ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERIA

DESARROLLO DE UN SERVIDOR LINUX COMO ACCESS POINT PROXY

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO INFORMÁTICO CON MENCIÓN EN REDES DE INFORMACIÓN

SONIA ELIZABETH JIJON CANDO

ejijon@iess.gov.ec

DIRECTOR: ING. PABLO RECALDE

pablo.recalde@avon.com

Quito, Mayo 2008

DECLARACIÓN

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

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

Sonia Elizabeth Jijón Cando

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Sonia Elizabeth Jijón Cando, bajo mi supervisión.

Ing. Pablo Recalde

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Primero y antes que nada, quiero dar gracias a Dios, por estar conmigo en cada paso que doy.

Agradezco a la Escuela Politécnica Nacional que a través de sus profesores guiaron mi formación profesional.

Extiendo mi agradecimiento al Ingeniero Pablo Recalde, por su colaboración y dirección en el presente proyecto.

Elizabeth Jijón Cando

DEDICATORIA

A mis padres y hermanos por su amor, apoyo y entrega incondicional en todas las etapas de mi vida.

Elizabeth Jijón Cando

RESUMEN

El proyecto que se propone consiste en configurar un equipo con una tarjeta inalámbrica y Sistema Operativo Linux, como Punto de Acceso y servidor Proxy para un ambiente de redes mixto entre Wireless y Ethernet, brindándoles de servicios de DHCP y Proxy Internet a los clientes.

Para lograr el objetivo propuesto se llevará a cabo la instalación de una tarjeta inalámbrica en un equipo Linux, dicha tarjeta incluye el chip atheros el cual a través de *Madwifi* pude configurarla en modo de operación Master, opción que facilita y permite la configuración del equipo como Access Point.

Para la configuración del servidor Proxy se utilizara el software libre Squid, el cual permite configurar:

El puerto Squid, es el que se encarga de atender las peticiones.

La cantidad de memoria para almacenar las paginas Web más solicitadas, reduciendo de esta manera el tiempo de respuesta,

La lista de control de acceso en la que se define a que usuarios o direcciones se permite el servicio.

Las reglas de control permiten o restringen el acceso a Internet a las listas de control.

Una vez concluida con la instalación y configuración se procede a las pruebas respectivas de conexión y funcionamiento.

Finalmente se concluye que entornos de bajo presupuesto la implementación de este proyecto es ideal, pues dado su bajo costo de desarrollo y mantenimiento es la mejor alternativa a las soluciones hardware convencionales.

CAPITULO I: FUNDAMENTOS DE TECNOLOGÍAS WIRELESS

El propósito de este proyecto es configurar un computador básico con una tarjeta inalámbrica poco sofisticada y Sistema Operativo Linux, como Punto de Acceso y servidor Proxy para un ambiente de redes mixto entre Wireless y Ethernet, brindándoles de servicios de DHCP y Proxy Internet a los clientes.

Se estima concluir en un periodo no mayor a 6 meses, tomando en cuenta que algunos de los componentes de software y de hardware necesarios para la implementación no son comunes en el mercado, y requieren de un estudio y análisis profundo para obtener los resultados esperados.

Wifi es un estándar de redes, de transmisión de datos, que asegura que los equipos inalámbricos para su interoperabilidad no necesitan ser del mismo fabricante, reduciendo de esta manera los costos.

La instalación y configuración es poco compleja, lo que permite que los usuarios tengan inmediatamente acceso a los servicios que provee, por lo que puede ser utilizada como extensión de la red alámbrica, reduciendo los costos de instalación y mantenimiento.

FUNDAMENTOS DE LA TECNOLOGIA WIRELESS

1.1. AMBIENTE WIRELESS

Wireless, en español Inalámbrico, se aplica al tipo de comunicación el cual utiliza como medio de transmisión el aire. Es decir, no se propaga por un medio físico, sino que utiliza modulación[1] de ondas de radio. Comunicación sin Cables.

[1] Conjunto de técnicas utilizadas para transporta una señal a través de otra portadora, permitiendo un mejor aprovechamiento del canal durante la transmisión.

En general, en la tecnología inalámbrica se puede utilizar ondas de radiofrecuencia[2] de baja potencia y en una banda específica de uso libre para transmitir. Bajo estas condiciones se ha propiciado el crecimiento de equipos que se conectan a través de Redes Inalámbricas, siendo el objetivo el evitar conectarse a través de cables en la comunicación de todo tipo de dispositivos.

En un ambiente inalámbrico al no tener cables de por medio para la transmisión se tiene como ventajas:

- Movilidad de los dispositivos que emiten o reciben dichos datos, esto significa entrega de la información en tiempo real en cualquier lugar del área de transmisión de la Red.
- Facilidad de Instalación, sin tener ningún tipo de obra para el tendido de cables.
- Flexibilidad al permitir llegar donde el cable no llega, realizar cambios sin reestructurar o rehacer cableado.
- Reducción de costos para los Administradores de Red, se les facilita la gestión de los puntos de la red, aumentando la productividad con mayores posibilidades de servicio.
- Escalabilidad para los cambios de la Red.

Sin embargo, en la parte de seguridad hay que prever muchas cosas, ya que al tener un equipo no autorizado en el área de transmisión puede ser que este ingrese a Red. Adicionalmente, pueden existir otras redes u otros dispositivos que utilicen los mismos rangos de Radiofrecuencia e interfieran en el área de transmisión de la Red.

1.1.1. RED LAN

Una Red de Área Local (LAN) constituye una forma de Interconectar equipos ubicados cerca unos de otros compartiendo recursos localmente. No es más que

[2] Espectro de Radiofrecuencia, porción en el que se pueden generar ondas producidas al aplicar corriente alterna en una antena.

un medio compartido junto con una serie de reglas que rigen el acceso ha dicho medio.

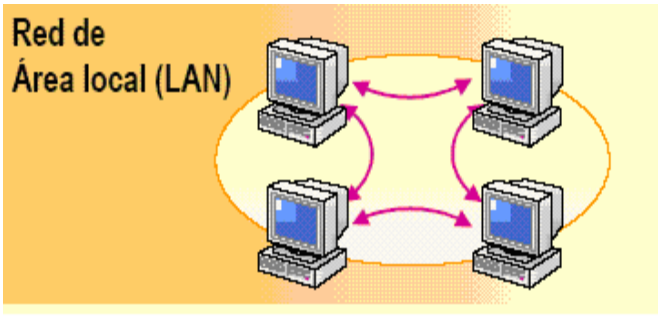

Figura 1: Red LAN

Fuente: http://www2.canalaudiovisual.com

Las redes de área local se componen de computadores, medios de Transmisión, dispositivos de control de tráfico de red y dispositivos periféricos. De esta manera se puede compartir de forma eficiente recursos como archivos e impresoras, y permitir la comunicación entre usuarios.

Las LAN están diseñadas para realizar lo siguiente:

- Operar dentro de un área geográfica limitada
- Permitir el acceso a recursos compartidos
- Proporcionar conectividad continua con los servicios locales
- Conectar dispositivos físicamente adyacentes

Una red LAN puede tener varias topologías[3], desde la más simple que es de un solo cable que es el medio compartido por todos los elementos de la red hasta topologías mixtas.

Entre los principales tipos de Topologías tenemos:

[3] Disposición física y/o lógica en la que se interconectan los nodos o dispositivos de una red.

- Topología de Bus, que es un medio compartido para todos los dispositivos y para el acceso se necesita que cada uno escuche si el medio está libre para la transmisión.
- Topología de Anillo, igualmente el medio se comparte, sin embargo aquí la información pasa por cada uno de los dispositivos hasta llegar al destino.
- Topología de Estrella, donde existe un dispositivo que centraliza el envió de información.
- Topología en estrella extendida, se desarrolla a partir de la topología en estrella, la cual enlaza estrellas individuales
- Topología jerárquica es similar a la Estrella Extendida, sin embargo, el sistema se enlaza con un computador que controla el tráfico de la topología.
- Topología en malla utiliza enlaces sobre todos los dispositivos, de esta manera no existe ningún tipo de interrupción en la comunicación.

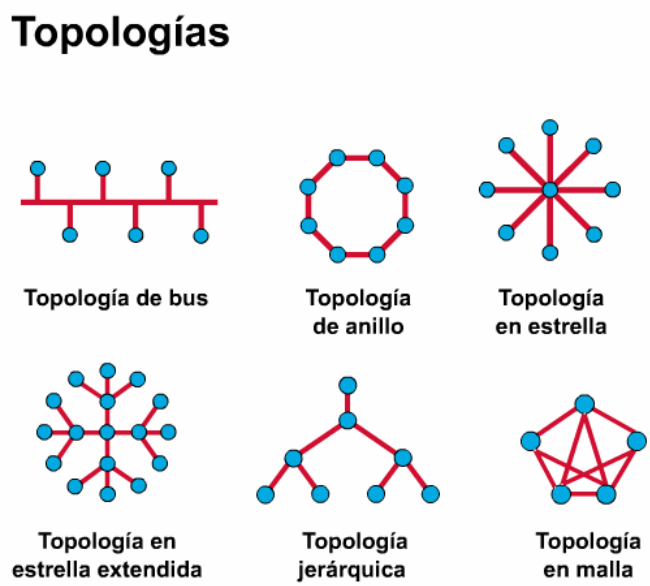

Figura 2: Topologías de Red

Fuente: Material Cisco Certificated Networking Associate

Como la topología define la estructura de una red, lo hace deacuerdo a la disposición de los cables (Topología Física) y a la manera como los dispositivos acceden a los medios (Topología Lógica).

Una Red LAN está compuesta de varios componentes:

- Host, que son aquellos componentes origen y destino de la información, es decir, los que emiten y reciben los datos.
- El Medio de Transmisión, por donde viajarán los datos enviados.
- Equipos de Interconexión, los cuales se encargarán de hacer llegar la información del origen al destino.

Como Host se puede tener todo aquel dispositivo que requiere u ofrece servicios sobre la red, como pueden ser las PC de usuario, Impresoras, Servidores, etc.

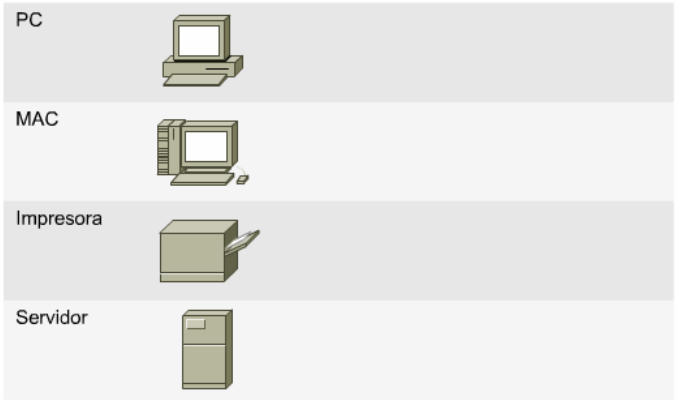

Figura 3: Tipos de Host

Fuente: Material Cisco Certificated Networking Asóciate

Para que los Host puedan comunicarse entre si es necesaria una interfaz de red llamada NIC(tarjeta de red), por sus siglas en ingles; que no es más que hardware y software para la comunicación entre dispositivos. Es decir, las tarjetas de red, pueden ser de varios tipos dependiendo de la tecnología de red a la cual se van a conectar.

Figura 4: NIC PCI[4] para PC

Fuente: http://www.system-net.net

Figura 5: NIC PCMCIA[5] para PC

Fuente: http://www.boker.cl

Figura 6: NIC PCI Inalámbrica para PC

Fuente: http://www.jaht.com

[4] Peripheral Component Interconnect, es un bus estándar para interconectar periféricos de 33 MHz, con una tasa de transferencia de 133 Mbps, ancho del bus de 32 o 64 bits

[5] Perdsonal Computer Memory Card International Associoation, es la versión de PCI pero para equipos portátiles, son de hasta 16 bits de ancho de bus

Los medios de transmisión son de diversos tipos y cada una de estas proporciona una característica especial a la red que conforman; así tenemos:

- Cable Coaxial, presenta mejor blindaje que el par trenzado, permitiendo mayor ancho de banda y alta inmunidad al ruido.

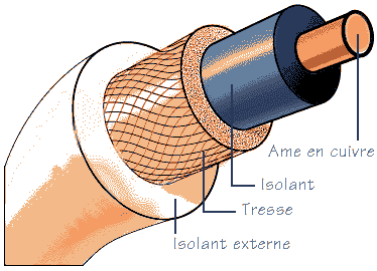

Figura 7: Coaxial
Fuente: http://www.alaide.com

- Par Trenzado, consta de ocho hilos de cobre aislados y enrollados entre ellos en forma helicoidal, para reducir la interferencia eléctrica. El ancho de banda depende del diámetro de los hilos y de la distancia. El más usado es el UTP (Unshielded Twiested Pair), cable no blindado, hay varias categorías o estándares (EIATIA 568A) de cables UTP y los más empleados son la categoría 6 y 5e. La diferencia entre estos es que la categoría 6 tiene más trenzas por longitud y aislantes de teflón lo que permiten reflejar menos interferencia.

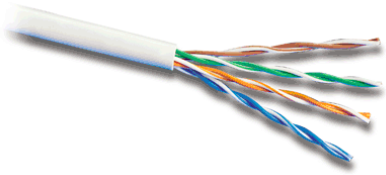

Figura 8: Par Trenzado
Fuente: http://www.comtec-comms.com

- Fibra Óptica, que tiene un gran ancho de banda, como una casi total inmunidad al ruido, y la interferencia y su atenuación[6] es casi nula. Hay dos tipos de fibra óptica: Monomodo donde un solo rayo de luz se propaga por la fibra, siendo esta más costosa y Multimodo donde múltiples rayos son trasmitidos al interior de la fibra.

Figura 9: Fibra Óptica
Fuente: http://www.intelprima.com

- Espectro Electromagnético, son las bandas de frecuencia[7] por las cuales se puede transmitir señales a través del aire, todo sistema inalámbrico usa una de estas bandas para transmitir los datos.

Existen muchos dispositivos usados para la Interconexión de Host y cada uno de ellos usa un método diferente con respecto al acceso al medio de transmisión, entre los más comunes se tiene:

- Repetidor, regenera las señales de red a nivel de bits para permitir que los bits viajen a mayor distancia a través de los medios. Los repetidores son dispositivos con dos puertos uno de entrada y uno de salida, dado que actúan sólo a nivel de bits y no tienen en cuenta ningún otro tipo de información.

[6] Perdida de potencia de una señal al ser transmitida cualquier medio de transmisión.
[7] Medida que indica el número de repeticiones de un fenómeno, relacionado con las repeticiones en una onda de señal electromagnética.

- Hub es similar al repetidor, es por ello que se denomina repetidor multipuesto, trabaja a nivel de bits para un gran número de hosts concentrando las señales. La diferencia es la cantidad de cables que se conectan al dispositivo. Las razones por las que se usan los hubs son crear un punto de conexión central para los medios y aumentar la confiabilidad de la red. La confiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. El hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) los mismos. En transmisiones Inalámbricas lo semejante a un hub es el Access Point que se lo revisará más adelante.

Figura 10: Hub
Fuente: Material Cisco Certificated Networking Associate

- Puente o Bridge, es un dispositivo diseñado para conectar dos segmentos de LAN su propósito es filtrar el tráfico, para que el tráfico local siga siendo local, pero permitiendo que el tráfico que se ha dirigido hacia allí pueda ser conectado con otras partes (segmentos) de la LAN.
- Switch, denominado puente multipuerto, al igual que el repetidor y el hub, la diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC[8] y los hubs no toman ninguna decisión, lo que hace que la LAN sea mucho más eficiente. El switch envía la

[8] Media Acces Control adress, identifica de manera única a una tarjeta o interfaz, esta compuesto por un hexadecimal de 48 bits.

información desde los puertos (las interfaces) de entrada hacia los puertos de salida, denominandose a este proceso conmutación.

Figura 11: Switch
Fuente: http://www.computerhope.com

- Router, toma decisiones basándose en grupos de direcciones de red, a diferencia de las direcciones MAC individuales, pueden también conectar distintas redes LAN. El propósito es examinar los datos (paquetes) entrantes, elegir cuál es la mejor ruta para llegar al destino y luego conmutarlos hacia el puerto de salida adecuado. El router puede tener tipos diversos de puertos de interfaz, que dependerán del tipo de red a la que se la quiere interconectar y de los medios de transmisión que están sujetas a estas redes.

Figura 12: Router y sus Interfaces
Fuente: Material Cisco Certificated Networking Associate

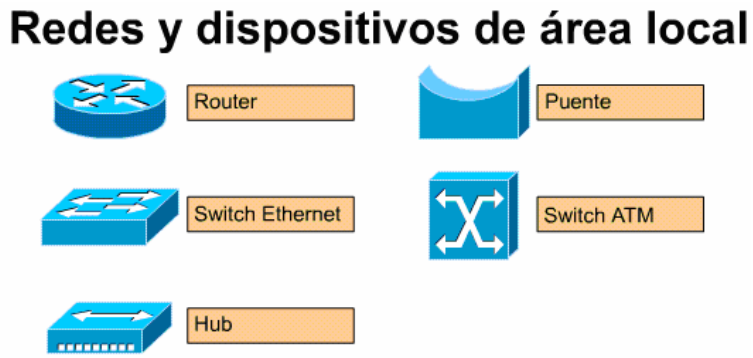

Figura 13: Redes y Dispositivos

Fuente: Material Cisco Certificated Networking Associate

Cada medio, dispositivo, y NIC, es una característica definitoria de una Red LAN, entre las principales se describe brevemente:

- Ethernet, que es la red LAN más usada hoy por hoy, existen varias clases de ellas y que han ido evolucionando y estandarizando con el paso del tiempo, desde 10BASET que eran basadas a 10 Mbps sobre par trenzado y sucesor del cable coaxial, luego pasando por 100BASET a 100 Mbps sobre par trenzado hasta las de alta velocidad 1000BASET sobre par trenzado y 1000BASEFX sobre fibra óptica. También se tiene los estándares de Ethernet Inalámbricas basadas en los estándares 802.11x. La topología lógica usada es la de bus y la física es de estrella extendida actualmente.
- Token Ring, red con topología lógica en anillo y física inicialmente en anillo y después en estrella. El acceso es a través de un toque de turno para la transmisión y su medio de transmisión es a través de par trenzado.
- FDDI, son un conjunto de anillos de fibra óptica redundantes, acceso con topología de bus y alcanzan mayores velocidades por el medio de transmisión. Muy usadas en instalaciones de Campus.

