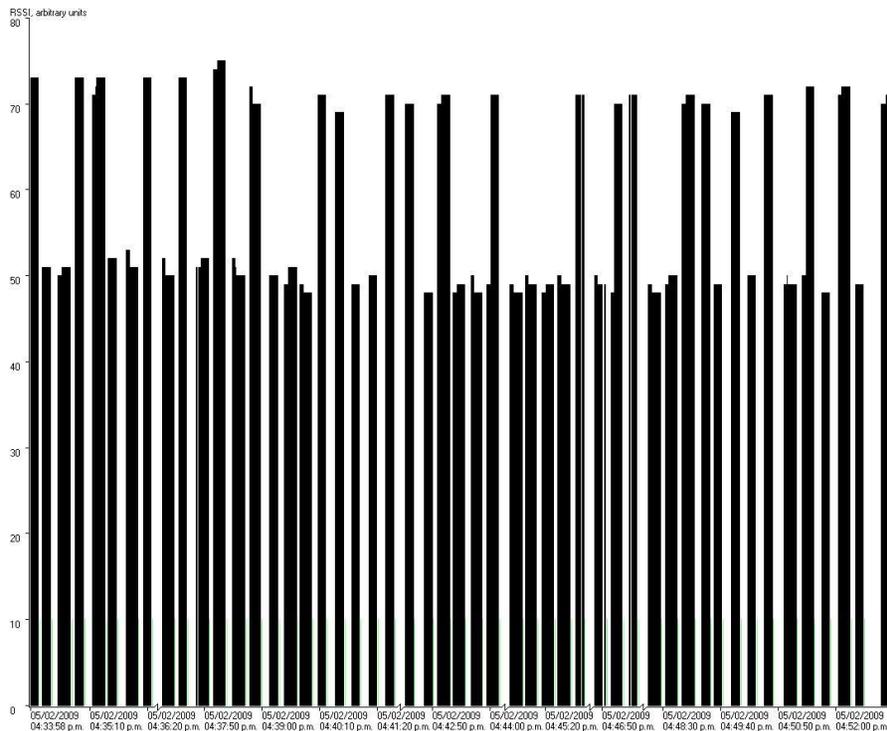
Señal obtenida en pisos 2 y 3 canal 5.



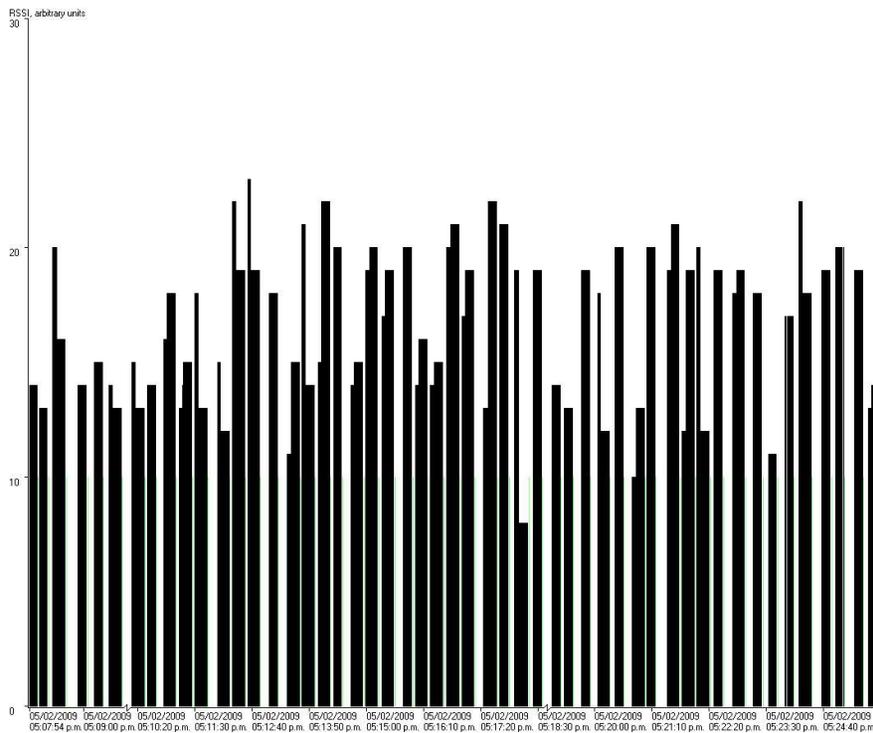
Señal obtenida en planta baja canal 5.

RSSI es la abreviatura en inglés de *Receive Signal Strength Indication*, Indicador de fuerza de señal de recepción. Este término se usa comúnmente para medir el nivel de fuerza de las señales recibidas en las redes inalámbricas (WIFI). Cuanto más alto sea el número, mejor captura de la misma.

3. Si en algún punto se observaba que la señal es baja, cambiábamos el canal y tomábamos nuevamente lecturas.



Señal obtenida en pisos 2 y 3 canal 10.



Señal obtenida en planta baja canal 10.

Estas pruebas se realizaron en cada piso de la biblioteca y sin la necesidad de colocar otro Access Point como repetidor.

Podemos mencionar algunas de las situaciones que se presentaron en la realización de estas pruebas:

Planta baja. En esta área la señal llegaba con buena señal y no presentaba problemas de atenuación considerables.

Primer Piso. Esta presentó pocos problemas, a pesar de que se encuentran los cubículos de asesoría y la sala audiovisual, el material de las paredes no atenúa en gran medida la señal y tampoco existen equipos que produzcan interferencias.

Segundo Piso y Tercer Piso. En estas áreas se encuentra un espacio abierto en donde la pérdida de señal es casi nula, el material de los muros y el espacio del lugar hicieron innecesaria la utilización de repetidores.

La mejor área para colocar el Access Point es el segundo piso en la parte final de uno de los pilares con los que cuenta la biblioteca así como una antena omnidireccional para tener el máximo alcance de la señal inalámbrica.

En el diseño e implementación de la red inalámbrica se trato de unificar eficacia y rendimiento, con la arquitectura de la biblioteca Enrique Rivero Borrel, tratando o evitando realizar alteraciones drásticas en la estructura de la biblioteca.

El software que utilizamos para realizar las mediciones se llama Network Netstumbler es un software de distribución freeware.

Netstumbler es un programa para Windows que permite detectar WLANs usando tarjetas wireless 802.11a, 802.11b y 802.11g (figura 3.3). Tiene varios usos, como:

- Verifica que nuestra red está bien configurada.
- Estudia la cobertura o señal que tenemos en diferentes puntos.
- Detecta otras redes que pueden causar interferencia a la nuestra.
- En útil para orientar antenas direccionales cuando queremos hacer enlaces de larga distancia, o simplemente para colocar la antena tarjeta en el punto con mejor calidad de la señal.
- Sirve para detectar puntos de acceso no autorizados.

- Sirve para detectar todos los AP's que están a nuestro alrededor.

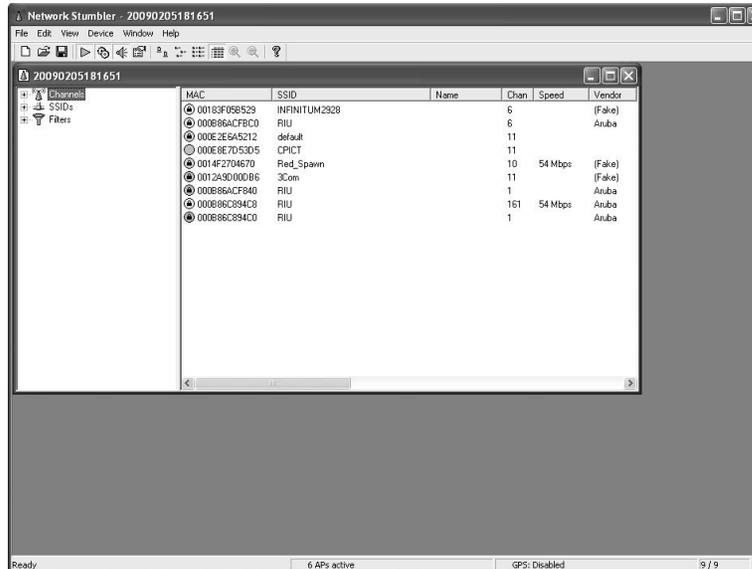


Figura 3.3. Netstumbler.

3.2 Necesidades actuales de la Biblioteca Enrique Rivero Borrell

La biblioteca Enrique Rivero Borrell como centro de resguardo bibliográfico, estudio y cultura, está enfocado a prestar servicios a los alumnos de la Facultad de Ingeniería para ello cuenta con una estructura académico-administrativa formada por profesores y trabajadores.

Uno de los objetivos de la implementación de la red inalámbrica en la biblioteca Enrique Rivero Borrell, es modernizar su estructura operativa, y que tal modernización de como resultado un mejor desempeño en los estudiantes de esta facultad.

Para lograr esta mejora es necesario considerar que actualmente los alumnos accedan a material bibliográfico en línea así como sitios o páginas en Internet como apoyo en sus materias de la carrera, para lo

cuales requiere contar con disponibilidad de recursos para poder acceder a este tipo de información y facilitar las actividades académicas que se desarrollan en la biblioteca, y brindarles nuevos servicios que les ayuden a desempeñarse de manera más eficiente y productiva.

Actualmente la biblioteca Enrique Rivero Borrell cuenta con una infraestructura moderna, sin embargo, no cuenta con la cualidad de movilidad que se requiere como acceso fácil a nodos de red, pocas tomas de corriente, ya que estas se encuentran obstruidas con cubículos para el uso de los alumnos, etc., para un desarrollo óptimo de sus alumnos y profesores.

Se debe considerar que existe una gran cantidad de estudiantes que cuentan con laptop's con tecnología inalámbrica integrada que no es aprovechada.

Es por todo lo anterior que se ha diseñado una red inalámbrica que provea la característica de movilidad que la biblioteca requiere, tomando como principal objetivo de esta implantación el desempeño eficaz y productivo de las actividades de sus integrantes, pero también observándolo como un proyecto rentable con la mejor relación costo-beneficio y permitiendo aprovechar al máximo todas las capacidades de la red y del personal que soporta su administración. Tal proyecto tiene como principales beneficios:

- Reducción de costos.
- Alta flexibilidad.
- Facilidad de implantación.

3.2.1 Aplicaciones y servicio de red.

Las aplicaciones y servicios que la red inalámbrica de la biblioteca Enrique Rivero Borrell ofrecerá son:

- Conexión a Internet.

Esto con la finalidad de que los alumnos puedan consultar páginas de internet, para obtener de ellas información de utilidad para sus labores estudiantiles.

- Correo electrónico.

Este tiene como fin le poder intercambiar información con compañeros relacionada con los quehaceres académicos, poder enviar tareas a profesores, etcétera.

- Mensajería instantánea.

Esto para intercambiar información en tiempo real con compañeros.

- Videoconferencia.

La videoconferencia es un sistema de comunicación que permite mantener reuniones colectivas entre varias personas que se encuentran en lugares distantes. Esto con la finalidad de que los alumnos puedan participar en conferencias y de esta forma actualizar sus conocimientos o adquirir nuevos.

- Reproducción de video.

Para que los alumnos pueden a tener acceso a documentales que se encuentran en Internet.

- Consulta de libros electrónicos.

La biblioteca a adquirido publicaciones digitales (libros electrónicos), y por medio de la red inalámbrica se les dará acceso a los alumnos a estos recursos.

- Consulta de tesis en tesiuam.

El alumno tenga acceso al catalogo de tesis de licenciatura, y posgrados con la que cuanta tesiuam.

Los usuarios de esta red inalámbrica solo podrán acceder a la red por medio del AP y no podrán acceder por medio de otra vía.

En cuanto al punto de acceso se refiere, deberá garantizar total compatibilidad y un funcionamiento, que satisfaga las necesidades y requerimientos de la biblioteca.

En la tabla 3.2 se muestra el ancho de banda que consumen ciertas aplicaciones de Internet.

Tabla 3.2. Ancho de banda consumido de algunas aplicaciones de Internet.

Aplicación	Ancho de banda/Usuario	Notas
Mensajes de texto	< 1Kbps	Como trafico es Infrecuente y asíncrono
Email	1 a 100Kbps	Es intermitente y asíncrono. Archivos adjuntos, virus y spam incrementan significativamente el uso del ancho de banda. Es importante aclarar que los servicios de webmail tal como Yahoo o Hotmail deben ser considerados como paginas Web no como email.
Paginas Web	50 a 100Kbps	Las páginas Web solo utilizan la red cuando un dato es requerido. La comunicación es asíncrona. Cuantos mas datos requieran (imágenes grandes, descargas, etc.) mayor es la utilización del ancho de banda.
Streaming audio	96 a 160Kbps	Cada usuario de este servicio usara una cantidad constante de ancho de banda.
Streaming video	64 a 200Kbps	Se evita la latencia utilizando buffers en el cliente. Requiere alta velocidad de conexión y baja latencia para trabajar adecuadamente.

Para estimar el throughput (velocidad con la que se envían y reciben datos) que necesitaría una red, sólo hay que multiplicar el número de usuarios esperados por el tipo de aplicación que usarían. Por ejemplo, 50 usuarios que usan principalmente el navegador Web consumirán entre 2.5 y 5Mbps o más en horas pico.

3.2.2 Conectividad.

El Access Point deberá estar colocado en la biblioteca de tal manera que los usuarios obtengan velocidades de conexión aceptables y que además cubran todas las posibles áreas de trabajo. Deberá estar configurado para evitar interferencias entre otros Ap's ubicados en el área ya que esto minimizaría el desempeño de la red inalámbrica.

3.2.3 Interoperabilidad.

La red inalámbrica deberá estar basada sobre estándares y normas que garanticen el funcionamiento conjunto entre los diversos elementos de software y hardware que son utilizados en la biblioteca Enrique Rivero Borrell.

3.2.4 Capacidad de desempeño.

El avance en el poder de procesamiento de equipos y la creación de aplicaciones que cada vez requieren de un mayor consumo de ancho de banda pueden llegar a ocasionar tráfico excesivo en la red.

El elemento de hardware de la red inalámbrica deberá de ser capaz de soportar la carga de trabajo para que permita ser configurado y llevar a cabo modificaciones y alcanzar un nivel de desempeño óptimo cuando sea necesario.

3.2.5 Administración.

El Access Point de la biblioteca deberá ser administrable para proporcionar monitoreo y análisis de tráfico, modificación de los parámetros de el equipo de manera remota y la generación de diagnósticos sobre el rendimiento y funcionamiento del dispositivo de red.

3.2.6 Tolerancia a fallos.

Siendo la red inalámbrica una subred de la red LAN, hereda las características tolerantes a fallos en la red. Actualmente la red de la biblioteca cuenta con:

- Enlace único, el cual asegura que todos los dispositivos principales de red estarán interconectados.
- Fuentes de poder interrumpibles, las cuales son capaces de soportar las operaciones de red durante interrupciones en el suministro de energía.

3.2.7 Flexibilidad topológica.

Las tecnologías de redes inalámbricas están apareciendo con gran rapidez. Por lo tanto, la tecnología que se escoja para la implantación de la red inalámbrica de la biblioteca deberá garantizar que en un futuro, ante el inevitable nacimiento de nuevas tecnologías, pueda ser integrada sin que cause conflictos en su operación. Además debe

permitir integrar dichas tecnologías sin necesidad de un rediseño total o peor aún, el desuso de ésta.

3.2.8 Documentación.

Es importante que la red inalámbrica de la biblioteca Enrique Rivero Borrell esté documentada en su totalidad para tener una base de información útil para la administración, mantenimiento y actualizaciones de la misma. Esta documentación puede estar constituida por manuales de instalación, operación y mantenimiento de los equipos de red, reportes de revisiones técnicas del hardware y su software asociado, los proyectos de migración y actualización, las instalaciones de nuevas versiones de software, la integración con otras tecnologías de red y la limpieza periódica de equipos.

3.3 Diseño y solución.

El objetivo principal es el de ofrecer el servicio de internet en las bibliotecas de la facultad de Ingeniería a los alumnos de ésta, con la finalidad de que tengan una herramienta más en su formación profesional.

Para tomar decisiones en el diseño se deben de considerar el objetivo principal y los siguientes factores:

- Tecnología.
Usar tecnología que se encuentre en el mercado y que cubra las necesidades.
- Acceso a usuarios autorizados.

Solo podrán hacer uso del servicio los alumnos inscritos en el semestre en curso y que se hayan registrado para el uso del servicio.

- Estructura física y lógica de la red.
Evitar lo más posible el realizar modificaciones a la estructura física y a la red de datos de la biblioteca.
- Administración.
La administración sea sencilla.
- Costo.
Los costos de la implementación sean bajos.

Tomando en cuenta estos factores y las pruebas realizadas a la infraestructura, es que se ha tomada la decisión de implementar la red inalámbrica para ofrecer el servicio de internet a los alumnos.

Una de las ventajas de esta solución es que se reducen los costos ya que estos se incrementarían en caso de que se quisiera implementar la red para los alumnos de forma cableada.

Otro punto a favor es que no se afectaría la infraestructura de la biblioteca ya que las modificaciones sería mínimas esto aunado que es una tecnología que avanza rápidamente.

En cuestión de la administración, se creará una página web en la que los alumnos se darán de alta para poder hacer uso del servicio (ver capítulo 4), en esta página cuando un alumno requiera realizar su registro lo primero que se realizara es verificar que el alumno se encuentre en la base de datos de alumnos inscritos en el semestre en curso, si es así se le permitirá continuar.

Ya que se haya verificado que es alumno de la facultad y que se encuentra inscrito en la facultad de Ingeniería se le desplegara una cuestionario que deberá de llenar para poder ser registrado en el servicio, en donde se le pedirán datos personales como del equipo con el que hará uso de la red inalámbrica, al terminar su registro se le enviará un correo electrónico de forma automática a la dirección que dio de alta en la que se le enviará el usuario y contraseña que utilizará para poder hacer uso de la red inalámbrica.

Se creara un filtro de dirección MAC para que solo el equipo que el alumno dio de alta en el registro sea el que pueda hacer uso del servicio de red inalámbrica (ver bridge página 104).

En cuestión de las direcciones IP's se utilizará un NAT para generar las direcciones IP's para los clientes, además de un servidor DHCP para la asignación automática de estas (ver página 104 y 105).

Con todo lo anterior hace que la administración se sencilla ya que todo se hace de forma automática.

También se realizar un filtrado web esto con la finalidad de evitar el que los alumnos consulten material inconveniente como podría ser paginas pornográficas, de contenido violento, etcétera, y de aplicaciones como podría ser Skype, etcétera (ver página 105).

La configuración lógica para la red inalámbrica quedaría de la siguiente manera:

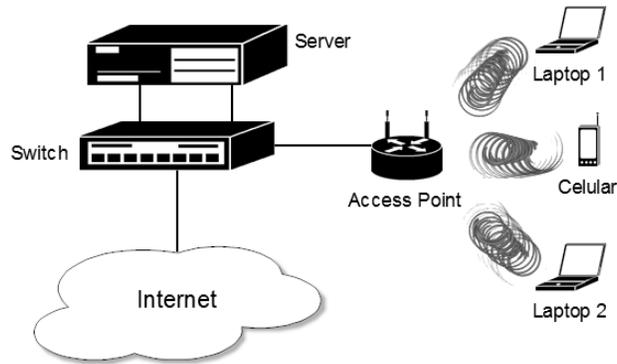


Figura 3.4. Configuración lógica red inalámbrica.

En lo que corresponde al servidor quedaría de la siguiente forma:

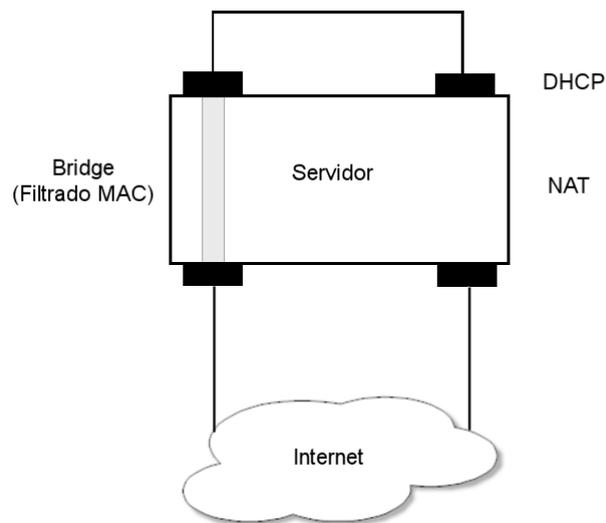


Figura 3.5. Diseño del servidor para la red inalámbrica.

En el servidor se montará los siguientes servicios:

- WEB.
- Base de datos.
- Filtrado de contenido.
- Firewall.

- Autenticación.
- Servidor de correos.

3.3.1 Arquitectura.

Configuración lógica de la Red Inalámbrica.

Actualmente la red de la biblioteca Enrique Rivero Borrell tiene la estructura que muestra la figura 3.6:

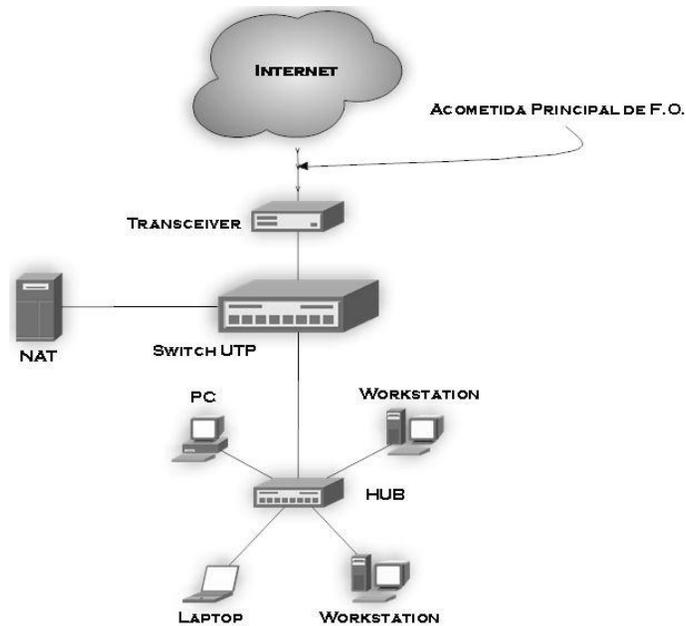


Figura 3.6. Estructura de la red actual en la biblioteca.

Al integrar la red inalámbrica a este esquema no es necesaria la modificación de éste ya que será una extensión de la red actual, y trabajarán de manera independiente, el esquema sería como el que se muestra en la figura 3.7:

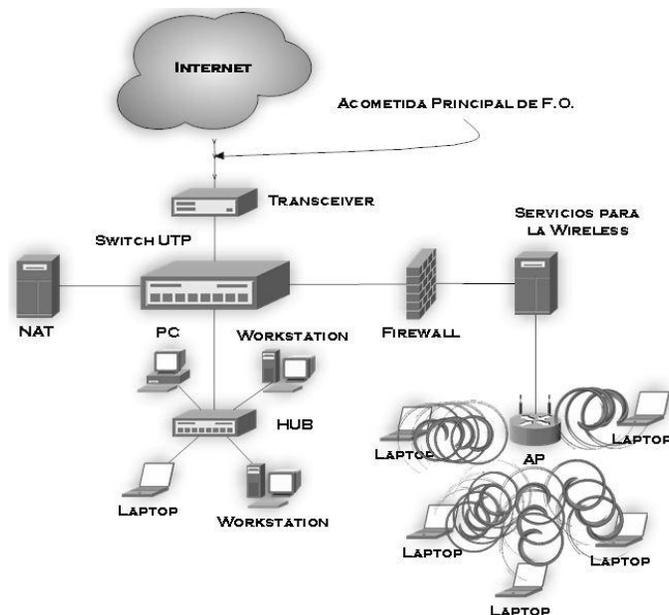


Figura 3.7. Estructura de la red al incorporar la red inalámbrica en la biblioteca.