Figura 14: Redes LAN
Fuente: Material Cisco Certificated Networking Associate

1.1.2. WIFI

Wi-Fi Alliance (anteriormente la Wireless Ethernet Compatibility Alliance), es una organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x. De esta manera, WiFi es un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE 802.11x.

Existen varios estándares de IEEE 802.11x, pero los principales son IEEE 802.11b e IEEE 802.11g que utilizan la Banda del Espectro Radioeléctrico de 2.4 GHz que está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente. El estándar IEEE 802.11n trabaja en la misma banda a una velocidad de 108 Mbps, aunque 802.11g es capaz de llegar a esta velocidad con técnicas de aceleración que teóricamente pueden duplicar la transferencia. También existe el estándar IEEE 802.11a, conocido como WIFI 5, opera en la banda de 5 GHz.

Figura 15: Tarjeta Wi-Fi para PalmOne.
Fuente: http://www.arsys.es

Como se mencionó anteriormente, las redes inalámbricas como WiFi enfrentan grandes retos como es en el área de la seguridad. Si el sistema es abierto se corre el riesgo de intrusión a la red instalada, sin embargo, existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de seguridad como el WEP (Wire Equivalent Privacy) y el WPA (WiFi Protected Access) que se encargan de autenticación, integridad y confidencialidad de los datos transmitidos o IPSEC (túneles IP).

La Red WiFi al ser una LAN Inalámbrica tiene las mismas características generales de las alámbricas y en ellas usamos:

- Acceso Point, que es el punto de acceso central de la red, es decir, como el hub en una LAN cableada. Por tanto estará compuesto por una antena para transmitir y recibir las señales de los host, trabajando y asignando una cierta frecuencia las cuales se les llama canales para evitar interferencia entre las señales.
- Los hosts deberán tener una NIC WiFi, si no viene incorporado existen varios tipos que se las puede colocar (PCI, PCMCIA, etc.).
- El Medio de Transmisión que sería el aire, a través de cada una de las frecuencias estándares para estas Redes.

EL alcance de la señal (área de cobertura) dependerá de lo siguiente:

- Potencia del Access Point
- Potencia de la NIC conectada al host
- Obstáculos en el medio que la señal deba atravesar (muros, metales) siendo recomendable que el Access Point se encuentre en el lugar más alto y céntrico del área de cobertura.
- Interferencias de otras señales extrañas al sistema instalado, como la frecuencia libre usada es la de 2.4GHz es común que ciertas microondas, teléfonos inalámbricos y otros dispositivos que trabajan en esta misma frecuencia generen interferencia sobre la señal transmitida deseada.

1.1.3. ANCHO DE BANDA

El ancho de banda es en señales, la anchura del rango de frecuencias donde se concentra la mayor potencia de la señal, se mide en Herzios. Una señal esta compuesta por varios componentes de frecuencia, entonces si una señal tiene un mayor número de componentes en varias frecuencias su ancho de banda también es mayor (Ver Figura 16).

En muchos de los casos, a nivel de señales digitales, se le llama Ancho de Banda a la Velocidad de Transmisión de la señal, esta medida en bits por segundo. No es más que la cantidad de datos transmitidos en una unidad de tiempo. Esta tasa de transferencia dependerá de factores como el Ancho de Banda (Herzios), Potencia de la Señal, Ruido en el sistema, etc.

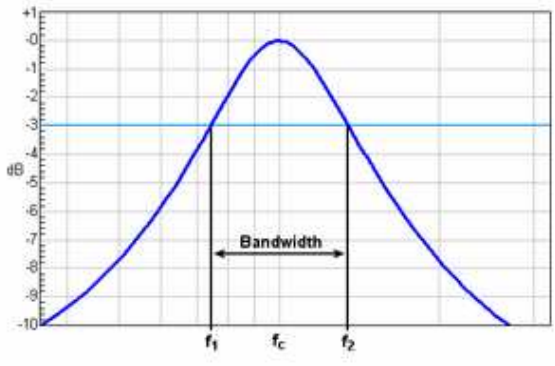

Figura 16: Ancho de Banda.
Fuente: http://es.wikipedia.org

1.1.4. PUNTOS DE ACCESO

Un Access Point (Punto de Acceso) es un dispositivo que concentra la señal de todos los dispositivos en una Red Inalámbrica, también ejerce funciones de puente entre una red con cable y una red Inalámbrica.

Un Access Point acepta la concentración de los datos de un número relativamente pequeño de Host a través de sus canales asignados en la frecuencia a la que funciona. Para que exista la correcta cobertura de la señal la antena debe estar en un punto específico seguro y lo recomendable es que sea lo más alto posible, de esta manera su radio podría llegar desde 30 metros hasta varios cientos.

El Host accede al Access Point a través de una NIC inalámbrica que proporcionan la interfaz entre el sistema y la red.

Figura 17: Access Point
Fuente: http://es.wikipedia.org

De este modo se evita el tendido de cables, proporcionando movilidad al sistema. A un Access Point se lo puede usar como puente entre dos redes cableadas de tal manera si la distancia es grande se las interconecte de esta manera, también se pueden interconectar varios y generar varias áreas de coberturas como celdas para el acceso de los host inalámbricos.

1.2. TECNOLOGIAS WIRELESS

1.2.1. 802.11b

802.11x es un conjunto de estándares de la IEEE[9] que definen las normas de funcionamiento de Redes Inalámbricas Locales (Wireless LAN). Estas normas utilizan seis tipos de modulación con los mismos protocolos de transmisión, trabajando a una frecuencia de 2.4 GHz o 5 GHz.

En 1999 la IEEE publicó la modificación al estándar, llamándola 802.11b, también conocida comercialmente como WiFi, la cual mejora la velocidad de transmisión de 1Mbps a 11Mbps que es la máxima velocidad a la cual puede llegar, sobre la misma frecuencia.

El método de acceso a la red es escuchando si en el medio no se está transmitiendo información para hacerlo, es decir el medio es compartido por todos los host de la red. Por el hecho de que en la banda de los 2.4 GHz, existen varios dispositivos que pueden causar interferencia, incluso redes similares alrededor del

[9] Institute of Electrical and Electronics Engineers, organizaci´on dedicada a la estandarización de tecnologías en las áreas de electrónica y telecomunicaciones.

sistema, la velocidad efectiva (througput) se reduce notablemente por la repetición de la información que ha llegado errónea. Por este motivo los dispositivos de la red reducen la velocidad de la transmisión siendo la velocidad alcanzada de hasta 6 Mbps la más común en este estándar.

1.2.2. 802.11a

Similar a 802.11b, en 1999 la IEEE publicó este estándar, pero este se demoró mas tiempo en salir al mercado y fue su aparición en el 2001. Es llamada también WiFi 5, por la banda de frecuencia en la cual trabaja.

802.11a opera en la banda de los 5GHz, lo que es una ventaja al no existir las interferencias que implican las redes a 2.4 GHz, pudiendo llegar a velocidades de hasta 54Mbps. Utiliza OFDM (Multiplexación por División de Frecuencias Ortogonales[10])

1.2.3. 802.11g

802.11g fue publicada en el 2003, con una nueva técnica de modulación. Trabaja en la banda de los 2.4 GHz al igual que 802.11b, pero alcanza velocidades de hasta 54 Mbps, similar a 802.11a.

Dispositivos que trabajan con el estándar 802.11b y 802.11g son compatibles entre si, sin embargo, trabajar con ambos estándares sobre un mismo sistema reduce la velocidad de transmisión hacia el 802.11b.

Además de estos estándares de 802.11x, existen otros que tiene que ver con la seguridad, calidad de servicio, etc. En la siguiente tabla 1, se especifican alguna de ellas. Además en la tabla 2 y 3 se especifican protocolos de seguridad y las características principales de estos estándares respectivamente.

[10] Técnica de Modulación Digital, para mejorar la calidad de la señal transmitida.

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

Tabla 1: Estándares 802.11x
Fuente: http://www.enterate.unam.mx

Mecanismo de seguridad	Descripción
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: - SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para accesar a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon). - Filtrado con dirección MAC (Control de Acceso al Medio): restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema

	de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. - WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación.
802.1X	Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y requiere de un protocolo de autenticación para reconocimiento mutuo.
WPA (Wi-Fi Protected Access)	Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras –Seguras– Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación. Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi.

Tabla 2: Seguridad en 802.11x
Fuente: http://www.enterate.unam.mx

Estándar	Velocidad máxima	Interface de aire	Ancho de banda de canal	Frecuencia	Disponibilidad
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz	Actual
802.11a	54 Mbps	OFDM	25 MHz	5.0 GHz	Actual
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2.4 GHz	Actual

Tabla 3: Características Principales de 802.11x
Fuente: http://www.eveliux.com

1.3. SISTEMAS OPERATIVOS CON SOPORTE WIRELESS

1.3.1. WINDOWS 2000

Es un Sistema Operativo de Microsoft que se lo puso al mercado en el año 2000, basado en su sistema anterior Windows NT.

Con este Sistema Operativo se introducen varias mejoras, como el sistema de archivos de FAT32 a NTFS, capacidades de codificar y comprimir archivos, mayor estabilidad del sistema, seguridad, etc.

Los requerimientos mínimos de Windows 2000 en Hardware son:

- Procesador Pentium de 166 MHz
- 64 MB de memoria en RAM
- 1 GB de disco duro Libres

Existen varias versiones del Windows 2000 y hasta 4 Service Pack (Mejoras al Sistema Operativo). Las versiones son:

- Professional, que está diseñado para el uso del usuario.
- Server, diseñado para los servidores principales.
- Advanced Server, un sistema de Server más robusto para aplicaciones de alto tráfico de acceso, seguridad y disponibilidad.
- Datacenter Server, es un sistema de servidor para almacenamientos grandes de datos.

Tomado en cuenta la aparición de las redes Lan Inalámbricas para antes del 2000, Windows 2000, ya trae características y drivers para la conexión de NICs de soporte para estas tecnologías. A Continuación se describe un ejemplo de configuración de una NIC inalámbrica (Figura 18).

Lo primero que se debe hacer es la instalación del Hardware, es decir, la instalación de la tarjeta inalámbrica. Se enciende el PC y al estar inicializado el sistema operativo reconocerá un hardware nuevo. Se debe instalar los drivers respectivos y será reconocido por el Windows 2000 y aparecerá un icono en las propiedades de la red (Figura 18).

Figura 18: Pantalla de Conexiones de Red Windows 2000

Fuente: https://www.riu.unam.mx

Ya ubicado el icono de red, se ingresa a las propiedades dando clic derecho (Figura19).

Figura 19: Pantalla de Configuración de Tarjeta de Red Windows 2000
Fuente: https://www.riu.unam.mx

Se selecciona Protocolo Internet (TCP/IP) y propiedades para configurar los parámetros necesarios para el acceso IP de la red. Este es un procedimiento general para la configuración de redes LAN basadas en TCP/IP (Figura 20)

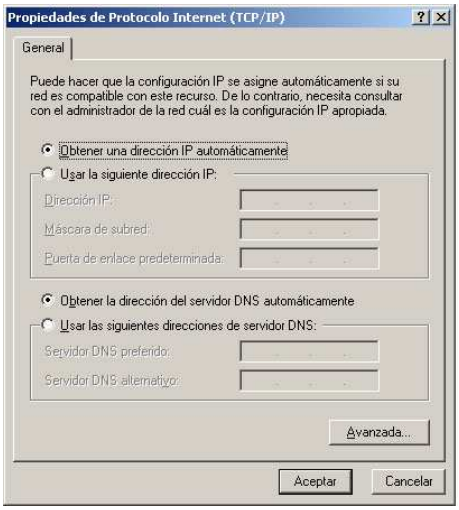

Figura 20: Pantalla de Propiedades TCP/IP Tarjeta de Red Windows 2000
Fuente: https://www.riu.unam.mx

En las propiedades de la tarjeta de Red se deberá configurar el nombre de identificación de la red (ESSID) (Figura 21).

Figura 21: Pantalla de Configuración de ESSID

Fuente: https://www.riu.unam.mx

Debe estar instalado el Service Pack 4, para que esto funcione correctamente y tenga el soporte completo a redes inalámbricas el Windows 2000.

Dependiendo de los drivers de la NIC inalámbrica, se podrá configurar otros parámetros o se obtendrá interfaces más completas en pantalla. Se configurará el nombre de la red, si existe autentificación, encriptación, etc.

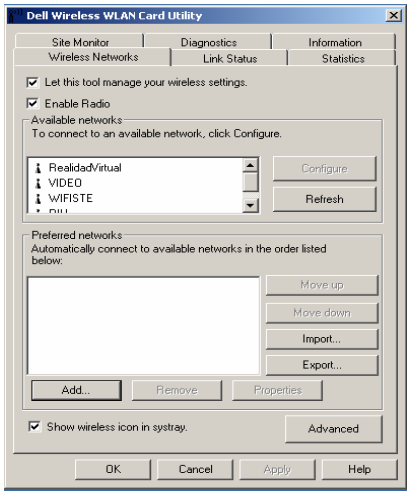

Figura 22: Drivers que reconocen ESSID

Fuente: https://www.riu.unam.mx

La figura siguiente muestra opciones de seguridad, con algunos de los protocolos más usados:

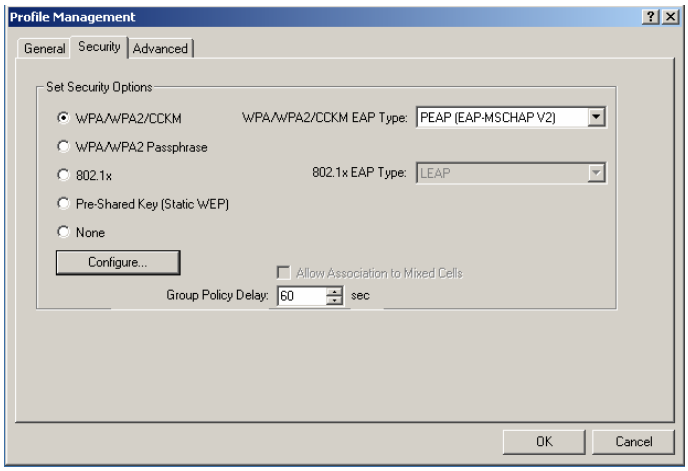

Figura 23: Driver con Seguridad

Fuente: https://www.riu.unam.mx

1.3.2. WINDOWS XP

Sistema Operativo lanzado al mercado en el 2001 por Microsoft. Las siglas de XP vienen de la palabra e**xp**erience. Es Sucesor de Windows 2000 y Millenium para ambientes de Hogar y Corporativo. Existen versiones en 32 bits y 64 bits.

Como mejoras a los Sistemas Operativos Windows anteriores se tiene:

- Inicio e hibernación.
- Desconexión de dispositivos externos sin el reinicio del Sistema Operativo.
- Interfaz de usuario mejorada.
- Herramientas de desarrollo de escritorio.
- Uso de multicuentas de usuarios.
- Escritorio Remoto.
- Interfaz Gráfica.

Con estás características se avanzó en la estabilidad, en la interfaz gráfica para un uso más simple y en la gestión del software.

En esta versión se introdujo la activación del software, permitiendo de esta manera evitar o controlar un poco más la piratería. Actualmente existe hasta el Service Pack 2, como mejoras al código del Sistema Operativo.

Existen varias versiones del Windows XP y son:

- Windows XP Home, que está orientado al usuario del hogar.
- Windows XP Professional, orientado al sector corporativo, este a diferencia de Home tiene características adicionales a nivel de red, como es el de unirse a un dominio de red (control de las computadores por servidores centrales en la red), el Control de Permisos a recursos compartidos, el Escritorio Remoto que implica conectarse remotamente y controlar la PC, etc.
- Windows Media Center, que tiene capacidades para convertirse en centro de medios multimedia, como por ejemplo la capacidad de adecuar un control remoto para la centralización de tareas como ver y grabar televisión.
- Windows XP Tablet PC Edition, que trabajan sobre portátiles con pantallas táctiles.
- Windows XP 64 Bits Edition, diseñada para soportar procesadores de tecnologías de 64 bits.
- Windows XP Starter Edition, que está diseñado para la experiencia inicial de un usuario con un Sistema Operativo Windows XP, se lo lanzó al Mercado de países de bajos recursos. Es muy limitado.
- Windows XP Embedded, diseñado para aparatos electrónicos diferentes a una PC.

Windows XP, viene con soporte a la mayoría de dispositivos inalámbricos, igual que Windows 2000.

Cuando la tarjeta WIFI ha sido instalada correctamente aparecerá un icono en las propiedades de sitios de red (Figura 24).

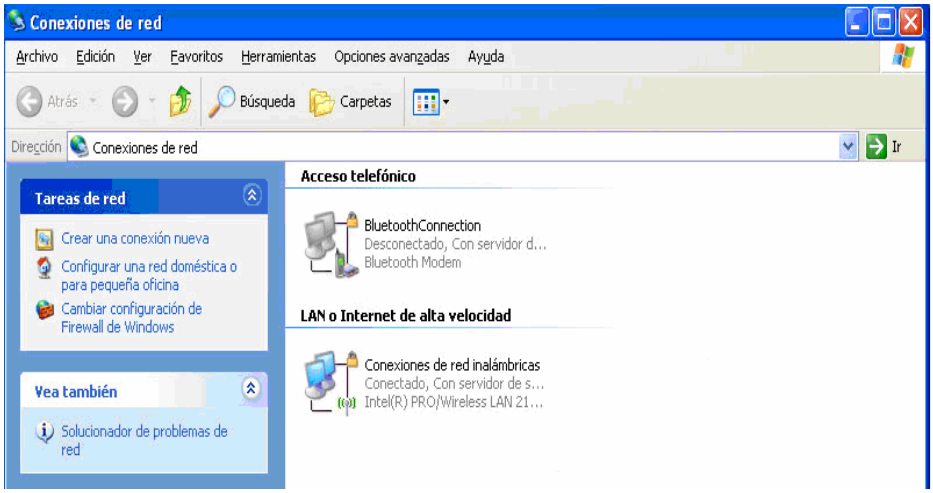

Figura 24: Pantalla de Conexiones de Red Windows XP

Fuente: https://www.riu.unam.mx

Ingresar a Propiedades de la conexión inalámbrica para configurar todos los parámetros TCP/IP (Figura 25 y Figura 26).