3.3.1.1 Red inalámbrica para alumnos de la Facultad de Ingeniería.

Es importante tener en cuenta lo siguiente:

- Definir lo que sería un usuario de la red inalámbrica.

Un usuario de la red inalámbrica será toda aquella persona que esté en el dominio de la Facultad de Ingeniería como:

- Profesores.
- Administrativos.
- Alumnos.

Los alumnos deben estar inscritos en el semestre en curso en la Facultad de Ingeniería.

Se debe de tener también en cuenta de que, debido a que no se tiene ninguna garantía del estado de la máquina, esto es, que tenga antivirus, parches, actualizaciones del sistema operativo, etc., no podrá tener acceso a los recursos del dominio y sólo podrá hacer uso de Internet (protocolo http, los demás puertos y protocolos quedan excluidos).

Parámetros de configuración del Access point.

Frecuencia.

Como se mencionó anteriormente el access point, lo utilizaremos en la frecuencia de 2.4 GHz. Debido al estándar 802.11b/g, aunque de ser necesario, se tiene la capacidad de ofrecer el servicio a 5GHz sin la modificación del esquema.

SSID.

El SSID (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red, es importante configurar un SSID que sea fácilmente identificable.

Autenticación y cifrado.

Se utilizará el WPA ya que es el protocolo más seguro hasta el momento, con esto será de manera obligatoria la autenticación mediante un servidor Radius y por el lado del cifrado de datos, AES resulta el estándar más fuerte (ver Radius página 104).

3.3.2 Mecanismos de acceso y filtrado.

3.3.2.1 Bases para el diseño del firewall.

Es importante tener en cuenta las siguientes consideraciones para la

elaboración de las políticas que se evaluarán e implementarán en el firewall y que regirán la red inalámbrica de la biblioteca:

- Recursos a los que podrán tener acceso los usuarios de la red inalámbrica.
- Políticas actuales que rigen la red de la Facultad de Ingeniería.
- Componentes de la red inalámbrica.

3.3.2.2 Políticas del firewall.

Existen mecanismos que permiten tener una verdadera equivalencia al cable, sin embargo, es importante que la red inalámbrica pase necesariamente por el firewall debido a que, con ello se subsana cualquier vulnerabilidad que puedan presentar dichos mecanismos. Los recursos a los que tendrán acceso los usuarios de la red inalámbrica deben ser solo para fin académico teniendo permisos diferentes a los que tienen derecho los usuarios que accedan mediante la red cableada. Por lo tanto, las políticas que se apliquen deberán ser las diferentes evitando así, que haya problemas entre redes.

La configuración del firewall se basará en una política restrictiva en donde se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar los servicios que se necesitan. Esta política es la más segura, ya que es más difícil permitir un error de tráfico potencialmente peligroso.

Al adoptar este tipo de política restrictiva se bloqueará todo el tráfico entrante que pasa por el firewall esto con la finalidad de proteger a los usuarios de nuestra red inalámbrica, solo permitiendo el acceso al servicio de DNS que utiliza el puerto 53, esto con la finalidad de

resolver los nombre de las paginas, también se bloqueara la utilidad ping que sirve para verificar el estado de conexión de algún host en la red, esto con la finalidad de evitar ataques y de que agentes externos malintencionados puedan verificar la configuración de nuestra subred y lanzar ataques como podrían ser de negación de servicios.

3.3.2.3 Política interna de la red Inalámbrica.

Las políticas de una red son un documento fundamental, sin el cual el rol de un administrador de sistemas no sólo se complica, sino que se vuelve imposible de realizar. Este documento guía al administrador en su labor. Un documento de políticas de red debe ser firmado por la persona que tenga el cargo más alto de la organización.

Solamente de esa manera tendrá suficiente autoridad para ser obligatorio para cualquiera. Algo importante, es recordar que todo documento obligatorio para todo usuario de la red también los es para el administrador.

Este documento generalmente es de un par de páginas en donde se describen las políticas más generales. En contraposición, los procedimientos de seguridad son documentos más largos y detallados que explican a detalle cómo se va a implementar cada uno de los puntos de las políticas. Los procedimientos deben presentar una estructura similar a la de las políticas, y cada uno de sus puntos debe servir de explicación a su contraparte en las políticas (ver página 191).

3.3.2.4 Componentes del acceso a la red.

- **Firewall OpenBSD.** Este software toma las decisiones de rehusar ó permitir el paso de cada uno de los paquetes que son recibidos. El

software examina cada datagrama para determinar si éste corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, éste será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado.

- **Bridge.** Contiene las reglas para aceptar o denegar el acceso a una dirección MAC que intente conectarse a la red inalámbrica, permite al administrador de red la implantación de una política de seguridad más que la que permite Packet Filter (ver página 161).
- **Radius.** Nos permite la autenticación y autorización para que un alumno se conecte a la red para acceder al servicio (ver página 179).

3.4 Administración de subredes y direcciones IP.

3.4.2 NAT.

Debido a la escasez de direcciones IP que pudiera presentarse, además de ser una práctica sana de administración y de que proporciona un nivel de seguridad, se hace necesaria la implantación del mecanismo NAT para la red inalámbrica, se utilizará una máscara de red para generar 256 direcciones IP (ver página 158).

3.4.3 DHCP.

La asignación de direcciones IP mediante DHCP se lleva a cabo de manera dinámica con IP's no homologados. Con esto el administrador se libera de preasignar manualmente a cada usuario una dirección IP. Por cuestiones de administración es conveniente seguir con tal práctica, ya que de esta manera se tendría un control sobre los usuarios que deseen hacer uso de la red inalámbrica (ver página 163).

3.4 Administración de Contenido en páginas WEB.

Squid. Es un popular programa de software libre que implementa un servidor proxy y un demonio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico (ver página 187).

CAPÍTULO IV

Automatización del Registro para acceder a la Red Inalámbrica

4.1 Análisis.

En este capítulo se describe el proceso de automatización en su fase de análisis y diseño para la creación del sistema de registro de usuarios, para poder hacer uso de la red inalámbrica de la biblioteca Enrique Rivero Borrell, en esta parte del capítulo se registran los requerimientos que tendrían que solicitarse cuando la red inalámbrica este en funcionamiento.

Así como en toda institución educativa, se realizan trámites administrativos, la biblioteca también los realiza para que un alumno pueda hacer uso de la red inalámbrica, se tendrían que seguir una serie de pasos para registrarse.

El alumno:

- Debe estar inscrito en el semestre.
- Acudir al lugar de registro en el horario indicado.
- Llenar una hoja de solicitud.
- Presentar copia de tira de materias e identificación con fotografía.
- Llevar su equipo para obtener dirección mac de su tarjeta de red.
- Esperar a que los datos sean corroborados para obtener clave de acceso.

Administrativo:

- Facilitarle al alumno la hoja de solicitud de uso de la red inalámbrica.
- Recibir la hoja de solicitud y copia de tira de materias e identificación con fotografía.
- Verificar los datos del alumno.

- Obtener la dirección MAC de la tarjeta de red del equipo del alumno.
- Proporcionar los datos de la tarjeta de red al administrador del servidor.
- Darle al alumno su clave de acceso.

Administrador del servidor:

- Dar de alta la dirección MAC del alumno en el servidor.
- Capturar los datos de las hojas de registro.
- Generar la clave de acceso del alumno para la red inalámbrica.

Éstos son los pasos que tiene que realizar para poder ofrecer el servicio de red inalámbrica en las bibliotecas de la facultad.

Aunque esto no parece muy importante es algo tedioso, presentando algunas desventajas y problemas como son las siguientes:

- El alumno no tenga identificación.
- El alumno no puede asistir en el horario indicado.
- El administrativo no se encuentre en su área de trabajo.
- El administrativo no apunta la dirección MAC correctamente.
- El administrador del servidor no se encuentre en su área de trabajo.
- El administrador del servidor no capture la dirección MAC correctamente.
- El administrador del servidor no genere correctamente la clave de usuario.
- El tiempo que tarda en realizarse el trámite completo.

Al observar los problemas que pueden surgir y tomando en cuenta que

existe además de un gasto en papelería y tiempo en la capacitación del personal que va a atender a los alumnos y del que va a administrar el servidor, tomando todos estos factores en cuenta es que se propone que se realice este proceso mediante una interfaz web que capture los datos solicitados y se realice el alta y la generación de la contraseña de red de manera automática y en tiempo real, esto con la finalidad de agilizar el trámite y hacerlo más eficiente.

4.1.1. Requerimientos generales del sistema de registro.

Debido a la problemática planteada se tiene la necesidad de crear un sistema de registro que facilite el proceso anteriormente descrito, para obtener los resultados en el menor tiempo, con mayor eficacia y veracidad. Por lo que se requiere que el sistema cuente con las siguientes características:

- El registro sea llenado vía Web.
- Restringir el acceso a los usuarios a fin de que sólo los alumnos inscritos puedan acceder a la red inalámbrica.
- Sólo los equipos de cómputo que registren los usuarios sean los que puedan hacer uso del servicio de red inalámbrica.
- Generar claves de acceso independientes para cada usuario.
- Se envíen los datos de acceso mediante correo electrónico a los usuarios solicitantes.

Los requerimientos anteriores nos permiten definir el hardware óptimo que se debe utilizar, el sistema operativo que satisfaga las necesidades, las aplicaciones de software que se usarán y los gastos totales de la implementación que no sean muy elevados.

- Hardware a utilizar.

Las características del servidor que se necesitan para una implementación óptima se especifican a continuación.

Características del servidor.

- ✓ Intel Pentium 4 (GenuineIntel 586-class) 2 Ghz.
- ✓ Memoria RAM 1024 MB.
- ✓ Disco duro de 80Gb.
- ✓ 4 tarjetas de red Ethernet 10/100.

Para la elección del AP se necesitan como mínimo los siguientes requerimientos:

- ✓ Velocidad de transferencia de datos 54 Mbps.
- ✓ Protocolo de interconexión de datos IEEE 802.11b, IEEE 802.11g.
- ✓ Banda de frecuencia 2.4 GHz.
- ✓ N° de canales seleccionables 10.
- ✓ Método de autenticación RADIUS.

- Sistema Operativo.

Para poder elegir un sistema operativo se tiene que tomar en cuenta que éste debe de satisfacer que sea libre, seguro y flexible, y uno de los sistemas operativos que cumplen o satisfacen estos requisitos es OpenBSD.

La filosofía de OpenBSD puede ser reducida a 3 palabras: libre, funcional y seguro. Libre hace referencia a su licencia, funcional se

refiere al estado en el cual se decide finalizar las versiones de los programas, y seguro por su extrema revisión y supervisión del código incluido en sus versiones.

Este sistema operativo, se concentra en la portabilidad, cumplimiento de normas y regulaciones, corrección, seguridad proactiva y criptografía integrada.

En este caso, OpenBSD servirá para implementar todos los servicios que se van a utilizar para realizar el sistema de registro para la red inalámbrica.

Toda la configuración de los servicios se hará o se implementará con herramientas GNU.

4.2 Configuración general de los servicios del sistema de registro.

Servicio DHCP.

Este protocolo permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma *dinámica* (es decir, sin intervención de alguna persona que esté frente al equipo). El objetivo principal es simplificar la administración de la red.

Servicio Bridge.

El servicio de bridge es el que va a permitir realizar el filtrado de direcciones MAC de la tarjeta de red inalámbrica de los equipos que se encuentren registrados y de esta forma limitar el acceso a la red a equipos que no estén registrados.

Servidor Radius.

El protocolo de autenticación Radius permite verificar que los datos del alumno que son el nombre de usuario y la contraseña son correctos utilizando esquemas de autenticación como WPA, TKIP o EAP. Si los datos son correctos, el servidor autorizará el acceso a los recursos de la red inalámbrica.

Nosotros utilizaremos el software FreeRadius, entre sus principales características está la factibilidad de usar software de Base de Datos como OpenLDAP, MySQL, PostgreSQL, Oracle y soporta varios protocolos de autenticación como EAP, con EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, MSCHAPv2 y subtipos de Cisco LEAP. Todos estos protocolos son usados en la mayoría de los equipos wireless de equipos portátiles y Access point del mercado.

Permite usar los estándares de encriptación WEP, WPA, WPA2, etc.

Base de datos.

Se implementará una base de datos para poder tener a la disposición la información de los alumnos que se encuentran inscritos en la Facultad de Ingeniería, junto con la información de los alumnos que se inscribieron al servicio de la red inalámbrica, también se generará otra base de datos que se utilizará en conjunto con el servidor FreeRadius para tener los datos de usuario y contraseña que pueden acceder a la red inalámbrica.

Se va a utilizar el manejador de base de datos MySQL que es el manejador OpenSource más popular. Su arquitectura lo hace extremadamente rápido y fácil de adaptar.

Servidor WEB.

Éste nos sirve para atender y responder las peticiones HTTP de los navegadores, aquí es donde se monta la página web.

Se va a utilizar Apache que es un servidor OpenSource HTTP para sistemas operativos modernos. Éste es seguro, eficiente y un servidor Web expandible, los servicios Apache están de acuerdo con los estándares HTTP actuales. Apache es el servidor Web más popular en el Internet.

Filtrado WEB.

Se instalará el programa Squid el cual tiene una amplia variedad de utilidades como por ejemplo caché de web, además de añadir filtrando el tráfico.

La aplicación se utilizará para denegar el acceso a ciertas páginas WEB y ciertas aplicaciones como por ejemplo el mensajero instantáneo Messenger y aplicaciones peer to peer.

Servidor de correos.

Es una aplicación que permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Se empleará para enviar al correo que el alumno haya registrado los datos de usuario y contraseña para acceder a la red inalámbrica.

También para recibir comentarios o sugerencias.

PHP.

Es un lenguaje de propósito general ampliamente usado y que está diseñado especialmente para desarrollo web y puede ser incrustado dentro de código HTML. Generalmente se ejecuta en un servidor web, tomando el código en PHP como su entrada y creando páginas web como salida. Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos y plataformas.

Este ayudará a corroborar si el alumno está inscrito y llenar el formulario de registro.

También ayudará a modificar archivos del sistema para poder dar acceso a los alumnos de acuerdo con la información de su tarjeta de red y enviar al correo del alumno la información de su usuario y contraseña que utilizará para acceder a la red inalámbrica.

4.2.1 Ports o paquetes pre compilados.

Para la configuración de los servicios se emplearán los paquetes o ports aquí una explicación:

Los paquetes son binarios precompilados de algunos de los programas más usados. Están preparados para usarlos directamente en un sistema OpenBSD.

El sistema de ports en OpenBSD está orientado a ser usado para crear el producto final: los paquetes. Al instalar un port, en primer lugar se crea un paquete y a continuación lo instala. Los paquetes están formados por un fichero *makefile*, ficheros de texto con descripciones y mensajes de instalación (*readme*, *install*, etc.), todos los parches necesarios para que el programa funcione en el sistema OpenBSD y una lista de ficheros con aquellos que deben ser incluidos en el paquete.

Éstos son en general los servicios que se utilizarán para ofrecer los recursos de la red inalámbrica en las bibliotecas de la Facultad de Ingeniería.

4.3 Beneficios del sistema de registro vía Web.

Los beneficios que alcanza el registro vía Web son los siguientes:

- El alumno puede acceder al registro desde cualquier lugar con conexión a Internet.
- Sólo los alumnos inscritos en el semestre pueden acceder al registro.
- Automáticamente se genera clave de usuario del alumno.
- Envío de la clave de usuario al correo electrónico del alumno.
- No se genera papeleo de registro.
- Sólo una persona puede hacerse cargo del mantenimiento de los servicios.
- Toda la configuración de los servicios se realiza en un solo equipo.

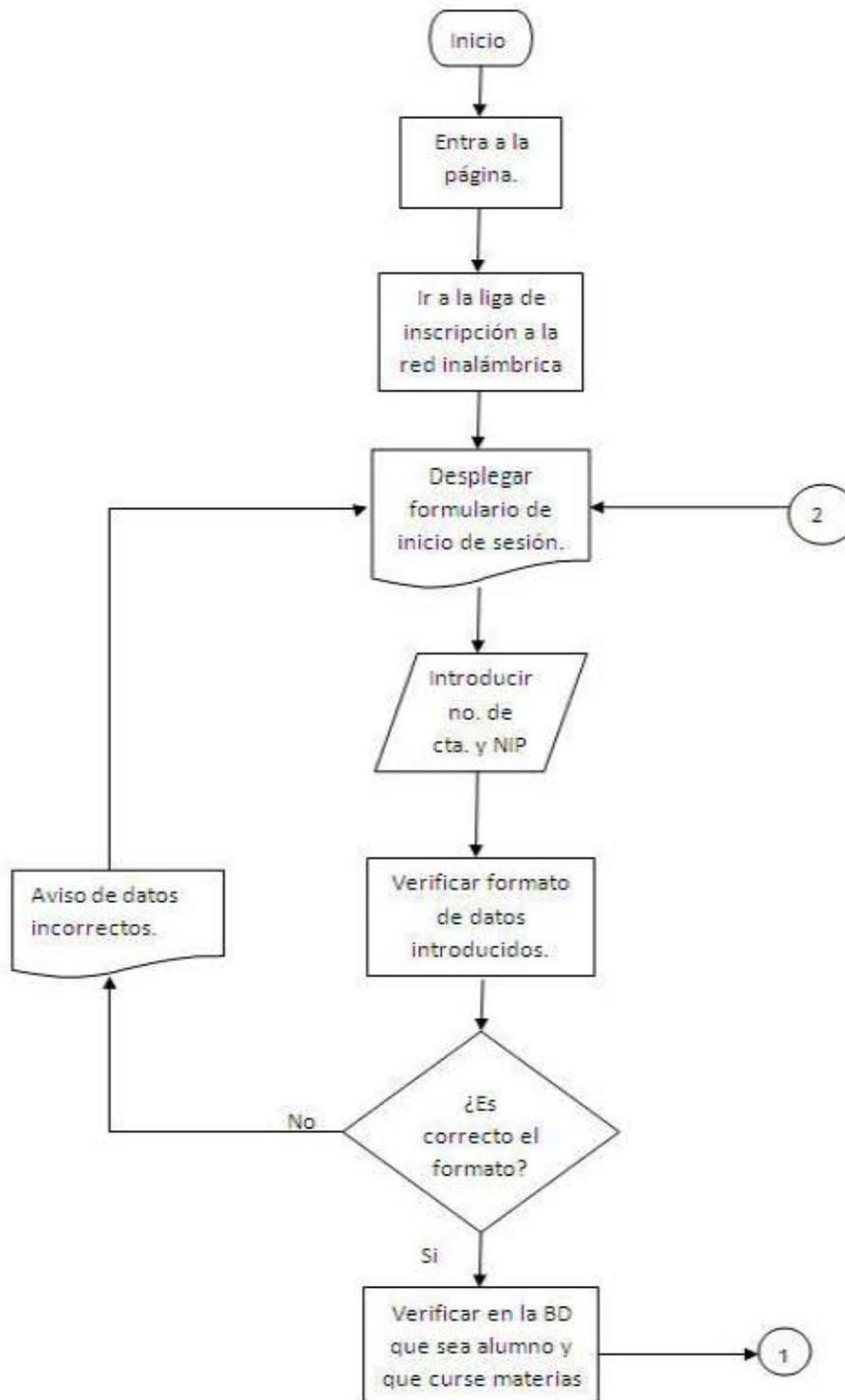
- El equipo es una PC de escritorio para evitar comprar un servidor en específico.

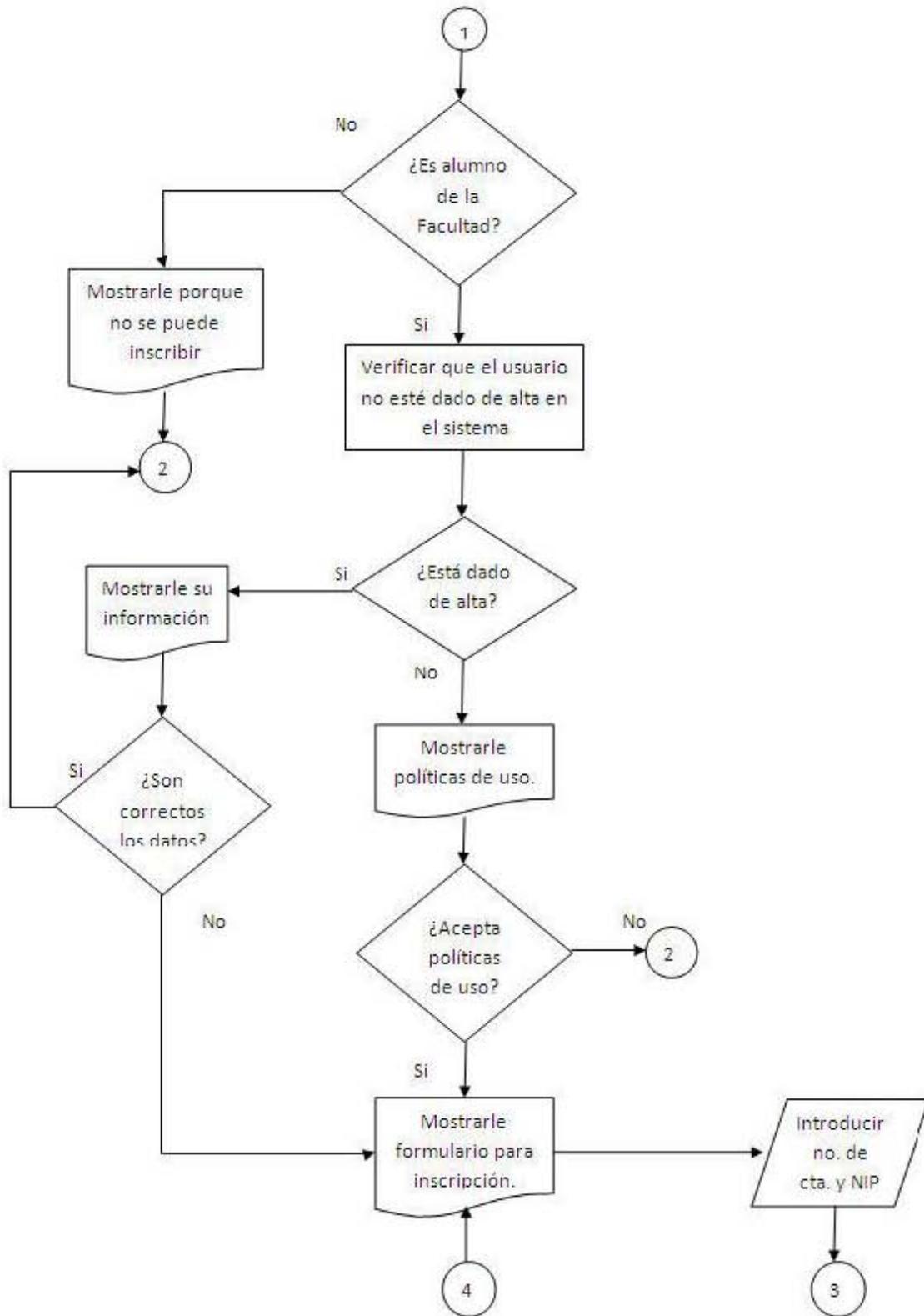
4.3.1 Pasos para la inscripción en línea.

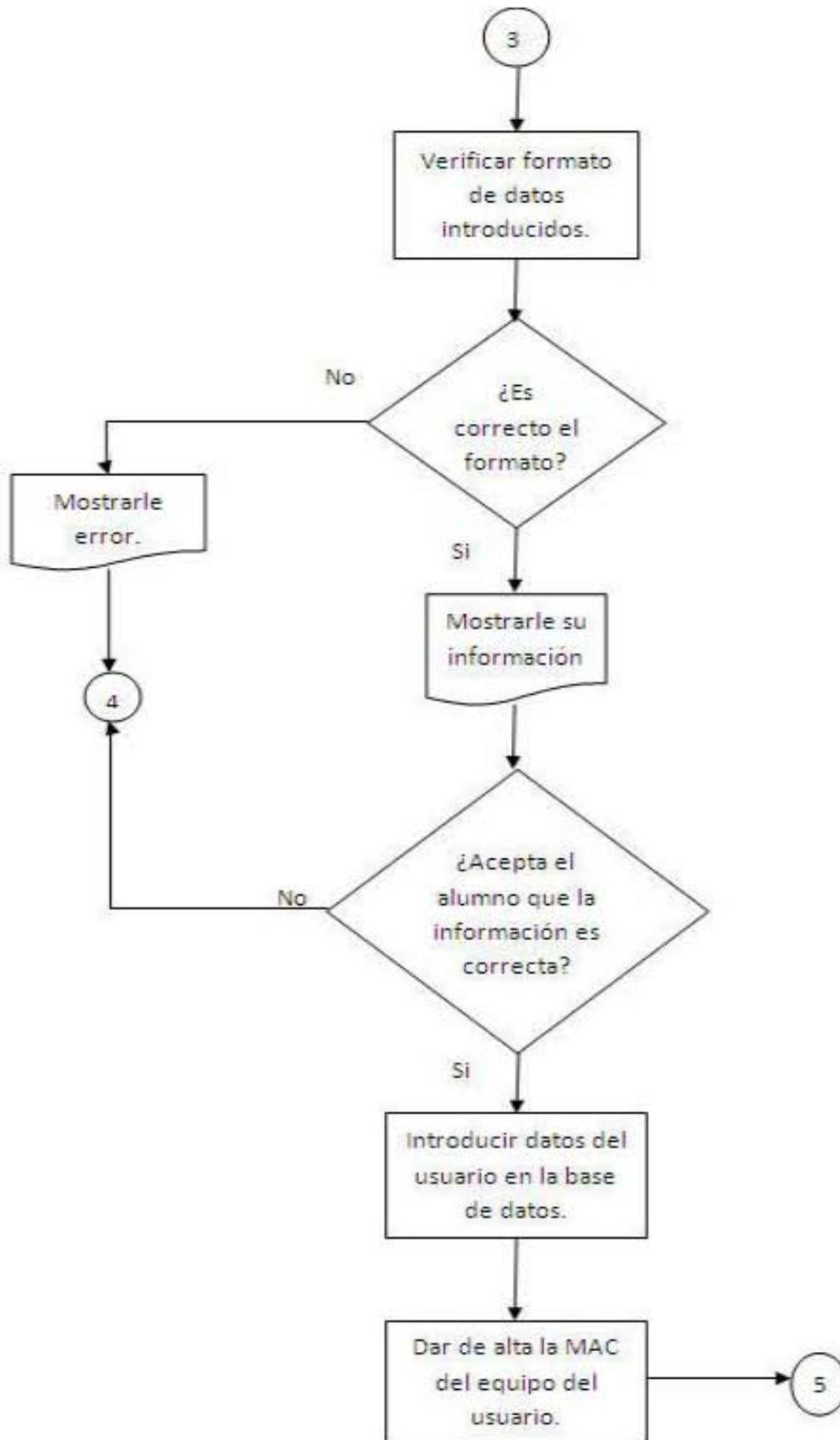
1. Entrar a la página.
2. Ir a la liga de inscripción de la red inalámbrica.
3. Desplegar formulario de inicio de sesión.
4. Introducir número de cuenta y NIP.
5. Verificar el formato de los datos introducidos por el usuario.
 - 5.1. Si no son correctos mandar aviso de datos incorrectos y volver al punto 3.
 - 5.2. Si son correctos, autenticar que los datos introducidos por el usuario correspondan a un alumno de la facultad que por lo menos tenga inscrita una materia, validándose en la base de datos.
 - 5.2.1. Si no corresponden a un alumno válido mostrar un mensaje del por que no se puede inscribir y pasar al punto 3.
 - 5.2.2. Si corresponden a un alumno, verificar que el usuario no se encuentra dado de alta en el sistema.
 - 5.2.2.1. Si no se encuentra dado de alta en el sistema, pasar al punto 6.
 - 5.2.2.2. Si se encuentra dado de alta mostrarle sus datos.
 - 5.2.2.2.1. Si acepta que son correctos mandarlo al punto tres.
 - 5.2.2.2.2. Si no acepta que son correctos mandarlo al punto 7 para que actualice su información.
6. Mostrarle las políticas de uso de la red inalámbrica junto con las sanciones a que se harán acreedores en caso de infringirlas.
 - 6.1. Si no acepta las políticas entonces no se le permita entrar al sistema y mandarlo al punto 3.
 - 6.2. Si las acepta pasar al punto 7.
7. Mostrarle el formulario para que el usuario introduzca su información.
8. Verificar que el formato de los datos introducidos sean correctos.
 - 8.1. Si no son correctos, desplegar mensaje de datos incorrectos y volver al punto 7.
 - 8.2. Si son correctos pasar al punto 9.
9. Mostrarle su información que introdujo para que el usuario la valide.

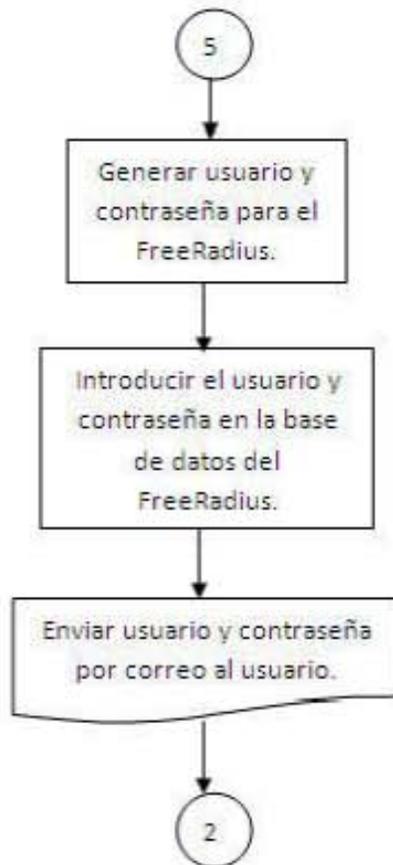
- 9.1. Si no acepta que es correcta mandarlo al punto 7 para que modifique su información correctamente.
- 9.2. Si acepta que la información es correcta pasar al punto 10.
10. Llenar los registros correspondientes de la base de datos con la información proporcionada por él usuario y activar el registro del usuario en la red inalámbrica.
11. Dar de alta su MAC address, para que se le pueda asignar una dirección IP a su equipo.
12. Generar usuario y contraseña para el alumno.
13. Introducir la información de usuario y contraseña en la base de datos del FreeRadius.
14. Enviar por correo al alumno su usuario y contraseña para que pueda acceder a los recursos de la red.

4.3.2 Diagrama de flujo del proceso de inscripción en línea.









4.3.3 Pantallas de la página de inscripción en línea.

En la figura 4.1 se muestra la pantalla de inicio del sistema de registro, aquí se les da la bienvenida a los alumnos, se puede observar que del lado derecho se muestran noticias de interés para los alumnos, del lado izquierdo se muestra una encuesta para saber la opinión de los alumnos con respecto a ciertos temas. También se muestran el número de visitantes y el menú.

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Miércoles 13 de mayo de 2009

Principal | Registrarse en la red inalámbrica | Ayuda | Contacto | Sitios de Interés

Número de Visitantes: 1644

Estas de acuerdo con la encuesta de los profesores via internet?
 Sí
 No
 No lo se

Bienvenidos a la página de inscripción a la red inalámbrica de las bibliotecas de la facultad de ingeniería.

Este servicio solo se ofrece a los alumnos de la facultad de ingeniería que se encuentre inscritos en alguna materia del semestre en curso.

Para el caso de alumnos sin derecho a inscripción pasar a las instalaciones de USECAD, que se encuentran en la planta baja del edificio C, conjunto Norte de la Facultad de Ingeniería.



Noticias

Es la UNAM, la universidad de México y la única nacional. José Nervo Robles (D-GCS) [Ver más...](#)

Mesa redonda: Los sistemas de gestión de la calidad. Mejor rectorado de la cultura organizacional. [Ver más...](#)

Programa Editorial de la Coordinación de Humanidades en el marco de la Feria Internacional del Libro. [Ver más...](#)

5º Curso taller de tecnologías suaves. [Ver más...](#)

Taller: Construcción de objetos de aprendizaje. [Ver más...](#)

En los primeros años de una relación no se detecta la epidemia (D-GCS) [Ver más...](#)

Convocatoria al Premio Nacional a la Juventud Indígena 2009. [Ver más...](#)

6ª Escuela de Investigación en Energía. [Ver más...](#)

Conferencia "El Futuro de la Energía" [Ver más...](#)

Coloquio "El mundo fascinante de las estrellas de neutrones" [Ver más...](#)

B.116 febrero 25, EN LOS OCEANOS, SI EXISTEN ORGANISMOS ENCEMOSOS [Ver más...](#)

B.117 febrero 25, IMPACTA PROFUNDAMENTE EL CAMBIO CLIMÁTICO A LAS AVES MIGRATORIAS [Ver más...](#)

B.118 febrero 26, INVESTIGAN EN LA UNAM, COMO DISMINUIR LA CONTAMINACIÓN POR CROMO [Ver más...](#)

Derechos Reservados USECAD 2009.

Figura 4.1 Pantalla de inicio de la página de registro.

Al dar click sobre la opción de contacto, se mostrará la ventana de la figura 4.2 en donde se proporcionan los números telefónicos y una dirección de correo, por si el alumno tiene alguna duda o por si requiere realizar algunas sugerencias.

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Jueves 14 de mayo de 2009

Principal | Registrarse en la red inalámbrica | Ayuda | Contacto | Sitios de Interés

Número de Visitantes:
1648

Estas de acuerdo con la encuesta de los profesores via internet?

Si
 No
 No lo se

Para dudas o sugerencias acudir a USECAD, que se encuentra en la planta baja del edificio C, conjunto Norte de la Facultad de Ingeniería.



O marcar a los telefonos: 56-22-09-60 al 63

O escribir a la dirección electronica: sosorte@CorreoSpawm.hell

Noticias

Es la UNAM, la universidad de México y la única nacional. José Narro Robles (DGCS)
[Ver más...](#)

Mesa redonda: Los sistemas de gestión de la calidad. Medio renovador de la cultura organizacional.
[Ver más...](#)

Programa Editorial de la Coordinación de Humanidades en el marco de la Feria Internacional del Libro.
[Ver más...](#)

5º Curso taller de tecnologías solares.
[Ver más...](#)

Taller: Construcción de objetos de aprendizaje.
[Ver más...](#)

En los primeros años de una relación no se detecta la violencia (DGCS)
[Ver más...](#)

Convocatoria al Premio Nacional a la Juventud Indígena 2009.
[Ver más...](#)

9ª Escuela de Investigación en Energía.
[Ver más...](#)

Conferencia "El Futuro de la Energía"
[Ver más...](#)

Coloquio: "El mundo fascinante de las estrellas de neutrones"
[Ver más...](#)

B.116 febrero 25, EN LOS OCEANOS, SI EXISTEN ORGANISMOS ENDEMICOS
[Ver más...](#)

B.117 febrero 25, IMPACTA PROFUNDAMENTE EL CAMBIO CLIMÁTICO A LAS AVES MIGRATORIAS
[Ver más...](#)

B.118 febrero 26, INVESTIGAN EN LA UNAM, COMO DISMINUIR LA CONTAMINACIÓN POR CROMO
[Ver más...](#)

Derechos Reservados USECAD 2009.

Figura 4.2 Pantalla de contacto de la página de registro.

En la opción de ayuda (figura 4.3) se proporcionan algunos tutoriales por si el alumno tiene alguna duda de cómo obtener la dirección MAC de su tarjeta de red inalámbrica, además de los manuales para poder configurar su tarjeta de red inalámbrica para poder hacer uso de los recursos.

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Jueves 14 de mayo de 2009.

Principal | Registrarse en la red inalámbrica | **Ayuda** | Contacto | Sitios de Interés

Número de Visitantes:
1650

Estas de acuerdo con la encuesta de los profesores via internet?
 Si
 No
 No lo se

Manual para obtener la dirección MAC de la tarjeta de red inalámbrica:

- [Windows](#)
- [Linux](#)
- [Macintosh](#)

Manual para configurar la tarjeta de red inalámbrica para poder hacer uso del servicio:

- [Windows](#)
- [Linux](#)
- [Macintosh](#)

Noticias

Es la UNAM, la universidad de México y la única nacional. José Narro Robles (DGCS) [Ver más...](#)

Mesa redonda: Los sistemas de gestión de la calidad. Medio renovador de la cultura organizacional. [Ver más...](#)

Programa Editorial de la Coordinación de Humanidades en el marco de la Feria Internacional del Libro. [Ver más...](#)

5º Curso taller de tecnologías solares. [Ver más...](#)

Taller: Construcción de objetos de aprendizaje. [Ver más...](#)

En los primeros años de una relación no se detecta la violencia (DGCS) [Ver más...](#)

Convocatoria al Premio Nacional a la Juventud Indígena 2009. [Ver más...](#)

9ª Escuela de Investigación en Energía. [Ver más...](#)

Conferencia "El Futuro de la Energía" [Ver más...](#)

Coloquio: "El mundo fascinante de las estrellas de neutrones" [Ver más...](#)

B.116 febrero 25, EN LOS OCEANOS, SI EXISTEN ORGANISMOS ENDEMICOS [Ver más...](#)

B.117 febrero 25, IMPACTA PROFUNDAMENTE EL CAMBIO CLIMATICO A LAS AVES MIGRATORIAS [Ver más...](#)

B.118 febrero 26, INVESTIGAN EN LA ENANA COMO DISMINUIR LA CONTAMINACIÓN POR CROMO [Ver más...](#)

Derechos Reservados USECAD 2009.

Figura 4.3 Pantalla de ayuda de la página de registro.

Al abrir la opción de sitios de interés se le proporcionarán al alumno algunas ligas de utilidad para él (figura 4.4).

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Jueves 14 de mayo de 2009.

Principal | Registrarse en la red inalámbrica | Ayuda | Contacto | **Sitios de Interés**

Número de Visitantes:
1651

Estas de acuerdo con la encuesta de los profesores via internet?
 Sí
 No
 No lo sé
Votar

[Página Principal de la UNAM.](#)
[Página Principal de la Facultad de Ingeniería.](#)
[Página de la División de Ciencias Básicas.](#)
[Página de Dirección General de Administración Escolar \(DGAE\).](#)
[Página de la Dirección General de Bibliotecas \(Catálogo de Bibliotecas\).](#)
[Página de la División de Ingeniería Eléctrica.](#)
[Página de la División de Ciencias de la Tierra.](#)
[Página de la División de Ingeniería Mecánica e Industrial.](#)
[Página de la División de Ingenierías Civil y Geomática.](#)
[Página del Palacio de Minería.](#)
[Página de la División de Ciencias Sociales y Humanidades.](#)
[Página de inscripciones de la Facultad de Ingeniería.](#)
[Página Unidad de Servicios de Computo Académico \(UNICA\).](#)
[Página de Servicios Académicos \(SSA\).](#)
[Página Dirección General de Actividades Deportivas y Recreativas.](#)
[Página del Bolsa de Trabajo de la UNAM.](#)
[Página de General de Servicios de Computo Académico \(DGSCA\).](#)

Noticias

Es la UNAM, la universidad de México y la única nacional José Narro Robles (DGCS)
[Ver más...](#)

Mesa redonda: Los sistemas de gestión de la calidad. Medio renovador de la cultura organizacional
[Ver más...](#)

Programa Editorial de la Coordinación de Humanidades en el marco de la Feria Internacional del Libro.
[Ver más...](#)

5º Curso taller de tecnologías solares.
[Ver más...](#)

Taller: Construcción de objetos de aprendizaje.
[Ver más...](#)

En los primeros años de una relación no se detecta la violencia (DGCS)
[Ver más...](#)

Convocatoria al Premio Nacional a la Juventud Indígena 2009
[Ver más...](#)

9ª Escuela de Investigación en Energía.
[Ver más...](#)

Conferencia "El Futuro de la Energía"
[Ver más...](#)

Coloquio "El mundo fascinante de las estrellas de neutrones"
[Ver más...](#)

B.116 febrero 25, EN LOS OCEANOS, SI EXISTEN ORGANISMOS ENDEMICOS
[Ver más...](#)

B.117 febrero 25, IMPACTA PROFUNDAMENTE EL CAMBIO CLIMÁTICO A LAS AVES MIGRATORIAS
[Ver más...](#)

B.118 febrero 26, INVESTIGAN EN LA UNAM, CÓMO DISMINUIR LA CONTAMINACIÓN POR CROMO
[Ver más...](#)

Derechos Reservados USECAD 2009.

Figura 4.4 Pantalla de ligas de interés de la página de registro.

Al dar click sobre el botón de “Registro en la red inalámbrica” se mostrarán las políticas y lineamientos (Figura 4.5) que se deben seguir o acatar para el uso de la red inalámbrica, si el alumno no las acepta se le regresará a la página de inicio si las acepta se la abrirá una ventana para que introduzca sus datos como son número de cuenta y NIP.

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Inicio | Registrar en la red inalámbrica | Ayuda | Contacto | Sobre de Internet
Miércoles 13 de marzo de 2008

Número de Visitantes
1046

¿Estas de acuerdo con la encuesta via wireless?
 Sí
 No
 No lo sé

Reglamento para el uso de equipo de cómputo y red inalámbrica de las bibliotecas "Enrique Rivero Borrell" y "Antonio Dovalí"

Toda persona que utilice el servicio de red inalámbrica de la biblioteca estará sujeto a los siguientes lineamientos:

El servicio de Internet está destinado primordialmente a la consulta en línea de material con fines puramente académicos.

Para tener acceso al servicio de red, el usuario previamente se deberá haber registrado en la página de inscripción de la red inalámbrica de las bibliotecas de facultad de ingeniería.

Notificar de inmediato cualquier anomalía presentada en la red al personal encargado para que corrija tal situación.

Queda prohibido:

- Compartir carpetas, archivos o impresoras en red.
- Utilizar los servicios de red con fines de lucro, entretenimiento personal, descarga de software, archivos de música, audio o video.
- Utilizar software que atente contra la seguridad de la red.
- Hacer mal uso de CHATS o círculos de conversación.
- El uso de altavoces, el usuario podrá escuchar archivos de audio utilizando solamente audífonos.
- Visitar páginas eróticas o pornográficas, así como colocar en los protectores de pantalla imágenes de este tipo pues se considera una falta de respeto a la institución.
- Atentar contra la información de otros usuarios.
- Ingresar o tratar de ingresar a otros equipos.
- Intercambio o distribución de contenido pornográfico.
- Propagar virus, gusanos u otro código malicioso ya sea con conocimiento o desconocimiento de ello.
- Usar la red para realizar actividades delictivas.
- Envío de mensajes no solicitados (spam).
- Atentar contra la disponibilidad, integridad, confidencialidad de la red.
- El uso simultáneo de una cuenta desde dos equipos diferentes.
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.

Dada la naturaleza del presente reglamento, su conocimiento y observancia son obligatorios para todos los usuarios que hagan uso de la red inalámbrica.

Su desconocimiento nunca podrá ser utilizado como excusa para evitar las sanciones correspondientes.

Sanciones

Al infringir las presentes políticas de uso de la red inalámbrica, el usuario se hará acreedor a las siguientes sanciones:

- *Expulsión temporal o definitiva de la facultad de perdiendo de la gravedad de la falta.*
- *Suspensión definitiva del servicio de red inalámbrica.*

Acepto

No acepto

Noticias

Es la UNAM, la Universidad de México y la Secretaría José María Robles (DOCS) ...

Mesa redonda: Los sistemas de gestión de la calidad. Medio recorrido en la cultura organizacional. ...

Programa Educativo de la Coordinación de Investigaciones en el área de la Física Interdisciplinaria del Libro. ...

El primer taller de tecnología solar. ...

Taller: Construcción de mapas de aptitud. ...

En los próximos días de esta edición se presentará la versión DOCS ...

Convocatoria al Premio Nacional a la Innovación Indígena 2009. ...

P. Escuela de Ingeniería en Energía. ...

Conferencia "El Futuro de la Energía". ...

Colegio: "El mundo comienza de las estrellas y continúa". ...

B 116 febrero 25, EN LOS OCEANOS, SI EXISTEN ORGANISMOS RESERVADOS. ...

B 117 febrero 25, IMPACTO PROYECTIVAMENTE EL CAMBIO CLIMÁTICO A LAS AVES MIGRATORIAS. ...

B 118 febrero 26, INVESTIGAN EN LA BAMA COMO CONSERVAR LA CONTAMINACIÓN POR OZONO. ...

Derechos Reservados USECAD. 2009

Figura 4.5 Políticas y lineamientos para el uso de la red inalámbrica.

Al aceptar las políticas se desplegará la pantalla de la figura 4.6 en donde se pide que el alumno introduzca su número de cuenta y el NIP para corroborarlos con la base de datos de alumnos inscritos.

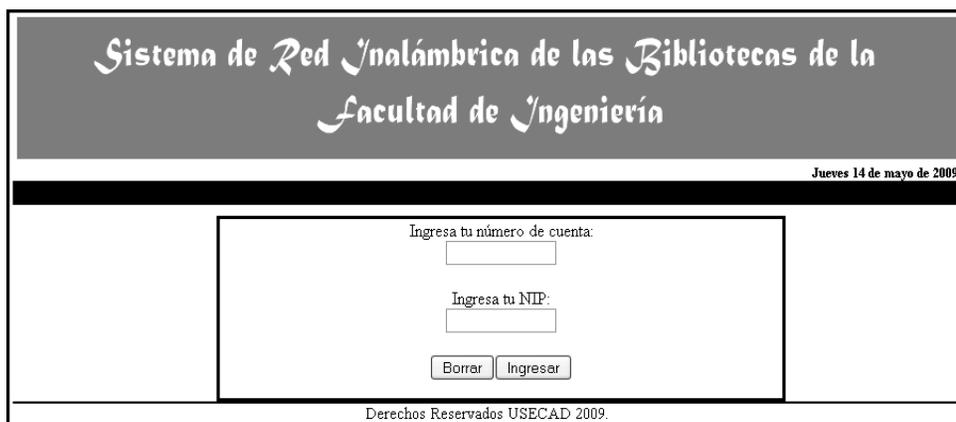


Figura 4.6 Ventana en donde el alumno introducirá su información.

Si el alumno introdujo incorrectamente sus datos se le desplegará esta misma ventana pero con una leyenda que le pedirá que verifique la información que ha introducido (figura 4.7).

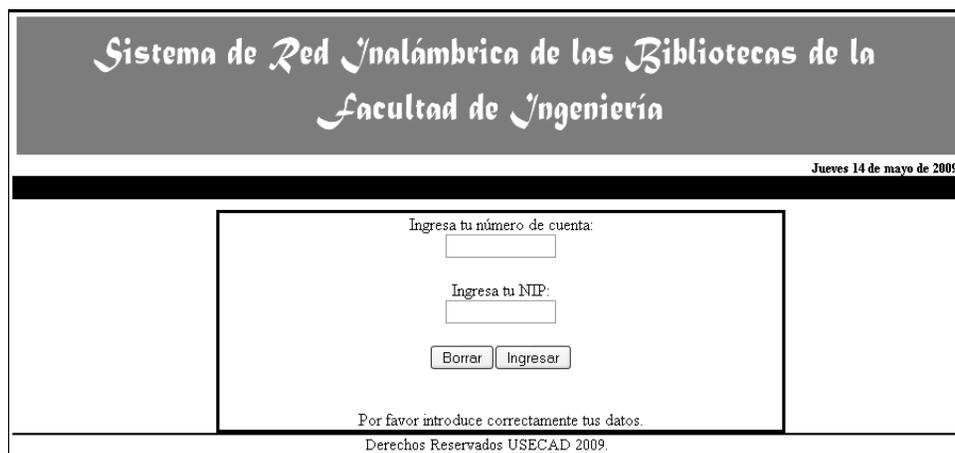


Figura 4.7 Error al introducir datos del alumno.