Figura 25: Pantalla de Configuración tarjeta de red Windows XP

Fuente: https://www.riu.unam.mx

Al igual que en las redes fisicas el TCP/IP puede configurarse de manera automática o manual (Figura 26).

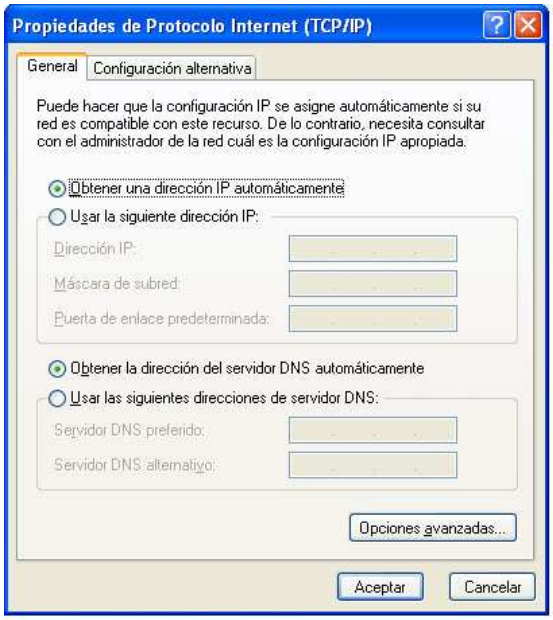

Figura 26: Pantalla de Propiedades TCP/IP Tarjeta de Red Windows XP

Fuente: https://www.riu.unam.mx

En la opción de “Redes Inalámbricas” (Figura 25), se podrá visualizar todas las redes que son detectadas por la tarjeta NIC y tienen proximidad con el dispositivo. Lo recomendable es que Windows automáticamente establezca la red a conectarse y lo hará tomando como criterio la más próxima, es decir con la mayor potencia. Se lo puede hacer manual también.

Figura 27: Opciones de Redes Inalámbricas Windows XP

Fuente: https://www.riu.unam.mx

Si en la opción Conexiones de red de Mis sitios de red, no se visualizan las redes o equipos inalámbricos cercanos, dar clic en “Ver redes inalámbricas” (Figura 27) para que descubra redes a su alrededor. Así se puede conectar a la deseada.

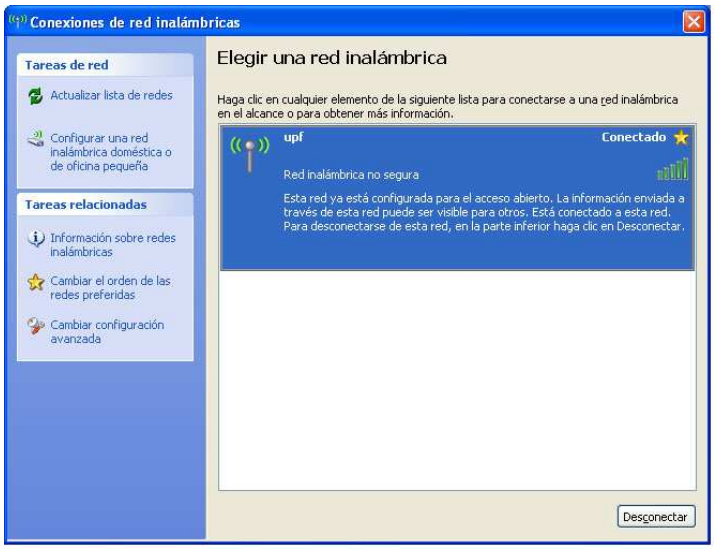

Figura 28: Pantalla de Redes Inalámbricas Cercanas Windows XP

Fuente: https://www.riu.unam.mx

1.3.3. WINDOWS MOVIL

Es un Sistema Operativo basado en API Win32[11], es compacto con aplicaciones básicas para trabajar con dispositivos móviles de pantalla pequeña y pocos recursos de procesamiento y memoria.

En algunas versiones incluye aplicaciones de Microsoft Office para dispositivos móviles, es decir, también tienen una serie de restricciones con respecto a sus versiones de Escritorio.

Existen varias versiones de Windows Mobile, se detalla las más importantes:
Windows Mobile 2003 viene en tres ediciones: Windows Mobile 2003 Pocket PC Edition, para Pocket PC[12], Windows Mobile 2003 Pocket Phone Edition, para Pocket PC con características de teléfonos móviles (celulares), Windows Mobile 2003 Pocket Smartphone Edition, para dispositivos que usan un teclado especial.

Windows Mobile 2003 Second Edition, conocida como Windows Mobile 2003SE, con opciones para cambiar la pantalla, Internet Explorer adecuado para el tipo de dispositivo, soporte VGA, soporte WiFi.
Windows Mobile 2005, con otra versión del Office, reproductor de media (Windows Media 10), soporte mejorado Bluetooth[13], Interfaz GPS[14], mejor sincronización de los datos, entre otras.

1.3.4. LINUX

[11] Interfaz de Application Programming Interface, componentes de software que ofrecen acceso a servicios del sistema Win32, funciones que estan en ciertas bibliotecas y trabajan bajo Windows.
[12] Pequeño ordenador de bolsillo mas conocido como PDA(Personal Digital Asistent).
[13] Estándar para la comunicación inalámbrica con una velocidad de transmisión máxima de de 720 Kbps en la banda de los 2.4 GHz.
[14] Global Positioning System, tecnología satelital que permite ubicar en cualquier parte del mundo a una persona u objeto.

Se denomina Linux al Sistema Operativo y al Núcleo[15] de código abierto, donde cualquier persona con el conocimiento adecuado podrá estudiarlo, usarlo y modificarlo.

El Sistema Operativo Linux está formado por el Núcleo Linux, bibliotecas y herramientas del proyecto GNU[16], de otros proyectos y grupos de software.

Linus Trovals fue quien creo el núcleo de Linux, tomando como base el proyecto GNU que había ya creado varios componentes de un Sistema Operativo que a su vez basándose en un sistema Unix[17] compuesto de software de libre desarrollo.

En la programación de Linux se puede compilar lenguajes como C, C++, Java, Ada, entre otros. Tiene todas las prestaciones de un Unix desarrollado, multitarea, memoria virtual, bibliotecas compartidas, carga a demanda, compartimiento de recursos y soporte de redes.

Existen varias versiones de Linux, pero en general todos tienen las siguientes características:

- Dispone de varios tipos de Sistemas de Archivos
- Entorno gráfico X-window[18], Motif[19] (Figura 29)

[15] Mas conocido como Kernel, es la parte fundamental de un Sistema Operativo, encargado de gestionar los recursos a través de servicios de llamadas
[16] Anunciado en septiembre de 1983, proyecto creado con el objetivo de obtener un sistema operativo totalmente libre.
[17] Sistema Multitarea y Multiusuario desarrollado por Bell y AT&T.
[18] Protocolo de Interacción gráfica en red entre un usuario y varios equipos. Es el encargado de mostrar la información gráfica independiente del sistema operativo
[19] Librería para la creación de entornos gráficos bajo X Windows, es un estándar IEEE 1295.

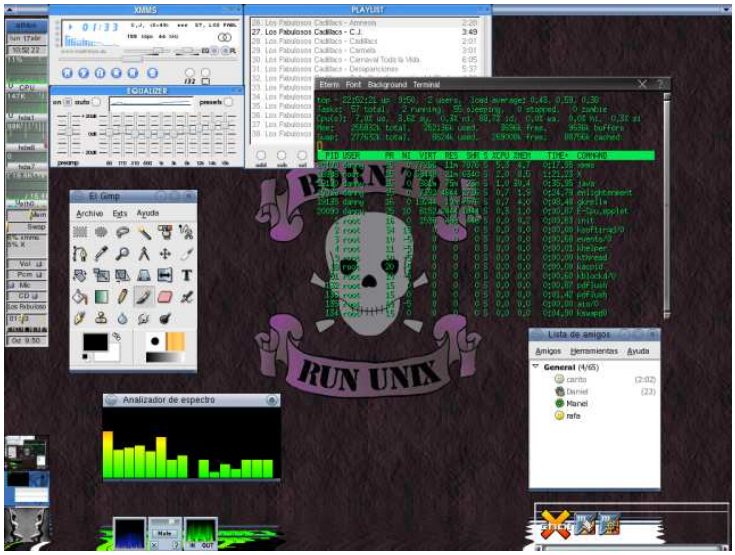

Figura 29: Sistema X Windows

Fuente: http://es.wikipedia.org

- Soporte en Redes WIFI
- Código Fuente de libre distribución y desarrollo
- Multitarea
- Multiusuario
- Con prestaciones de Seguridad
- Control de Dispositivos

Red Hat Linux es una de las versiones más populares de Linux, creada por Red Hat que es una de las empresas responsables de la creación y distribución de Linux.

Las características que diferencian a Red Hat de las otras versiones son:

- Interfaz gráfica llamada Anaconda, que está diseñado para usuarios sin experiencia, desde la versión 8 de Red Hat.
- Herramienta Lokkit para la configuración de capacidades.
- Entorno de Escritorio Gráfico.
- Ciertos Soportes para multimedia no viene integrados, al que soporte para archivos NTFS, pero se puede pagar los permisos e instalarlo.

WIFI sobre Red Hat

Las versiones de Red Hat empiezan con la versión 1.0, hasta la versión 9.0.

Año	Número	Nombre	Soporta Wireless
1994	1.1		No
1995	1.2		No
1995	2.1		No
1995	2.2		No
1996	3.0.3	Picasso	No
1996	4.0	Colgate	No
1997	4.1	Vanderbilt	No
1997	4.2	Biltmore	No
1997	5.0	Hurricane	No
1998	5.1	Maniatan	No
1998	5.2	Apollo	No
1999	6.0	Hedwig	No
1999	6.1	Cartean	No
2000	6.2	Zoot	No
2000	7	Guinness	Si
2001	7.1	Seawolf	Si
2001	7.2	Enigma	Si
2001	7.3	Valhalla	Si
2002	8.0	Psyche	Si
2003	9	Shrike	Si

Tabla 4: Versiones de Red Hat

Fuente: http://es.wikipedia.org

Red Hat Linux se fusionó con el Proyecto Fedora Linux orientado a la comunidad de usuarios. El nuevo plan es extraer el código base de Fedora para crear nuevas distribuciones de Red Hat Enterprise Linux.

Año	Número	Nombre	Soporta Wireless
2003	Fedora Core 1	Yarrow	Si
2004	Fedora Core 1 para x86-64	Yarrow	Si
2004	Fedora Core 2	Tettnang	Si
2004	Fedora Core 3	Heidelberg	Si
2005	Fedora Core 4	Stentz	Si
2006	Fedora Core 5	Bordeaux	Si
2006	Fedora Core 6	Zod	Si

Tabla 5: Versiones de Fedora

Fuente: http://es.wikipedia.org

Año	Número	Nombre	Soporte Wireless
2002	RedHat Enterprise Linux 1		SI
2002	RedHat Enterprise Linux 2.1	Pensacola	SI
2003	RedHat Enterprise Linux 3	Taroon	SI
2005	RedHat Enterprise Linux 4		SI

Tabla 6: Versiones de Linux Enterprise

Fuente: http://es.wikipedia.org

Para configurar una conexión de Host inalámbrico sobre un sistema Red Hat se procede de la siguiente manera:

Se coloca la NIC inalámbrica, la misma debe contener drivers para la versión Red Hat instalada, para que el sistema operativo reconozca la tarjeta.

Las Interfases de red se configuran en el fichero:

/etc/sysconfig/network-scripts/ifcfg-ethX

o

/etc/sysconfig/network-scripts/ifcfg-wlan0

Requiere los siguientes parámetros:

DEVICE=eth1

MODE=managed

ESSID="Nombre_de_red"
RATE=auto
TXPOWER=auto
KEY="s:mi_clave" # Solo si va encriptado
BOOTPROTO=static
IPADDR=”dirección IP”
BROADCAST=”dirección de Broadcast”
NETMASK=”mascara de subred”
NETWORK=”identificados de subred IP”
ONBOOT=yes

El comando **iwconfig** se utiliza para configurar los parámetros especiales de redes inalámbricas, como nombre de la red, frecuencia, modo, velocidad, encriptación.

Mandrake Linux llamado en la actualidad Mandrivia Linux, es otra versión para usuarios medios, las características principales son:

- Disponible en más de 74 idiomas.
- Fácil Instalación
- Entorno Gráfico llamado KDE
- Mandrake Control Center, para la administración del Linux y configuración de Linux.

Mandrake version 5.1 hasta la version 10.2 son las primeras versiones, usualmente tenian una duracion de 2 meses, realizados las correciones devidas aparecen Mandrivia Linux 2006 y 2007.

Año	Número	Nombre	Soporte Wireless
1998	5.1	Venice	NO
1998	5.2	Leeloo	NO
1999	5.3	Festen	NO
1999	6.0	Venus	NO
1999	6.1	Helios	NO
2000	7.0	Air	NO
2000	7.1	Helium	NO
2000	7.2	Odyssey (llamada Ulysses durante la beta)	NO
2001	8.0	Traktopel	SI
2001	8.1	Vitamin	SI
2002	8.2	Bluebird	SI
2002	9.0	Dolphin	SI
2003	9.1	Bamboo	SI
2003	9.2	FiveStar	SI
2004	10.0	Community y Oficial	SI
2004	10.1	Community	SI
2004	10.1	Oficial	SI
2005	10.2	Limited Edition 2005	SI
2005	2006.0	Mandrivia Linux 2006	SI
2006	2007.0	Mandrivia Linux 2007	SI

Tabla 7: Versiones de Mandrivia

Fuente: es.wikipedia.org/wiki/Mandriva_Linux

CentOS (Community Enterprise Operating System) es igual a nivel binario que Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

Los desarrolladores de CentOS usan el código fuente de Red Hat Enterprice para crear un producto final que es muy similar y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni soportado por Red Hat. Tomando en cuenta que Red Hat Enterprice aunque utiliza un código abierto si se debe comprar una licencia para su uso.

CentOS usa yum para bajar e instalar las actualizaciones, que es una herramienta también utilizada por Fedora Core.

Los requerimientos básicos en hardware para instalar CentOS son:

- Memoria RAM: 64 MB (mínimo).
- Espacio en Disco Duro: 512 MB (mínimo) - 2 GB (recomendado).
- Procesadores x86 o compatible, Itanium (Procesador de 64 bits de Intel), Athlon 64 (Procesador de 64 bits de AMD), PowerPC/32 (Procesador 32 bits de Macintosh) y otros.

El 14 de mayo de 2004 CentOS 2 fue liberado. Esta versión está basada en la versión 2.1 de Red Hat Enterprise Linux. A continuación una tabla de las versiones de CentOS:

Año	Número	Descripcion	Soporte Wireless
2004	2.0	Basada en Red Hat Enterprise 2.1	SI
2004	3.1	quarterly update 1	SI
	3.2	quarterly update 2,nunca fue liberado	SI
2004	3.3	quarterly update 3, liberado para arquitecturas i386, AMD64	SI
2005	3.4	quarterly update 4, para arquitecturas i386, ia64, s390, s390x	SI
2005	3.5	Para arquitecturas i386	SI
2005	3.6		SI
2006	3.7		SI
2006	3.8		SI
2005	4.0	Basado en Red Hat Enterprice 4.0, arquitecturas i386, ia64, x86_64	SI
2005	4.1	Para arquitectura ia64, x86_64	SI
2005	4.2		SI
2006	4.3	Para arquitecturas i386, x86_64, ia64	SI
2006	4.4		SI

Tabla 8: Versiones de CentOS

CentOS al estar basado en Red Hat Enterprise, tiene los mismos ficheros y parámetros de conficuracion para soporte sobre Wireless.

Como se puede ver, todos los Sistemas Operativos actuales manejan soporte para redes inalámbricas. El uso de un Sistema Operativo u otro dependerá de muchos factores. Como son los desarrollados por Microsoft los más difundidos y de mayor uso, es probable que sea la primera opción, sin embargo, la flexibilidad de desarrollo y el costo de Linux es una opción muy factible ya que se ha demostrado en este capítulo la facilidad de configuración en diferentes versiones de ambientes Linux para el soporte a dispositivos inalámbricos.

CAPITULO II: CARACTERÍSTICAS FÍSICAS Y LÓGICAS DE DISPOSITIVOS WÍRELESS

2.1. CARACTERÍSTICAS FÍSICAS DE UN ACCESS POINT

Como ya se vio en el Capítulo anterior el Access Point o Punto de acceso es la unidad de conexión central entre la red cableada y los dispositivos de WLAN. Un Access Point recibe y emite datos, tanto a través de cables Ethernet, como también de forma inalámbrica a través de 802.11x. Otras funciones son, por ejemplo, el control de las herramientas de seguridad de la red.

2.1.1. FRECUENCIAS

Cuando los electrones se mueven crean ondas electro magnéticas que se pueden propagar por el espacio libre. El físico británico James Clek Maxwell predijo estas ondas en 1865 y el físico alemán Heinrich Hertz las produjo y observo por primera vez en 1887.

La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia (f*)*, y se mide en Hz. La citación entre dos máximos consecutivos se llama longitud de onda y se designa de forma universal con la letra griega λ (lambda)[20].

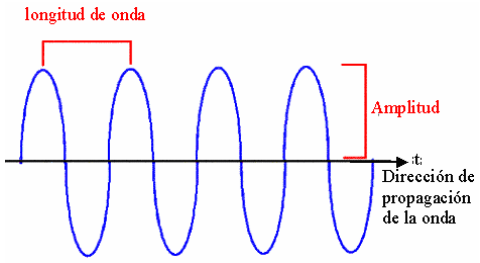

Figura 30: Frecuencia y Longitud de Onda

Fuente: http://www.monografias.com

[20] Fuente: Redes de Computadoras, ANDREW TANENBAUM Tercera Edición

La corriente alterna pertenece a la frecuencia que generan los alternadores o generadores de las centrales eléctricas, hidroeléctricas que otorgan corriente para uso industrial, general y doméstico. La frecuencia de esta corriente es 60 Hz.