Al introducir correctamente los datos y si el alumno se encuentra inscrito se desplegará una ventana con los datos obtenidos de la base de datos, como son nombre, número de cuenta y carrera, y un formulario (figura 4.8 y 4.9).

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Domingo 24 de octubre de 2010

Ingresar tu número de cuenta:
096178225

Ingresar tu NIP:
•••••

Borrar Ingresar

Derechos Reservados USECAD 2009.

Figura 4.8 introduciendo datos del alumno.

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería

Miércoles 2 de marzo de 2011

Datos Personales

Nombre: Trejo Cruz Ulises Bernardo
Número de Cuenta: 096178225
Carrera: Ingeniería en Computación

Email:
Teléfono Casa:
Teléfono Celular (sin 044):
Dirección:

Datos Computadora

Marca: HP
Modelo:
Número de Serie:
Dirección MAC (separado por ":"): 00:00:00:00:00:00
Sistema Operativo: Windows

Registrar Cancelar

Derechos Reservados USECAD 2009.

Figura 4.9 Ventana con los datos obtenidos de la base de datos y formulario.

El usuario deberá llenar el formulario con los datos que se le solicitan (figura 4.10).

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería
Miércoles 2 de marzo de 2011

Datos Personales

Nombre: Trejo Cruz Ulises Bernardo
Número de Cuenta: 096178225
Carrera: Ingeniería en Computación

Email:	uliestrejocruz@gmail.com
Teléfono Casa:	56552487
Teléfono Celular (sin 044):	552742959
Dirección:	Av. Siempre Viva No. 55 Delegación Tlalpan C.P. 14568 México D.F.

Datos Computadora

Marca:	HP
Modelo:	dv400 fx
Número de Serie:	CND9344VPX
Dirección MAC (separado por ":"):	00:11:22:33:44:55
Sistema Operativo:	Windows

Registrar Cancelar

Derechos Reservados USECAD 2009.

Figura 4.10 Formulario con datos del alumno.

Si el usuario no llena un campo o si el formato no es el correcto le aparecerá una leyenda pidiéndole que verifique los campos.

Sistema de Red Inalámbrica de las Bibliotecas de la Facultad de Ingeniería
Miércoles 2 de marzo de 2011

Datos Personales

Nombre: Trejo Cruz Ulises Bernardo
Número de Cuenta: 096178225
Carrera: Ingeniería en Computación

Email:	
Teléfono Casa:	
Teléfono Celular (sin 044):	
Dirección:	

Datos Computadora

Marca:	HP
Modelo:	
Número de Serie:	
Dirección MAC (separado por ":"):	00:00:00:00:00:00
Sistema Operativo:	Windows

Registrar Cancelar

Favor de verificar los campos.

Derechos Reservados USECAD 2009.

Figura 4.11 Pantalla indicándole al alumno que verifique su información.

Ya que el alumno llene de forma correcta el formulario y dé click al botón registrar, se le mostrará una ventana (figura 4.12) informándole que su registro se ha realizado correctamente y el siguiente paso que debe seguir.



Figura 4.12 Ventana informando de registro exitoso.

En esta ventana se le informa al alumno que debe revisar su correo electrónico porque a éste se le enviará su usuario y contraseña (figura 4.13).

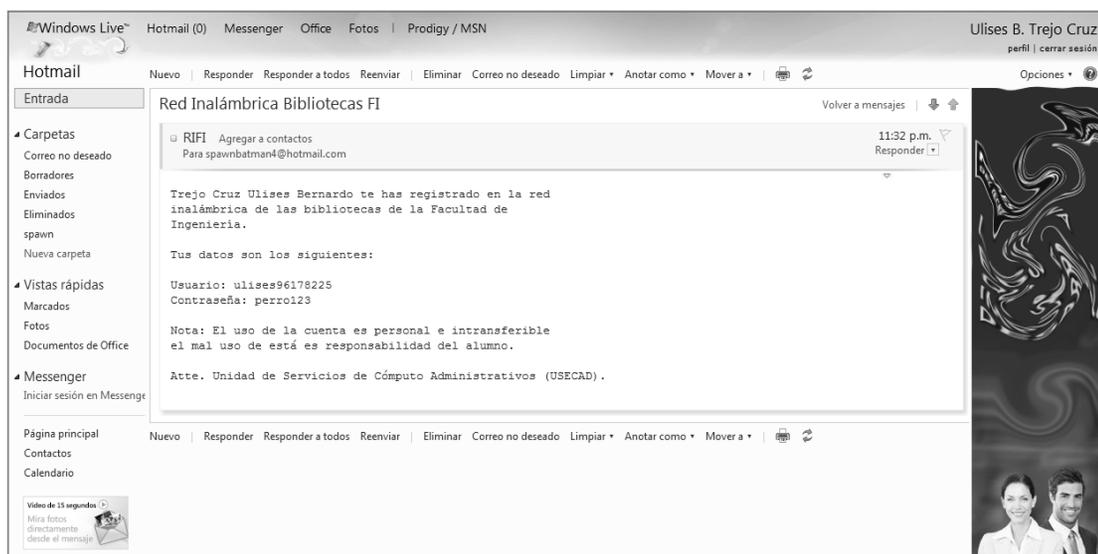


Figura 4.13 Correo con la información para acceder a la red inalámbrica.

Ya con esta información el alumno podrá conectarse a la red inalámbrica de las Bibliotecas de la Facultad de Ingeniería.

Para poder conectarse a la red inalámbrica el alumno debe realizar un escaneo de redes inalámbricas con el objetivo de detectar la red inalámbrica de las Bibliotecas (figura 4.14).

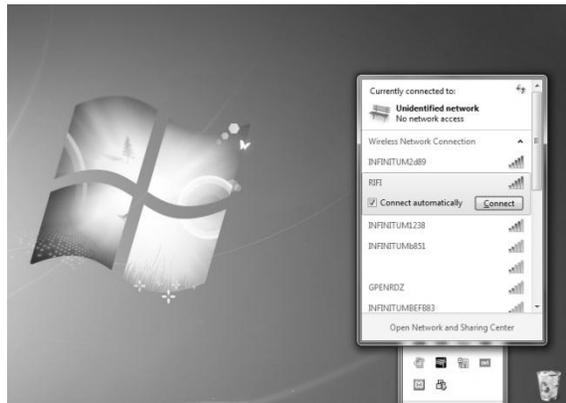


Figura 4.14 Escaneo de redes inalámbricas.

Al conectarse a esta red se le pedirá el usuario y contraseña que se le enviaron al alumno a su correo electrónico (figura 4.15 y 4.16).

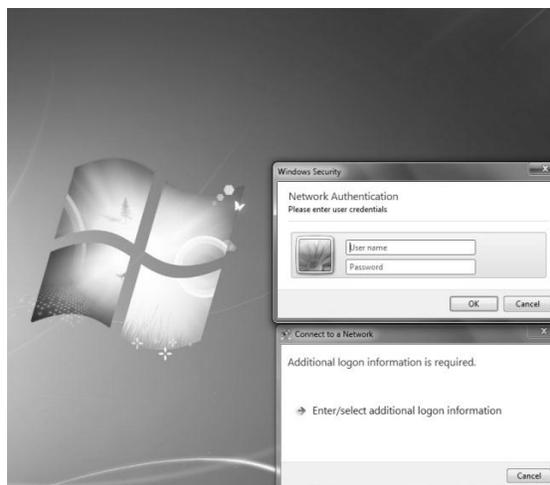


Figura 4.15 Ventana para introducir datos de alumnos.

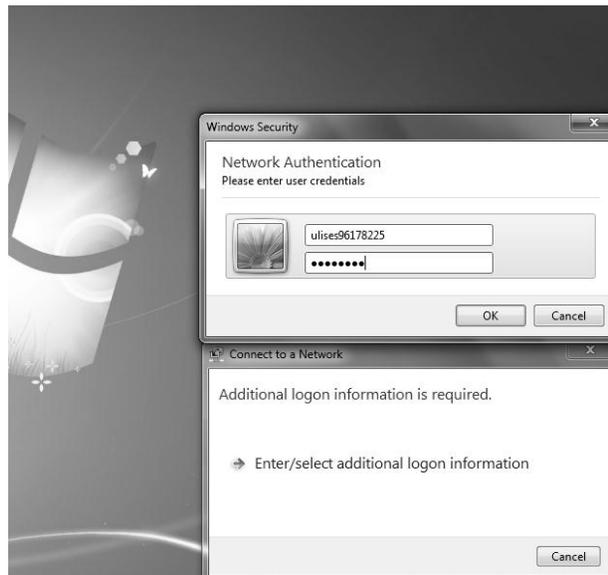


Figura 4.16 Introducción de datos del alumno.

Al introducir estos datos se le dará acceso al alumno a los recursos de la red inalámbrica de la Biblioteca de la Facultad de Ingeniería (figura 4.17, 4.18 y 4.19).



Figura 4.17 Acceso a la red inalámbrica.

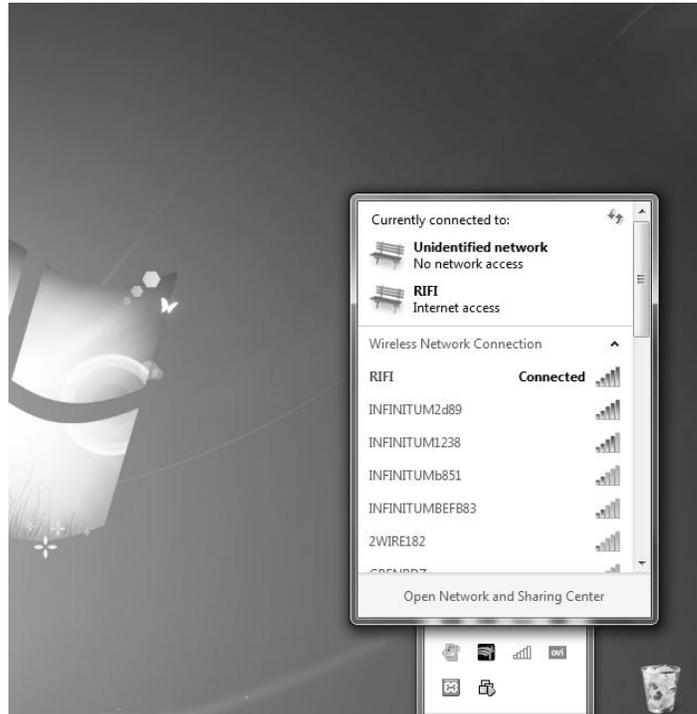


Figura 4.18 Conexión a la red inalámbrica de la biblioteca.



Figura 4.19 Navegación en internet.

CONCLUSIONES

En la actualidad el uso de la tecnología y, específicamente el uso de las computadoras y comunicaciones se ha extendido a todos los campos de la actividad laboral. Las bibliotecas no han sido la excepción y mucho menos tratándose de las bibliotecas de la Facultad de Ingeniería.

La problemática planteada tiene su origen en la inexistencia de suficientes puntos de red para cubrir la cantidad de nuevos usuarios que necesitan conectarse a la misma en la biblioteca Enrique Rivero Borrell.

Con la elaboración del presente trabajo profesional, el análisis de los requerimientos, el diseño e implementación del sistema de acceso a la red inalámbrica a los usuarios de la biblioteca Enrique Rivero Borrell de la Facultad de Ingeniería, se cumplió con el objetivo de ofrecer una alternativa para brindar el servicio de acceso a internet a los usuarios, este servicio hoy en día es de vital importancia para la formación académica de un Ingeniero ya que permite refirmar y ampliar los conocimientos adquiridos con información de primera mano y actualizada, también permite a la biblioteca ampliar el catálogo de servicios ofreciendo libros, publicaciones, conferencias, cursos y toda clase de información referente a la Ingeniería y temas en general, todo esto en su gran mayoría de manera gratuita. Es así por lo que este trabajo arrojó las siguientes conclusiones que hacen posible lo antes mencionado ayudando a la vida académica de la Facultad de ingeniería.

Se logró crear un sistema integral compuesto por una red inalámbrica, un sistema de registro de usuarios y un sistema de seguridad hace que el uso por parte de los usuarios del servicio de internet en la biblioteca sea lo más eficiente y transparente para los usuarios, para ello se

realizó un estudio de diversas tecnologías que pudieran ser parte de este proyecto escogiendo aquellas que brindaran los beneficios en eficiencia, costo, manejabilidad, escalabilidad que hace que el costo-beneficio en comparación con otras propuestas en cuanto a implementación, administración y uso de ésta sea la más aceptable.

Como resultado de un análisis para la implementación de una red inalámbrica para el acceso a internet por parte de los usuarios de la biblioteca se cumplió el objetivo de cubrir gran parte del espacio posible que abarca la biblioteca, la red inalámbrica puede ser usada no solamente para el servicio a los usuarios sino también para los servicios de administración de la biblioteca, se aprovechó en lo mayor posible la arquitectura del edificio utilizando la menor cantidad de puntos de acceso posible y afectando en menor medida la estructura de ésta, las labores y operación de la biblioteca no se verán afectadas en la implementación de la red, la facilidad de desplazamiento que los usuarios tendrán para ir de un lugar a otro y seguir conectado dentro de la biblioteca es uno de los mayores beneficios que se tienen al implementar la red inalámbrica y el número de usuarios sólo estará limitado al ancho de banda disponible. Si se compara por poner un ejemplo, con el uso de una LAN cableada se habría tenido que hacer un gasto considerable en la instalación de los nodos en mano de obra y material, también se vería afectada la estructura del edificio y las labores y operación de la biblioteca no se podrían llevar a cabo de una manera habitual, el número de usuarios estaría limitado al número de nodos instalados. Por éstos y otros motivos como facilitar la administración de la red y una mejor respuesta en la solución de incidentes hace que esta propuesta aventaje a otras y sea la más viable.

Los conocimientos adquiridos en conjunto con la formación que recibimos en la Facultad de Ingeniería permitió analizar el problema y resolverlo de la forma más adecuada. La información que recibida a lo largo de toda la carrera es bastante y a pesar de que en algunas ocasiones es muy general, debido a lo corto de los semestres, esta información contiene conocimientos sólidos que sirven como base para enfrentar algún problema en nuestra vida personal y laboral.

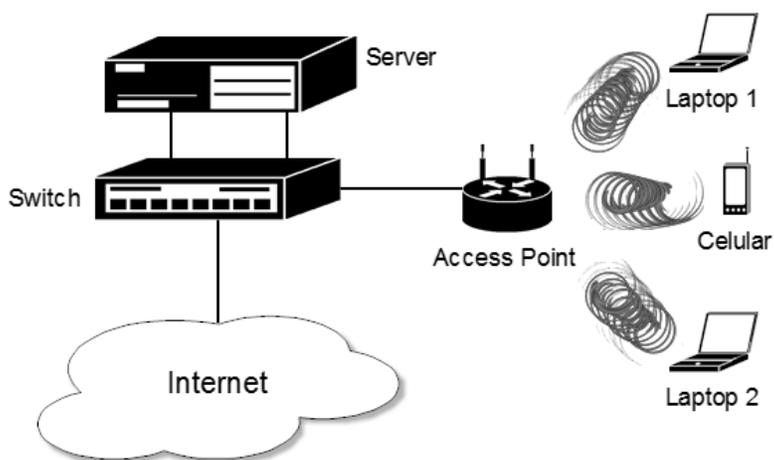
Es importante mencionar que las redes inalámbricas representan una alternativa funcional y cada vez más necesaria debido a los constantes desarrollos en su ámbito. En la actualidad no resulta un sustituto a las redes cableadas, sino un complemento más a éstas.

Anexos

Anexo 1. Implementación.

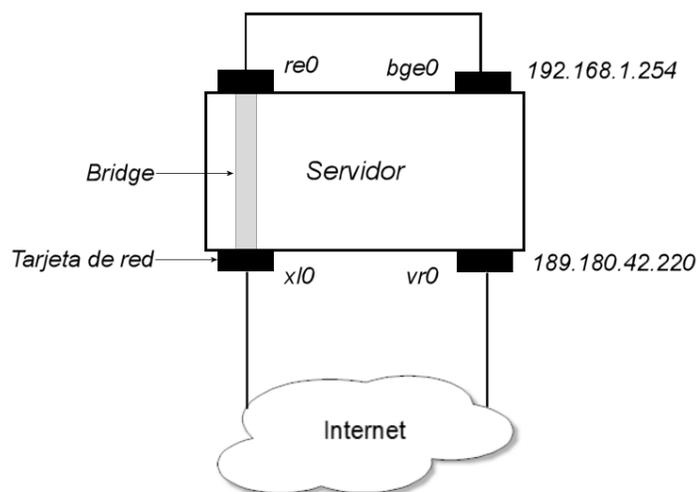
La implementación del sistema estará bajo el sistema operativo OpenBSD ya que es uno de los sistemas operativos más seguros después de su instalación registrando solo dos agujeros de seguridad en más de diez años (ver anexo 2 y 3).

En la siguiente figura se muestra el esquema de conexión de los dispositivos que conforman la red inalámbrica.



Esquema de conexión.

En el siguiente esquema se ilustra la configuración del bridge y de las tarjetas de red del servidor (ver anexo 4 y 5).



Esquema configuración.

Uno de los problemas con que se cuenta es que no se cuentan con suficientes direcciones IP para los clientes y por esta razón es que se utiliza un servidor NAT (ver anexo 4) para que a partir de una dirección IP podamos generar varias IP's, además que tratamos a nuestra red inalámbrica como una subred.

Para realizar la configuración TCP/IP se apoya de un servidor DHCP (ver anexo 6) ya que por medio de este se realiza la configuración automáticamente de los clientes que conformaran la red inalámbrica.

Una de las necesidades es la de restringir la configuración TCP/IP solo a los clientes que se hayan registrados en la página web, para esto se realiza un filtrado por medio de la dirección física MAC, para que solo estas direcciones sean a las que se le pueda asignar la configuración (ver anexo 5).

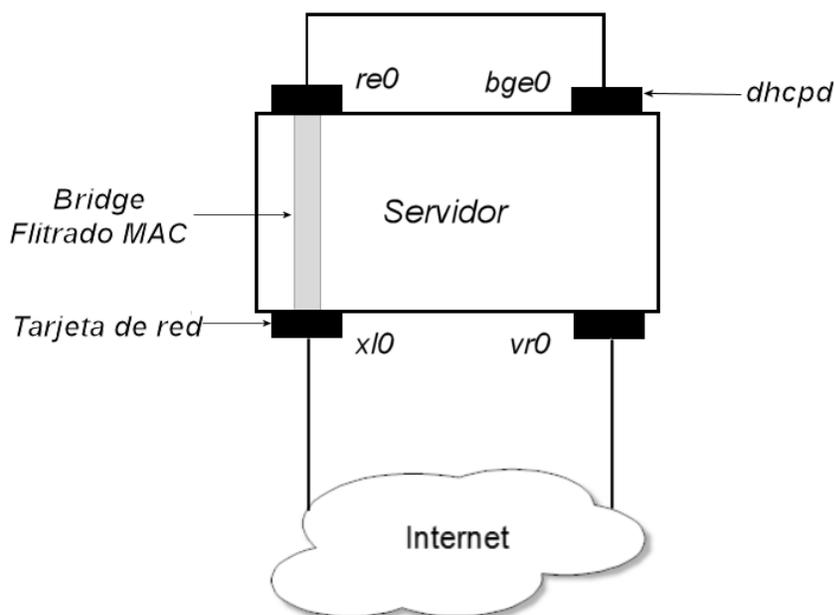


Diagrama filtrado MAC.

Es necesario una aplicación web para poder realizar el registro automático de los usuarios y esta debe de encontrarse instalada en el servidor, para esto se apoya de un servidor LAMP (Linux, Apache, MySQL y PHP) (ver anexo 8), además de utilizar la herramienta PHPMyAdmin (ver anexo 9) para la administración de la base de datos.

Después de realizar el registro el sistema generará el usuario y la contraseña para el acceso a la red, se actualizara la información de la base de datos (ver anexo 13) y los servidores con la información correspondiente.

Se le enviará un correo electrónico al cliente con el usuario y la clave generada, así como un manual de configuración de acuerdo al sistema operativo del equipo (ver anexo 7).

Para controlar el acceso a la red inalámbrica solo para los usuarios registrados, se apoya de un servidor RADIUS en el cual se validan los accesos de los clientes verificando su usuario y contraseña que se les asigna y envía a su correo (ver anexo 10).

Uno de los requerimientos es el de restringir el acceso a los clientes a ciertas páginas como por ejemplo de descargas, porno, de violencia, etcétera y a aplicaciones como podrían ser FTP, Telnet, clientes de mensajes instantáneos, etcétera, este tipo de filtrado se implementa con la aplicación squid (ver anexo 11).

Anexo 2. Instalación de OpenBSD 4.5.

OpenBSD dispone de un proceso de instalación adaptable y robusto en modo texto, y puede ser instalado desde un simple disquete. La mayoría de las plataformas siguen un proceso de instalación similar; no obstante hay algunas diferencias.

En la mayoría de las plataformas, la instalación de OpenBSD utiliza un kernel especial con un número de utilidades y scripts de instalación empujados en una imagen precargada en memoria. Una vez que este kernel ha arrancado, el sistema operativo es extraído de una serie de ficheros (.tgz) comprimidos con tar. Hay varias formas de arrancar el kernel que se utilizará durante la instalación.

- **Disquete o disco flexible:** Existen imágenes que pueden ser utilizadas para crear discos. Los nombres más comunes para estas imágenes son algo como floppy45.fs, aunque hay plataformas que disponen de varias imágenes diferentes.
- **CD-ROM:** Varias plataformas disponen de imágenes de CD-ROM auto arrancables, lo que permite la creación de CDs de arranque. Las imágenes para grabar son del estilo install45.iso.
- **Red:** Determinadas plataformas soportan el arranque por red (por ejemplo usando PXE u otro tipo de arranque por red).
- **Escribiendo una imagen de un sistema de ficheros al disco duro:** una imagen de un sistema de ficheros que puede ser escrita directamente a una partición ya existente, y entonces puede ser arrancada.
- **Cinta de arranque:** Algunas plataformas soportan el arranque desde cinta. Estas cintas pueden ser creadas siguiendo los pasos descritos en las instrucciones del fichero *INSTALL.plataforma*.

No todas las plataformas soportan todas las opciones de arranque.

- **alpha:** Disquete, CD-ROM, escribiendo una imagen de un sistema de ficheros al disco duro.
- **amd64:** Disquete, CD-ROM, red.
- **cats:** CD-ROM.
- **hp300:** CD-ROM, red.
- **hppa:** red.
- **i386:** Disquete, CD, red.
- **mac68k:** Arrancable utilizando herramientas desde un Mac OS. Más información en el fichero *INSTALL.mac68k*
- **macppc:** CD-ROM, red.
- **mvme68k:** Red, cinta de arranque.
- **mvme88k:** Red, cinta de arranque.
- **sparc:** Disquete, CD-ROM, red, escribiendo una imagen de un sistema de ficheros al disco duro.

- **sparc64:** Disquete (U1/U2 solamente), CD-ROM, red, escribiendo una imagen de un sistema de ficheros al disco duro.
- **vax:** Disquete, red.

Durante el proceso de arranque, el kernel y todos los programas necesarios para la instalación son cargados en memoria.

Se podrá finalizar el proceso de instalación de OpenBSD prácticamente en cualquier punto pulsando CTRL-C, y volver a empezar sin necesidad de reiniciar, simplemente ejecutando `install` en el intérprete de comandos.

Después del arranque se verá lo siguiente en pantalla:

```
rootdev=0x1100 rrootdev=0x2f00 rawdev=0x2f02
erase ^?, werase ^W, kill ^U, intr ^C, status ^T
(I)install, (U)pgrade or (S)hell? I
```

Las opciones son descritas a continuación.

- **Install:** Carga OpenBSD en el sistema, sobre escribiendo lo que pudiese estar previamente en el mismo. Se debe de tener en cuenta que es posible dejar algunas particiones intactas a lo largo de este proceso, como una partición que contenga el directorio `/home`. De otra forma, toda información será sobre escrita.
- **Upgrade:** Instala un nuevo grupo de ficheros de instalación en esta máquina, pero no sobre escribe ninguna información de configuración, datos de los usuarios ni programas adicionales. No se da formato al disco ni se sobre escriben los directorios `/etc` y `/var`.
- **Shell:** En algunas ocasiones, necesitarás realizar tareas de reparación o mantenimiento sobre un sistema que no arranca un kernel normal. Esta opción te permitirá llevar a cabo estas tareas de mantenimiento sobre el sistema.

```
Welcome to the OpenBSD/i386 4.5 install program.
```

```
This program will help you install OpenBSD in a simple and rational way. At
any prompt except password prompts you can run a shell command by typing
'!foo', or escape to a shell by typing '!'. Default answers are shown in []'s
and are selected by pressing RETURN. At any time you can exit this program by
pressing Control-C and then RETURN, but quitting during an install can leave
your system in an inconsistent state.
```

```
Specify terminal type: [vt220] Enter
kbd(8) mapping? ('?' for list) [none] Enter
```

En la mayoría de los casos el tipo de terminal por defecto es adecuado, de todas formas, si estás utilizando una consola en puerto serie para la instalación, no utilices la opción por defecto y responde correctamente.

Si no se elige una tabla de códigos de teclado, se asumirá una configuración de teclado norteamericana (US).

IS YOUR DATA BACKED UP? As with anything that modifies disk contents, this program can cause SIGNIFICANT data loss.

It is often helpful to have the installation notes handy. For complex disk configurations, relevant disk hardware manuals and a calculator are useful.

Proceed with install? [no] **y**

Si se elige la opción por defecto aquí, el proceso de instalación terminará y te llevará a un intérprete de comandos.

La configuración de los discos en OpenBSD varía ligeramente entre las diferentes plataformas. Primero se define el trozo (slice) del disco duro que utilizaremos con OpenBSD utilizando fdisk, para luego dividir ese trozo del disco en particiones utilizando disklabel.

Hay dos capas de particionamiento en varias plataformas OpenBSD. La primera, que puede ser considerada como el particionamiento del sistema operativo, es aquella que define el espacio propio que ocupará cada sistema operativo en el disco duro. La segunda es la que define como será particionado en sistemas de ficheros individuales el espacio asignado a OpenBSD.

Cool! Let's get to it...

You will now initialize the disk(s) that OpenBSD will use. To enable all available security features you should configure the disk(s) to allow the creation of separate filesystems for /, /tmp, /var, /usr, and /home.

Available disks are: wd0.

Which one is the root disk? (or done) [wd0] **Enter**

El disco raíz (root disk) es el disco duro desde el que arrancará el sistema, y normalmente aquel en el que reside el espacio destinado para swap. Los discos IDE aparecerán como wd0, wd1, etc., los discos SCSI, así como posibles dispositivos RAID, aparecerán como sd0, sd1, y sucesivos. Todos aquellos discos

encontrados por OpenBSD aparecerán en esta lista -- Si existen discos duros que no aparezcan en esta lista, se trata de hardware no soportado o mal configurado.

Do you want to use **all** of wd0 for OpenBSD? [no] yes **Enter**

Si se responde "yes" a esta pregunta, la totalidad del disco duro será utilizada para OpenBSD. Esto conllevará que tanto el sector primario de arranque (Master Boot Record o MBR) como la tabla de particiones del disco duro serán escritos a disco - una partición del tamaño de todo el disco será configurada como una partición de tipo OpenBSD y será marcada como partición arrancable (bootable partition). Esta será una elección habitual para la mayoría de los usos en producción de OpenBSD.

Para desplegar la ayuda es necesario teclear "?".

> ?

Available commands:

- ? [cmdnd] - this message or command specific help.
- a [part] - add new partition.
- b - set OpenBSD disk boundaries.
- c [part] - change partition size.
- D - set label to default.
- d [part] - delete partition.
- e - edit drive parameters.
- g [b|d|u] - use [b]ios, [d]isk or [u]ser geometry.
- m - show entire OpenBSD man page for disklabel.
- M [part] - modify existing partition.
- n [part] - set the mount point for a partition.
- p [unit] - print label.
- q - quit and save changes.
- r - recalculate free space.
- s [path] - save label to file.
- u - undo last change.
- w - write label to disk.
- X - toggle expert mode.
- x - exit without saving changes.
- z - zero out partition table.

Numeric parameters may use suffixes to indicate units:

- 'b' for bytes, 'c' for cylinders, 'k' for kilobytes, 'm' for megabytes,
- 'g' for gigabytes or no suffix for sectors (usually 512 bytes).
- '%' for percent of total disk size, '&' for percent of free space.

Non-sector units will be rounded to the nearest cylinder.

Entering '?' at most prompts will give you (simple) context sensitive help.

>

- **p** - muestra por pantalla las particiones actuales, y puedes utilizar los modificadores **k**, **m** o **g** para kilobytes, megabytes o gigabytes.
- **D** - Limpia cualquier particion existente. **m** - Modifica una entrada existente dentro del disklabel.
- **a** – Crea una nueva partición.
- **d** – Nos ayuda a eliminar una partición en específico.

En el disco raíz, las dos particiones 'a' y 'b' tienen que ser creadas. El proceso de instalación no continuará hasta que estas dos particiones existan, 'a' será utilizada para albergar el sistema de ficheros raíz '/' y 'b' será utilizado para el espacio de swap.

Es recomendable mantener separados /, /tmp, /var, /usr, /home junto a una partición de swap.

El siguiente es un ejemplo de particiones para OpenBSD:

wd0a:	/(root)	- 1 G.
wd0b:	(swap)	- 500 M.
wd0d:	/tmp	- 300 M
wd0e:	/var	- 1 G.
wd0f:	/usr	- 3G.
wd0g:	/home	- 4G.

```
> a a
offset: [63] Enter
size: [39166407] 1g
Rounding to nearest cylinder: 2104452
FS type: [4.2BSD] Enter
mount point: [none] /
> a b
offset: [2104515] Enter
size: [37061955] 500m
Rounding to nearest cylinder: 1028160
FS type: [swap] Enter
> a d
offset: [3132675] Enter
size: [36033795] 300m
Rounding to nearest cylinder: 245952
FS type: [4.2BSD] Enter
mount point: [none] /tmp
> a e
offset: [3759210] Enter
size: [35407260] 1g
Rounding to nearest cylinder: 2104515
```

```

FS type: [4.2BSD] Enter
mount point: [none] /var
> a f
offset: [5863725] Enter
size: [27005262] 3g
Rounding to nearest cylinder: 6297400
FS type: [4.2BSD] Enter
mount point: [none] /usr
> a g
offset: [12161205] Enter
size: [27005265] 4g
Rounding to nearest cylinder: 8401995
FS type: [4.2BSD] Enter
mount point: [none] /home
> p m
OpenBSD area : 0.0M-19124.3M ; size : 19124.2M ; free : 9003.6M
      size      offset fstype [fsize bsize cpge]
a:   1027.6M      0.0M 4.2BSD  2048 16384  16 # /
b:    502.0M     1027.6M  swap
c:   19130.0M      0.0M  unused    0    0
d:    305.9M     1529.6M 4.2BSD  2048 16384  16 # /tmp
e:    1027.6M     1835.6M 4.2BSD  2048 16384  16 # /var
f:    3074.9M     2863.1M 4.2BSD  2048 16384  16 # /usr
g:    4102.5M     5938.1M 4.2BSD  2048 16384  16 # /home
> q
Write new label?: [y] Enter

```

La partición c simboliza el disco duro al completo no se tiene que modificar.

En el siguiente paso se verifica que el particionamiento que se ha realizado sea correcto.

```

Mount point for wd0d (size=321024k)? (or 'none' or 'done') [/tmp] Enter
Mount point for wd0e (size=1024m)? (or 'none' or 'done') [/var] Enter
Mount point for wd0g (size=3072m)? (or 'none' or 'done') [/usr] Enter
Mount point for wd0g (size=4096m)? (or 'none' or 'done') [/home] Enter
Mount point for wd0d (size=321024k)? (or 'none' or 'done') [/tmp] done
No more disks to initialize.

```

```

OpenBSD filesystems:
wd0a /
wd0d /tmp
wd0e /var
wd0f /usr
wd0g /home

```

```
The next step *DESTROYS* all existing data on these partitions!
Are you really sure that you're ready to proceed? [no] y
/dev/rwd0a: 307440 sectors in 305 cylinders of 16 tracks, 63 sectors
           1027.6MB in 1 cyl groups (306 c/g, 150.61MB/g, 19328 i/g)
/dev/rwd0d: 245952 sectors in 244 cylinders of 16 tracks, 63 sectors
           305.9MB in 1 cyl groups (244 c/g, 120.09MB/g, 15360 i/g)
/dev/rwd0e: 164304 sectors in 163 cylinders of 16 tracks, 63 sectors
           1027.6MB in 1 cyl groups (164 c/g, 80.72MB/g, 10368 i/g)
/dev/rwd0f: 6291936 sectors in 6242 cylinders of 16 tracks, 63 sectors
           3072.2MB in 20 cyl groups (328 c/g, 161.44MB/g, 20608 i/g)
/dev/rwd0g: 8388576 sectors in 8322 cylinders of 16 tracks, 63 sectors
           4102.5.0MB in 26 cyl groups (328 c/g, 161.44MB/g, 20608 i/g)
/dev/wd0a on /mnt type ffs (rw, asynchronous, local, ctime=Thu Oct 20 00:03:14 2
005)
/dev/wd0h on /mnt/home type ffs (rw, asynchronous, local, nodev, nosuid, ctime=T
hu Oct 11 00:03:14 2010)
/dev/wd0d on /mnt/tmp type ffs (rw, asynchronous, local, nodev, nosuid, ctime=Th
u Oct 11 00:03:15 2010)
/dev/wd0g on /mnt/usr type ffs (rw, asynchronous, local, nodev, ctime=Thu Oct 20
00:03:15 2010)
/dev/wd0e on /mnt/var type ffs (rw, asynchronous, local, nodev, nosuid, ctime=Th
u Oct 11 00:03:15 2010)
```

Ahora se tiene que establecer un nombre para el sistema. Esté valor, junto al nombre de dominio DNS se almacenará en el fichero `/etc/myname` que es utilizado durante un arranque normal para establecer el nombre del sistema. Si no se establece un nombre de dominio para el sistema, se utilizará el valor por defecto `'my.domain'`.

```
Enter system hostname (short form, e.g. 'foo'): tesis
```

El paso siguiente consiste en configurar la red. La red tiene que ser obligatoriamente configurada si se planea realizar la instalación por FTP o NFS.

```
Configure the network? [yes] Enter
Available interfaces are: fxp0.
Which one do you wish to initialize? (or 'done') [fxp0] Enter
Symbolic (host) name for fxp0? [tesis] Enter
The default media for fxp0 is
    media: Ethernet autoselect (100baseTX full-duplex)
Do you want to change the default media? [no] Enter
IP address for fxp0? (or 'dhcp') 199.185.137.55
Netmask? [255.255.255.0] Enter
IPv6 address for fxp0? (or 'rtsol' or 'none') [none]
No more interfaces to initialize.
DNS domain name? (e.g. 'bar.com') [my.domain] fi-a.unam.mx
DNS nameserver? (IP address or 'none') [none] 199.185.137.1
Use the nameserver now? [yes] Enter
Default route? (IP address, 'dhcp' or 'none') 199.185.137.128
add net default: gateway 199.185.137.128
Edit hosts with ed? [no] Enter
Do you want to do any manual network configuration? [no] Enter
```

En el ejemplo anterior, se utilizó una dirección IP estática. Como aparece indicado, puedes utilizar también "dhcp" en la mayoría de las plataformas (no en Alpha), si tu entorno lo soporta. En el caso de DHCP, la mayoría de la información será recabada del servidor de DHCP remoto, tendrás la opción de confirmarlo. Este es un ejemplo de una configuración de red que forma parte de una instalación, pero esta vez llevada a cabo con DHCP:

```
Configure the network? [yes] Enter
Available interfaces are: fxp0.
Which one do you wish to initialize? (or 'done') [fxp0] Enter
Symbolic (host) name for fxp0? [tesis] Enter
The default media for fxp0 is
    media: Ethernet autoselect (100baseTX full-duplex)
Do you want to change the default media? [no] Enter
IP address for fxp0? (or 'dhcp') dhcp
Issuing hostname-associated DHCP request for fxp0.
Sending on Socket/fallback/fallback-net
DHCPDISCOVER on fxp0 to 255.255.255.255 port 67 interval 1
DHCPOFFER from 199.185.137.128
DHCPREQUEST on fxp0 to 255.255.255.255 port 67
DHCPACK from 199.185.137.128
New Network Number: 199.185.137.0
New Broadcast Address: 199.185.137.255
bound to 199.185.137.55 -- renewal in 43200 seconds.
Done - no available interfaces found.
DNS domain name? (e.g. 'bar.com') [fi-a.unam.mx] Enter
DNS nameserver? (IP address or 'none') [199.185.137.1] Enter
Use the nameserver now? [yes] Enter
Default route? (IP address, 'dhcp' or 'none') [199.185.137.128] Enter
Edit hosts with ed? [no] Enter
Do you want to do any manual network configuration? [no] Enter
```

Lo siguiente es establecer la contraseña para la cuenta de superusuario (root):

```
Password for root account? (will not echo) pAssWOrd
Password for root account? (again) pAssWOrd
```

Luego se tiene que elegir el medio de instalación. Las opciones son las siguientes:

```
Let's install the sets!
Location of sets? (cd disk ftp http or 'done') [cd] Enter
Available CD-ROMs are: cd0.
```

En este ejemplo instalaremos desde CD-ROM.

Después nos preguntara por el directorio en el que se encuentran los ficheros de la instalación, que es 4.5/i386/ en los CD's oficiales.

Lo siguiente es seleccionar los ficheros que se desean instalar. Por defecto están seleccionados todos los ficheros X.

Select sets by entering a set name, a file name pattern or 'all'. De-select sets by prepending a '-' to the set name, file name pattern or 'all'. Selected sets are labeled '[x]'.

```
[X] bsd
[X] bsd.rd
[ ] bsd.mp
[X] base45.tgz
[X] etc45.tgz
[X] misc45.tgz
[X] comp45.tgz
[X] man45.tgz
[X] game45.tgz
[ ] xbase45.tgz
[ ] xetc45.tgz
[ ] xshare45.tgz
[ ] xfont45.tgz
[ ] xserv45.tgz
```

File Name? (or 'done') [bsd.mp] **all**

```
[X] bsd
[X] bsd.rd
[X] bsd.mp
[X] base45.tgz
[X] etc45.tgz
[X] misc45.tgz
[X] comp45.tgz
[X] man45.tgz
[X] game45.tgz
[X] xbase45.tgz
[X] xetc45.tgz
[X] xshare45.tgz
[X] xfont45.tgz
[X] xserv45.tgz
```

Los paquetes mínimos que se requieren para que funcione OpenBSD son base45.tgz, etc45.tgz y bsd.

Esta es una pequeña descripción de la función de cada paquete:

- **bsd** Esto es el kernel.
- **bsd.mp** Kernel multiprocesador.
- **bsd.rd** RAM disk kernel
- **base38.tgz** Contiene el sistema base de OpenBSD
- **etc38.tgz** Contiene todos los ficheros de /etc

- **comp38.tgz** Contiene el compilador y sus herramientas.
- **man38.tgz** Contiene las páginas de manual.
- **misc38.tgz** Información adicional y documentación de configuración.
- **game38.tgz** Contiene los juegos para OpenBSD
- **xbase38.tgz** Contiene la instalación base de X11.
- **xetc38.tgz** Ficheros de configuración de /etc/X11 y /etc/fonts.
- **xfont38.tgz** Contiene el servidor de fuentes de X11.
- **xserv38.tgz** Contiene los servidores X de X11.
- **xshare38.tgz** Configuraciones locales del entorno X.

Una vez que se ha decidido correctamente qué sets de ficheros se quieren instalar, se preguntará si se está seguro de extraer los contenidos de esos sets, y a continuación serán instalados.

```
File Name? (or 'done') [done] Enter
Ready to install sets? [yes] Enter
Getting bsd ...
100% |*****| 5157 KB 00:08
Getting bsd.rd ...
100% |*****| 4549 KB 00:02
Getting bsd.mp ...
100% |*****| 5202 KB 00:03
Getting base38.tgz ...
100% |*****| 35928 KB 00:25
Getting etc38.tgz ...
100% |*****| 1123 KB 00:01
Getting misc38.tgz ...
100% |*****| 2222 KB 00:01
Getting comp38.tgz ...
100% |*****| 20522 KB 00:17
Getting man38.tgz ...
100% |*****| 7234 KB 00:05
Getting game38.tgz ...
100% |*****| 2538 KB 00:01
Getting xbase38.tgz ...
100% |*****| 10225 KB 00:07
Getting xetc38.tgz ...
100% |*****| 93384 00:00
Getting xshare38.tgz ...
100% |*****| 1986 KB 00:02
Getting xfont38.tgz ...
100% |*****| 32438 KB 00:23
Getting xserv38.tgz ...
100% |*****| 18172 KB 00:14
```

Location of sets? (cd disk ftp http or 'done') [done] **Enter**

A continuación, se harán una serie de preguntas sobre algunos parámetros de configuración del sistema recién instalados. Lo primero es si sshd debería de ser iniciado en el arranque.

Start sshd(8) by default? [yes] **Enter**

Lo siguiente es la opción de arrancar OpenNTPD en el arranque. OpenNTPD es una buena forma de mantener sincronizado el reloj del sistema.

Start ntpd(8) by default? [no] **Enter**

Ahora preguntará si se requiere utilizar el entorno X en este sistema. Si se responde que 'Y' (si), /etc/sysctl.conf será modificado para incluir la línea machdep.allowaperture=1 o machdep.allowaperture=2.

Do you expect to run the X Window System? [yes] **no Enter**

Después se preguntará si se quiere utilizar una consola en puerto serie con este sistema, en lugar de un monitor y teclado estándar.

Lo último será elegir la zona horaria (time zone). Dependiendo de donde esté situado el sistema, puede que existan varias respuestas válidas para esta pregunta. En el siguiente ejemplo, utilizaremos México/General.

Si se escribe “?” en el intérprete (prompt) se mostrara en la pantalla todas las opciones disponibles.

```
What timezone are you in? ('?' for list) [Canada/Mountain] ?
Africa/  Chile/  GB-Eire  Israel  NZ-CHAT  Turkey
America/ Cuba    GMT      Jamaica Navajo   UCT
Antarctica/ EET    GMT+0    Japan    PRC      US/
Arctic/  EST    GMT-0    Kwajalein PST8PDT  UTC
Asia/    EST5EDT GMT0     Libya    Pacific/ Universal
Atlantic/ Egypt  Greenwich MET      Poland   W-SU
Australia/ Eire    HST      MST      Portugal WET
Brazil/  Etc/    Hongkong MST7MDT  ROC      Zulu
CET      Europe/ Iceland Mexico/  ROK      posix/
CST6CDT  Factory Indian/  Mideast/ Singapore posixrules
Canada/  GB      Iran     NZ      SystemV/ right/
What timezone are you in? ('?' for list) [Canada/Mountain] Mexico
What sub-timezone of 'US' are you in? ('?' for list) ?
BajaNorte BajaSur General
```

```
Select a sub-timezone of 'Mexico' ('?' for list): General
Setting local timezone to 'Mexico/General'...done.
Making all device nodes...done.
Installing boot block...
boot: /mnt/boot
proto: /usr/mdec/biosboot
device: /dev/rwd0c
/usr/mdec/biosboot: entry point 0
proto bootblock size 512
/mnt/boot is 3 blocks x 16384 bytes
fs block shift 2; part offset 3069360; inode block 152, offset 4136
using MBR partition 1: type 166 (0xa6) offset 3069360 (0x2ed5b0)
done.

CONGRATULATIONS! Your OpenBSD install has been successfully completed!
To boot the new system, enter halt at the command prompt. Once the
system has halted, reset the machine and boot from the disk.
# halt
syncing disks... done

The operating system has halted.
Please press any key to reboot.
```

Se encuentra ya instalado OpenBSD en el sistema, ya puede ser iniciado por primera vez.

Anexo 3. Actualización de OpenBSD.

Para realizar la actualización de OpenBSD, es necesario descargar del sitio oficial de OpenBSD los archivos correspondientes a la versión de OpenBSD por actualizar. Para ello desde la máquina con el sistema instalado hay que realizar lo siguiente:

Teclear:

```
# ftp ftp.OpenBSD.org
```

Lo que nos conducirá al sitio en la red de OpenBSD, donde para poder ingresar se solicitara un nombre de usuario y una contraseña

```
Name (ftp.OpenBSD.org:root): anonymous  
Who are you impersonating today?  
Password: xxxxxx@xxxxx
```

Para realizar el registro es necesario que en el nombre de usuario (Name) coloquemos anonymous, y en Password coloquemos alguna dirección de correo electrónico (no es necesario una dirección real, lo importante es que en ese campo se coloque un conjunto de caracteres entre los cuales se encuentre @), como se muestra en el ejemplo anterior.

```
320-  
230- Welcome to Sunsite Alberta  
230-Login Successful  
230Your data rate unrestricted  
Remote system type is Unix  
Using binary mode to transfer files
```

Una vez registrados es necesario ingresar al directorio *pub/OpenBSD/patches/4.5/common*. Para ello es necesario teclear:

```
# cd pub/OpenBSD/patches/4.5/common
```

Se ejecuta el comando *'ls'* para listar los archivos y con el comando *'get'* se realiza la descarga de los archivos *'patch'* contenidos en el directorio, que son los archivos que actualizan el sistema.

```
# ls
-r- -r- -r- - 1 1114 1114          80859 May12 00:10 001_sendmail.patch
-r- -r- -r- - 1 1114 1114          226 May02 15:04 002_xorg.patch

226 There everyone likes a Gorila

#get 001_sendmail.patch

local: 001_sendmail.patch      remote: 001_sendamil.patch
227 Entering Passive Mode (129,128,5,191,168,82)
150 Opening BINARY mode data connection for 001_sendmail.patch (80859 bytes)

100% |*****| 80859 00:01

226 Wow, that seem to have worked.
80859 bytes received in 1.33 seconds (59.35 Kb/s)
```

Una vez terminada la descarga de los archivos, es necesario salir y realizar la instalación. Para ello se teclea lo siguiente.

```
# exit
# ls
```

Con *'exit'* salimos del sitio OpenBSD.org y con *'ls'* vemos que los archivos hayan sido descargados.

Para realizar la instalación es necesario seguir las instrucciones que se encuentran dentro del archivo mismo. Es necesario entonces abrir una nueva terminal (**ctrl + alt + F2**) y ubicarnos en el directorio donde se descargo el archivo. Una vez ahí es necesario teclear el comando *'more'* para poder observar las instrucciones de instalación del archivo.

```
#more 001_sendmail.patch

Apply by doing:

    cd /usr/src
    patch -p0 < 001_sendmail.patch

And then rebuild and install sendmail:

    cd gnu/usr.sbin/sendmail
```

```
make obj
  make depend
  make
  make install
```

Para llevarlas a cabo es necesario regresar a la terminal donde originalmente estábamos trabajando y ejecutar cada una de las instrucciones en el orden que vienen establecidas.

```
# cd /usr/src
# patch -p0 < 001_sendmail.patch
# cd gnu/usr.sbin/sendmail
# make obj
# make depend
# make
# make install
```

Aquí es recomendable que al empezar la actualización se distinga cuales son del kernel estos dejarlos al último.

Como punto último hay que compilar el kernel el procedimiento es el siguiente:

```
# cd /sys/arch/i386/conf
# config GENERIC
# cd ../compile/GENERIC
# make depend
# make
# cp bsd /bsd.old
# cp /sys/arch/i386/compile/GENERIC/bsd /bsd
```

Anexo 4. Configuración de las tarjetas de red y del servidor NAT en OpenBSD.