En las comunicaciones inalámbricas se usan varias frecuencias para la transmisión por el espacio libre y estas están definidas en el Espectro Electromagnético. Las Bandas de Frecuencia del Espectro Electromagnético se detallan a continuación:

- ELF (Frecuencias extremadamente bajas): 30 a 300 Hz
- VF (Frecuencias de voz): 300 a 3000 KHz
- VLF (Frecuencias muy bajas): 3 a 30 KHz
- LF (Frecuencias bajas): 30 a 300 KHz
- MF (Frecuencias medias): 300 a 3000 KHz
- HF (Frecuencias altas): 3 a 30 MHz
- VHF (Frecuencias muy altas): 30 a 300 MHz
- UHF (Frecuencias ultra altas): 300 MHz a 3000 MHz
- SHF (Frecuencia súper altas): 3 a 30 GHz
- EHF (Frecuencias extremadamente altas): 30 a 300 GHz
- Luz infraroja: 0.3 a 300 THz
- Luz ultravioleta: 0.3 a 3 PHz
- Rayos X: 30 a 300 PHz
- Rayos gamma: 0.3 a 3 Ehz
- Rayos cósmicos: 3 a 30 Ehz

Desde las frecuencias de 20 Hz son audibles para el oído humano (agudos), son los sonidos detectados por el humano. En estas frecuencias se encuentra la transmisión de la telefonía fija[21].

Las ondas de radio son fáciles de generar, pueden viajar grandes distancias y penetrar edificios. En las bandas VLF, LF y MF, las ondas de radio siguen la

[21] Telefonía Convencional. Sistema de comunicación diseñado para la transmisión de voz por medio de señales eléctricas

superficie de la tierra, siendo su problema principal en comunicaciones de datos por su pequeño ancho de banda (Figura 16).

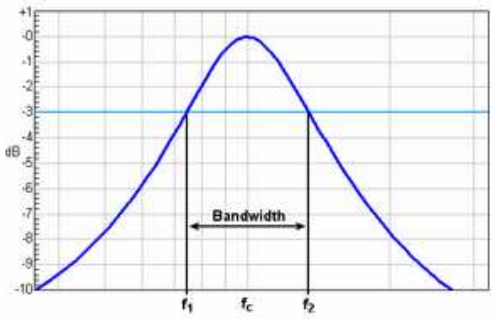

Figura 16: Ancho de Banda.
Fuente: http://es.wikipedia.org

En HF y VHF las ondas terrestres tienden a ser absorbidas por la tierra. Sin embargo las ondas que llegan a la ionosfera y la troposfera (100 a 500 Km. de la altura de la Tierra) son refractadas y devueltas a la Tierra. Por múltiples reflexiones pueden alcanzar grandes distancias (Figura 30).

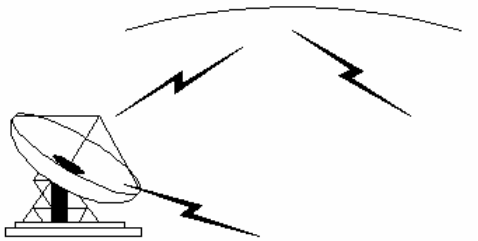

Figura 31: Absorción y Reflexión de las Ondas HF y VHF

Encima de los 100 MHz se llaman Microondas, el haz es bastante directivo, lo cual da una mayor relación señal a ruido* El hecho de viajar en línea recta (línea de vista) limita su alcance, existiendo la necesidad de usar repetidoras, esto es por los obstáculos que puedan existir entre los puntos de transmisión. Es decir, las microondas no atraviesan edificios y pueden originarse varios trayectos, llegando estas desfasadas, originándose el fenómeno conocido como

* Margen que hay entre la información y el ruido en el sistema. Fuente: http://es.wikipedia.org

desvanecimiento por múltiples trayectorias. Por encima de los 8 GHz se presenta el problema de absorción de las ondas por lluvia. La Banda de los 2.4 GHz está dentro de la transmisión por Microondas.

Los rayos infrarrojos abarcan aproximadamente desde los 3,0 x 10^{11} Hz (300 GHz) hasta los 3,8 x 10^{14}Hz (380 THz). Cualquier molécula cuya temperatura sea superior a 0º Kelvin (cero absoluto, equivalente a – 273º C), emite rayos infrarrojos. Los rayos infrarrojos de baja potencia se utilizan para accionar diferentes dispositivos de control remoto como, por ejemplo, el mando de los televisores, intercomunicación entre equipos y dispositivos informáticos. Son relativamente direccionales, baratas y fáciles de construir, pero no atraviesan objetos sólidos.

La radiación de la luz visible es la que permite ver los objetos. Se localiza aproximadamente entre 3,8 x 10^{14} Hz (380 THz). Esta es la única parte del espectro electromagnético visible para el ojo humano. El Sol es la principal fuente de luz visible.
La luz ultravioleta está comprendida entre los 7,5 x 10^{14} Hz (75 THz) y los 3,0 x 10^{16} Hz de frecuencia del espectro electromagnético.

Las radiaciones de rayos-x abarcan desde los 3,0 x 10^{16} (30 PHz), hasta los 3,0 x 10^{19} Hz de frecuencia dentro del espectro electromagnético. Las radiaciones de esos rayos son invisibles para el ojo humano, pero pueden atravesar diferentes tipos objetos.

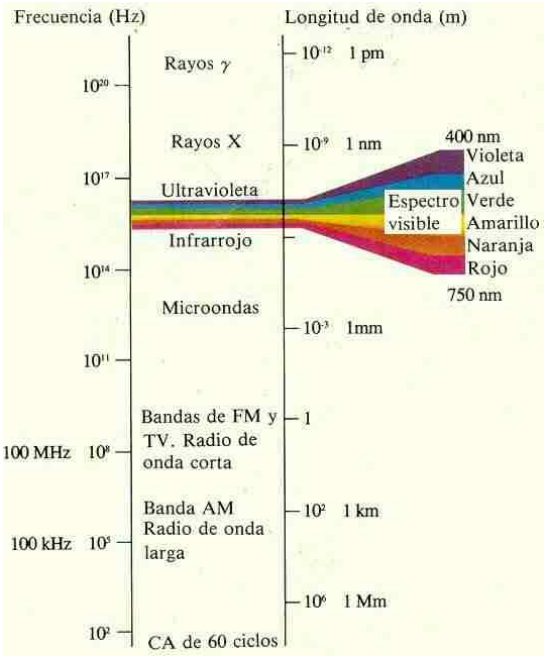

Figura 32: Espectro Electromagnético
Fuente: http://www.asifunciona.com/

Los Access Points con estándares 802.11x utilizan las bandas de frecuencia comprendidas en los 2.4 GHz (802.11b y g) y en los 5 GHz (802.11b). En las versiones b y g del estándar se definen 11 canales en USA y 13 en Europa para ser usados por dispositivos inalámbricos, sin embargo, estos canales se solapan entre ellos generando interferencias y quedan 3 y 4 canales respectivamente utilizables, cada canal tiene un ancho de banda de 22 MHz desde los 2.400 GHz hasta los 2.483,5 GHz. En la versión a se puede llegar a tener 8 canales sin solapamiento con un ancho de banda de 455 MHz por canal desde 5.15 GHz hasta 5.35 y desde los 5.470 GHz hasta 5.725 GHz.

2.1.2. POTENCIAS

La potencia es la velocidad a la que se consume la energía eléctrica, es el cuociente entre el Trabajo eléctrico y el tiempo, siendo su unidad de medida el Watt (W), y su expresa de la siguiente forma:

$$P = \frac{T}{t}$$

Donde:

P	=	Potencia en Watts (W).
T	=	Trabajo en Joule.
t	=	Tiempo en segundos

A la potencia también se le puede relacionar con la intensidad (corriente) y el voltaje quedando de esta manera:

$$P = I*V$$

Donde:

P	=	Potencia en Watts (W).
I	=	Corriente en Amperios (A).
V	=	Voltaje en Volteos (V).

En una onda eléctrica la potencia de la señal es variable, llamada así a la potencia máxima como Amplitud de la onda que es la diferencia entre los puntos mínimos y máximos en la oscilación de una onda (Figura 29).

De igual manera en un ancho de banda determinado la frecuencia central es aquella en la cual está concentrada la mayor potencia.

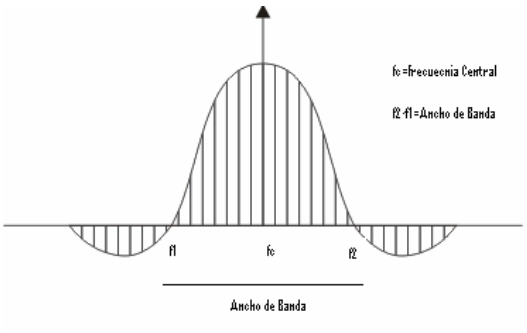

Figura 33: Ancho de Banda y Frecuencia Central

Un Access Point de estándar 802.11x no sobrepasa los 100mW de potencia. Esta potencia es fijada por los organismos de estandarización según niveles de no riesgo para la salud.

2.1.3. ANTENAS

Las antenas son dispositivos conductores que transmiten y reciben ondas de radio, en la transmisión convierten las ondas que pasan a través de un medio guiado (como un cable) en ondas electromagnéticas que viajarán por el espacio libre y en la recepción convierten estas ondas electromagnéticas en ondas guiadas.

Si una corriente circula sobre un material conductor se creará un campo magnético y eléctrico en sus alrededores. En el diseño de una Antena se debe tomar en cuenta lo longitud de onda de la señal a transmitir, de esta dependerá la aplicación y las medidas de la antena.

El tamaño de las antenas se relaciona con la longitud de onda de la señal será transmitida o recibida por dicha antena, siendo un múltiplo o submúltiplo de la longitud de onda. Igualmente dependiendo de la frecuencia de trabajo dependerá su forma y orientación.

Los parámetros de una antena dentro de un sistema son:

- Impedancia[22]: a la antena se le conectará a un transmisor y debe radiar el máximo de potencia con el mínimo de pérdidas. Es decir, la impedancia debe ser la mínima posible.
- Eficiencia: está relacionado con la impedancia y es la relación entre la potencia que se le aplica a la antena y la potencia radiada por la misma.
- Ganancia: Incremento de potencia de la señal. La ganancia es una relación entre la potencia de entrada y la potencia de salida, en el caso de las antenas es la relación entre la potencia entregada a la antena y la potencia

[22] Oposición al paso de corriente en un circuito, Relación entre el voltaje y la corriente (V/I).

irradiada a una cierta distancia. Se mide en decibelios[23]. Lo contrario de la Ganancia es la atenuación que es pérdida de potencia de la señal.

- Polarización: se refiere a la orientación del campo de radiación. Se puede polarizar en forma lineal (vertical u horizontal), en forma elíptica o circular.

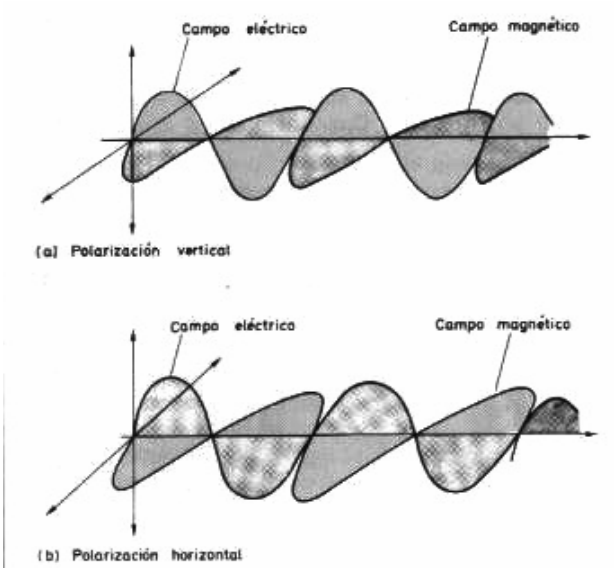

Figura 34: Polarización Lineal
Fuente: http://www.geocities.com/

- Ancho del Haz: es la separación angular del haz de señal que es irradiado por la antena.

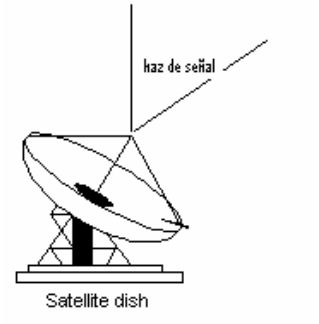

Figura 35: Haz de Señal

[23] Medida de ganancia o atenuación, unidad de medida en dB, un dB=10log(p2/P1)

- Ancho de Banda: es el rango de frecuencias de operación donde la antena trabaja satisfactoriamente. Es decir, donde la antena irradia mayor potencia.
- Directividad: es la relación entre la potencia máxima radiada en una dirección y el total de potencia radiada a una cierta distancia. A la Ganancia se le puede calcular con la multiplicación de la Directividad por la Eficiencia.

Se tienen varios tipos de antenas, estas dependerán de las características antes mencionadas:

- Antenas Hilo: son antenas de conductores hilo, es decir, son de sección despreciable respecto a la longitud de onda, normalmente son de 1 longitud de onda.
- Lineal: está construida por un conductor rectilíneo.

Figura 36: Antena Lineal
Fuente: http://www.atel.com.pl

- Multibanda: abarca muchas frecuencias. De onda corta

Figura 37: Antena Multibanda
Fuente: http://www.ea4az.com

- Yagi: tiene varios elementos paralelos, muy usada en la recepción de señales de televisión (50 MHz a 86 MHz).

Figura 38: Antena Yagui para UHF
Fuente: http://www.superrobotica.com

- VHF y UHF: usadas en estos rangos de frecuencia.

Figura 39: Antena UHF
Fuente: http://www.aquiario.com.br

- De apertura: utilizan superficies para direccional el haz de señal, la ganancia de estas antenas está relacionado con la superficie, es decir, a mayor tamaño mayor ganancia.

    - De Reflector o Parabólica: provista de un reflector, tiene forma parabólica, esférica o como bocina. Son muy direccionales y son usadas en transmisiones satelitales.

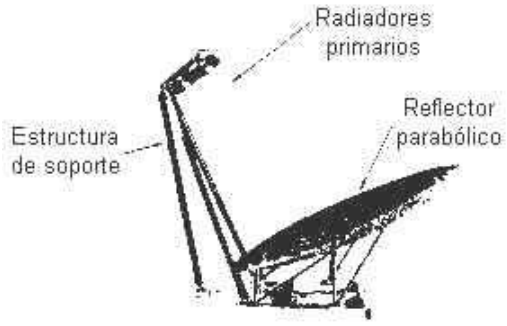

Figura 40: Reflectores Parabólicos
Fuente: http://platea.pntic.mec.es

    - De Bocina: permiten alcanzar directividades moderadas, pero presentan desadaptación en la boca de la guía.

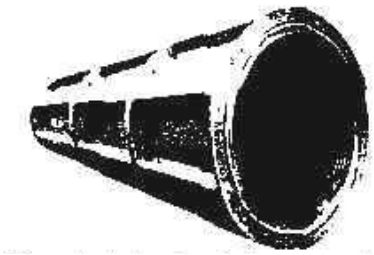

Figura 41: Antena Bocina
Fuente: http://platea.pntic.mec.es

- Bocinas Reflectoras: la alimentación de este tipo de antenas consiste en uno o varios radiadores de tipo bocina.

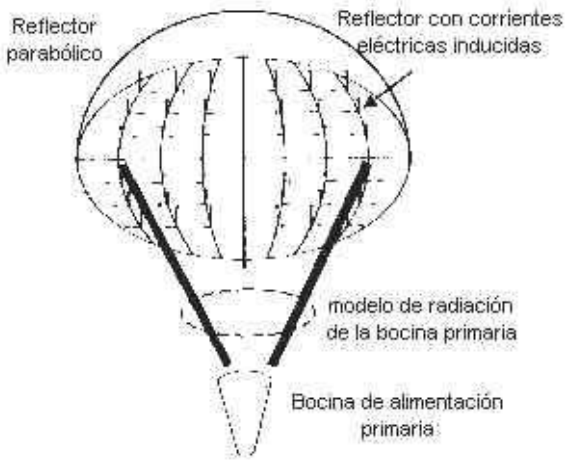

Figura 42: Bocinas Reflectoras
Fuente: http://platea.pntic.mec.es

La Radiación de estas antenas, según el tipo, puede ser directiva u omnidireccional (en todas las Direcciones), dependerá de la aplicación y el área que se quiere cubrir con la señal radiada su utilización.

En los equipos de estándares 802.11x se usan antenas lineales comúnmente. Si se lo va a trabajar para realizar una cobertura de varios host se colocaría una Ommnidireccional, y si se los va usar como bridge para enlazar dos Access Points se colocaría con antenas Directivas. EL tipo de antenas a escoger dependerá del

área de cobertura a dar servicio inalámbrico, es decir en un Campus se podría escoger una antena de mayor ganancia para incrementar la cobertura.

2.2. CARACTERÍSTICAS LÓGICAS DE UN SISTEMA OPERATIVO CON SOPORTE WIRELESS.

Para que un Sistema Operativo pueda tener soporte a sistemas inalámbricos debe manejar los protocolos de red que vienen inmersos en estos sistemas. También debe tener el soporte de drivers para cada uno de los dispositivos hardware que son necesarios para estos sistemas. En el Capitulo anterior se cita aquellos Sistemas Operativos que más son usados con soporte a redes 802.11x.

2.2.1. MANEJO LIBRERÍAS, MÓDULOS

Un Módulo es un conjunto de subprogramas encapsulados e independientes que forman una unidad con identidad propia. Hacen que sea más simple la estructuración del código al estar todos juntos haciendo referencia a un mismo concepto. Se pueden reutilizar para otros programas.

Una Librería es un módulo predefinido y son proporcionados por el lenguaje utilizado para la programación de otros módulos.

Los Ficheros principales de un módulo son: el de especificación donde se colocan los elementos del módulo y el de implementación donde se encuentra el código fuente propio de dicho modulo donde se implementas las funciones.

En el fichero de especificaciones se encuentra lo siguiente:

- Definición de Tipos de Datos que utiliza el módulo.
- Subprogramas, procedimientos y funciones. Solo se encuentra la cabecera de los subprogramas.

En la implementación se encuentran los siguientes elementos:

- La implementación de los subprogramas indicados en la especificación del módulo.
- Se puede encontrar subprogramas auxiliares.
- Tipos y variables necesarias para implementar los subprogramas.

El usuario de dichos módulos los recibe terminados y complilados[24] en forma de librería. En el momento del montaje se unen todos los ficheros compilados creándose un solo fichero ejecutable. Es decir, para compilar se siguen los siguientes pasos:

- Se compila el fichero para verificar errores
- Se compilan los ficheros en los que se encuentran las implementaciones de los subprogramas del módulo.

Se pueden compilar tantas veces como se quieran siempre y cuando lo ficheros no hayan sido modificados. Se crea un proyecto en el que se incluyen todos los ficheros que forman parte de la aplicación.

2.2.2. SOPORTE DE PROTOCOLOS DE RED, BASADOS EN WIRELESS

Un Sistema Operativo que tiene soporte para redes Inalámbricas debe tener módulos que soporten cada uno de los protocolos de los estándares específicos de estos Sistemas. En general, tienen protocolos de comunicación, control y seguridad. Cada estándar especifica los protocolos usados, estos estándares se trataron en el Capítulo 1 (802.11x).

2.2.3. PROTOCOLOS DE COMUNICACIÓN: TCP/IP

Muchas de las redes LAN actuales utilizan los protocolos de TCP/IP y las Wireless LAN de igual forma. Incluso los protocolos usados por TCP/IP son la

[24] Proceso que traduce el código fuente en lenguaje de máquina

base de la comunicación en el Internet. Un Sistema Operativo que tiene la funcionalidad de conectarse a redes LAN y redes Inalámbricas contiene el soporte a estos protocolos. A continuación se detalla el entorno de TCP/IP como una arquitectura de red establecida.

TCP/IP es un modelo por capas y cada capa tiene un conjunto de reglas llamadas protocolos para la comunicación con su igual en el destino del envío de la información.

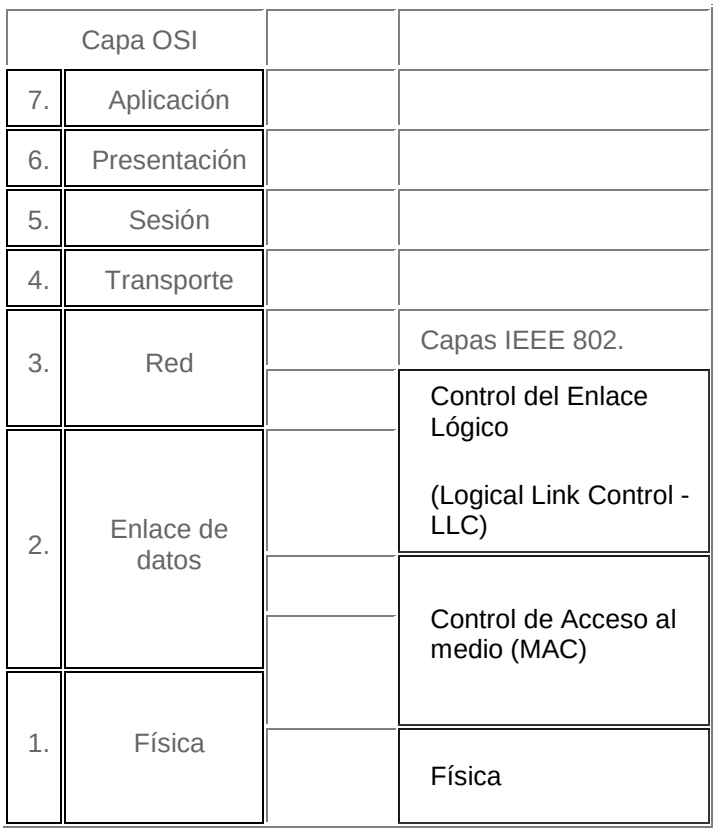

Figura 43: Relación entre IEEE 802y el Modelo OSI del ISO

Fuente: Material Cisco Certificated Networking Associate

LLC(Control del Enlace Lógico) especifica los mecanismos para el direccionamiento de estaciones conectadas al medio y controla el cambio de datos entre usuarios de la red. Su formato esta basado en el protocolo HDLC.

Cada una de las capas del modelo TCP/IP tiene su propia funcionalidad y un conjunto de protocolos necesarios para realizarlo:

- Capa Física y Control de Acceso al Medio (MAC) Controla el acceso al medio de transmisión logrando el uso ordenado y eficiente del medio. La función del MAC es permitir que dispositivos compartan la capacidad de transmisión de la red.

  El estandar 802 presenta algunas opciones de control de Acceso al Medio, asociadas a medios físicos, como:

  - 802.3

    MAC:

    CSMA/CD, ethernet

    Física:

    Coaxial, par trenzado, fibra óptica
  - 802.4

    MAC:

    Token bus

    Física:

    Coaxial, fibra óptica
  - 802.5

    MAC:

    Token ring

    Física:

    Par trenzado
  - 802.6

    MAC:

    DQDB

    Física:

    Fibra óptica
  - 802.11

    MAC:

    CSM, WLAN

Física:

Inalámbrico

- 802.12

  MAC:

  Prioridad

  Física:

  Par trenzado

- 802.16

  MAC:

  WLAN, Banda Larga

  Física:

  Inalámbrico

- Capa de aplicación. Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos.

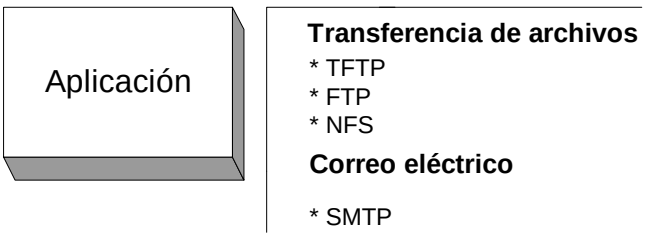

Figura 44: Capa Aplicación

Fuente: Material Cisco Certificated Networking Associate

- Capa de transporte. La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. Significa que los segmentos de la Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.

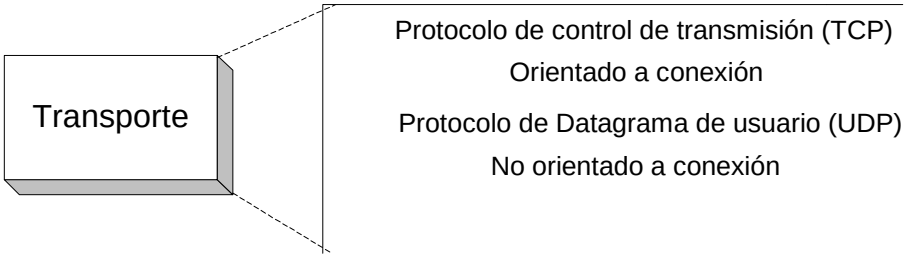

Figura 45: Capa Transporte
Fuente: Material Cisco Certificated Networking Associate

- Capa de Internet. El propósito de la capa de Internet es enviar paquetes origen desde cualquier red y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

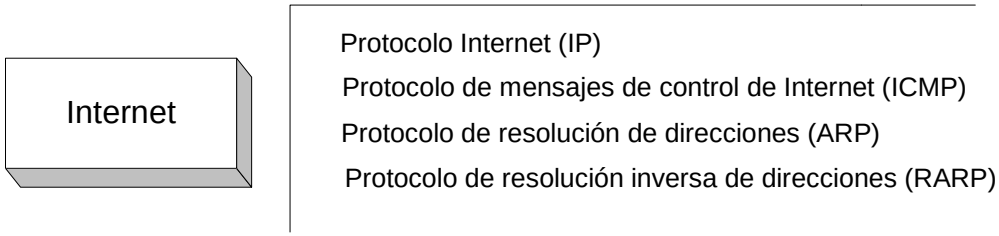

Figura 46: Capa Internet
Fuente: Material Cisco Certificated Networking Associate

- Capa de red. Capa de red. El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Esta capa de acceso de red es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. También especifica los medios de transmisión, como es en WIFI el aire el medio.

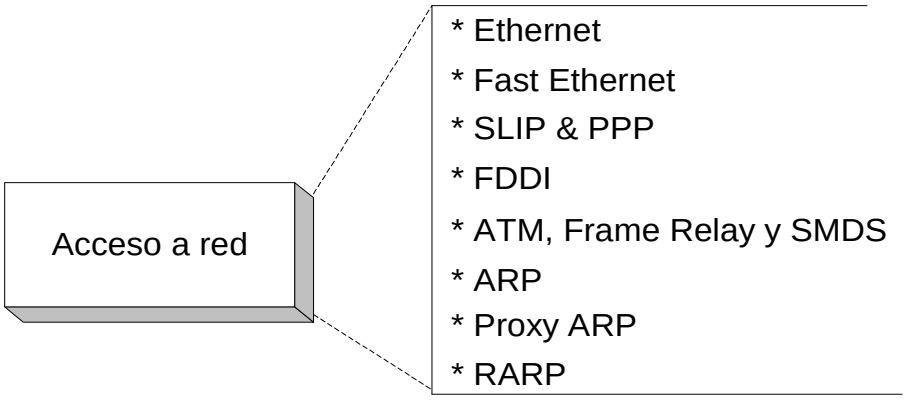

Figura 47: Capa Red
Fuente: Material Cisco Certificated Networking Associate

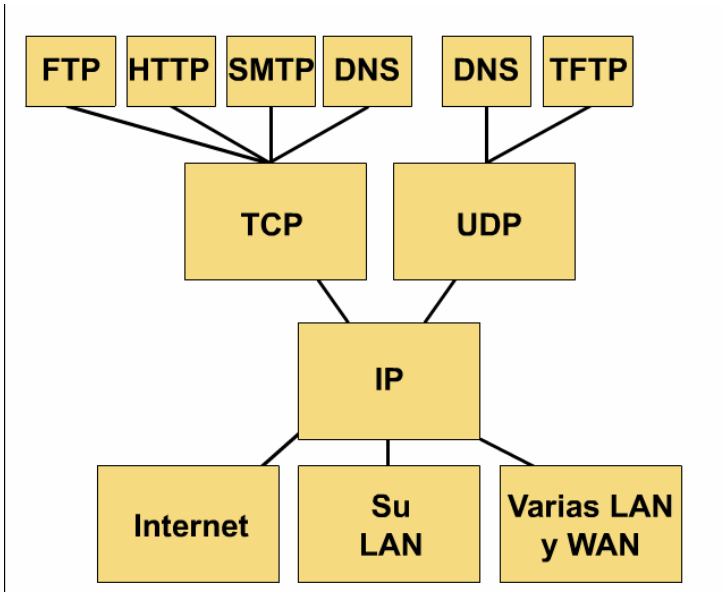

Figura 48: Diagrama de Protocolos TCP/IP
Fuente: Material Cisco Certificated Networking Associate

2.3. SOPORTE DE LINUX A REDES WIRELESS

Linux tiene mucho soporte para Redes Wireless, puede trabajar en las siguientes configuraciones:

- Ad-hoc: son redes par a par, esto significa que cada host es igual en la red que los otros host, simplemente se configura los parámetros normales de red TCP/IP y el nombre de la Red a cada host. Si es deseado se configuraría parámetros de encriptación.

Figura 49: Redes para a par
Fuente: http://www.netarroba.com.mx/anteriores/informe84.html

- Master: para esta configuración se tendrá que configurar a uno de los host como servidor principal donde se concentrará en tráfico de la red, es decir un host haría de las veces de un Access Point. Además se le pueden colocar ciertos parámetros como son el enrutamiento o el servicio DHCP (Dynamic Host Configuration Protocol) que sirve para dar el servicio de asignación automática de direcciones IPs a los host clientes. Es un esquema de red cliente-servidor.

El requerimiento de hardware adicional que debe tener el host con Sistema Operativo Linux es la tarjeta inalámbrica y que este tenga soporte de drivers.

Se deberá colocar los módulos del Kernel necesarios para el soporte Wireless, estos ya existentes, y configurar los parámetros necesarios para la conexión.

Si se desea colocar seguridades básicas, por defecto viene soporte para encriptación WEP.

De esta manera el host con Linux se conectará a una red inalámbrica existente con un Access Point, puede trabajar tipo Ad-hoc o puede hacer la de Access Point con ciertos parámetros adicionales.

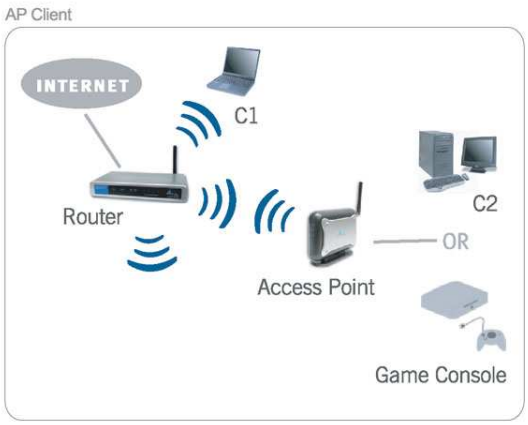

Figura 50: Sistema Inalámbrico
Fuente: http://www.airlink101.com

CAPITULO III: DESARROLLO DE UN SERVIDOR LINUX COMO ACCESS POINT PROXY

En todas las versiones actuales de Linux viene incluido en su kernel soporte para redes inalámbricas como se pudo ver en el capítulo anterior. Es decir, vienen módulos y librerías que dan soporte a estas tecnologías para la transmisión de los datos que serán revisadas en el presente capítulo, junto con la configuración para los diferentes modos o servicios que existen.

El afan de este capítulo es mostrar una posible coniguracion para dotar a una linux con wifi.

3.1. COMPILACIÓN DEL KERNEL PARA SOPORTE WIRELESS

Durante la instalación del Sistema Operativo se pueden escoger los módulos que necesarios para los diferentes servicios que ofrece la versión de Linux que se está instalando.

Si se requiere soporte para redes inalámbricas, seleccionar soporte general para redes donde estan todos los módulos, aunque es recomendable ejecutar la instalación completa para darle toda la funcionalidad posible al equipo a utilizar.

Si en la instalación original del equipo no se han anexado los módulos necesarios, estos se los pueden agregar con los cds de instalación. Y posteriormente compilarlos con el comando make.

3.1.1. KENEL2.4+

Con el comando make se podrá compilar todos módulos que se desee para configurar el kernel del sistema operativo.

- Paso a Paso, significa recorrer todo a través de la opción **make_config**.
- Por Menús, que se lo lleva a cabo a través de la opción **make_menuconfig**.
- Menús gráficos, a través de la opción **make xconfig**.

Para el método de menús se necesitan librerías que se ocupan de los menús en la consola, y en la fuente del Kernel se escribe **#make_menuconfig**, y se obtiene un menú de configuración para el soporte de hardware y protocolos.

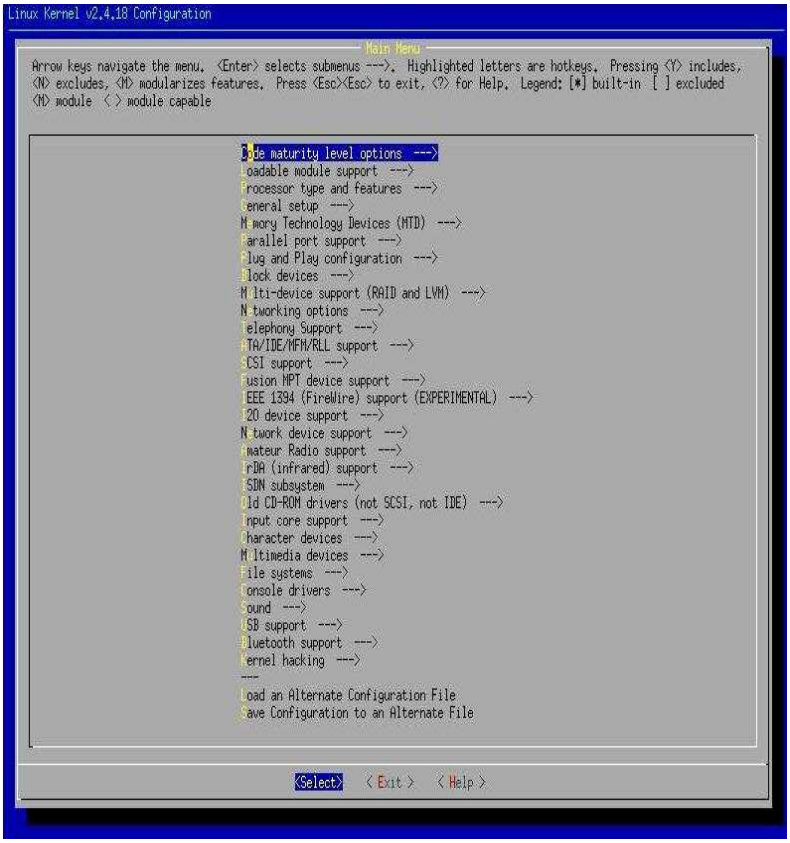

Figura 51: make_menuconfig
Fuente http://bulma.net

En dicho menú encontramos varios grupos de opciones de configuración, sin embargo se nombrará solo los principales y los que tienen que ver con la configuración de redes:

- General setup: tiene varios submenus:
  - Networking support: Para soporte de redes e Internet.
  - PCI support: si el sistema tiene hardware PCI.
  - PCI access mode: especifica cómo se detectaran los PCI's, por Bios (BIOS), directamente por kernel sin la Bios (Direct) y automático

(Any) donde el kernel primero tratara de detectarlo directamente y si falla usara la BIOS.

- PCI device name database: habilita la base de datos de todos los dispositivos PCI conocidos.
- MCA support: habilita la Arquitectura MicroCanal que es un bus de sistema similar a PCI o ISA.
- Support for hot-pluggable devices: para conectar dispositivos que se pueden colocar y sacar sin tener la necesidad de apagar el equipo.
- PCMCIA/CardBus support: para soporte a tarjetas PCMCIA.