Para configurar un servidor NAT es necesario contar con dos tarjetas de red, posteriormente se procede a configurarlas:

Al tener ya instaladas las tarjetas de red se debe tomar la decisión de cuál de estas tarjetas va a trabajar como tarjeta interna y cual como tarjeta externa.

Con la instrucción *'ifconfig -a'* se proporciona la información de las tarjetas de red que se encuentran instaladas, tal y como se muestra a continuación:

```
-bash-3.00# ifconfig -a
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 33224
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
bge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    address: 00:12:3f:53:24:c3
    media: Ethernet autoselect (10baseT half-duplex)
    status: active
    inet 132.248.54.115 netmask 0xfffff00 broadcast 132.248.54.255
    inet6 fe80::212:3fff:fe53:24c3%bge0 prefixlen 64 scopeid 0x1
vr0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    address: 00:02:44:8c:9a:03
    media: Ethernet autoselect (100baseTX)
    status: active
    inet 192.168.115.254 netmask 0xfffff00 broadcast 192.168.115.255
    inet6 fe80::202:44ff:fe8c:9a03%vr0 prefixlen 64 scopeid 0x2
pflog0: flags=141<UP,RUNNING,PROMISC> mtu 33224
pfsync0: flags=0<> mtu 2020
enc0: flags=0<> mtu 1536
```

Nota: aquí podemos observar que en el equipo se encuentran instaladas dos tarjetas, bge0 y vr0, donde bge y vr son simplemente las marcas de las tarjetas de red.

Se tiene que verificar que las dos tarjetas se encuentren en el directorio */etc*, tal y como se muestra a continuación:

```
group          motd
hostname.bge0  mrouted.conf
hostname.vr0   mtree
hosts          mygate
```

En caso de no encontrarse se necesitan crear con la instrucción *'touch'* como por ejemplo supongamos que *hostname.vr0* no aparece en la lista.

```
# touch /etc/hostname.vr0
```

Al ya tener los archivos y decidido cuál va a ser la tarjeta interna y externa, se procede a asignar un IP a la tarjeta externa (en este caso se decidió que fuera vr0) por la que van a salir los usuarios de nuestro servidor, de la siguiente manera:

```
# vi /etc/hostname.vr0
```

Con esta instrucción editamos el archivo, una vez estando dentro del editor se introduce el IP asignado junto con la máscara de subred, como se muestra a continuación:

```
inet 189.180.42.220 255.255.255.0
```

Posteriormente se procede a salvarlo.

Se realiza el mismo procedimiento con la tarjeta que va a trabajar como tarjeta de red interna, solo que para la tarjeta interna se debe de asignar el IP del segmento con el que van a estar trabajando los clientes y que va a ser la puerta de enlace:

```
inet 192.168.1.254 255.255.255.0
```

Con la máscara asignada se están asignando solamente un determinado rango de direcciones, en este caso son 256 IP lógicas.

Se necesita editar el archivo */etc/sysctl.conf* modificándole la línea:

```
#net.inet.ip.forwarding=1 ó net.inet.ip.forwarding=0
```

Por:

```
net.inet.ip.forwarding=1
```

Salvar.

También se debe de editar el archivo */etc/rc.conf* modificándole la siguiente línea:

```
pf=NO
```

Por:

```
pf=YES
```

Editar el archivo */etc/pf.conf* donde aparecen dos líneas indicando cuál es tu tarjeta interna y externa, hay modificar de acuerdo a la decisión tomada.

Aparece:

```
ext_if="xl1"  
int_if="xl0"
```

Por:

```
ext_if="vr0"  
int_if="bge0"
```

Y en las líneas donde aparece scrub y nat, cambiarlas por lo siguiente:

```
scrub in all  
nat on $ext_if from $int_if:network to any -> $ext_if
```

Anexo 5. Configuración del Bridge y filtrado MAC.

Para configurar el bridge se necesita tener dos tarjetas de red instaladas en el equipo y posteriormente crear sus archivos de configuración bajo */etc*, como por ejemplo:

```
/etc/hostname.re0
```

Donde re0 es la marca de la tarjeta de red, esta nos la da el comando *ifconfig* - a como por ejemplo:

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 33204
    priority: 0
    groups: lo
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x5
re0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    lladdr 00:50:fc:f0:b9:4f
    priority: 0
    media: Ethernet autoselect (100baseTX full-duplex)
    status: active
xl0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    lladdr 00:04:76:2b:1a:14
    priority: 0
    media: Ethernet autoselect (none)
    status: no carrier
enc0: flags=0<> mtu 1536
    priority: 0
pflog0: flags=141<UP,RUNNING,PROMISC> mtu 33204
    priority: 0
```

Después de crear los archivos de configuración de cada tarjeta de red, se deben de editar escribiendo en cada una lo siguiente:

```
media autoselect up
```

Con esto las tarjetas de red se levantarán sin necesidad de tener una IP.

Se debe de crear el siguiente archivo bajo */etc*:

```
/etc/bridgename.bridge0
```

En donde se colocaran las tarjetas de red que serán parte del bridge como se muestra a continuación:

```
add re0
add xl0
up
```

Por último se escribe lo siguiente en la línea de comandos para crear el bridge:

```
# ifconfig bridge0 create
```

Con esto se tiene ya creado el bridge bajo OpenBSD.

Para realizar el filtrado MAC se emplea el bridge, y para ello se necesita crear el archivo bajo */etc*:

```
# touch /etc/bridgename.bridge0.rules
```

En este archivo se colocarán las direcciones MAC que se permitirán salir de la siguiente forma:

```
pass in on xl0 src 00:90:4b:23:8b:13
pass in on xl0 src 00:11:22:33:44:55
pass .....
block in on xl0
```

Se utiliza la tarjeta de red externa en este ejemplo se usó *xl0*.

Colocando al final la línea *block in on xl0* para que cualquier otra dirección MAC sea bloqueada.

Para cargar estas reglas de filtrado se escribe en la línea de comandos:

```
# brconfig bridge0 rulefile /etc/bridgename.bridge0.rules
```

Y para dar de baja las reglas:

```
# brconfig bridge0 flushrule vr0
```

Anexo 6. Servidor DHCP en OpenBSD.

Para configurar el servidor DHCP en OpenBSD se necesita editar el fichero `/etc/rc.conf`.

Cambiar la línea:

```
dhcpcd_flags=NO
```

Por:

```
dhcpcd_flags=""
```

```

ripd_flags=NO          # for normal use: ""
mrouted_flags=NO      # for normal use: "", if activated
                      # be sure to enable multicast_router below.
dvmrpd_flags=NO       # for normal use: ""
ospfd_flags=NO        # for normal use: ""
ospf6d_flags=NO       # for normal use: ""
bgpd_flags=NO         # for normal use: ""
rarpd_flags=NO        # for normal use: "-a"
bootparamd_flags=NO  # for normal use: ""
rbootd_flags=NO       # for normal use: ""
sshd_flags=""         # for normal use: ""
named_flags=NO        # for normal use: ""
rdate_flags=NO        # for normal use: [RFC868-host] or [-n RFC2030-host]
timed_flags=NO        # for normal use: ""
ldattach_flags=NO     # for normal use: "[options] linedisc cua-device"
ntpd_flags=NO         # for normal use: ""
isakmpd_flags=NO     # for normal use: ""
sasynod_flags=NO     # for normal use: ""
mopd_flags=NO         # for normal use: "-a"
apmd_flags=NO         # for normal use: ""
dhcpcd_flags=""       # for normal use: ""
dhcrelay_flags=NO    # for normal use: "-i interface [server]"
rtadvd_flags=NO      # for normal use: list of interfaces
                      # be sure to set net.inet6.ip6.forwarding=1
route6d_flags=NO     # for normal use: ""
                      # be sure to set net.inet6.ip6.forwarding=1
rtsold_flags=NO      # for normal use: interface
                      # be sure to set net.inet6.ip6.forwarding=0
                      # be sure to set net.inet6.ip6.accept_rtadv=1
lpd_flags=NO         # for normal use: "" (or "-l" for debugging)
sensorsd_flags=NO    # for normal use: ""
hotplugd_flags=NO    # for normal use: ""
watchdogd_flags=NO   # for normal use: ""
ftpproxy_flags=NO    # for normal use: ""
hostapd_flags=NO     # for normal use: ""
ifstated_flags=NO    # for normal use: ""
relayd_flags=NO      # for normal use: ""
snmpd_flags=NO       # for normal use: ""

# use -u to disable chroot, see httpd(8)
httpd_flags=""       # for normal use: "" (or "-DSSL" after reading ssl(8))

# For normal use: "-L sm-mta -bd -q30m", and note there is a cron job
sendmail_flags="-L sm-mta -C/etc/mail/sendmail.cf -bd -q30m"
spamd_flags=NO       # for normal use: "" and see spamd(8)
spamd_black=NO       # set to YES to run spamd without greylisting
spamlogd_flags=""    # use eg. "-i interface" and see spamlogd(8)

```

Se necesita crear el archivo *dhcpd.interfaces* y editarlo colocando la tarjeta que se desee que dhcpd permanezca a la escucha aquí se pone la tarjeta de red que tenga nuestro sistema:

```
# cat > /etc/dhcpd.interfaces bge0
```

Luego editamos */etc/dhcpd.conf*.

```
#      $OpenBSD: dhcpd.conf,v 1.2 2008/10/03 11:41:21 sthen Exp $
#
# DHCP server options.
# See dhcpd.conf(5) and dhcpd(8) for more information.
#
# Network:          192.168.1.0/255.255.255.0
# Domain name:     fi-a.unam.mx
# Name servers:    132.248.204.1 and 132.248.10.2
# Default router:  192.168.1.254
# Addresses:       192.168.1.5 - 192.168.1.250
#
option domain-name "fi-a.unam.mx";
option domain-name-servers 132.248.204.1, 132.248.10.2;

subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers 192.168.1.254;

    range 192.168.1.5 192.168.1.250;
}

```

Para iniciar el demonio dhcpd colocamos en la línea de comandos:

```
# /usr/sbin/dhcpd
```

Para darlo de baja ahí que hacerlo matando el proceso con:

```
# ps -aux
```

```
-bash-4.0# ps -aux
USER      PID %CPU %MEM    VSZ   RSS Tt  STAT   STARTED      TIME COMMAND
root         1  0.0  0.0    444    100 ??  Ss      11:08AM    0:00.03 sshd: [accepted] (
root         7  0.0  0.0    444    100 ??  Ss      60Oct10   0:00.72 /sbin/init
root    14198  0.0  0.1    508    272 ??  Is      60Oct10   0:00.07 syslogd: [priv] (s
_syslogd 28794  0.0  0.1    544    620 ??  S       60Oct10   0:18.93 syslogd -a /var/ww
root         5  0.0  0.0    508         4 ??  Is      60Oct10   0:00.00 pflogd: [priv] (pf
_pflogd 27021  0.0  0.0    572     76 ??  S       60Oct10   0:19.13 pflogd: [running]
root    27353  0.0  0.0    472         4 ??  Is      60Oct10   0:00.03 inetd
root    15454  0.0  0.1    612    476 ??  Ss      60Oct10   0:22.85 /usr/sbin/sshd
root    19932  0.0  0.0   1508         4 ??  Is      60Oct10   0:00.01 /usr/local/sbin/sq
_squid   1282  0.0 46.5 703776 243484 ??  S       60Oct10   69:32.78 (squid) (squid)
root    6545  0.0  0.1    588    516 ??  Ss      60Oct10   0:01.49 cron
root    1522  0.0  0.3   1224   1632 ??  Ss      60Oct10   0:23.57 sendmail: acceptin
_squid   17099  0.0  0.1    412    288 ??  Ss      60Oct10   0:25.82 (unlinkd) (unlinkd
_dhcpd   10752  0.0  0.1    692    740 ??  Is      11:08AM   0:00.55 /usr/sbin/dhcpd
root    29103  0.3  0.5   3300  2488 ??  Ss      11:08AM   0:00.10 sshd: root@tty0 (
sshd     16341  0.0  0.3   1888   1784 ??  S       11:08AM   0:00.00 sshd: [net] (sshd)
root    24581  0.0  0.3    792   1692 p0  Ss      11:08AM   0:00.03 -bash (bash)
root    14221  0.0  0.0    372    204 p0  R+      11:08AM   0:00.00 ps -aux
root    26231  0.0  0.0    440         4 C0  Is+     60Oct10   0:00.01 /usr/libexec/getty
root     5834  0.0  0.0    364         4 C1  Is+     60Oct10   0:00.00 /usr/libexec/getty
root    21099  0.0  0.0    324         4 C2  Is+     60Oct10   0:00.00 /usr/libexec/getty
root    17999  0.0  0.0    400         4 C3  Is+     60Oct10   0:00.00 /usr/libexec/getty

```

Y observar el PID que corresponde al demonio de DHCP con el siguiente comando:

```
# kill -9 "PID del proceso"
```

Anexo 7. Servidor de Correos

El MTA que viene instalado por default en OpenBSD es Sendmail así que se trabajara con este MTA.

Por defecto, el agente de transporte de correo Sendmail no acepta conexiones de red desde ningún equipo excepto la computadora local. Para configurar Sendmail como un servidor para otros clientes se debe de realizar lo siguiente:

Se necesita editar el archivo *rc.conf* que viene bajo */etc* y modificar la linea:

```
sendmail_flags="-L sm-mta -C/etc/mail/localhost.cf -bd -q30m"
```

Por:

```
sendmail_flags="-L sm-mta -C/etc/mail/sendmail.cf -bd -q30m"
```

La bitacora queda en:

```
/var/log/mailman
```

Y ya con esto se tiene configurado el servidor de correos listo para enviar y recibir correos.

A continuación se presenta una prueba del servicio de correos:

```
# telnet localhost 25
```

```
Trying ::1...
```

```
Connected to localhost.
```

```
Escape character is '^['.
```

```
220 zaratustra.fi-a.unam.mx ESMTP Sendmail 8.14.3/8.14.3; Mon, 11 Oct 2010 18:08:21 -0500 (CDT)
```

```
HELO Spawn
```

```
250 zaratustra.fi-a.unam.mx Hello root@localhost.fi-a.unam.mx [IPv6:::1], pleased to meet you
```

```
MAIL FROM: <root@localhost>
```

```
250 2.1.0 <root@localhost>... Sender ok
```

RCPT TO: <root@localhost>

250 2.1.5 <root@localhost>... Recipient ok

DATA

354 Enter mail, end with "." on a line by itself

Hola Spawn

probando

.

250 2.0.0 o9BN8LNN027157 Message accepted for delivery

quit

221 2.0.0 zaratustra.fi-a.unam.mx closing connection

Connection closed by foreign host.

Anexo 8. Apache, PHP y MySQL en OpenBSD 4.5

- *Apache.*

En OpenBSD no es necesario instalar Apache. OpenBSD 4.5 ya viene con la versión 1.3 revisada y mejorada por el Proyecto OpenBSD. Esta versión cuenta con soporte para SSL/TLS y DSO.

Para iniciar y detener *httpd* cuando se requiera se pueden usar los siguientes comandos.

Para iniciar el servidor Apache:

```
# apachectl start
```

Para detener el servidor Apache:

```
# apachectl stop
```

Para Apache se inicie al arrancar OpenBSD solo se tiene que editar el archivo:

```
/etc/rc.conf
```

En este archivo necesitamos buscar la siguiente línea:

```
httpd_flags=NO
```

Editarla para que quede así:

```
httpd_flags=""
```

Una vez editado el archivo lo guardamos. La próxima vez que se inicie OpenBSD 4.5 Apache se iniciará de forma automática.

Si aparece el mensaje: **It worked!**, seguido de más información, entonces Apache ya funciona correctamente.

OpenBSD

Apache

It Worked!

If you can see this page, then the people who own this host have just activated the [Apache Web server](#) software included with their [OpenBSD System](#). They now have to add content to this directory and replace this placeholder page, or else point the server at their real content.

Documentation

The Apache manual is available with distribution as part of the [misc](#) file set. Especially read the SSL documentation carefully within the manual, in addition to the [ssl\(8\)](#) and [httpd\(8\)](#) manual pages.

Graphics

You are free to use the image below on an Apache-powered web server.



You can also use the image below on an [OpenBSD](#)-powered web server. Many other [OpenBSD images](#) are also available.



These images are also appropriate for a webserver using [mod_ssl](#) with [openSSL](#) cryptography.



- *PHP.*

Para instalar PHP en OpenBSD 4.5 se puede usar el siguiente comando:

```
pkg_add ftp://ftp.OpenBSD.org/pub/OpenBSD/4.5/packages/i386/php5-core-5.2.8p0.tgz
```

Una vez que se ha agregado el paquete PHP ahora hay que habilitar el módulo de PHP en Apache:

Para hacerlo se necesita crear un enlace simbólico de:

```
/var/www/conf/modules.sample/php5.conf a /var/www/conf/modules/php5.conf.
```

Esto se hace con este comando:

```
# ln -s /var/www/conf/modules.sample/php5.conf \  
/var/www/conf/modules
```

Dado que Apache esta "chrootado" por default en OpenBSD hay que crear el directorio de apoyo `/var/www/tmp` para PHP de la siguiente forma:

```
# mkdir -p /var/www/tmp
```

Se modifican los permisos para este directorio para que PHP pueda leer y escribir en el:

```
# chmod 777 /var/www/tmp
```

Ya se tiene Apache con soporte para PHP. Se pueden realizar algunas pruebas para comprobar que todo funciona bien, para hacerlo se crea un archivo con la extensión .php.

```
#cat > /var/www/htdocs/test.php
<?php
phpinfo();
?>
//Presionamos CTRL + D para terminar.
```

Hay que reiniciar Apache para que los cambios tengan efecto.

```
# apachectl stop
# apachectl start
```

Verificamos que funcione colocando en un navegador *http://localhost/test.php*

Debe aparecer una página con bastante información sobre la versión de PHP instalada. Si es así el soporte para PHP está listo.

PHP Credits

Configuration

PHP Core

Directive	Local Value	Master Value
allow_call_time_pass_reference	Off	Off
allow_url_fopen	Off	Off
allow_url_include	Off	Off
always_populate_raw_post_data	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	no value	no value
default_mimetype	text/html	text/html
define_syslog_variables	Off	Off
disable_classes	no value	no value
disable_functions	no value	no value
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
dofref_ext	no value	no value
dofref_root	no value	no value
enable_dl	On	On
error_append_string	no value	no value
error_log	no value	no value
error_prepend_string	no value	no value
error_reporting	5143	5143
expose_php	On	On
extension_dir	/var/www/lib/php/modules	/var/www/lib/php/modules
file_uploads	On	On

- *MySQL*.

Se instala el paquete MySQL con:

```
ftp://ftp.OpenBSD.org/pub/OpenBSD/4.5/packages/i386/mysql-server-5.0.77.tgz
```

Hay que configurar MySQL para que pueda ser usado, para ello se usa el comando:

```
# /usr/local/bin/mysql_install_db
```

```
# /usr/local/bin/mysql_install_db
Installing MySQL system tables...
OK
Filling help tables...
OK
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
/usr/local/bin/mysqladmin -u root password 'new-password'
/usr/local/bin/mysqladmin -u root -h zaratustra.fi-a.unam.mx password 'new-password'

Alternatively you can run:
/usr/local/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default. This is
strongly recommended for production servers.

See the manual for more instructions.

Please report any problems with the /usr/local/bin/mysqlbug script!

The latest information about MySQL is available on the web at
http://www.mysql.com
Support MySQL by buying support/licenses at http://shop.mysql.com
```

Ya se puede iniciar MySQL escribiendo el siguiente comando:

```
# mysqld_safe &
```

El siguiente paso es opcional, se trata de configurar MySQL de forma segura removiendo todas las bases y los accesos por default usando la herramienta *mysql_secure_installation*.

Esto es muy recomendable para servidores en producción.

Básicamente lo que se hace con este script es:

- Generar una contraseña para root (si no existiera).
- Remover los usuarios anónimos.
- Deshabilitar el acceso remoto a root.
- Remover la base de datos test o prueba.
- Actualizar las tablas de privilegios.

A continuación el comando y los mensajes que se presentan. En este caso optamos por la opción si (Y) en todas las preguntas para hacer más seguro al servidor de MySQL.

```
# /usr/local/bin/mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL
```

MySQL

SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current password for the root user. If you've just installed MySQL, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL root user without the proper authorisation.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.

Remove anonymous users? [Y/n] Y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
... Success!

By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? [Y/n] Y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? [Y/n] Y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MySQL installation should now be secure.

Thanks for using MySQL!

Creemos una base de datos y un usuario para poder trabajar con MySQL.

```
# mysql -u root -p
```

```
Enter password:
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.
```

```
Your MySQL connection id is 11
```

```
Server version: 5.0.51a-log OpenBSD port: mysql-server-5.0.51ap1
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

```
mysql> CREATE DATABASE base01;
```

```
Query OK, 1 row affected (0.01 sec)
```

```
mysql> GRANT ALL PRIVILEGES ON base01.* TO
```

```
-> "usuariobase01"@"localhost" IDENTIFIED BY
```

```
-> "ultrasecreto";
```

```
Query OK, 0 rows affected (0.05 sec)
```

```
mysql> FLUSH PRIVILEGES;
```

```
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> EXIT
```

```
Bye
```

Ya se tiene instalado y configurado MySQL en el equipo, además contamos con un nombre de usuario y una contraseña. Ahora se necesita instalar el paquete necesario para que PHP pueda trabajar con MySQL.

```
ftp://ftp.OpenBSD.org/pub/OpenBSD/4.5/packages/i386/php5-mysql-5.2.8.tgz
```

Se necesite crear un enlace simbólico más:

```
# ln -fs /var/www/conf/php5.sample/mysql.ini \  
/var/www/conf/php5/mysql.ini
```

Para que PHP pueda conectarse con MySQL se debe de crear un directorio de soporte para PHP y un enlace simbólico más.

```
# mkdir -p /var/www/var/run/mysql  
# ln -f /var/run/mysql/mysql.sock /var/www/var/run/mysql/mysql.sock
```

- *Probando Apache, PHP y MySQL juntos.*

Para comprobar los tres servicios es necesario crear un archivo de prueba.

```
# cat > /var/www/htdocs/testmysql.php  
<?php  
/** Conectandose a la base de datos **/  
$enlace = mysql_connect('localhost', 'usuariobase01', 'ultrasecreto')  
or die('Falló la conexión, error<br>' . mysql_error());  
  
mysql_close($enlace);  
  
echo '<br><br>La configuracion fue un exito. Felicidades!';  
  
?>
```

Reiniciar apache.

```
# apachectl -k stop  
# apachectl -k graceful
```

Finalmente escribir *testmysql.php* en el navegador web.

<http://localhost/testmysql.php>

A rectangular box with a thin black border containing the text "La configuracion fue un exito. Felicidades!".

La configuracion fue un exito. Felicidades!

Si es así, entonces la configuración de PHP y MySQL ha sido exitosa.

Anexo 9. Instalación y configuración de phpMyAdmin.

Para la administración de la base de datos en MySQL por medio de una página web, se utiliza la herramienta phpMyAdmin.

Para la instalación se utiliza el comando:

```
# pkg_add ftp://ftp.OpenBSD.org/pub/OpenBSD/4.5/packages/i386/phpMyAdmin-2.11.9.4.tgz
```

La instalación de phpMyAdmin se encuentra en la siguiente ruta:

/var/www/phpMyAdmin.