- Networking options:
  - Packet socket: para las aplicaciones con comunicación directa con la red.
  - Packet socket: mmapped IO: se activará el protocolo Packet que usará un mecanismo de Entrada/Salida (I/O).
  - Network packet filtering (replaces ipchains): para filtreo de paquetes.
  - Socket Filtering: para filtreo de sockets, muy usado en conexiones mediante PPP.
  - Unix domain sockets: para dar soporte a el acceso a la red mediante el estándar UNIX.
  - TCP/IP networking: para conexiones TCP/IP.
  - Asynchronous Transfer Mode (ATM) escoja esta opción si tiene una red LAN.
  - 802.1Q VLAN Support: para soporte a VLANs (Virtual LAN). Se debe instalar un programa vconfig y configurarlo.
  - The IPX protocol: para soporte al protocolo Novel network.
  - Appletalk protocol support Appletalk: para soporte a Appletalk que es la forma por la que los computadores Apple se comunican entre ellos en la red.
  - DECnet Support: para soporte a DECnet que es un protocolo usado en algunos productos hechos por Digital (Compaq).
  - 802.1d Ethernet Bridging: para usar el equipo como puente ethernet.
  - CCITT X.25 Packet Layer es un grupo de protocolos de red estandarizados.

  - WAN router: para enrutamiento a nivel de WAN, el hardware debe tener este soporte.
  - Fast switching: permite la comunicación directa entre interfaces de tarjetas de red. No es compatible con "Network packet filtering".
  - Forwarding between high speed interfaces: habilita NIC (Network Interface Card) durante periodos de congestión extrema.
- Telephony Support: este menú permite configurar un MODEM telefónico
- Network device support: para soporte a dispositivos de Red.
  - ARCnet devices: para soporte a tarjeta ARCnet (Red LAN tipo Token Ring).
  - Dummy net driver support: para conexiones SLIP o PPP.
  - Bonding driver support: para soporte a múltiples canales conjuntos de tarjetas ethernet.
  - Ethernet (10 or 100Mbit): submenú para configurar la tarjeta de red ethernet de 10 o 100 Mbits.
  - Ethernet (1000 Mbit) para configurar una tarjeta ethernet de 1000Mbits.
  - FDDI driver support Fiber Distributed Data Interface (FDDI): para la configuraciónde tarjetas FDDI.
  - HIPPI driver support HIgh Performance Parallel Interface (HIPPI) permite una transmisión entre 800Mbits/segundo y 1600Mbits/segundo dual o simple. HIPPI puede funcionar sobre cableado de cobre de hasta 25 metros o de fibra de hasta 300 metros en multi-modo o 10 Kilometros en modo-simple.
  - PLIP (parallel port) si desea conectar dos o más Hosts mediante el puerto paralelo.
  - PPP (point-to-point protocol) support: para soporte PPP este protocolo.
  - SLIP (serial line) support: para soporte al protocolo SLIP.
  - Wireless LAN (non-hamradio): para soporte a red local Wireless.
  - Token Ring devices: para soporte a redes Token Ring.
  - Fibre Channel driver support: soporte a el protocolo serie de gran velocidad que se usa para conectar dispositivos de gran almacenaje.

    - Red Creek Hardware VPN: driver para el hardware que proporciona una Red Privada Virtual (Virtual Private Network).
    - Wan interfaces: para soporte a redes WAN.
    - IrDA (infrared) support: el protocolo Interfared Data Associations (IrDA) es usado para interfaces de comunicación wireless.
    - ISDN subsystem: para soporte a redes de servicios digitales RDSI.
- Character devices:
    - Virtual Terminal: para soporte a terminales virtuales o consolas virtuales.
    - Support for console on virtual Terminal: da soporte para usar una consola en un terminal virtual.
    - Parallel printer support: para soporte a impresoras conectadas al puerto paralelo.
    - Support for user-space parallel port device drivers: para programas que han de acceder al puerto paralelo.
    - Network File Systems: desde este submenú se podrá configurar sistemas de archivos network.
- Console drivers:
    - Bluetooth support: en este menú se da soporte para redes Bluetooth.

Estas son algunas de las opciones de configuración, para preparar el kernel para redes inalámbricas se usarán las que configuran el soporte para este tipo de redes y sus protocolos.

Configurado cada uno de los datos se selecciona en el menú la opción:

Save Configuration to Alternate File, guarda la configuración en un archivo.
Seleccionar exit.

Para configurar y preparar las dependencias del kernel necesarias para efectuar la compilación.

 # make dep

Terminado el proceso se eliminan ficheros objetos y demás archivos de la versión anterior de esta manera se limpian las "impurezas".

 # make clean

Para compilar:

Opciones escogidas como módulos

 # make modules

Diversos módulos.

 # make modules_install

Los comandos anteriores se pueden escribir en una sola línea.

 # make dep && make clean && make bzImage && make modules && make modules_install

Cuando se requiere comenzar una compilación en limpio y eliminar la actual se utiliza:

 # make mrproper

Para conservar la configuración se copia en un directorio diferente a ".config". Finalmente, para un mayor orden se cargar la imagen creada en el directorio /boot.

Dar nombre a la imagen, normalmente se lo hace colocando la versión del Kernel, como ejemplo "kernel-2.4.18".

 # mv /usr/src/linux/arch/i386/boot/bzImage /boot/"nombre de la imagen"

System.map es un mapa de booteo del sistema, es decir una tabla que da el orden al booteo, y debe estar en el directorio /boot.

 # mv /usr/src/linux/ boot /System.map

Dependiendo del sistema de arranque con el que se trabaje, el arranque de la imagen se debe configurar el LILO o el GRUB, con LILO sería de la siguiente forma:

 # joe /etc/lilo.conf

image = /boot/”nombre de la imagen”

label = Linux

```
/etc/lilo.conf
boot                    =               /dev/had
map                 =                   /boot/System.map
delay                   =               20
timeout                 =               50
prompt
default                 =               Linux
vga                     =               791
root                =                   /dev/hda2
read-only
lba32
install=/boot/boot.b
image = /boot/linux-2.4.18
label = Linux
#En caso de tener otro sistema operativo, lo añadimos a continuación
other = /dev/hdb1
label = otroOS
```

Figura 52: Ejemplo del archivo /etc/lilo.conf

Fuente http://bulma.net

De existir más compilaciones del Kernel es conveniente crear otras entradas en el sistema de arranque. Por tanto se debe renombrar la imagen del kernel. **# mv /boot/linux-x.y.z /boot/”nombre de la otra imagen”**

```
etc/lilo.conf
boot                    =               /dev/had
map                 =                   /boot/System.map
delay                   =               20
timeout                 =               50
prompt
default                 =               Linux
vga                     =               791
root                =                   /dev/hda2
read-only
lba32
install=/boot/boot.b
image = /boot/linux-2.4.18 #Nueva imagen
label = Linux
image = /boot/linux-2.4.17.OLD #Antigua Imagen (segura)
label = Linux.SAFE
other = /dev/hdb1
label = otroOS
```

Figura 53: 2do Ejemplo del archivo /etc/lilo.conf

Fuente http://bulma.net

Realizadas las modificaciones en dicho archivo, se carga la nueva configuración

en el sistema de arranque.

 # /etc/lilo.conf

Reiniciar el sistema seleccionando la etiqueta cargar la nueva imagen del kernel.

3.2. LINUX RED WIRELESS, CONFIGURACION

La configuración de Linux para conectarse a un Access Point se denomina Modo Infraestructura, que consiste en colocar a la tarjeta inalámbrica en modo “managed”. Hay que habilitar el soporte de Cardbus en el kernel en el setup del Linux de esta manera:

General Setup: PCI-PCMCIA CardBus Support (Soporte de la tarjeta Inalámbrica Colocada).

- Seleccionar Cardbus Support
- Seleccionar los drivers a través de Networking Device Support: Wireless LAN (non-hamradio).
- Escoger las opciones y sub opciones de la tarjeta que se está usando.

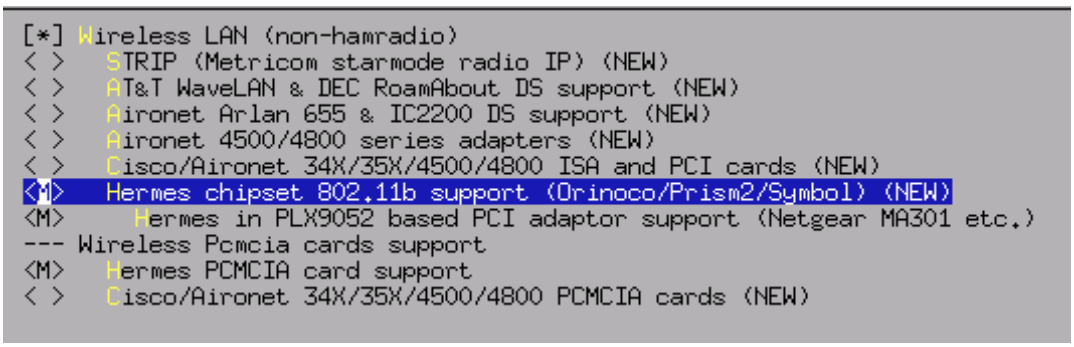

Figura 54: Ejemplo Configuración Cardbus

Fuente http://bulma.net

El momento de la configuración se debe compilar el kernel para comprobar que estén instalados todos los paquetes de soporte de la tarjeta inalámbrica, verificando también que estén creados todos los ficheros correspondientes en el

directorio /etc/ y se configuran los datos de red que se necesitarán para la conexión.

Si dentro de Kernel no existe soporte para algún tipo de tarjeta inalámbrica, se debe encontrar alguna compatible y compilar los drivers de dicha tarjeta.
En Red Hat se configura en el fichero /etc/sysconfig/network-scripts/ifcfg-ethX. Los parámetros a configurar son los siguientes:

DEVICE=eth1
MODE=managed
ESSID="Nombre_de_red"
RATE=auto
TXPOWER=auto
KEY="s:mi_clave" (Solo si va encriptado)
BOOTPROTO=static
IPADDR="dirección ip del host"
BROADCAST="dirección de broadcast" (ultima dirección ip del segmento para broadcast)
NETMASK="mascara de red"
NETWORK="identificador de red"
ONBOOT=yes

3.3. CONFIGURACIÓN DEL KERNEL PARA CONVERTIR A LINUX EN ACCESS POINT

Concluidos los pasos anteriores se inicia la configuración de un Access Point con Linux.

Se coloca a la tarjeta inalámbrica en modo Master y de esta manera se conectarán desde cualquier otro sistema operativo con soporte wireless al Linux, incluso si se coloca algún tipo de autentificación y encriptación. El Linux de esta manera se convertirá en un servidor de acceso para toda la red, realizando bridging, e incluso se puede configurar como servidor DHCP.

Como ya se cuenta con casi todo lo referente a drivers, se procede a configurar la red.

3.3.1. MÓDULO WIRELESS

Como se revisó en pasos anteriores, para la configuración del Kernel existen varios módulos que sirven para soporte en redes IP y Wireless, con estos se configurarán para el soporte requerido:

Un paquete muy usado para la configuración del Kernel para soporte Wireless en cualquiera de sus modos es el llamado **MadWIFI** y sirve en cualquiera de las versiones superiores a Kernel 2.4.

MadWIFI es un software desarrollado para tarjetas wireless con chipset Atheros. Sus siglas significan “Multiband Atheros Driver for Wireless Fidelity”, es decir, provee de drivers para el kernel de Linux, soportando chipset Atheros. Con el driver la tarjeta inalámbrica aparecerá como una interface de red dentro del sistema, permitiendo que se pueda configurar la tarjeta de una manera simple usando el ifconfig, iwconfig, etc.

Las características principales son las siguientes:

- Modos de Operación:
    - Ad-hoc: El equipo actúa como parte de una red ad-hoc[25].
    - Managed: El equipo actúa como cliente de una red de infraestructura[26].
    - Master: El equipo actúa como un Access Point.
    - Repetear: El equipo solo reenvía los paquetes recibidos de otros nodos inalámbricos.
    - Secondary: El equipo actúa como un backup de un Master o Repetear.
    - Monitor: El equipo solo recibe paquetes en modo de monitoreo.
    - Auto: Configuración automática empezando por Ad-hoc y siguiendo en Managed.

[25] Una red Adhoc es aquella que no necesita de puntos de acceso para transmitir
[26] La red de Infraestructura no depende de puntos de acceso.

- MadWIFI, no soporta todavía dispositivos usb, solo posee drivers para dispositivos PCI o miniPCI.
- La mayoría de Chipset Atheros es soportado.
- Soporta WEP y WPA/802.11i.
- En modo AP soporta autentificación 802.11x.

Como requerimientos básicos para cargar los módulos de MadWIFI se tiene:

- Kernel 2.4.23 o superior y 2.6.x. Otros podrían trabajar, pero no son soportados.
- Que el Kernel soporte y tenga habilitado los siguientes módulos:
- CONFIG_CRYPTO
- CONFIG_SYSCTL
- CONFIG_NET_RADIO. Extensiones Wireless.
- Tener una tarjeta Inalámbrica (PCI, miniPCI o PCMICIA) con chipset Atheros. Ver Tabla de Tarjetas Compatibles.
- Que este en modo root, es decir, de administrador del equipo.

A continuación se muestra una tabla de tarjetas inalámbricas 802.11x, las cuales vienen fabricadas con chipset de marca Atheros, es decir, son las tarjetas compatibles con MadWIFI.

Manufacturer	Form factor		
	PCI	PCMCIA	MiniPCI
3Com	3CRDAG675	3CRWE154A72 3CRPAG175	
Airlink101	AWLH-4030	AWLC4030	
Airvast		XN-100 XN-110 WN-190g	XN-200 XN-210 WN-390g
Alfa	AWPCI83 AWPCI16G AWPCI36	GWPC005 AWPC006G GWPC007	AWPCI08s AWPCI06G
AT&T	6500G 6550G	6700G 6750G	
Cisco	PI21AG	CB21AG	
Corega	CG-WLPCI54AG	CG-WLCB54AG	

		CG-WLBARAG-P CG-WLAP54AG-P	
Delta Networks		LM-WB521	
D-Link	DWL-G510 rev B * DWL-A520 DWL-AB520 DWL-G520 DWL-AG520 DWL-AG530	DWL-G630 * DWL-A650 DWL-AB650 DWL-G650 * DWL-G650 DWL-AG650 DWL-AG660	
Elecom	LD-WL54G/PCI LD-WL54AG/PCI LD-WL5411A/B	LD-WL54/CB LD-WL54G/CB LD-WL54AG/CB	
Fujitsu-Siemens		FMV-JW481 E5454/CB	
Manufacturer	**Form factor**		
	PCI	**PCMCIA**	**MiniPCI**
Gemtek		WL-511 WL-571	WL-550
Gigabyte	GN-WPEAG	GN-WMAG GN-WLMA101	GN-WIAG01 GN-WIAG02
Global Sun	GL 5054VP	GL 245401-OA GL 505401 GL 505402	GL 2454MP GL 5054MP GL 5254MP
IBM		22P7501 31P9101	91P7263 31P9701
Intel	WPCI5000	WCB5000	WM3A5000
I-O Data	WN-AG/PCI	WN-A54/CB WN-AB/CB WN-AG/CB WN-AG/CB2	
Lancom	PCI-54ag PCI-54[a]	MC-54ag MC-54ab MC-54g	
Linksys	WMP55AG	WPC51AB WPC54A WPC55AG	
Netgear	HA311 WG311 v1 * WAG311 WG311T	HA501 WAB501 WAG511 WG511T	
Philips		PH 10819	PH 11107
Planet	WL-8310	WL-3560	
Planex		GW-NS540a GW-NS54AG GW-NS54SG	
Promix	8482WD Gold 8482JP Gold	8470-WD/FC Gold 8470-WD	

		8470-FC 8471-WD Silver 8471WD 8480-WD/JP Gold 8480WD 8480JP 8481-WD/JP Silver 8481WD 8481JP	
Samsung		SWL-5200N	
Senao		NL-3054CB * NL-5054CB	NL-3054 MP NL-5354 MP
Sharp		DC2B1DZ/// DC2B1EZ///	DC2G1EZ///
Manufacturer	**Form factor**		
	PCI	**PCMCIA**	**MiniPCI**
Sony		PCWA-C500 PCWA-C300S PCWA-C700 PCWA-C800S	
SparkLAN	WL-760A WL-660GS	WL-711A WL-611GS	WMIA-112AG WMIA-123AG WMIA-139AG
TDK		WN-5CB01 WN-DCB03 WN-GCB03	WN-5MP01 WN-GMP03 WN-DMP03
Tellus		C6100	M6100
Toshiba		TransCube 20	
TP-Link	TL-WN550G TL-WN650G	TL-WN510G TL-WN610G	
Xnet	PWG600A *	EWG660A *	

Tabla 9: Compatibilidad de Dispositivos MadWIFI.
Fuente: http: / /atheros.rapla.net

El módulo MadWIFI se puede obtener bajándose una copia de varias fuentes en el Internet. La fuente más confiable es sourceforce.net donde se encontrarán las revisiones más estables.

Se utilizo la versión de la dirección del MadWIFI:
http://downloads.sourceforge.net/madwifi/madwifi-0.9.3.1.tar.gz?modtime=1179910675&big_mirror=0

Los drivers de cada tarjeta no necesariamente soportan todos los modos de trabajo, sin embargo, todas soportan al menos el modo Ad-hoc y el Management. Para este proyecto se ha utilizado la tarjeta PCI DWL-G520 del fabricante DLINK, basado en chipset Atheros. Esta tarjeta soporta hasta el modo master que es el indicado para configurar como AP. También se ha utilizado el modo Ad-hoc para el modo de ruteo para acceso a otras redes o en su defecto al Internet.

MadWIFI provee el driver con el que se podrá configurar los diferentes modos de trabajo. Siendo un driver para cada versión de Kernel. Además colocar los rpm en un directorio, de preferencia en /usr/src/, desde un terminal de consola como root se instala de la siguiente manera:

rpm –ivh madwifi*.rpm –C /usr/src/

Cada módulo se instalan en la ruta /lib/modules/$(uname –r)/updates/net siendo ath_pci el módulo principal.