Para que funcione phpMyAdmin se necesitan habilitar los módulos:

- php5-gd
- php5-mbstring
- php5-mcrypt

Se crean las siguientes ligas para su funcionamiento:

```
# ln -fs /var/www/conf/php5.sample/gd.ini /var/www/conf/php5/gd.ini
# ln -fs /var/www/conf/php5.sample/mbstring.ini /var/www/conf/php5/mbstring.ini
# ln -fs /var/www/conf/php5.sample/mcrypt.ini /var/www/conf/php5/mcrypt.ini
```

Como el apache se encuentra chrootado se necesita crear la liga:

```
# ln -s ../phpMyAdmin /var/www/htdocs/phpMyAdmin
```

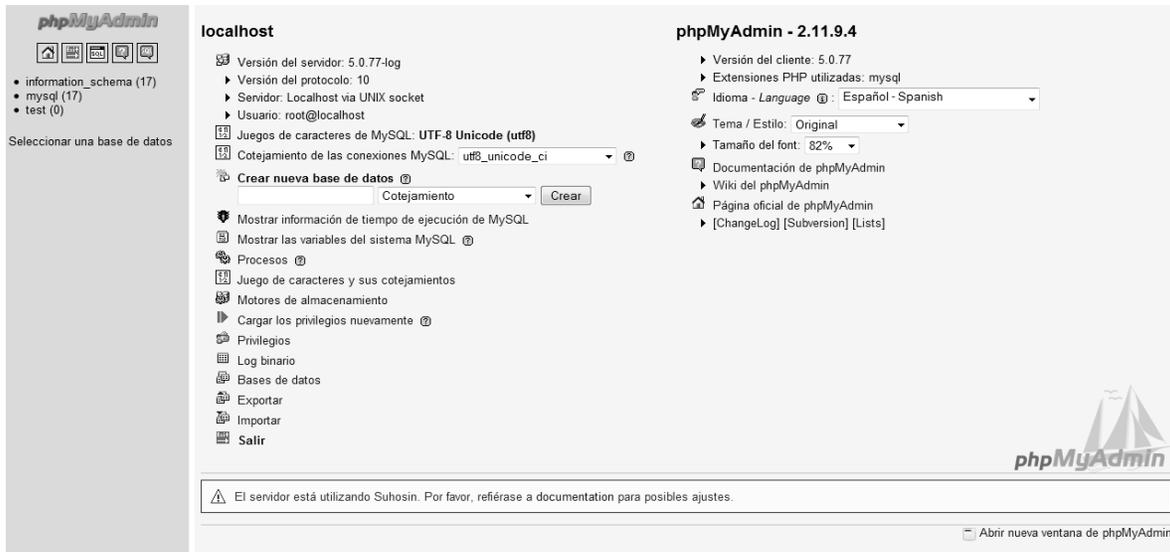
Para verificar que el phpMyAdmin se encuentra correctamente funcionando se necesita escribir en un navegador web:

http://<localhost>/phpMyAdmin/index.php

Y debe de aparecer la siguiente pantalla:



Y al introducir el usuario y contraseña válidos para la base de datos debe de aparecer la siguiente pantalla:



Anexo 10. Servidor Radius en OpenBSD.

Actualmente, FreeRADIUS permite su instalación mediante la descarga y compilación del código fuente, sin embargo, para su mejor manejo, resulta más práctico realizar la instalación por medio de ports de OpenBSD.

```
# pkg_add ftp://ftp.OpenBSD.org/pub/OpenBSD/4.5/packages/i386/freeradius-ldap-2.0.1.tgz
gdbm-1.8.3p0: complete
freeradius-2.0.1p0: complete
freeradius-ldap-2.0.1: complete
--- freeradius-2.0.1p0 -----
```

Después de que el ports fue instalado se anexa el siguiente script en */etc/rc.local* para cada vez que reinicie el sistema operativo se inicie la aplicación FreeRADIUS.

```
if [ -x /usr/local/sbin/radiusd ]; then
    install -d -o _freeradius /var/run/radiusd
    echo -n ' radiusd'; /usr/local/sbin/radiusd
fi
```

Al instalarse los paquetes, se ejecutan; para poder configurarlos, deben pararse con el siguiente comando:

```
# /etc/init.d/freeradius stop
```

- *Configuración.*

FreeRADIUS cuenta con diversos archivos que deben configurarse para lograr que funcione como se requiera. Los principales son:

- radiusd.conf
- users
- clients.conf
- sql.conf
- eap.conf

Todos localizados en */etc/freeradius*.

Radiusd.conf

Aquí solamente es necesario cambiar los argumentos relacionados con SQL, EAP y la configuración del dominio al que los clientes se conectarán. SQL se configura

para que RADIUS se conecte a él para comparar la información de autenticación. EAP es el protocolo para la autenticación de usuario, usada normalmente en redes inalámbricas.

Este archivo de configuración es demasiado largo así que aquí sólo se presentan las secciones de interés que fueron modificadas. Para comenzar, debe sustituirse todo del directorio de configuración encontrado en el archivo por el directorio actual de FreeRADIUS, en nuestro caso `/etc/freeradius`.

```
modules {
  pap {
    auto_header = yes
  }
  chap {
    authtype = CHAP
  }
  pam {
    pam_auth = radiusd
  }
  unix {
    cache = no
    cache_reload = 600
    radwtmp = ${logdir}/radwtmp
  }
  $INCLUDE /etc/freeradius/eap.conf
  mschap {
    authtype = MS-CHAP
    use_mppe = yes
    require_encryption = yes
    require_strong = no
    with_ntdomain_hack = yes
  }
  ldap {
    server = "ldap.your.domain"
    basedn = "o=My Org,c=UA"
    filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
    start_tls = no
    access_attr = "dialupAccess"
    dictionary_mapping = ${raddbdir}/ldap.attrmap
    ldap_connections_number = 5
    timeout = 4
    timelimit = 3
    net_timeout = 1
  }
  preprocess {
```

```
huntgroups = /etc/freeradius/huntgroups
hints = /etc/freeradius/hints
with_ascend_hack = no
ascend_channels_per_line = 23
with_ntdomain_hack = yes
with_specialix_jetstream_hack = no
with_cisco_vsa_hack = no
}
ippool main_pool {
range-start = 192.168.1.1
range-stop = 192.168.1.254
netmask = 255.255.255.0
cache-size = 800
session-db = ${raddbdir}/db.ippool
ip-index = ${raddbdir}/db.ipindex
override = no
maximum-timeout = 0
}
}
instantiate {
exec
expr
}
authorize {
preprocess
chap
mschap
suffix
eap
files
sql
}
authenticate {
Auth-Type PAP {
pap
}
Auth-Type CHAP {
chap
}
Auth-Type MS-CHAP {
mschap
}
unix
eap
}
```

```
preacct {
preprocess
acct_unique
suffix
}
accounting {
detail
unix
radutmp
sql
}
session {
radutmp
sql
}
post-auth {
sql
}
pre-proxy {
}
post-proxy {
eap }
```

Sql.conf.

Se decidió usar MySQL como administrar a los usuarios de RADIUS debido a que permite administrarlos de forma simple y flexible. Es más sencillo agregar campos a una base de datos que modificar los archivos de configuración de FreeRADIUS.

Una vez que en el archivo de configuración 'radiusd.conf' se ha activado el soporte para SQL, debemos configurar el archivo 'sql.conf' que contiene información sobre el servidor SQL y las consultas que se deben hacer para obtener la información de los usuarios.

```
sql {
driver = "rlm_sql_mysql"
server = "localhost"
login = "root"
password = "mysql"
radius_db = "radius"
acct_table1 = "radacct"
acct_table2 = "radacct"
postauth_table = "radpostauth"
authcheck_table = "radcheck"
authreply_table = "radreply"
```

```
groupcheck_table = "radgroupcheck"
groupreply_table = "radgroupreply"
usergroup_table = "usergroup"
nas_table = "nas"
deletestalesessions = yes
sqltrace = no
sqltracefile = ${logdir}/sqltrace.sql
num_sql_socks = 5
connect_failure_retry_delay = 60
sql_user_name = "%{User-Name}"
}
```

Eap.conf.

Se configura este archivo para que EAP (Extensible Authentication Protocol) funcione como protocolo de autenticación. EAP se utilizará como PEAP (Protected EAP). El cual, a su vez, usará MSCHAPV2 (Microsoft Challenge-Handshake Authentication Protocol).

Además se requiere establecer la lista de certificados.

```
eap {
default_eap_type = peap
timer_expire = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no
md5 {
}
leap {
}
gtc {
auth_type = PAP
}
tls {
private_key_password = whatever
private_key_file = /etc/freeradius/certs/cert-srv.pem
certificate_file = /etc/freeradius/certs/cert-srv.pem
CA_file = /etc/freeradius/certs/demoCA/cacert.pem
dh_file = /etc/freeradius/certs/dh
random_file = /dev/urandom
}
peap {
default_eap_type = mschapv2
}
```

```
}  
mschapv2 {  
}  
}
```

Una vez configurado este archivo, deben crearse ligas simbólicas a los certificados que EAP necesita, para que pueda localizarlos. Para ello, se entra al directorio donde se guardan los certificados y se ejecuta un *rehash*.

```
# cd /etc/freeradius/certs
```

```
# c_rehash
```

Users

Este archivo es el que contiene la información de los usuarios que pueden acceder a la red, en caso de que no se use otro método. En nuestro caso, este archivo no tiene mucho uso puesto que se usó una base de datos en MySQL.

Todas las configuraciones que tengan como usuario default, son las que se asignarán a los usuarios en caso de que no estén especificadas para ellos.

Clients.conf

Aquí se especifican los IPs o subredes desde las cuales se aceptarán peticiones. Si llega una petición de acceso desde un IP que no esté registrado aquí, el servidor RADIUS simplemente la ignora, negándole el acceso. En nuestro caso se acepta al localhost y al AP que enviará las solicitudes.

```
client 127.0.0.1 {  
secret = supersecretradiuskey  
shortname = some_name  
}  
client 192.168.119.1 {  
secret = ulises  
shortname = rifi  
}
```

Para correr FreeRADIUS, una vez hechas todas estas modificaciones, se escribe el comando:

```
# /usr/sbin/freeradius start
```

Configuración de MySQL

FreeRADIUS hace uso de una base de datos llamada radius.

Primero se entra a MySQL y se ejecuta el siguiente comando, para crearla:

```
mysql> create database radius;
```

Después, en la línea de comandos, se correrá un script que FreeRADIUS trae consigo:

```
# cd /usr/share/doc/packages/freeradius/doc/examples/  
# mysql -u root -p radius < mysql.sql
```

Así ya se cuenta con una base de datos para la autenticación. Las tablas más importantes son:

- *usergroup*: Se define a qué grupo pertenecen los usuario. Sus atributos son:
 - ✓ id. Identificador de registro.
 - ✓ UserName. Nombre de usuario.
 - ✓ GroupName. Grupo al que pertenece el usuario.

- *radcheck*: Aquí se definen las contraseñas de cada usuario. Sus atributos son:
 - ✓ id. Identificador de registro.
 - ✓ UserName. Nombre de usuario.
 - ✓ Attribute. Tipo de contraseña. En nuestro caso, 'User-Password'.
 - ✓ Op. Es el operador que se usará para la comprobación. Para este caso '=='.
 - ✓ Value. La contraseña.

- *radreply*: En esta tabla se definen los atributos sobre la conexión y sesión de los usuarios; por ejemplo, IP asignada y tiempo de espera máximo. En este caso, permitimos que se asignen los de DEFAULT contenidos en el archivo 'users'; por lo tanto, no insertamos nada en la tabla.

- *radgroupreply*: Similar a radcheck pero permite establecer atributos a un grupo de usuarios completo. Atributos:
 - ✓ id. Identificador de registro.
 - ✓ GroupName. Nombre de grupo.
 - ✓ Attribute. Nombre del atributo que se quiere agregar.
 - ✓ El tipo de autenticación: 'Auth-Type'.
 - ✓ Op. Es el operador para la comprobación. Para este caso ':='.
 - ✓ Value. El valor del atributo. Nuestro Auth-Type es 'EAP'.

Las tablas para FreeRADIUS quedarían de la siguiente forma:

```
mysql> select * from usergroup;
+----+-----+-----+
| id | UserName | GroupName |
+----+-----+-----+
| 1 | Enrique | dynamic |
| 2 | Adrian | dynamic |
+----+-----+-----+
```

```
mysql> select * from radcheck;
+----+-----+-----+-----+-----+
| id | UserName | Attribute | Op | Value |
+----+-----+-----+-----+-----+
| 1 | Enrique | User-Password | := | perro123 |
| 2 | Adrian | User-Password | := | gato456 |
+----+-----+-----+-----+-----+
```

```
mysql> select * from radgroupreply;
+----+-----+-----+-----+-----+
| id | GroupName | Attribute | Op | Value |
+----+-----+-----+-----+-----+
| 34 | dynamic | Auth-Type | := | EAP |
+----+-----+-----+-----+-----+
```

Anexo 11. Filtrado de contenido con Squid.

Para realizar la instalación de la aplicación sea hace por medio de los paquetes pre compilados de OpenBSD:

```
pkg_add ftp://ftp.openbsd.org/pub/OpenBSD/4.5/packages/i386/squid-2.7.STABLE6-ldap-snmp.tgz
```

Después de que el port fue instalado se anexa el siguiente script en */etc/rc.local* para que cada vez que reinicie el sistema operativo se inicie la aplicación squid automáticamente.

```
if [ -x /usr/local/sbin/squid ]; then
    echo -n ' squid';    /usr/local/sbin/squid
fi
```

Se edita el archivo de configuración */etc/squid/squid.conf* de acuerdo con las necesidades.

El archivo de configuración queda de la siguiente forma:

```
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

acl redlocal src 192.168.1.0/255.255.255.0
```

```
acl porno url_regex "/etc/squid/pag_porno"
acl desdir url_regex "/etc/squid/pag_descargas_directas"
acl pagpro url_regex "/etc/squid/pag_prohibidas"
acl webmsn url_regex "/etc/squid/pag_web_messenger"
acl palabras url_regex "/etc/squid/palabras_filtradas"
acl usrmsn src "/etc/squid/usuarios_messenger"
acl usrvip src "/etc/squid/usuarios_vip"
http_access allow usrvip
http_access deny palabras
http_access deny porno
http_access deny desdir
http_access deny pagpro
http_access allow usrmsn
http_access deny webmsn
http_access allow redlocal
http_access deny all

icp_access allow localnet
icp_access deny all

http_port 3128 transparent

hierarchy_stoplist cgi-bin ?

cache_mem 64 MB
maximum_object_size_in_memory 64 KB
cache_dir ufs /var/squid/cache 32768 16 256

access_log /var/squid/logs/access.log squid
refresh_pattern ^ftp:      1440 20% 10080
refresh_pattern ^gopher:  1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern .         0 20% 4320

acl shoutcast rep_header X-HTTP09-First-Line ^ICY.[0-9]
upgrade_http0.9 deny shoutcast
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache

error_directory /usr/local/share/squid/errors/Spanish
dns_nameservers 132.248.204.1 132.248.1.3 132.248.10.2
coredump_dir /var/squid/cache
```

Se utilizara una cache de 30 GB en */var/squid/cache*.

Se crean unos archivos bajo `/etc/squid/` quedando de la siguiente forma:

```
-rw-r--r-- root mib.txt
-rw-r--r-- root mime.conf
-rw-r--r-- root pag_descargas_directas
-rw-r--r-- root pag_porno
-rw-r--r-- root pag_prohibidas
-rw-r--r-- root pag_web_messenger
-rw-r--r-- root palabras_filtradas
-rw-r--r-- root scrip_squid
-rw-r--r-- root squid.conf
-rw-r--r-- root usuarios_messenger
-rw-r--r-- root usuarios_vip
```

En donde:

```
-rw-r--r-- root pag_descargas_directas
-rw-r--r-- root pag_porno
-rw-r--r-- root pag_prohibidas
-rw-r--r-- root pag_web_messenger
-rw-r--r-- root palabras_filtradas
-rw-r--r-- root usuarios_messenger
-rw-r--r-- root usuarios_vip
```

Es donde colocaremos las páginas que no quieren que visiten los usuarios, el acceso a ciertos usuarios a aplicaciones como messenger, los usuarios que podrán acceder a todo, etcétera.

El squid se configura de manera transparente, esto quiere decir que el usuario no se da cuenta de que sus peticiones son hechas al servidor squid y no a internet directamente, para lograr esto es necesario redireccionar todas las peticiones al puerto de squid que es el 3128, esto se hace colocando la siguiente línea en el archivo `/etc/pf.conf`:

```
 rdr in on $int_if inet proto { tcp, udp } from any to any port www -> 127.0.0.1 port 3128
```

Anexo 12. Políticas del servicio.

Sobre los usuarios del servicio.

- Podrán hacer uso del servicio todos los alumnos, activos de la Facultad de Ingeniería.

Sobre la solicitud del servicio.

- Deberá registrar sus datos personales y los de su computadora en la página web de registro para activarles el servicio.
- Los datos de la computadora que deberá proporcionar son los siguientes:
 - ✓ Marca.
 - ✓ Modelo.
 - ✓ Número de serie.
 - ✓ Sistema Operativo.
 - ✓ Dirección MAC (identificador asociado a la tarjeta de red).
- Los datos personales que proporcionara son los siguientes:
 - ✓ Teléfono de casa.
 - ✓ Teléfono celular.
 - ✓ Correo electrónico.
 - ✓ Dirección.
- En caso que se cambie de computadora, tarjeta de red, teléfono, etcétera, debe de actualizar sus datos.
- El servicio es por tiempo limitado y coincide con los periodos escolares, por lo que deberá renovarse al inicio de cada periodo escolar.

Sobre el uso del servicio.

- Los servicios proporcionados serán únicamente acceso a Internet y acceso a servicios locales basados en Web como es el correo electrónico y la información de los recursos de la Biblioteca Enrique Rivero Borrell.
- El servicio no incluye acceso a los servidores de aplicaciones e impresión.
- Es responsabilidad del usuario el tipo de información que consulta, ya que esta puede ser de contenido inapropiado.

- Algunos recursos y servicios de la red Internet son privados y existen derechos sobre ellos, por lo que el acceso no autorizado a estos es responsabilidad única del usuario.
- El administrador de la red inalámbrica se reserva el derecho de cancelar temporal o definitivamente el servicio cuando se haga uso inapropiado del sistema. Se considera uso inapropiado actividades como:
 - Compartir carpetas, archivos o impresoras en red.
 - Utilizar los servicios de red con fines de lucro, entretenimiento personal, descarga de software, archivos de música, audio o video.
 - Utilizar software que atente contra la seguridad de la red.
 - Hacer mal uso de CHATS, redes sociales o círculos de conversación.
 - El uso de altavoces, el usuario podrá escuchar archivos de audio utilizando solamente audífonos.
 - Visitar páginas eróticas o pornográficas, así como colocar en los protectores de pantalla imágenes de este tipo pues se considera una falta de respeto a la institución.
 - Atentar contra la información de otros usuarios.
 - Ingresar o tratar de ingresar a otros equipos.
 - Intercambio o distribución de contenido pornográfico.
 - Propagar virus, gusanos u otro código malicioso.
 - Usar la red para realizar actividades delictivas.
 - Envío de mensajes no solicitados (spam).
 - Atentar contra la disponibilidad, integridad, confidencialidad de la red.
 - El uso simultáneo de una cuenta desde dos equipos diferentes.
 - Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Se generará un reporte que irá directamente al expediente del usuario.
- La seguridad informática del equipo de cómputo es responsabilidad del usuario del servicio, este deberá de proteger su computadora con programas antivirus actualizados, cerrar todo acceso libre a su equipo como pudieran ser las cuentas públicas sin contraseña y actualizaciones del sistema operativo.

Sobre el soporte del servicio.

- El administrador de la red se compromete a mantener en buen funcionamiento la operación de la red.

- El administrador de la red no proporcionará el servicio de configuración de las tarjetas de las computadoras de los usuarios ya que es responsabilidad del fabricante o del usuario la correcta configuración de los dispositivos de la computadora.
- No es responsabilidad del administrador de la red la configuración del sistema operativo o de cualquier otro software instalado en el equipo del usuario.
- Se proporcionará manuales de configuración en forma digital para soporte técnico a los usuarios.

Nota: Habrá equipos cuya configuración no sea compatible para otorgar el servicio, es necesario documentarse con su proveedor para saber si es posible conectarlas al servicio.

Anexo 13. Base de datos.

La base de datos para el registro a la red inalámbrica contiene las siguientes tablas:

- *tb_alumnos_insc.*
- *tb_alumnos_dat.*
- *tb_carreras.*
- *tb_datos_eq.*

En la tabla *tb_alumnos_insc* están los registros de los alumnos que se encuentran inscritos en el semestre en curso, esta tabla la proporciona la Unidad de Servicios de Computo Administrativo (USECAD), de ella solo se requieren los siguientes atributos:

- Cuenta.
- Nombre.
- Clave.
- Contraseña.

El campo *Cuenta* contiene el número de cuenta del alumno este atributo es la llave primaria de la tabla, el atributo *Nombre* contiene el nombre completo del alumno, al atributo *Clave* contiene la clave de la carrera en la que se encuentra inscrito el alumno, esta es la llave foránea de la tabla y por último el atributo *Contraseña* contiene la contraseña que el alumno utiliza para poderse reinscribir.

Contamos que si un alumno se encuentra registrado en esta tabla quiere decir que por lo menos se encuentra cursando una materia en el semestre en curso.

La tabla *tb_carreras* también la proporciona la Unidad de Servicios de Computo Administrativo, en esta se encuentran los registros de las carreras que se imparten en la Facultad de Ingeniería con su respectiva clave. Los atributos de esta tabla son:

- Clave.
- Nombre.
- Clave_Nva.

El atributo *Clave* es la llave primaria de esta tabla

En la tabla *tb_datos_eq* es donde se van a guardar los registros con la información que el usuario proporcione de su computadora los atributos de esta tabla son:

- Mac.
- Marca.

- Modelo.
- No_Serie.
- Sist_Op.
- Cuenta.

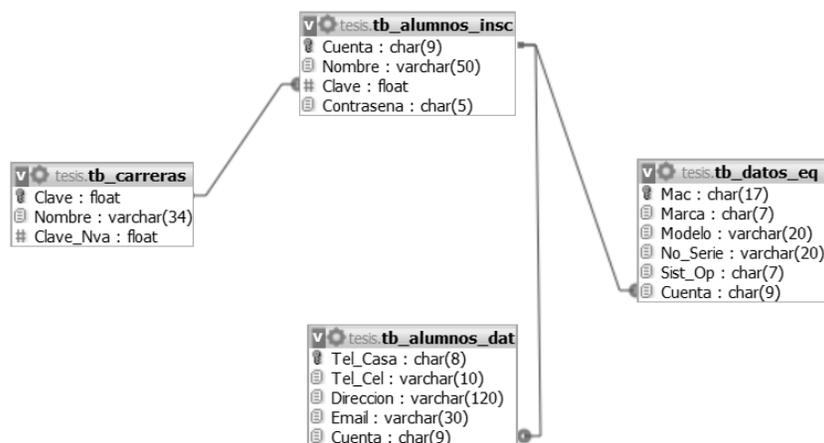
El atributo *Mac* se refiere a la dirección física de la tarjeta de red inalámbrica de la computadora este atributo es la llave primaria de esta tabla, *Marca* es el fabricante de la computadora, *Modelo* hace referencia al modelo de fabricación de la computadora, el atributo *Sist_Op* es el sistema operativo que el usuario utilizara para conectarse a la red inalámbrica y cuenta en el número de cuenta de alumno, este último atributo será nuestra llave foránea.

En la tabla *tb_alumnos_dat* contendrá los siguientes campos:

- Tel_Casa.
- Tel_Cel.
- Direccion.
- Email.
- Cuenta.

El atributo *Tel_Casa* contiene la información que el alumno proporcione de un teléfono fijo donde localizarlo este atributo será nuestra llave primaria, el atributo *Tel_Cel* tendrá el número de teléfono de celular (este campo no es obligatorio), el atributo *Direccion* contendrá la información referente a la dirección de residencia del alumno, el atributo *Email* tendrá el correo electrónico donde poder enviar información al alumno y el atributo *Cuenta* contiene el número de cuenta del alumno este último atributo es la llave foránea de esta tabla.

El mapa entidad – relación (MER) de la base de datos queda de la siguiente forma:



Mapa entidad – relación.

Índice de Tablas y Figuras

Contenido	Pagina
Capítulo I	
Figura 1.1 Fibra óptica multimodo índice escalonado.....	8
Figura 1.2 Fibra óptica multimodo índice gradual.....	8
Figura 1.3 Fibra óptica monomodo.....	9
Figura 1.4 Tipos de conectores para fibra óptica.....	10
Figura 1.5 Subsistema de cableado estructurado.....	13
Figura 1.6 Topología de red bus.....	17
Figura 1.7 Topología de red anillo.....	17
Figura 1.8 Topología de red estrella.....	18
Figura 1.9 Red inalámbrica.....	30
Figura 1.10 Crecimiento del mercado.....	32
Figura 1.11 Access Point.....	36
Figura 1.12 Radiador isotrópico.....	37
Figura 1.13 Patrón Azimutal.....	38
Figura 1.14 Zona de cobertura en los tipos de antenas.....	39
Figura 1.15 Antena de sector.....	41
Figura 1.16 Antena de panel.....	41
Figura 1.17 Antena Yagi.....	42
Figura 1.18 Antena Parabólica.....	42
Figura 1.19 Antena dipolo.....	43
Figura 1.20 Topología AD-HOC.....	55
Figura 1.21 Topología infraestructura.....	56
Tabla 1.1 Categorías de UTP.....	11
Tabla 1.2 Ventajas y desventajas redes inalámbricas.....	34
Tabla 1.3 Canal y frecuencia IEEE 802.11b para 22 Mhz.....	48
Tabla 1.4 Canal y frecuencia IEEE 802.11a para 20 Mhz.....	49
Capítulo II	
Figura 2.1 Biblioteca Enrique Rivero Borrell.....	64
Figura 2.2 Sótano de la biblioteca.....	68
Figura 2.3 Planta baja de la biblioteca.....	69
Figura 2.4 Primer piso de la biblioteca.....	69
Figura 2.5 Segundo piso de la biblioteca.....	70
Figura 2.6 Tercer piso de la biblioteca.....	70
Figura 2.7 Conexiones 110.....	72
Figura 2.8 Croquis red sótano de la biblioteca.....	74
Figura 2.9 Croquis red planta baja de la biblioteca.....	75
Figura 2.10 Croquis red primer piso de la biblioteca.....	75
Figura 2.11 Croquis red segundo piso de la biblioteca.....	76
Figura 2.12 Croquis red tercer piso de la biblioteca.....	76
Tabla 2.1. Nodos de red usados por la biblioteca.....	77

Capítulo III

Figura 3.1 Ubicación access point segundo piso.....	82
Figura 3.2 Áreas de cobertura.....	83
Figura 3.3. Netstumbler.....	88
Figura 3.4. Configuración lógica red inalámbrica.....	98
Figura 3.5. Diseño del servidor para la red inalámbrica.....	98
Figura 3.6. Estructura de la red actual en la biblioteca.....	99
Figura 3.7. Estructura de la red al incorporar la red inalámbrica en la biblioteca.....	100
Tabla 3.1 Grado de atenuación en algunos materiales.....	81
Tabla 3.2. Ancho de banda consumido de algunas aplicaciones de Internet.....	92

Capítulo IV

Figura 4.1 Pantalla de inicio de la página de registro.....	122
Figura 4.2 Pantalla de contacto de la página de registro.....	123
Figura 4.3 Pantalla de ayuda de la página de registro.....	124
Figura 4.4 Pantalla de ligas de interés de la página de registro.....	125
Figura 4.5 Políticas y lineamientos para el uso de la red inalámbrica.....	126
Figura 4.6 Ventana en donde el alumno introducirá su información.....	127
Figura 4.7 Error al introducir datos del alumno.....	127
Figura 4.8 introduciendo datos del alumno.....	128
Figura 4.9 Ventana con los datos obtenidos de la base de datos y formulario.....	128
Figura 4.10 Formulario con datos del alumno.....	129
Figura 4.11 Pantalla indicándole al alumno que verifique su información.....	129
Figura 4.12 Ventana informando de registro exitoso.....	130
Figura 4.13 Correo con la información para acceder a la red inalámbrica.....	130
Figura 4.14 Escaneo de redes inalámbricas.....	131
Figura 4.15 Ventana para introducir datos de alumnos.....	131
Figura 4.16 Introducción de datos del alumno.....	132
Figura 4.17 Acceso a la red inalámbrica.....	132
Figura 4.18 Conexión a la red inalámbrica de la biblioteca.....	133
Figura 4.19 Navegación en Internet.....	133

GLOSARIO

Access Server: Acceso a la red. Es un punto de entrada que permite a los usuarios o clientes acceder a una red.

Ad hoc: Es una locución latina que significa literalmente «para esto». Generalmente se refiere a una solución elaborada específicamente para un problema o fin preciso y, por tanto, no es generalizable ni utilizable para otros propósitos. Se usa pues para referirse a algo que es adecuado sólo para un determinado fin. En sentido amplio, *ad hoc* puede traducirse como «específico» o «específicamente».

AP: Access Point, Punto de Acceso. Es el equipo de la red inalámbrica que se encarga de gestionar las comunicaciones de todos los dispositivos que forman la red. El punto de acceso no sólo se utiliza para controlar las comunicaciones internas de la red, sino que también hace de puente en las comunicaciones con las redes externas (redes cableadas e Internet).

Ángulo de inserción: Ángulo formado por los dos lados del inserto que se unen en el punto de corte. Los ángulos de inserción más grandes son más fuertes que los ángulos más pequeños.

AUI: Attachment Unit Interface, Interfaz de Unidad de Anexión. Es una parte de los estándares IEEE Ethernet que especifica como un cable será conectado a una tarjeta Ethernet. AUI especifica un cable coaxial conectado a un transceptor (un transmisor-receptor) que se enchufa en un socket de 15 pines en la tarjeta de interfaz de red (NIC o network interface card). Un cable AUI puede tener hasta 50 metros de largo.

Bridge: Puente. Es un dispositivo que interconecta dos redes que utilizan el mismo protocolo haciéndolas funcionar como si se tratara de una sola red.

Celosía: Una estructura reticular de barras rectas interconectadas en nudos formando triángulos planos (retículos planos). En muchos países se les conoce como armaduras

Cifrado: El cifrado consiste en transformar un texto en claro (inteligible por todos) mediante un mecanismo de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.

Código: La forma que toma la información que se intercambia entre la Fuente (el emisor) y el Destino (el receptor) de un lazo informático.

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance, Acceso Múltiple por Detección de Portadora con Evitación de Colisión. Es el sistema que emplean Wi-Fi para negociar las comunicaciones entre los distintos dispositivos. Este sistema evita que dos dispositivos puedan hacer uso del medio simultáneamente (evita la colisión).

DB: Decibel. Es una unidad que mide la relación entre dos valores. Por ejemplo, la relación entre la señal y el ruido o la ganancia se miden en decibeles. Esta unidad se representa por las letras dB y utiliza una escala logarítmica.

dBd: Abreviación para los decibeles de ganancia de la antena en referencia a una antena clásica y sencilla, un dipolo de media onda, es decir dos ramales cada uno de un cuarto de onda, a esta antena se le otorga 0 dBd de ganancia.

DBi: Abreviación para los decibeles de ganancia de la antena en referencia a la ganancia de una antena isotrópica (de aquí proviene la i). Una antena isotrópica es una antena teórica que radia con una simetría perfecta en las tres dimensiones. Las antenas del mundo real tienen patrones de radiación que están muy lejos de ser simétricos, pero este efecto generalmente se aprovecha por el diseñador del sistema para optimizar la cobertura de un área geográfica específica.

DHCP: Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host. Es un protocolo que permite que un servidor asigne dinámicamente las direcciones IP a los equipos clientes conforme éstos las van necesitando.

Dispersión modal: La dispersión modal, o *dispersión intermodal*, determina la capacidad de ancho de banda de las fibras multimodo. Las velocidades de grupo de los diferentes modos varían y conducen a un ensanchamiento del retardo de grupo o dispersión intermodal. El máximo retardo viene dado por la expresión:

$$\frac{\tau}{L} = \frac{\Delta n}{2c} = \frac{(NA)^2}{2nc}$$

Los límites de la dispersión son proporcionales, por tanto, al cuadro de la apertura numérica. Para fibras de índice gradual con perfil parabólico, el valor máximo está dado por:

$$\frac{\tau}{L} = \frac{n\Delta^2}{2c} = \frac{[NA(o)]^4}{8n^3c}$$

Para este tipo de fibras, la capacidad limitada por la dispersión es $2/\delta$ veces mayor que para fibras de salto de índice con el mismo valor de δ . Ya que δ es aproximadamente próximo al 1 por ciento, la capacidad de las fibras de índice gradual puede ser dos órdenes de magnitud superior a la de fibras de salto de índice. Las capacidades expresadas para fibras multimodo representan el peor de los casos estimados. La pérdida modal diferencial y el acoplamiento modal son causas que hacen improbable el cumplimiento de las expresiones mencionadas. Los modos de orden superior sufren una atenuación diferencial mayor debido a la mayor radiación del acoplamiento de modos. Esto reduce la apertura numérica efectiva, disminuyendo la dispersión modal. La mezcla de

modos es un efecto debido a las imperfecciones estructurales, inhomogeneidades del índice de refracción, fluctuaciones en el diámetro y extrañas birrefringencia, y todo ello conduce a una ecualización de la velocidad modal. El acoplamiento modal reduce el ensanchamiento de las velocidades en la medida en que los modos acoplados tienden a poseer una velocidad promedio común de propagación. En las fibras de índice gradual, las velocidades modales están casi ecualizados. La mezcla modal y las pérdidas diferenciales tienen un pequeño efecto sobre la expresión que representa a la dispersión.

DNS: Domain Name System, Sistema de Nombres de Dominio. Este sistema es el encargado de traducir los nombres de dominio (como fi.unam.mx) de los equipos conectados a Internet en direcciones IP (como 128.56.78.2).

EMI: Electromagnetic Interference, Interferencia Electromagnética. Es cualquier señal o emisión, radiada en el espacio o conducida a través de un cable de alimentación o señal, que pone en peligro el funcionamiento de la navegación por radio u otro servicio de comunicaciones por radio autorizado.

Encriptación: La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

ERO: European Radiocommunications Office. Oficina Europea de Radiocomunicaciones. La Oficina Europea de Radiocomunicaciones (ERO) se inició formalmente el 6 de mayo de 1991 y se encuentra en Copenhague, Dinamarca. ERO es la oficina permanente de apoyo al Comité de Comunicaciones Electrónicas (ECC) ECC es el Comité que reúne a los y las autoridades reguladoras de las telecomunicaciones de radio de los 45 países miembros de la CEPT.

Espectro Disperso. El espectro disperso es una técnica de comunicación, que trabaja en un amplio ancho de banda, por ejemplo una estación radial en la banda de FM ocupa aprox. 0.2 MHz, y como la banda de FM es de 88-108 MHz, entonces se tendrá en la banda de FM $(108 - 88)/0.2 = 100$ emisoras.

Si por el contrario quisiéramos tener 300 emisoras, en la misma banda de FM tendríamos que disminuir el ancho de banda de cada emisora, esto ocasionaría grandes problemas ya que causaría interferencias entre estaciones cercanas.

Usualmente en una comunicación se requiere que el transmisor transmita una amplitud de banda lo más pequeña posible, pero lo suficientemente grande como para transmitir la información deseada.

El espectro disperso consiste en elegir un ancho de banda lo más grande posible de lo que se necesite para enviar la información enviándolas por trocitos en frecuencias diferentes (Frecuencia Hopping), y en un receptor normal solo se escucharía pequeños zumbidos, para escuchar la información

en si, hace falta tener el decodificador adecuado por lo cual esta técnica de transmisión es segura.

FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos. Es un protocolo de Internet que permite transferir archivos de un equipo a otro.

FTAM: File Transfer Access and Management, Gestión y Acceso de Transferencia de Archivos. Es un protocolo de uso de la ISO, ofrece servicios de la transferencia de archivo entre el cliente y los sistemas del servidor en un ambiente abierto. FTAM también proporciona el acceso a los archivos y a la gestión de archivos en sistemas diversos.

HTML: HypertText Markup Language, Lenguaje de Diseño de Hipertexto. Se trata de un formato especial de archivos sobre el que está basa la estructura del servicio WWW (World Wide Web).

HTTP: Hypertext Transfer Protocol, Protocolo de Transporte de Hipertexto. Es el protocolo que se utiliza en Internet para transferir la información web.

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos Electrónicos. Es una asociación mundial de ingenieros de este sector. El IEEE forma también el comité de normalización que recomienda al ANSI (órgano estadounidense de normalización) sobre los estándares de tecnologías de redes de área local.

IMAP: Internet Message Access Protocol, Protocolo de Acceso a Mensajes de Internet. Es un protocolo estándar para el manejo de correo electrónico. En éste protocolo cliente / servidor el correo electrónico es recibido y almacenado para los usuarios en el servidor del proveedor. Permite consultar únicamente los encabezados (remitente, titulo, tamaño) del mensaje antes de decidir si descargar, almacenar o eliminarlo.

IR: Infrared, Infrarrojo. Es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas. Consecuentemente, tiene menor frecuencia que la luz visible y mayor que las microondas. Su rango de longitudes de onda va desde unos 0,7 hasta los 300 micrómetros.

ISO: International Standard Organization, Organización Internacional para la Normalización. Esta organización ha definido los protocolos de comunicaciones conocidos como ISO/OSI, utilizado por las redes públicas de conmutación de paquetes.

Isotópico: Material que posee las mismas propiedades físicas en todas las direcciones. También llamado isótropo

ITU: International Telecommunications Union, Unión Internacional de telecomunicaciones. Es el organismo especializado de la Organización de las

Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Kevlar. Poliparafenileno tereftalamida es una poliamida sintetizada por primera vez por la química Stephanie Kwolek en 1965, quien trabajaba para DuPont. La obtención de las fibras de Kevlar fue complicada, destacando el aporte de Herbert Blades, que solucionó el problema de qué disolvente emplear para el procesado. Finalmente, DuPont empezó a comercializarlo en 1972. Es muy resistente y su mecanización resulta muy difícil.

Key Crackers: (key generator, generador de llave, clave, serial, número de llave). Programa que suele ser pequeño y que permite generar una clave (serial, llave, key o número de registración) para una aplicación shareware específica. El objetivo es obtener una aplicación sin restricciones, como si el usuario la hubiese comprado.

LAN: Local Area Network, Red de Área local. Es una red de datos que interconecta equipos situados en el entorno de un edificio o de las oficinas de una empresa dentro de ese edificio. Una red local permite a sus usuarios compartir información y recursos de la red, como impresoras o líneas de comunicaciones.

LMDS: Local Multipoint Distribution Service, Sistema de Distribución Local Multipunto. Es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Packet Sniffers: es un programa de captura de las tramas de una red.

Password: Contraseña. Es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un equipo, o a un programa. En sistemas multiusuarios, cada usuario debe incorporar su contraseña antes de que el equipo responda a los comandos.

Patrón azimutal: La forma de irradiar de una antena si la estuviéramos observando desde arriba

POP: Post Office Protocol, Protocolo de Oficina de Correos. Protocolo diseñado para permitir a sistemas de usuario individual leer correo electrónico almacenado en un servidor.

Ports: *Ports collection* o *Port trees*, *Colección de Puertos y Puerto de Árboles*. Son un conjunto de archivos del tipo make (herramienta de generación o automatización de código) y parches, de los sistemas operativos BSD: FreeBSD, NetBSD y OpenBSD. Por otra parte, es un método simple de instalación de software o creación de paquetes binarios. Son usualmente la base de los sistemas de gestión de paquetes, con ports gestionando la creación de paquetes y herramientas adicionales gestión, eliminación de

paquetes, actualizaciones y otras acciones cómo gestión de dependencias entre paquetes.

Proxy: El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

MIMO: Multiple-input Multiple-output, Múltiple entrada múltiple salida. Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores. 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.

Modelo OSI: El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

NAT: Network Address Translation, Traducción de Direcciones de Red. Es un estándar que le permite a las redes locales conectadas a Internet utilizar su propio sistema de numeración IP privado compartiendo los números IP públicos. Los usuarios de la red pueden acceder a Internet a través del router, pero el resto de usuarios de Internet no pueden acceder directamente a los equipos de la red local.

Radiofrecuencia: También denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz. Las ondas electromagnéticas de esta región del espectro se pueden transmitir aplicando la corriente alterna originada en un generador a una antena.

Router: Es un sistema utilizado para transferir datos entre dos redes que utilizan un mismo protocolo. Un router puede ser un dispositivo software, hardware o una combinación de ambos.

RJ45: Es el nombre que recibe el conector un conector estándar que se utiliza habitualmente en el cableado de las redes locales Ethernet 10BASET y 100BASET.

SMTP: Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo. Se trata del protocolo en el que se basa el servicio de correo electrónico en Internet. Este protocolo define el formato que deben tener los mensajes y cómo éstos deben ser transferidos.

SNMP: Simple Network Management Protocol, Protocolo Simple de Administración de Red. Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SSH: Secure Shell, Intérprete de órdenes Segura. Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

STP: Shielded Twisted Pair, Par Trenzado Apantallado. Es un cable similar al UTP con la diferencia que cada par tiene una pantalla protectora, además de tener una lámina externa de aluminio o de cobre trenzado alrededor del conjunto de pares, diseñada para reducir la absorción del ruido eléctrico.

Streaming: es un término que se refiere a ver u oír un archivo directamente en una página web sin necesidad de descargarlo antes al ordenador

S/STP: Screened Shielded Twisted Pair, Apantallado Par Trenzado Apantallado. Es un cable que además de la protección del STP, añade una malla metálica que ayuda a reducir las interferencias próximas al cable. Este tipo de cable también se denomina también S/FTP: Screened Fully Shielded Twisted Pair.

TCP/IP: Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo Internet. Normas técnicas de actuación que fijan el interfuncionamiento de las redes que forman parte de Internet.

Topología: Se define como la cadena de comunicación que los nodos que conforman una red usan para comunicarse. Un ejemplo claro de esto es la topología de árbol, la cual es llamada así por su apariencia la cual puede comenzar con la inserción del servicio de internet desde el proveedor, pasando por el router, luego por un switch y este deriva a otro switch u otro router o sencillamente a los hosts (estaciones de trabajo, pc o como quieran llamarle), el resultado de esto es una red con apariencia de árbol porque desde el primer router que se tiene se ramifica la distribución de internet dando lugar a la creación de nuevas redes y/o subredes tanto internas como externas.

Transceiver: (Transductor) Dispositivo que recibe la potencia de un sistema mecánico, electromagnético o acústico y lo transmite a otro, generalmente en forma distinta. El micrófono y el altavoz son ejemplos de transductores. En comunicaciones (informática) es un transmisor/receptor de señales de radio frecuencia (RF), sirve para conectar aparatos por vía inalámbrica.

UTP: Unshielded Twisted Pair, Par Trenzado sin Apantallar. Son cables de pares trenzados sin apantallar (Son más flexibles que los cables apantallados), se utilizan para diferentes tecnologías de red local. Su coste en comparación con otros cables de red es menor pero producen más errores que otros tipos de cable al no estar apantallados en caso de existir algún tipo de interferencia, además tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.

WAP: Wireless Application Protocol, Protocolo de Aplicaciones Inalámbricas. Es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, por ejemplo, acceso a servicios de Internet desde un teléfono móvil. Se trata de la especificación de un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos, se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.

Web Crackers: Programa que realiza un ataque de diccionario sobre páginas web que requieren de usuario y password.

WEP: *Wired Equivalent Privacy*, Privacidad Equivalente a Cableado. Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

WiMAX: Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas. Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el IEEE 802.16. Una de sus ventajas es dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados (zonas rurales).

WLAN: Wireless Local Area Network, Redes Inalámbricas de Área Local. Es un sistema de comunicación de datos inalámbrico flexible, 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.

WPA: Wi-Fi Protected Access, Acceso Protegido Wi-Fi. Es un sistema para proteger las redes inalámbricas; su finalidad es corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo WEP.

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida (PSK, Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

WPA2: Wi-Fi Protected Access 2, Acceso Protegido Wi-Fi 2. Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA

Bibliografía

“A field guide to wireless LAN’s for administrators and power users”.

Maufer Thomas.
Prentice Hall, 2003

“Apuntes de Redes”.

Viguera Villaseñor, Marco.
UNAM 2003.

“A field guide to wireless LAN’s for administrators and power users”.

Maufer Thomas.
Prentice Hall, 2003

“Building a wireless office”

Hield Gilbert.
Auerbach publications, 2003

“Building Wireless Community Networks”

Flickenger Rob.
ED O’Reilly, Enero 2002

“Manual de Redes Inalámbricas”.

Reid Neil, Seide Ron.
Mc Graw-Hill Interamerica, 2004

“Redes de Área Local”

Molina Francisco José.
Alfaomega-Rama, 2006

“Redes de comunicaciones, conceptos, fundamentos y arquitecturas Básicas”.

León-García Alberto e Wiidjaja Indra.
McGraw Hill, 2002

“Wi-Fi Cómo construir una red inalámbrica”.

Carballar José Antonio.
Alfaomega-Rama, 2005

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”.

IEEE 802.11. 1999.
ANSI/IEEE Standard 802.11, 1999 Edition.

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band”.

IEEE 802.11a. 1999.
ANSI/IEEE Standard 802.11a, 1999 Edition.

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 2.4 GHz Band”.

IEEE 802.11b. 1999.
ANSI/IEEE Standard 802.11b, 1999 Edition.

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band”.
IEEE 802.11g. 2003.
ANSI/IEEE Standard 802.11g, 2003 Edition.

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements”.
IEEE 802.11i. 2004.
ANSI/IEEE Standard 802.11i, 2004 Edition.

Mesografía

Apache
<http://www.apache.org/>
(Consulta: 14/08/2010).

Free Radius
<http://freeradius.org/>
(Consulta: 10/07/2010).

IEEE
<http://www.ieee.org>
(Consulta: 11/11/2009).

LAMP
<http://www.lamphowto.com/>
(Consulta: 20/08/2010).

Microsoft
<http://www.microsoft.com/spain/technet>
(Consulta: 03/07/2009).

Monografías
<http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml>
(Consulta: 21/09/2010).

MySQL
<http://www.mysql.com/>
(Consulta: 14/07/2010).

OpenBSD
<http://www.openbsd.org/>
(Consulta: 06/06/2009).

PHP

<http://www.php.net/>
(Consulta: 22/08/2010).

Seguridad Wi-fi: WEP, WPA y WPA2

http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
(Consulta: 04/06/2010).

Squid-Cache

<http://www.squid-cache.org/>
(Consulta: 15/07/2010).

Wi-fi

<http://www.wi-fi.org/>
(Consulta: 12/08/2009).

Wikipedia

<http://www.wikipedia.org/>

http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica#Caracter.C3.ADsticas
(Consulta: 16/06/2009).

http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
(Consulta: 17/06/2009).

http://es.wikipedia.org/wiki/IEEE_802.11#802.11_legacy
(Consulta: 16/06/2009).

http://es.wikipedia.org/wiki/IEEE_802.11#802.11a
(Consulta: 18/06/2009).

<http://www.laserwifi.com/estander802a.11.htm>
(Consulta: 22/06/2009).

http://es.wikipedia.org/wiki/IEEE_802.11#802.11b
(Consulta: 21/06/2009).

http://es.wikipedia.org/wiki/IEEE_802.11#802.11g
(Consulta: 01/07/2009).

http://es.wikipedia.org/wiki/IEEE_802.11#802.11n
(Consulta: 06/07/2009).

[http://es.wikipedia.org/wiki/Adaptador_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Adaptador_(inform%C3%A1tica))
(Consulta: 15/06/2009).

WiMAX Forum

<http://www.wimaxforum.org/>
(Consulta: 26/11/2009).