Reiniciar el sistema y comprobar que hayan sido cargados los driver con el comando:

lsmod | grep ath_pci .

Como ya se ha revisado con iwconfig se podrá configurar los parámetros para redes inalámbricas y con ifconfig parámetros normales de redes IP.

La configuración de cada uno de los modos se detalla a continuación:

- Modo Ad-Hoc:
  - **Detener el servicio de red.**

    service network stop
    ifconfig ath0 down
    ifconfig eth0 down
  - **Desactivar la interfase inalámbrica y extensions.**

    wlanconfig ath0 destroy
  - **Crear la interface wifi0 de ath0 pero en modo Ad-Hoc.**

    wlanconfig ath0 create wlandev wifi0 wlanmode adhoc
  - **Activar la interface inalámbrica.**

ifconfig ath0 up

- **Definir el estándar de trabajo, 802.11a, b o g .**

  iwpriv ath0 mode 3 --> modo 802.11g

- **Definir el canal de trabajo, rango de frecuencia en que trabajará.**

  iwconfig ath0 channel 6

- **Identificar el número de canales disponibles.**

  iwlist channel

- **Especificar el ESSID.**

  iwconfig ath0 essid "TesisWiFi"

- **Opcion Automática, se utiliza cuando no se conoce el ESSID .**

  iwconfig ath0 ap any

- **Configurar el servicio de red, si se dispone de un servidor DHCP.**

  dhclient ath0

- **Configuración manual de la red.**

  ifconfig ath0 192.168.10.77 netmask 255.255.255.0 up

  ifconfig eth0 205.235.2.206 netmask 255.255.255.252 up

  route add -net 0.0.0.0 netmask 0.0.0.0 gw 205.235.2.205

La configuración de la tarjeta se comprueba con los comandos ifconfig y haciendo ping (paquetes ICMP que generan ecos en la red y se verifica respuestas de un destino determinado) hacia otros equipos en la red. Con el comando iwconfig se observa los parámetros inalámbricos de la conexión.

- Modo Managed.
  - **Interrumpir el servicio de red.**

    service network stop

    ifconfig ath0 down

    ifconfig eth0 down

  - **Desactivar la interfase inalámbrica y extensiones.**

    wlanconfig ath0 destroy

  - **Crear la extensión wifi0 de ath0 pero en modo Manager.**

    wlanconfig ath0 create wlandev wifi0 wlanmode managed

  - **Activar la interface inalámbrica.**

    ifconfig ath0 up

  - **Especificar el estándar de trabajo.**

    iwpriv ath0 mode 0 --> modo automático

iwpriv ath0 mode 1 --> modo 802.11ª

iwpriv ath0 mode 2 --> modo 802.11b

iwpriv ath0 mode 3 --> modo 802.11g

- **Identificar el número de canales disponibles.**

  iwlist channel

- **Definir el canal de trabajo.**

  iwconfig ath0 channel 4

- **Identificar los ESSID disponibles.**

  iwlist scanning

- **Relacionar el Access Point indicando el ESSID.**

  iwconfig ath0 essid "TesisAP"

- **O la opción automática.**

  iwconfig ath0 ap any

- **Activar el cifrado WEP, solicita contraseña.**

  iwconfig ath0 key “s:”

  La contraseña en modo ASCII, son 5 caracteres para cifrado de 40 bits y de 13 para 128 bits. Cuando la contraseña se encuentra en modo hexadecimal no se debe digitar la inicial “s:”, se introduce directamente la clave con 5 o 13 caracteres especificado en hexadecimal.

- **Configurar el servicio de red, si se dispone de un servidor DHCP.**

  dhclient ath0

- **Configuración manual de la red.**

  ifconfig ath0 192.168.10.77 netmask 255.255.255.0 up

  ifconfig eth0 205.235.2.206 netmask 255.255.255.252 up

  route add -net 0.0.0.0 netmask 0.0.0.0 gw 205.235.2.205

- Modo Master.

  La tarjeta PCI D-Link modelo DWL-G520, debido a que la tarjeta soporta en su driver madwifi el modo de operación Master, el equipo se comportará como un AP (Access Point).

  La PC en modo Master debe crear un puente entre el puerto ethernet y el puerto inalámbrico, para ello se debe activar la funcionalidad bridge (puente) del kernel instalando el paquete bridge-utils.

  yum install bridge-utils.

Los clientes de este Access Point pueden obtener direcciones automáticamente si se activa el servicio de DHCP o en su defecto si existe un servidor DHCP hacia el puerto ethernet del AP.

- **Desactivar el servicio de red.**

  service network stop
- **Crear la interface inalámbrica en modo Access Point.**

  wlanconfig ath0 destroy

  wlanconfig ath0 create wlandev wifi0 wlanmode ap
- **Se activa la interface Ethernet y la inalámbrica.**

  Sin especificar IP

  ifconfig ath0 0.0.0.0 up

  ifconfig eth0 0.0.0.0 up

  Especificando IP

  ifconfig ath0 192.168.10.77 netmask 255.255.255.0 up

  ifconfig eth0 205.235.2.206 netmask 255.255.255.252 up

  route add -net 0.0.0.0 netmask 0.0.0.0 gw 205.235.2.205
- **Seleccionar modo de estándar.**

  iwpriv ath0 mode 2
- **Escoger el canal**

  iwconfig ath0 essid “TesisWiFi” channel 7
- **Se crea el Puente.**

  brctl addbr br0
- **Establecer el puente entre las interfaces ethernet e inalámbrica.**

  brctl addif br0 eth0

  brctl addif br0 ath0
- **Activar el Puente**

  Sin definir IP.

  ifconfig br0 0.0.0.0 up

  Definiendo IP.

  ifconfig ath0 192.168.10.77 netmask 255.255.255.0 up

De esta manera el equipo se comporta como un punto de acceso o Access Point, permitiendo que los equipos clientes se conectaran identificando el ESSID.

Para mejorar el área de cobertura el equipo debe estar ubicado en una posición geográfica optima, también pueden mejorar la ganancia de la señal y aumentar la cobertura con la variedad de antenas existentes en el mercado.

Si los rpm del driver de madwifi al momento de instalarse no configuraron adecuadamente en el archivo /etc/sysconfig/network-scripts/ifcfg-ath0, se puede añadir las siguientes líneas de comando:

DEVICE=ath0
ONBOOT=yes
TYPE=Wireless
MODE= Managed, Ad-Hoc o Master (una de estos modos)
EESID=TesisWIfI
CHANNEL=canal
RATE=auto
TXPOWER=auto
BOOTPROTO=static
IPADDR=192.168.10.77
BROADCAST=192.168.10.255
NETMASK=255.255.255.0
NETWORK=192.168.10.0
KEY=”s:claveTesisWiFi”

Para el cifrado WEP en el caso de Fedora y Red Hat se emplea el archivo adicional:

/etc/sysconfig/network-scripts/keys-ath0
KEY=” s:claveTesisWiFi”

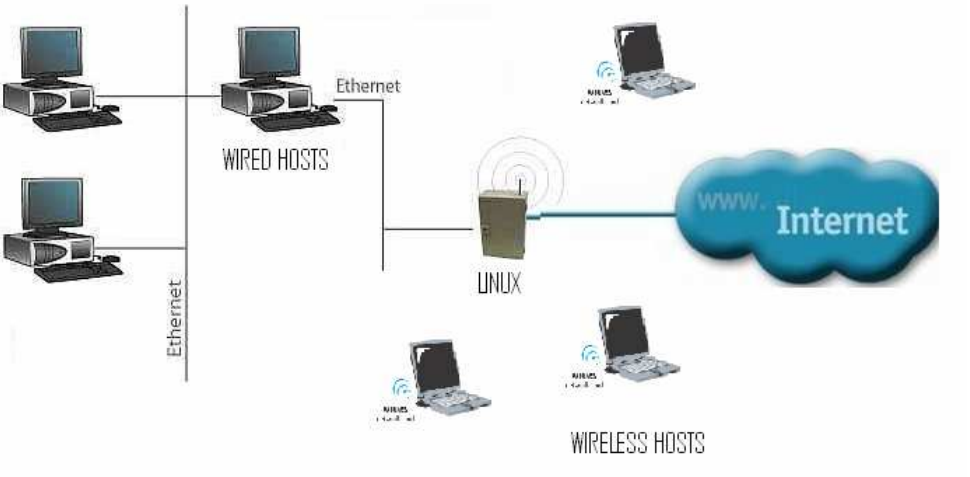

Figura 55: Sistema Wireless con Linux

3.3.2. ENTREGA DE DIRECCIONAMIENTO DHCP

Una de las funcionalidades comunes en los Access Points es la de ser además Servidor de direcciones IP (DHCP), de esta manera cuando un Host va a conectarse en la red va a obtener todos los parámetros necesarios para realizar una conexión en la red como son la dirección, máscara y puerta de enlace, además que también se pueden obtener las direcciones de los DNSs existentes. En Linux dicha configuración se la obtiene de la siguiente manera:

Editar el fichero de configuración:
/etc/dhcpd.conf

Deberá contener las líneas siguientes:

```
ddns-update-style interim;
ignore client-updates;
shared-network miredlocal {
        subnet 192.168.10.0 netmask 255.255.255.0 {
        option routers 192.168.10.177;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.10.255;
        option domain-name-servers 205.235.2.130;
        range 192.168.10.200 192.168.10.254;
```

```
        default-lease-time 21600;
        max-lease-time 43200;
        }
DHCPDARGS=eth1
```

Grabar y salir.

Para iniciar por primera vez el servicio dhcpd, ejecutar el siguiente comando:

/sbin/service dhcpd Start

Para hacer que los cambios hechos a la configuración del servicio surtan efecto:

/sbin/service dhcpd restart

Detener el servicio con el comando:

/sbin/service dhcpd stop

Agregar el servicio dhcpd al arranque del sistema:

/sbin/chkconfig dhcpd on

El servicio DHCP estará presente para todas las interfaces creadas en el sistema.

3.3.3. ESTABLECIMIENTO DEL PROXY[27] WIRELESS

El servicio más común es el cache de contenidos de red, es decir, un cache de páginas y ficheros disponibles en la red en servidores http remotos. De esta manera los clientes acceden a estos servicios de una manera más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un URL (Uniform Resource Locator) el Proxy busca el resultado del URL dentro del caché. Si éste es encontrado, el Proxy responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el Proxy lo traerá desde el servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado

[27] Proxy es un dispositivo que permite a los clientes realizar conexiones de red indirectas hacia otros servicios de red. También se le puede usar como corta fuego, con filtrado de paquetes.

luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de respuestas a solicitudes (hits).

Un paquete del Linux para Proxy Transparente[28] es el Squid. Entre otras cosas, Squid puede funcionar como Proxy y caché de contenido para los protocolos HTTP, FTP, Proxy de SSL (Capa de Servicio de Seguridad, Security Service Layer), aceleración HTTP, caché de consultas DNS, filtreo de contenido y control de acceso por IP y por usuario.

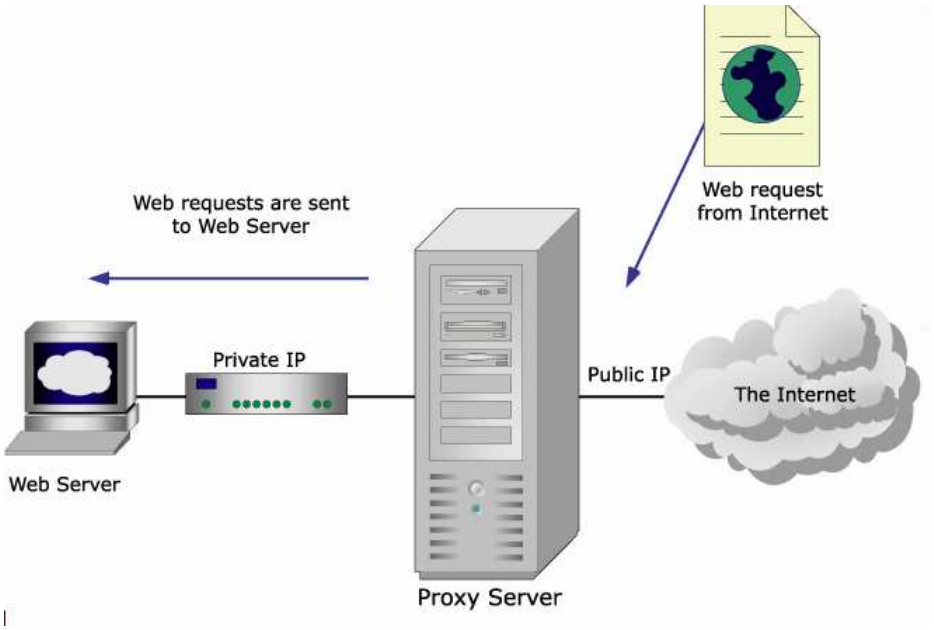

Figura 56: Proxy
Fuente: www.more.net

Si el Sistema Operativo es CentOS se lo instala de la siguiente manera:

yum -y install squid httpd

Si se tiene un sistema con Red Hat™ Enterprise Linux se lo instala de la siguiente manera:

up2date -i squid httpd

[28] Significa que es transparente para los hosts clientes de este servicio, cuando no es transparente se tendrá que configurar el servicio de Proxy en el navegador, mientras que con este servicio no hace falta.

Con iptables se puede generar reglas necesarias para el Enmascaramiento de IP. Que viene ya instalado en el Kernel. Para CentOS.

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf.

Squid esta compuesto por mas de 3000 lineas de codigo, que configuran varios parámetros por defecto. Para las pruebas se cambiaran los siguientes:

- Puerto para Squid
  De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.
- Cache_mem.
  El parámetro cache_mem establece la cantidad de memoria para:

  - Objetos en Transito
  - Objetos frecuentemente utilizados
  - Objetos negativamente almacenados en cache

  El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos frecuentemente utilizados y aquellos negativamente almacenados en el caché podrán utilizar la memoria no utilizada hasta que esta sea requerida.
- cache_dir
  El parámetro cache_dir se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. Se puede incrementar el tamaño del caché. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. En la línea de ejemplo el 8000 significan 8000 MB de cache, los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno.
- Listas de Control de Acceso

Si la lista de control de acceso abarcará a toda la red local se define la IP correspondiente a la red y la máscara de la sub-red.

También puede definirse una Lista de Control de Acceso especificando un fichero localizado en cualquier parte del disco duro, y la cual contiene una lista de direcciones IP.

- Reglas de Control de Acceso
  Las reglas de control de acceso definen si se permite o no el acceso hacia Squid.
- httpd_accel_host
- httpd_accel_port

El detalle de las lineas de codigo afectadas para cada uno de los parametros se encuentran en el **ANEXO3.**

3.4. PRUEBAS DE FUNCIONAMIENTO

Teniendo a la mano el estudió del funcionamiento de Linux en un sistema inalámbrico, se ha buscado hardware y software para probar como trabaja y si este sistema de estudio es estable para aplicaciones de laboratorio.

Para las pruebas se ha usado un equipo con las siguientes características:

- Mainboard. Biostar U8638
- Procesador: Intel Pentium 4, 1.6 Ghz, 256 KB de cache.
- Memoria RAM: Markvision de 256 MB.
- Disco Duro: Samsung de 80 GB.
- Optico: Samsung 52X
- Tarjeta Red: 10/100 Mbps. Incorporada
- MODEM: 56 kbps incorporada
- Tarjeta Inalámbrica: DLINK DWL-G520 de 54 Mbps (con chipset Atheros compatible con MadWIFI).
- Sistema Operativo: Centos 4.4 con Kernel 2.6.9-42

El sistema completo consta de lo siguiente:

- Equipo Servidor de pruebas.
- 2 equipos Wireless con sistema operativo Windows XP.
- Equipos no Wireless para conexión por cable.
- Switch para la conexión de los equipos no inalámbricos.
- Conexión a Internet.

Los parámetros de Red que usarán para pruebas según modo de operación son las siguientes:

- Managed:
  - Segmento de Red 192.168.10.0
  - Máscara 255.255.255.0
  - Servidor Gateway: 205.235.2.205
  - Equipo de Pruebas 192.168.10.15
  - DNS 205.235.2.130 205.235.2.131

En el caso de colocar un DHCP Server:

- DHCP Server: 192.168.10.177
- ESSID: TesisAP del Access Point al cual depende.
- Master:
  - Segmento de Red 192.168.10.0
  - Máscara 255.255.255.0
  - Servidor Gateway: 205.235.2.205
  - Equipo de Pruebas puerto 192.168.10.15
  - DNS 205.235.2.130 205.235.2.131
  - ESSID: TesisWiFi.
- Ad-hoc (Modo para Ruteo):
  - Segmento de la Red cableada 192.168.10.0
  - Máscara 255.255.255.0

- Servidor Gateway: 205.235.2.205
- Equipo de Pruebas en su puerto ethernet 192.168.0.17
- DNS 205.235.2.130 205.235.2.131
- ESSID: TesisWiFi.
- Segmento de la Red inalámbrica 192.168.10.0
- Máscara 255.255.255.0

Para el modo Manager se configura los parámetros para ser cliente de un Access Point, quedando la interface inalámbrica de esta manera:

[root@ServerAP ~]# ifconfig

ath0 Link encap:Ethernet HWaddr 00:1B:11:00:DF:1F
inet addr:192.168.10.77 Bcast:192.168.10.255 Mask:255.255.255.0
inet6 addr: fe80::21b:11ff:fe00:df1f/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:70 (70.0 b)

eth0 Link encap:Ethernet HWaddr 00:E0:4C:7F:7B:40
inet addr:192.168.10.177 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: fe80::2e0:4cff:fe7f:7b40/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1031 errors:0 dropped:0 overruns:0 frame:0
TX packets:193 errors:0 dropped:0 overruns:1 carrier:0
collisions:0 txqueuelen:1000
RX bytes:74561 (72.8 KiB) TX bytes:26037 (25.4 KiB)
Interrupt:5 Base address:0xd000

wifi0 Link encap:UNSPEC HWaddr 00-1B-11-00-DF-1F-00-00-00-00-00-00-00-00-00-00
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:199
RX bytes:0 (0.0 b) TX bytes:1260 (1.2 KiB)
Interrupt:3

Para probar que existe una conexión correcta y el equipo se encuentra enlazado, primero se prueba con el comando ping si se tiene repuesta al Access Point y a cualquier equipo de la red:

#Equipo conectado con cableado

```
[root@ServerAP ~]# ping 192.168.10.250
PING 192.168.10.250 (192.168.10.250) 56(84) bytes of data.
64 bytes from 192.168.10.250: icmp_seq=0 ttl=128 time=0.994 ms
64 bytes from 192.168.10.250: icmp_seq=1 ttl=128 time=0.386 ms
64 bytes from 192.168.10.250: icmp_seq=2 ttl=128 time=0.402 ms
64 bytes from 192.168.10.250: icmp_seq=3 ttl=128 time=0.402 ms
```

#Equipo conectado con WIFI

```
[root@ServerAP ~]# ping 192.168.10.15
PING 192.168.10.15 (192.168.10.15) 56(84) bytes of data.
64 bytes from 192.168.10.15: icmp_seq=0 ttl=128 time=0.994 ms
64 bytes from 192.168.10.15: icmp_seq=1 ttl=128 time=0.386 ms
64 bytes from 192.168.10.15: icmp_seq=2 ttl=128 time=0.402 ms
64 bytes from 192.168.10.15: icmp_seq=3 ttl=128 time=0.402 ms
```

De esta menera tenemos una prueba básica de la conexión.

En el modo Manager el equipo de pruebas es un Access Point, configurados los parámetros queda de la siguiente manera:

```
[root@ServerAP ~]# ifconfig
ath0      Link encap:Ethernet  HWaddr 00:1B:11:00:DF:1F
          inet addr:192.168.10.77  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::21b:11ff:fe00:df1f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:70 (70.0 b)

eth0      Link encap:Ethernet  HWaddr 00:E0:4C:7F:7B:40
          inet addr:192.168.10.177  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::2e0:4cff:fe7f:7b40/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1031 errors:0 dropped:0 overruns:0 frame:0
```

TX packets:193 errors:0 dropped:0 overruns:1 carrier:0
collisions:0 txqueuelen:1000
RX bytes:74561 (72.8 KiB) TX bytes:26037 (25.4 KiB)
Interrupt:5 Base address:0xd000

wifi0 Link encap:UNSPEC HWaddr 00-1B-11-00-DF-1F-00-00-00-00-00-00-00-00-00-00
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:199
RX bytes:0 (0.0 b) TX bytes:1260 (1.2 KiB)
Interrupt:3

Para que el equipo se convierta en un servidor de entrega de direcciones IP, se configura el dhcp.conf **ANEXO1**.

Las pruebas en este modo consisten en conectar al menos dos equipos inalámbricos con el ESSID configurado en el equipo Access Point. EL cliente puede tener configurado manualmente los parámetros IP, caso contrario dependería del Access Point para tener estos parámetros, si es así, se debe verificar primero si ha sido configurado automáticamente estos parámetros. De esta manera se comprueba que existe conexión con el equipo en modo Master.

Se realiza la prueba básica de respuesta de conexión con el comando ping, tanto al equipo de prueba en modo Master como a un equipo inalámbrico y un equipo por cable.

```
[root@ServerAP ~]# ping 192.168.10.250
PING 192.168.10.250 (192.168.10.250) 56(84) bytes of data.
64 bytes from 192.168.10.250: icmp_seq=0 ttl=128 time=0.994 ms
64 bytes from 192.168.10.250: icmp_seq=1 ttl=128 time=0.386 ms
64 bytes from 192.168.10.250: icmp_seq=2 ttl=128 time=0.402 ms
64 bytes from 192.168.10.250: icmp_seq=3 ttl=128 time=0.402 ms
```

Si existe en la red algún gateway que nos conecte a Internet, también se puede probar con un navegador de Internet.

Con el modo Ad-hoc se ha probado al equipo de prueba como un ruteador inalámbrico o como gateway hacia el Internet. Además de la configuración tradicional del modo Ad-hoc también se debe configurar los diferentes servicios como son la de Proxy y Firewall.

Los equipos clientes tanto inalámbricos como por cable que dependen de el equipo de prueba pueden tener dirección IP fija o automática, para lo segundo el equipo de prueba deberá tener configurado el DHCP Server, **ANEXO1**.
Se realizan las mismas pruebas de conectividad con el comando ping hacia el equipo de prueba y otros clientes inalámbricos o por cable que dependan de el.

```
[root@ServerAP ~]# ping 192.168.10.250
PING 192.168.10.250 (192.168.10.250) 56(84) bytes of data.
64 bytes from 192.168.10.250: icmp_seq=0 ttl=128 time=0.994 ms
64 bytes from 192.168.10.250: icmp_seq=1 ttl=128 time=0.386 ms
64 bytes from 192.168.10.250: icmp_seq=2 ttl=128 time=0.402 ms
64 bytes from 192.168.10.250: icmp_seq=3 ttl=128 time=0.402
```

Para configurar el Proxy se usa el archivo squid.conf y se levanta el servicio, **ANEXO2**.

De esta manera el equipo de pruebas hara cacheo de contenido web y entregará permisos tipo Internet Firewall como:

- Accesibilidad por cliente.
- Accesibilidad por Direccionamiento IP.
- Accesibilidad de Contenido.
- Accesibilidad por tiempo de conexión.

Por último se puede generar un archivo ejecutable donde se pueden configurar otras opciones de seguridad y accesibilidad. En el equipo de pruebas se ha creado un archivo donde se ejecutarán varias reglas de conectividad y permisos como firewall, además que se han aumentado las líneas para subir los servicios de red necesarios para que en modo Ad_hoc trabaje como ruteador ANEXO3.

Una vez concluidos los procesos anteriores se prueba la conectivida hacia otras redes e Internet, así mismo que cada uno de los permisos configurados esté funcionando.

3.5. ANÁLISIS TÉCNICO Y ECONÓMICO

3.5.1. FACTIBILIDAD TÉCNICA

Actualmente Linux tiene soporte sobre una gran cantidad de hardware, sin embargo, no es total. Donde normalmente se encuentra problemas es sobre el soporte a tarjetas de video o sonido, sin embargo, para lo propuesto en este proyecto eso no es crítico.

El soporte a dispositivos de almacenamiento es muy amplio, no habiendo a este nivel problemas para cargar el sistema operativo. Simplemente se debe tener en cuenta un detalle, para la tecnología PATA[29] o conocida como IDE el soporte es total, pero para la tecnología SATA[30] el Kernel que lo soporta es el 2.6.x, aunque algunas versiones anteriores tienen parches.

A nivel de tarjetas de red el soporte es muy amplio, sobre todo a las tarjetas ethernet. Sin embargo, para tarjetas inalámbricas no todas son soportadas y en el mercado todavía se ve restringido en cierta manera el obternerlas.

El modelo usado en este proyecto es una de las más difundidas por el fabricante DLINK, pero como se pudo apreciar, existe una lista de compatibilidad muy pequeña frente a la infinidad de fabricantes y modelos de estos dispositivos que existen en el mercado.

Teniendo el hardware compatible con la versión de Linux con el cual se desea trabajar, ya es solamente cuestión de configurar y subir los servicios que se desean.

---

[29] Dispositivos de Almacenamiento que tienen bus de comunicación paralelo hacia el mainboard del computador

[30] Dispositivos de Almacenamiento que tienen bus de comunicación Serial hacia el mainboard del computador

Con Linux se puede tener un mejor control del tráfico de la red, la seguridad y el acceso a recursos. Se pueden tener muchas caraterísticas avanzadas a nivel de servicios y ser personalizadas según la demanda de la red. Adiconal a los servicios básicos de DHCP, Proxy y Firewall que un equipo de accesibilidad inalámbrica puede dar, también Linux podría entregar servicios de Web Server, Mail Server, DNS Server, Servidor de Archivos e Impresión entre otros, caraterísticas que dispositivos de acceso inalámbricos no tienen.

3.5.2. FACTIBILIDAD ECONÓMICA

Actualmente se tienen muchas opciones en el mercado para accesibilidad inalámbrica como Access Points y Ruteadores Inalámbricos.
Los más económicos que simplemente dan accesibilidad y entregan pocas características en lo que es seguridad, accesibilidad y cifrado, estos equipos están mas enfocados para el hogar o pequeñas empresas. Su costo está fluctuando entre los $50 dólares y los $200.

Equipos más avanzados pueden llegar a csupererar los $1000 dólares, estos son muy completos con caraterísticas muy especializadas.
Una Desktop (computador de escritorio) de última generación puede llegar a costar desde $400 dólares y llegar a superar los $1000 dólares. Hardware de servidor igualmente puede costar desde $800 dólares en adelante. Cualquiera con las características inalñambricas necesarias.

Viéndolo de esta manera, adquirir un hardware de última generación para cargar Linux y configurarlo solamente como un punto de conectividad inalámbrica como un access Point o un Ruteador Inalámbrico es costoso, además que se subutiliza la capacidad del sistema. Tomando en cuenta se que puede encontrar harware especializado para este objetivo a costos muy económicos.

En contraste, si el objetivo del sistema es dar varios servicios y entre ellos está el de conectarse a una red inalámbrica o dar acceso inalámbrico puede ser muy provechoso.

Sin embargo, en las pruebas realizadas el equipo usado no es de última generación. Más bien se ha usado un equipo que su tecnología ha caducado, aunque puede ser utilizado para las opciones básicas de un computador de escritorio, pero sus características son muy bajas para soportar de manera rápida y eficiente o simplemente no soportar la mayoría hadware o software que se tiene en el mercado actualmente.

Esto puede mostrar una manera de aprovechar hardware, dándole un uso específico y con una buena respuesta para un sistema de Red con apenas una inversión de $40 dólares que cuesta una tarjeta de red inalámbrica compatible. Se tienen precios de tarjetas inalámbricas desde $40 dólares hasta alrededor de los $200 dólares. Siendo una buena opción a harware que se está por desechar.

CUADRO DE FACTIBILIDAD ECONOMICA

	AP	**ROUTER**	**SERVER**
PROYECTO	400	400	400
DLINK	60	100	-
CISCO	200	600	-
SERVER	-	-	SOBRE 1000

Tabla 10: Comparación precios de Harward con utilizados en el Proyecto

3.5.4. FACTIBILIDAD LOGISTICA

La logística de un sistema como estos, dependerá de la ubicación de los equipos que lo compondrán.

Los equipos que lo componen son computadores personales. Uno que es el Linux que se usara como punto de acceso, los hosts inalámbricos y los hosts que se conectarán por cable. Además todo aquel dispositivo de conectividad como pueden ser switches para dar puertos de acceso a cada uno de los host por cable. Además están los materiales que se usan para dicha conectividad y ubicación de los equipos, como son el cableado, muebles, canaletas, cajetines, etc. Es decir, todo lo necesario para crear una habitación de trabajo.

Al equipo Linux configurado como punto de acceso se lo deberá colocar en un lugar estratégico, generalmente céntrico a todos los host inalámbricos, para que la potencia de la señal sea onmidireccional a la geografía de la habitación donde se la está colocando.

Si se desea que el área de cobertura sea mayor, se colocarán igualmente antenas de mayor ganancia y en línea de vista a los dispositivos que se quieren conectar a la red inalámbrica.

3.5.4. FACTIBILIDAD OPERATIVA.

Se ha podido observar como se configura un sistema de este tipo, que equipos se pueden usar y cuanto cuesta ponerlo en marcha, por último como montarlo. Es decir, como ponerlo operativo.

Los sistemas basados en Linux son flexibles y muy estables, lo que significa que el mantenerlo operativo es a largo plazo. Esto nos da confiabilidad en el sistema

El soporte de hardware para Linux cada vez es más amplio, lo que significa que se tendrá mayor soporte a nuevas plataformas. De esta manera, el cambio de hardware a nivel de equipos, partes y piezas no es una limitante para parar un sistema.

Toda configuración en Linux puede ser guardada, de esta manera se puede cargar en otro harware los parámetros del sistema. Esto sirve para el mantenimiento del sistema y para tener control sobre fallas.

En general, el mantenimiento es mucho más simple actualmente para Linux y sus costos bajos.

A continuación se colocará una tabla de comparación de las factibilidades entre varios fabricantes y el sistema del proyecto.

CUADRO COMPARATIVO DE COSTOS ACCESS POINT-ROUTER

	PROYECTO	DLINK ACCESS POINT2100	DLINK DI-524	CISCO 878W	CISCO AIRONET 1200
HARDWARE	200	60	100	600	200
SISTEMA OPERATIVO	0	0	0	0	0
MADWIFI	0	0	0	0	0
CONFIGURACION	100	50	70	200	100
TARJETA DE RED INALÁMBRICA	40	0	0	0	0
MANTENIMIENTO ANUAL	60	150	150	100	100
TOTAL	400	260	320	900	400

CARACTERISTICAS				
Access Point-Router	Access Point	Access Point Router	Access Point Router	Access Point
Proxy Server	DHCP Server	DHCP Server	VPN	DHCP Server
DHCP Server	Security	Security	Management	Security
Firewall	Management	VPN	DHCP Server	Management
QoS		Management	Firewall	
Hardware nivel bajo		Firewall	Security	
Software Server-Descktop			NAT	
Security				
VPN				
Management				
NAT				

Tabla 11: Comparación

CONCLUSIONES Y RECOMENDACIÓNES.

CONCLUSIONES

- Todos los equipos que conforman la red inalámbrica deben tener los mismos estandares de comunicación para evitar problemas de compatibilidad, al momento de la instalación.
- La tarjeta inalámbrica que se escoja necesariamente debe incluir chip atheros, este permite el modo de operación *master*, y que el dispositivo trabaje como Acces Point.
- DHCP al ser configurado en la misma tarjeta de red inalambrica, por medio de la creación de una tarjeta virtual, no presenta problemas hasta con 2 equipos, si se conectan más equipos, se satura el canal de Internet en el switch lo que retarda el tiempo de respuesta, lo óptimo es lograr una distribución de carga.
- Al ser el servicio Proxy la base del proyecto, a éste se le asigna la más alta prioridad de ejecución, de esta manera esta dedicado a la distribución de Internet, cualquier otro proceso se ejecuta cuando ya no existan peticiones del servicio.
- Madwifi y Squid permiten una configuración fácil, rápida y económica de los servicios requeridos en el proyecto.
- Las configuraciones realizadas estan previstas en equipos que no van ha ser desconectados constantemente, en cambio los equipos del caso de estudio van a estar en constante encendido y apagado razón por la cual se a creado el script *reglas.sh* el cual contiene lineas de codigo para levantar los servicios de red en modo Ad_hoc para que trabaje como ruteador, opciones de seguridad, accesibilidad y prioridad, reglas de conectividad y permisos, y puede ser ejecutado en cualquier momento.
- Los cambios de configuración que se requiera después de la instalacion pueden realizarse mientras los servicios estan ejecutandose, sin necesidad de suspender los mismos y sin perdida de tiempo con el comando
  Squid –k rc configure

- Todo el sofware utilizado en el proyecto está libre del pago de costosas licencias por uso, o restringidas a determinado número de usuarios, lo que lo diferencia de otros sistemas operativos y equipos que prestan el mismo servicio.

RECOMENDACIONES

- Escoger las herramientas adecuadas tanto de hardware como de software compatible con Linux, reduce el tiempo de desarrollo.
- Verificar las características del hardware que se necesita para que el software funcione.
- Escoger la tarjeta inalámbrica con chip atheros, esta característica permite que el software madwifi cargue los drivers necesarios para la configuración del servicio wireless, sin embargo de recomienda investigar otros fabricantes.
- Antes de configurar madwifi se deben eliminar todas las tarjetas instaladas por defecto, pues causa conflictos con las existentes.
- El servicio de DHCP debe ser configurado en una tarjeta virtual inalámbrica de ser posible, para evitar que el canal de comunicación se sature.
- Squid requiere al menos una lista de control de acceso y una regla de control de acceso en su configuración.
- Limitar en el Firewall los puertos que permiten el acceso de intrusos.
- Utilizar enmascaramiento de IP para utilizar Squid como servidor de protocolos smtp, pop3, etc.
- Realizar un respaldo de la configuración de la configuración de la tarjeta y del servicio Proxy.
- En entornos de bajo presupuesto la implementación de este proyecto es ideal, pues dado su bajo costo de desarrollo y mantenimiento es la alternativa ideal a las soluciones hardware convencionales.
- Idealmente la instalación del Acces Point bajo Linux funciona en hardware tipo clon, sin embargo para entornos de mayor exigencia, equipos de marca representan buen rendimiento.
- El desarrollo de proyectos y prototipos de este tipo deben fomentarse, pues debido a su “facilidad” de construcción y bajos costos se alinean a la política de estado del actual presidente.

BIBLIOGRAFIA

Artículos:

"La hora de las LAN inalámbricas", Comunicaciones World Noviembre 2001.

"Redes Ciudadanas libres", Comunicaciones World Marzo 2002
Adolfo Vázquez.

"Llega el Linux de las comunicaciones", PC Actual Abril 2002
Javier Renovell Gómez.

"CCNA Material", Cisco Systems.

Webs:

http://www.wi-fi.org

http://www.freenetworks.org

http://www.fatamorgana.com/bertolinux/wireless/english/wireless.HOWTO.html

http://es.wikipedia.org

http://www2.canalaudiovisual.com/ezine/books/acREDES/2redes02.htm

http://www.arsys.es/ayuda/directorio/infraestructura-tecnica/red-datos.htm

http://www.boker.cl

http://www.system-net.net

http://www.jaht.com

http://www.comtec-comms.com

http://www.alaide.com

http://www.intelprima.com

http://www.computerhope.com

http://www.wlana.org/learn/educate.htm

http://www.unincca.edu.co/boletin/indice.htm

http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

http://www.intel.com/ebusiness/strategies/wireless/wlan/standards.htm

https://www.riu.unam.mx

https://www.monografias.com

http://bulma.net

http://www.radioptica.com

http://www.etse.urv.es

http://www.atrpms.net/dist/fc6/madwifi

http: / /atheros.rapla.net

https://www.sourceforce.net

http://www.linuxparatodos.net/portal/staticpages /index.php?page=19-0-como-squid-general. Squid

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS