DECLARACIÓN JURAMENTADA

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

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

……

PABLO DAVID PROAÑO GALARZA

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado

DISEÑO E IMPLEMENTACIÓN DE UN PORTAL CAUTIVO UTILIZANDO UN ENRUTADOR INALÁMBRICO DE BAJO COSTO Y UN SISTEMA OPERATIVO DE CÓDIGO ABIERTO.

Realizado por el alumno

PABLO DAVID PROAÑO GALARZA

Como requisito para la obtención del título de

INGENIERO EN SISTEMAS DE INFORMÁTICA Y REDES DE INFORMACIÓN.

Ha sido dirigido por el profesor

Ing. DAVID GONZÁLEZ

Quien considera que constituye un trabajo original de su autor.

……

Ing. DAVID GONZÁLEZ

Director

Los profesores informantes

Ing. Viviana Guerrón Sierra, e

Ing. Santiago Mena

Después de revisar el trabajo escrito presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador.

..... ……..

Ing. VIVIANA GUERRÓN SIERRA Ing. SANTIAGO MENA

DEDICATORIA

Hace tanto tiempo que he esperado el momento de poder colocar la última piedra a este proyecto, un proyecto de mucho esfuerzo y sacrificio, de noches sin dormir y de resultados satisfactorios. Sin embargo no lo hubiese conseguido, sin las constantes bendiciones de mi Dios, el cual ha iluminado toda mi vida, y que me ha escuchado en momentos buenos y malos. Que sería de mí, sin las protecciones de la Virgen de Guadalupe, que me ha protegido constantemente en mis caídas, y me ha levantado. De la misma manera, mi Madre, Yolanda Galarza, que de su mano he avanzado por los caminos de la vida, que jamás me ha dejado solo y que me ha ayudado increíblemente, sin dudarlo, sin descansar, esforzándose para que yo y mi hermana alcancemos el éxito, es imposible describir todo lo que le agradezco a mi madre, sin embargo algo que puede valer es: gracias mamita, sin ti no podría escribir estas palabras. Mi hermana Katya Parada, qué más puedo pedir que una mejor amiga en casa, una niña que me llena de felicidad todos los días, que me ayuda con su inteligencia en todos mis proyectos, y que me escucha siempre. Mi padre Pablo Proaño, aun que a veces muy alejado por razones que así quiso la vida, me ha dado tanto conocimiento, de este mundo y de otros, además de ponerme en el lugar y en el momento indicado para aprovechar las oportunidades, me ha enseñado, que si quiero algo, tengo que conseguirlo yo mismo. Carlos Parada, mi segundo padre, el cual me apoyo muchos años y que me ha enseñado tantas cosas, pero la más importante: superación. A mis Abuelitos y a mis tíos que me han protegido desde pequeño.

Esto es un pequeño pago que yo puedo hacer por el sufrimiento que le causé a mis seres queridos hace algunos años, gracias a todo su apoyo puedo llegar a escribir estas palabras.

Para finalizar, recuerdo que mi abuelito Alberto, algún día me dijo que él iba a estar conmigo hasta que yo me graduara y que no me preocupara, pues aun que no es así, se que el cuida de mí y de mi familia en todo momento, esto es para usted.

AGRADECIMIENTOS

Gracias a la Universidad Internacional SEK por abrirme sus puertas. A la Ingeniera Viviana Guerrón, por creer en mí y a mi tutor David González por su apoyo en este proyecto tan significativo en mi vida.

Mi familia es muy extensa, y tendría que escribir un documento igual de grande para describir todo lo que han hecho en mi vida. Sin embargo, el día de hoy tengo a gran parte de ellos reunidos en mi casa, gracias a todos ustedes, gracias a mis abuelitos, a mis tios y primos.

Gracias a mi primo Daniel, que siempre camina a mi lado, en todos los momentos de la vida, llegando a ser mí hermano. A mi novia May Martínez que me apoyó desde el inicio de este proyecto hasta su finalización y que hace de mi vida un desafío constante. A mis amigos, los cuales son pocos pero con eso me basta, porque cada uno de ellos me ha entregado parte de su vida.

Mis amigos y compañeros del DRT de la Universidad Israel, Edwin, Santiago, Danny, los cuales me recibieron como un joven con ganas de aprender, y que me apoyaron en todos los momentos de mi vida profesional, de igual forma gracias a Cecilia y Víctor Proaño, que me dieron la oportunidad de demostrar mis capacidades y que dieron inicio a lo que hoy he terminado.

RESUMEN EJECUTIVO

En la actualidad se pueden encontrar Redes Inalámbricas de Área Local (WLAN) en lugares públicos que proveen de internet gratuito, sin embargo estas redes crean una dificultad para los propietarios debido a que la mayoría de ellas no tienen ningún control por estar abiertas. Para ayudar a solucionar de forma económica esta problemática se realizó la modificación de hardware y software en un enrutador inalámbrico de bajo costo, para instalar un *firmware* con un Sistema Operativo de Software libre; en el cual, se implementaron varias herramientas de red, entre ellas la puerta de enlace del sistema de administración y control de redes llamado WifiDog, el cual maneja los usuarios que se conectan a la red, el ancho de banda que consumen y el tiempo que tienen para su uso. Esta puerta de enlace se conecta por internet hacia un único servidor de autentificación, en donde los clientes se registran o inician sesión. La comercialización del enrutador inalámbrico modificado, se prevé hacer con una licencia anual para conectarse a un solo servidor de autentificación, a un bajo costo y dirigido a un nicho de mercado específico.

ABSTRACT

Nowdays the Wireless Local Area Networks (WLAN) are easyly found in public places to provide free internet, however this kind of networks create a difficulty for the owners for the reason that most of them have no control because they are open. To solve this problem in cheapest mode, is necesary make a change in the hardware and the software of a wireless router to install a firmware with a free software operating system, in which, was implemented various network tools, including a Captive Portal called WifiDog, that manage the users connecting to the network, the bandwidth consumed and the time they have to use. This gateway connects to a single internet authentication server, where customers can register or login. The marketing of the amended wireless router is expected to make an annual license to connect to an authentication server, at a low cost and aimed at a specific market niche

ÍNDICE DEL CONTENIDO

ÍNDICE DE ILUSTRACIONES.

ÍNDICE DE TABLAS

CAPITULO I

1.1.INTRODUCCIÓN

En los últimos años los avances tecnológicos han creado equipos de uso móvil que cada vez son más accesibles para los usuarios; como son las computadoras portátiles, las computadoras de bolsillo, los celulares y recientemente las computadoras ultra portátiles que están listas para la conectividad móvil.

El uso de los Puntos de Acceso a internet Gratuitos en lugares abiertos como: cafeterías, centros comerciales, hoteles, restaurantes, plazas e instituciones educativas han ido incrementándose de forma acelerada debido a la gran penetración de los servicios en línea en el último lustro, permitiendo de esta forma a usuarios móviles enlazarse con el mundo de manera gratuita, rápida y sobre todo fácil. Además, los últimos avances en el desarrollo de equipos inalámbricos y su fabricación en serie, han sido elementos claves en el desarrollo de este tipo de tecnologías; sin embargo, dicho crecimiento también ha traído consigo dificultades principalmente relacionadas con la administración de este tipo de redes, debido a que estas manejan requerimientos distintos a las de una red cableada siendo la mayor dificultad el control de acceso y políticas de administración de usuarios.

Cuando se implementa una red inalámbrica gratuita, se tiene que considerar que los usuarios por lo general no son fijos, y solamente permanecen por un tiempo limitado en la red; en consecuencia, se crea un inconveniente para los propietarios, debido que al crear este tipo de redes es necesario realizar un control de funcionalidades de la navegación y

uso de la red hacia los usuarios, fijar políticas para el tiempo de uso del servicio, el ancho de banda que pueden utilizar y restringir aplicaciones y protocolos de alto consumo de recursos; sin embargo, la gran mayoría de propietarios de Puntos de Acceso a internet Gratuitos no tienen conocimientos sobre redes de transmisión de datos, debido a que su uso representa un valor agregado de la organización para el usuario y por otro lado estos lugares habitualmente no tienen la necesidad de contratar a un administrador de red.

1.2. ANTECEDENTES

En el Ecuador las redes inalámbricas gratuitas que se implementan mantienen una configuración básica, la cual consiste en un Punto de Acceso Inalámbrico conectado al equipo del proveedor de internet. Dicha configuración no permite el manejo adecuado de la red, por lo que si se requiere mantener algún control, aparece la necesidad de contratar parcialmente o a tiempo completo a un profesional en redes para que configure y administre la red, y adicionalmente es necesario adquirir un equipo que tenga las capacidades para hacer las funciones de administración, lo que genera un gasto extra. Por otro lado, en caso que la configuración este conectada directamente de un punto de acceso inalámbrico al equipo de conexión a internet, no se tendrá ningún tipo de control para la navegación, usuarios, ancho de banda o servicios y protocolos permitidos, lo que provocara el uso desmedido de los recursos de red.

Existen dos formas de controlar el acceso a una red inalámbrica:

- Dejar el sistema abierto para cualquier usuario.
- Configurar un sistema de seguridad que maneje un esquema de clave compartida, autentificación por dirección física, o algo más complejo y además costoso, como los servidores de inicio de sesión.

1.3. SITUACIÓN ACTUAL

En el mercado de hoy existen soluciones que permiten el control de usuarios, manejo de ancho de banda y otras utilidades de red, las cuales ayudan al control del tráfico que viaja por la red inalámbrica, restringiendo el uso de protocolos que puedan causar una sobre carga en la red, y además protegiendo la privacidad de los usuarios controlando el tipo de información que puede ser enviada y recibida, además de brindar una calidad de servicio en protocolos que requieren una prioridad más alta dentro de la red, como por ejemplo la comunicación a través de Voz sobre IP.

El conjunto de utilidades para el control de la navegación en internet y uso de la red local es conocido como Portal Cautivo; sin embargo, para la configuración dichas utilidades, es necesario tener conocimientos en sistemas operativos tipo servidor, complementados con redes de información y por lo menos un equipo al que se le puedan instalar las herramientas necesarias; por otro lado, en el mercado hay soluciones integrales embebidas que permiten realizar todas estas funciones descritas sin la necesidad de un alto conocimiento de redes, pero el alto costo de estos equipos pone fuera del alcance de la mayoría de los usuarios.

1.4. JUSTIFICACIÓN E IMPORTANCIA

Un portal cautivo es un conjunto de herramientas para la administración de la red, las cuales controlan los servicios y protocolos que pueden ser utilizados como por ejemplo: el ancho de banda asignado por usuario, el tiempo de uso del servicio, control de tráfico que viaja por la red etc. Cuando un usuario intenta establecer conexión para navegar en internet, es redirigido a una página web de autentificación en donde se le solicita credenciales de inicio de sesión; o en su defecto, se le informa las condiciones de uso del servicio inalámbrico, luego de que se haya autentificado podrá hacer uso de la red o del internet.

Existen soluciones de software libre para portales cautivos que permiten su instalación en máquinas con un sistema operativo GNU/LINUX, las cuales funcionan como servidor de autentificación, y los puntos de acceso de red inalámbrica se los instala con una configuración básica; sin embargo, esta configuración puede resultar costosa, debido a que se necesita tener un equipo al que se le pueda instalar un sistema operativo de servidor, conocimientos de dicho sistema operativo y además los puntos de acceso necesarios para dar cobertura inalámbrica.

Una de las ventajas que da el software libre es que se lo puede instalar en máquinas de menores recursos e inclusive en distintas tecnologías de procesador y de arquitectura, lo cual permite realizar migraciones a plataformas distintas a las tradicionales. En el mercado actual existen equipos que funcionan como enrutadores y puntos de acceso inalámbricos, que permiten la instalación de un sistema operativo basado en software libre GNU/LINUX en sus *"chips set*[1]*"* por tener capacidades altas de procesamiento y de memoria, en los que se puede añadir software que este compilado para la tecnología del procesador y para el sistema operativo.

Cuando una organización requiere la implementación de un servidor de portal cautivo basado en software libre, puede optar por la contratación de un profesional de sistemas que tenga conocimiento en esta tecnología y, la adquisición del hardware necesario para su implementación. En la actualidad los profesionales de sistemas calificados, tienen honorarios que se basan en la complejidad de la problemática a resolver.

La solución que se presenta en este proyecto para el control de los puntos de acceso inalámbricos gratuitos, es la instalación de un sistema operativo de software libre basado en GNU/Linux en un enrutador inalámbrico de bajo costo, en donde se configurarán las herramientas necesarias para la administración, control de usuarios, manejo de ancho de banda y otras utilidades de red. Llevará instalado una distribución de GNU/LINUX migrada a la tecnología del procesador, el cual contará con las herramientas de red

1 Procesador y tarjeta madre.

necesarias para la administración, y además se lo podrá adquirir con diferentes modificaciones de hardware para diferentes tipos de servicio, como puede ser la ampliación de memoria. Este enrutador modificado se conectara vía internet a un servidor de autentificación preconfigurado.

El Servidor de Autentificación planteado para este proyecto, manejara a los usuarios y mantendrá las configuraciones de los nodos de portal cautivo en los enrutadores inalámbricos embebidos, permitiendo que el usuario final no deba de preocuparse por el mantenimiento del servidor ni de las configuraciones de red y, por un pago anual de bajo costo podrá disminuir los gastos que representa la adquisición de equipos de autentificación y manejo de redes inalámbricas gratuitas.

Cuando el servicio de portal cautivo ha sido implementado en la red, el propietario o administrador de la organización solo se encarga de realizar configuraciones y tareas de mantenimiento básicas por ejemplo: agregar usuarios, cambiar políticas de ancho de banda o de tiempo permitido para la navegación.

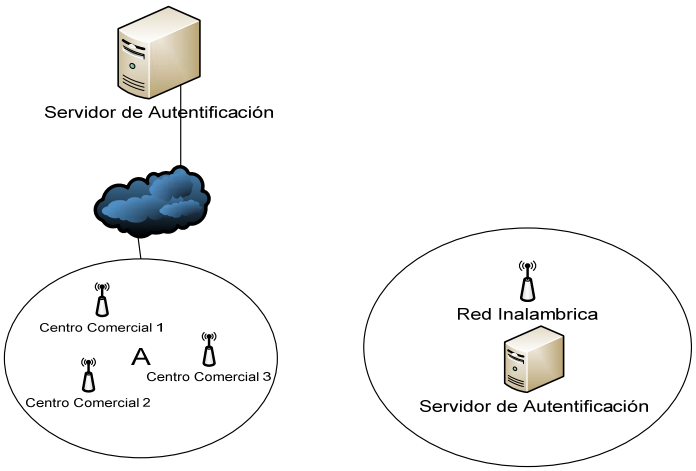


Ilustración 1-1 Diferencia entre una instalación aislada de portal cautivo frente a los múltiples nodos conectados a un solo servidor de autentificación

En la ilustración 1-1 se puede observar la diferencia entre una instalación aislada de portales cautivos, la cual utiliza un servidor de autentificación para cada nodo inalámbrico,

a diferencia de la solución planteada en este proyecto, que utiliza un solo servidor de autentificación para varios nodos que se conectan a él mediante internet.

Tabla 1-1 Comparación estimada de costo entre tipos de instalación de portales cautivos de software libre.

Equipo	Tipo de Configuración	Detalles	Características	Funciones.	Costo Estimado
Punto de Acceso Wifi + Servidor de Portal Cautivo	Avanzada, se requiere conocimiento en redes y sistemas operativos.	Punto de Acceso Inalámbrico D-link Dwl-7100ap	Punto de Acceso Inalámbrico 802.11G, 4 puertos fast ethernet y web access. Acepta un máximo 50 conexiones, (ZonaTecnologica)	El equipo es utilizado como punto de acceso, se conecta al servidor de autentificación,	80$
		Servidor HP Proliant ML150G5 (gama baja)	Quad Core Xeon E5405 2.0GHz; 3GB RAM; DISCO DURO 500GB. (ZonaTecnologica)	El equipo debe tener una configuración de base para servidor: Gnu / Linux, PostgreQSL, PostFix, Apache2, PHP5.	1500$
		Configuración de herramientas necesarias: (estimando 20 horas de trabajo de un profesional en redes que cobre 40 dólares la hora.)	Profesional de sistemas con conocimiento en redes y sistemas operativos de servidor.	Se instala Wifidog (Autentificación y Puerta de enlace) en el servidor.	800$
		Total:			**2380 $ Dólares**
Equipo Embebido de Portales cautivos + Pago de licencia anual	El equipo esta pre-configurado y se enlaza directamente a un solo servidor de portal cautivo accesible desde internet.	Enrutador Inalámbrico WRT54GL. Modificado el firmware para soportar GNU / LINUX.	Enrutador Inalámbrico, 4 puertos Fast Ethernet y 1 puerto Wan. Acepta más de 100 conexiones simultáneas y web Access.	Este equipo conecta la red del cliente con sus 4 puertos LAN y red inalámbrica, re direcciona los intentos de acceso al servidor de autentificación.	200$
		Servidor de Autentificación, conectado a internet con IP publica.	Este equipo es usado para todos los nodos de portal cautivo y su pago es Anual, que se desglosa del costo del equipo.	Equipo configurado con GNU / LINUX, PostgreQSL, PostFix, Apache2, PHP5, Wifidog	100 $
		Total:			**300 $**

Las diferencias de precios estimadas de un enrutador inalámbrico embebido con todas las herramientas necesarias para controlar la red, que va conectado a un solo servidor de autentificación, frente a la adquisición y configuración de un servidor de portal cautivo individual son altas como se puede ver en la Tabla 1-1, por su costo unitario de la configuración por parte de un profesional de sistemas y la compra de un equipo servidor.

1.5.OBJETIVOS

1.5.1. Objetivo General

Implementar un prototipo de servidor de acceso y puerta de enlace embebido con capacidades de portal cautivo utilizando un enrutador inalámbrico de bajo costo con un sistema operativo de software libre y un servidor de autentificación de software libre.

1.5.2. Objetivos Específicos

- Definir el equipo inalámbrico que mejor se adapte en costo y rendimiento para ser utilizado en este proyecto.

- Instalar GNU/LINUX en un equipo enrutador inalámbrico de bajo costo.

- Agregar las herramientas necesarias para la administración que sean utilizadas mediante el explorador web y que además permita la navegación con perfiles de usuario, calidad de servicio, control de ancho de banda y control de navegación.

- Implementar un servidor de autenticación.

- Realizar la instalación del portal cautivo embebido de bajo costo en una zona donde sea factible realizar pruebas con diferentes tipos de usuarios.

- Comparar las ventajas de un portal cautivo embebido en un equipo de bajo costo frente a soluciones del mercado e implementaciones en equipos servidores.

1.6. DELIMITACIÓN DEL TEMA

El alcance de la implementación de este proyecto con fines de pruebas y para su demostración se limitará a:

- 1 enrutador y punto de acceso conectado a internet.
- Un servidor en donde se instalara el servidor de autenticación conectado a internet.
- 10 usuarios para pruebas.

1.7. DISEÑO METODOLÓGICO

1.7.1. Investigación Exploratoria.

Para el desarrollo de este proyecto se ha utilizado la Investigación Exploratoria debido a que en la Universidad Internacional SEK no existen investigaciones previas sobre el objeto de estudio, y por lo tanto se requiere explorar e indagar, con el fin de alcanzar el objetivo planteado.

Explorar significa incursionar en un territorio desconocido. Por lo tanto, se utilizará la investigación exploratoria cuando no se conoce el tema por investigar, o cuando nuestro conocimiento es impreciso, lo cual impide obtener conclusiones adelantadas. La investigación exploratoria termina cuando, a partir de los datos recolectados, se adquiere el suficiente conocimiento como para saber qué factores son relevantes al problema y cuáles no.

1.7.2. Recolección de datos

Se recolectará datos progresivamente mientras se vaya modificando el hardware y software del enrutador inalámbrico. Además se utilizara el apoyo de libros de modificación de hardware y de documentación de libre circulación de la comunidad de software libre.

1.7.3. Metodología de investigación

Se utilizará metodologías de la investigación que permitan obtener información, utilizando el método HIPOTÉTICO-DEDUCTIVO ya que en él se plantea una hipótesis que se puede analizar deductiva o inductivamente y posteriormente comprobarla experimentalmente, es decir que se busca que la parte teórica no pierda su sentido, por ello la teoría se relaciona posteriormente con la realidad.

La deducción, tiene a su favor que sigue pasos sencillos, lógicos y obvios que permiten el descubrimiento de información que se pasa por alto; por otro lado, en la inducción se encuentran aspectos importantes a tener en cuenta para realizar una investigación como por ejemplo la cantidad de elementos del objeto de estudio, que tanta información se puede extraer de estos elementos, las características comunes entre ellos, etc.

CAPITULO II

2. INTRODUCCIÓN A LAS REDES INALÁMBRICAS DE ÁREA LOCAL

2.1. REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN)

En los últimos años las redes de área local inalámbricas WLAN (*Wireless Local Area Network*) han ido ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad utilizar cables para estar conectados a un determinado lugar.

Con las WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas.

Pero no solamente encuentran aplicación en las empresas, sino que su extensión a ambientes públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (Hotspots) en las próximas redes de tercera generación (*3G*) se ven como las aplicaciones de más interés durante los próximos años.

Las nuevas posibilidades que ofrecen las WLANs son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

2.2. VENTAJAS DE LAS REDES INALÁMBRICAS.

Las redes inalámbricas proporcionan a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público en el que están desplegadas.

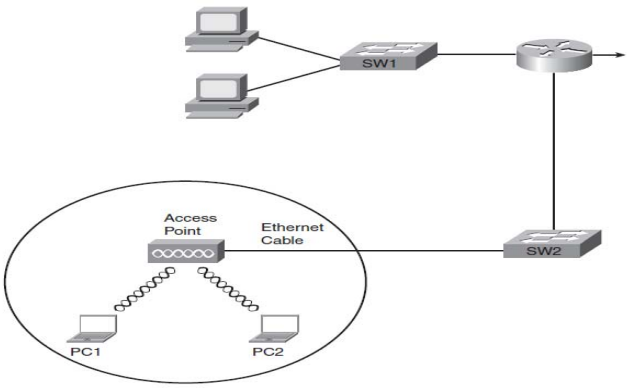
Según un estudio de IDC (International Data Corporation)[2], en el tercer trimestre del 2008 se produjo el punto de inflexión a partir del cual los fabricantes de equipos informáticos empezaron a enviar más equipos portátiles que de sobremesa en todo el mundo. En 2009, los trabajadores móviles constituyen el 26,8% de los recursos de trabajo mundiales, cifra que llegará al 30,4% para el año 2011 o, lo que es lo mismo, alrededor de mil millones de empleados[3]. Esta transición despeja todas las dudas sobre la preferencia de los usuarios a ser más móviles, ya sea para trabajar mientras viajan o, sencillamente, en casa.

Tal y como confirma un estudio de Aberdeen Group[4], el 52% del total de los recursos humanos no trabajan en las oficinas centrales corporativas. Los constantes cambios a los que las estructuras empresariales están sometidas son un elemento de presión para los profesionales de TI a la hora de proporcionar una infraestructura segura y flexible de conexión de los usuarios remotos y las sucursales, cuidando al mismo tiempo de no aumentar los costos.

2 IDC Worldwide Quarterly PC Tracker, diciembre de 2008
3 Fuente: http://www.aberdeen.com/summary/report/benchmark/4637-RA-branch-office-network.asp
4 IDC, "Worldwide Mobile Worker Population 2007–2011 Forecast," doc. nº 209813, diciembre de 2007

El IEEE (*Electrical and Electronics Engineers*) define las normas para las Redes Inalámbricas de Área Local (WLAN), utilizando la familia de redes 802.11 WLAN. Esta norma define el formato de un marco con una cabecera y portadora, con el encabezado incluido y la dirección *MAC* de destino, cada uno en 6 bytes longitud.

La instalación de una WLAN es rápida, fácil y elimina la necesidad de extender cables a través de paredes y techos. La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada. Los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas.



[5]

Ilustración 2-1 Ejemplo de una red WLAN en una cafetería

En el grafico anterior se puede observar que la cafetería ofrece acceso gratuito a Internet a través de redes WLAN al mismo tiempo que permite la conectividad de los dispositivos de que utilizan la misma red para la comunicación hacia el internet

La mayor diferencia entre las redes inalámbricas WLAN y las redes cableadas LAN radica en el hecho de que las redes WLAN usan ondas de radio, para transmitir datos, mientras que Ethernet usa señales eléctricas que fluyen a través de un cable de cobre (o de fibra óptica). Las ondas de radio pasan a través del espacio, por lo que técnicamente no es

[5] (Cisco Systems, 2008)

necesario un medio de transmisión física. Sin embargo, la presencia de objetos físicos como: paredes, objetos metálicos, y otros obstáculos, se interpone en el camino de las señales de radio inalámbrica. Para manejar el uso de las frecuencias las WLAN se utiliza el algoritmo "Carrier Sense Multiple Access With Collision Avoidance" (CSMA / CA) el cual se está explicado en el capitulo 2.4.2 para aplicar la lógica y evitar el mayor número de colisiones posibles[6].

2.3. PUNTOS DE ACCESO INALÁMBRICOS GRATUITOS (HOTSPOTS).

Los Puntos de acceso Inalámbricos Gratuitos o Wifi Hotspots son soluciones inalámbricas diseñadas para servir a algún tipo de establecimiento, como una cafetería, tienda de libros, los aeropuertos, lobby de hotel o cualquier otro establecimiento que preste servicios a las a los clientes que son transitorios en ese lugar.

Un Hotspot inalámbrico generalmente está configurado de tres formas: la primera se la utiliza abriendo la señal de la red inalámbrica para compartir el punto de acceso a internet gratuitamente sin poner ningún tipo de protección o sistema de autentificación que permita solamente a los usuarios registrados ingresar a la red. Los administradores de Hotspots abiertos sin ningún tipo de control tal vez no estén conscientes del peligro que corren, tanto ellos como quienes se conecten a la misma.

La segunda forma de configuración de un Hotspot es establecer contraseñas compartidas de acceso, las cuales son entregadas previa solicitud de las mismas a los clientes, sin embargo esta configuración no resulta ser la más adecuada por que se utiliza una sola contraseña, y puede ser distribuida sin control. La tercera forma de configuración es la

6 (IEEE, 2004)

implementación de un servicio de autentificación individual por equipo o cliente, el cual puede ser RADIUS, LDAP[7] o un Portal Cautivo.

Existe un problema al momento de dejar un Hotspot sin ninguna autentificación ya que no hay ningún tipo de control ni de seguimiento a los usuarios. Por lo que, muchas personas pueden tener intenciones maliciosas y lucrativas.

Para garantizar la privacidad de los demás usuarios que utilizan las redes inalámbricas gratuitas es necesaria la implementación de algún servicio que controle el uso de la red, a los usuarios y los permisos y restricciones a los que deben de someterse para utilizar estas redes.

2.4. MODOS DE OPERACIÓN EN REDES INALÁMBRICAS IEEE 802.11

En 1997, el IEEE aprobó el primer estándar IEEE Std 802.11-1997 para redes WLAN. Esta norma fue define una subcapa de control de acceso al medio (MAC por sus siglas en ingles) y tres capas físicas. Las capas físicas utilizan la banda base de la Infrared (IR), Frequency Hopping Spread Spectrum (FHSS) en la banda de 2,4 GHz, y un espectro ensanchado por secuencia directa (DSSS) a una velocidad entre 1 y 2 Mbps de operación[8].

De las organizaciones que figuran en la tabla 2-1, IEEE desarrolla las normas específicas para los diferentes tipos de redes WLAN que se utilizan actualmente. Estas normas deben tener en cuenta la frecuencia de las opciones escogidas por los diferentes organismos reguladores en todo el mundo, como la FCC en los EE.UU. y de la UIT-R, que en definitiva está controlada por las Naciones Unidas (ONU).

7 LDAP (Lightweight Directory Access Protocol) es un protocolo que permite el acceso a un servicio de directorio distribuido para buscar diversa información en un entorno de red
8 (IEEE, 2004)

Tabla 2-1 Roles de las organizaciones en la estandarización del 802.11

Organización	**Rol en la estandarización.**
ITU-R	La normalización de las comunicaciones en todo el mundo que utilizan la energía radiada, en particular la gestión de la asignación de frecuencias
IEEE	Estandarización de Redes Inalámbricas de Área Local WLAN 802.11
Wifi-Alliance	Un consorcio de la industria que fomenta la interoperabilidad de los productos a los que aplican sus normas a través de WLAN. Atreves del programa de certificación Wi-Fi concede certificados de operatividad.
Federal Communications Commission (FCC)	La agencia gubernamental de los Estados Unidos que regula el uso de varias frecuencias de comunicación en ese país.

IEEE ha ratificado cuatro principales normas WLAN: 802.11, 802.11a, 802.11b, 802.11g. En la Tabla 2-2 se enumeran los detalles básicos de cada WLAN estándar.

Tabla 2-2 Estándares actuales de 802.11

Características	**802.11a**	**802.11b**	**802.11g**
Año de ratificación	1999	1999	2003
Velocidad Máxima utilizando DSSS	-	11 Mbps	11 Mbps
Velocidad máxima utilizando OFDM	54 Mbps	-	54 Mbps
Banda de Frecuencia	5 GHz	2.4 GHz	2.4 GHz
Canales (sin superposición)	23 (12)	11 (3)	11 (3)
Velocidades requeridas por el estándar	6, 12, 24	1, 2, 5.5, 11	6, 12, 24

2.4.1. Arquitectura en el Estándar IEEE 8002.11

La arquitectura de la IEEE 802.11 WLAN está diseñada para apoyar una red donde la mayoría de la toma de decisiones se distribuye a las estaciones móviles. Esta arquitectura tiene varias ventajas, además de ser muy tolerante de las fallas en todos los equipos de la WLAN y la eliminación de los posibles cuellos de botella en la red. La arquitectura es muy flexible, puede soportar redes pequeñas transitorias y las grandes redes permanentes o semipermanentes. Además, Modos de operación para ahorro de energía de operación se basan en la arquitectura y protocolos para prolongar la duración de la batería de los equipos móviles, sin perder la conectividad de red. La arquitectura IEEE 802.11 incluye varios componentes: la estación, el Punto de Acceso (AP, Access Point), el medio inalámbrico, el conjunto de servicios básicos y la extensión del conjunto de servicios. La arquitectura también incluye la estación de servicios y los servicios de distribución.

La arquitectura 802.11 incluye un nivel de multi dirección que no ha estado presente en anteriores LAN. Este nivel de multi dirección, ofrece la capacidad de que un equipo pueda movilizarse a lo largo de una WLAN aparentando estar físicamente conectado por cable. En otras palabras, este nivel aparenta usar un largo cable que le permite al equipo dejar de ser estacionario. Esta modificación realizada por IEEE 802.11 permite que todos los protocolos de red existentes puedan ejecutarse en una WLAN sin ningún tipo de consideraciones especiales[9].

2.4.1.1. La Estación.

La estación es el componente que conecta con el medio inalámbrico. Se compone de un MAC y la capa física. En general, la estación puede ser denominada el adaptador de red o tarjeta de interfaz de red (NIC). Estos nombres pueden ser más familiares para los usuarios

9 (Cisco Systems, 2008)

de las redes de cable. Los equipos de estación pueden ser: móviles, portátiles o estacionarios.

2.4.1.2. Basic Service Set (BSS)

La arquitectura WLAN IEEE 802.11 está construida en torno a un conjunto de servicios básicos (BSS, Basic Service Set). Un BSS es un conjunto de estaciones que se comunican entre sí. Los BSS no se refieren en general a una zona determinada, debido a las incertidumbres de la propagación electromagnética. Cuando todas las estaciones en el BSS son las estaciones móviles y no hay conexión a una red cableada, Se puede decir que un BSS es un BSS independiente (IBSS).

2.4.1.3. SSID (Service Set IDentifier)

El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes ad-hoc, utilizan el BSSID (*Basic Service Set IDentifier*); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

2.4.1.4. Independent Basic Service Set (IBSS)

Un IBSS también conocido como (Ad-Hoc) es normalmente una red de corta duración, con un pequeño número de estaciones, que se ha creado para un fin determinado, por ejemplo, para el intercambio de datos con un proveedor en el pasillo del edificio de una empresa o para colaborar en una presentación en una conferencia.

Para poder entender un IBSS se puede tomar como ejemplo un cable UTP cruzado, el cual sirve para comunicar dos equipos sin la necesidad de un repetidor, entonces en una WLAN en modo IBSS los equipos móviles pueden comunicarse entre sí manteniendo conexiones unidireccionales de corto alcance. Si una estación móvil quiere comunicarse con otra, debe estar en el rango de comunicación directa como se muestra en la siguiente figura.

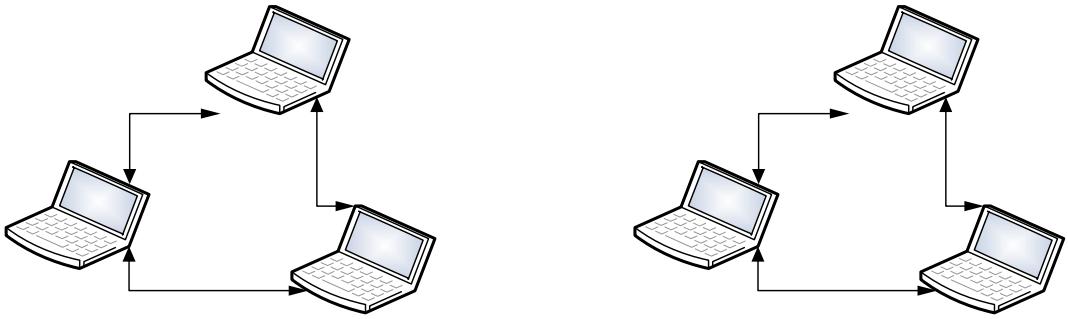


Ilustración 2-2 Independent Basic Service Set (IBSS) modo AD-HOC

2.4.1.5. Infraestructura.

Cuando un BSS incluye un punto de acceso, el BSS ya no es independiente y se llama una BSS de infraestructura, pero son referenciados simplemente como un BSS. Un AP (Access Point) es una estación que también proporciona servicios de distribución.

En una infraestructura BSS, todas las estaciones móviles se comunican con el AP. El AP proporciona la conexión a la LAN cableada, si la hubiere. Por lo tanto, si una estación móvil en el BSS se debe comunicar con otra estación móvil, la comunicación se envía en primer lugar a la AP y luego se la reenvía a la otra estación móvil. Esto hace que las comunicaciones que se originan al principio y al final de la misma BSS consuman dos veces el ancho de banda. Si bien esto parece ser un costo importante, los beneficios proporcionados por el AP son muy superiores a este costo. Uno de los beneficios proporcionados por el AP es la memoria del tráfico de una estación móvil y la potencia y rango de distribución de señal, mientras que la estación está funcionando en un estado de energía muy bajo.

2.4.1.6. Infraestructura con más de un AP, Extended Service Set (ESS)

Uno de los beneficios de la WLAN es la movilidad que proporciona a sus usuarios. Esta movilidad no sería de gran utilidad si fuera confinada a una sola BSS. IEEE 802.11 amplía la gama de la movilidad que proporciona a través de Extended Service Set (ESS). Un ESS es un conjunto de Access Points (AP), los cuales pueden comunicarse entre sí y esto permite que se transmita el tráfico de un AP a otro para facilitar la circulación de estaciones móviles. El AP realiza esta comunicación a través de un medio llamado *Distribution System* (DS).[10].

2.4.2. Codificación Inalámbrica y No superposición de Canales.

Cuando se envían datos a través de una red WLAN, se puede cambiar la señal de radio de frecuencia, amplitud y fase. para controlar las interferencias de señal son necesarias las codificaciones inalámbricas y el uso de la no superposición de canales, como se lo explica a continuación.

10 (IEEE, 2004)

***Frequency Hopping Spread Spectrum* (FHSS)** utiliza todas las frecuencias en la banda 2.4 GHZ, saltándose a diferentes frecuencias de ser necesario. Mediante el uso de frecuencias ligeramente diferentes de las transmisiones consecutivas, un dispositivo puede esperar y evitar interferencias de otros dispositivos que utilizan la misma banda, sucediendo en el envío de datos en algunas frecuencias. El original WLAN 802.11 usa FHSS, pero los actuales estándares (802.11a, 802.11b, 802.11g) no lo hacen.

***Direct Sequence Spread Spectrum* (DSSS)** es la segunda clase general de tipo de codificación para las redes WLAN. Diseñado para su uso en la banda de 2,4 GHz sin licencia, DSSS utiliza uno de los varios canales o frecuencias. Esta banda tiene un ancho de banda de 82 MHz, con un rango de 2,402 GHz a 2,483 GHz, en esta banda puede haber superposición de 11 diferentes canales DSSS.

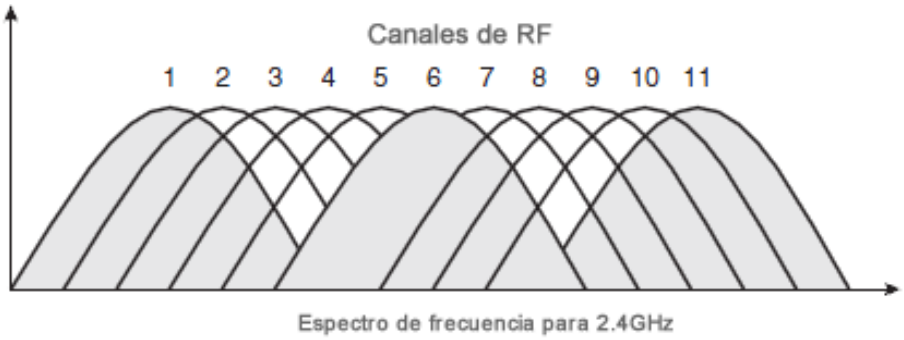


Ilustración 2-3 Grafico de el espectro de frecuencia de 802.11[11]

La importancia de la no superposición de los canales es que cuando se diseña un ESS WLAN (con más de un AP), Los AP con la superposición de áreas de cobertura deben ser configurados para utilizar los diferentes canales de no superposición.

11 (BookSprint, 2007)

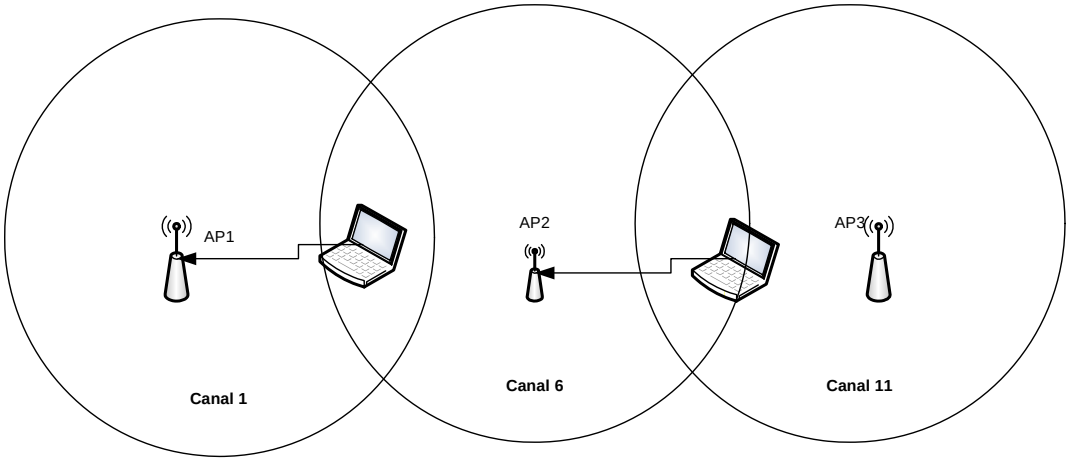


Ilustración 2-4 Ejemplo de la no superposición de canales

Como se puede observar en el grafico anterior, los dispositivos en una BSS (dispositivos comunicándose a través de un AP) puede enviar al mismo tiempo que los otros dos BSSs y no interferir unos con otros, porque cada uno utiliza las ligeras diferencias en las frecuencias de los canales de no superposición. Por ejemplo, PC1 y PC2 podrían sentarse al lado de los demás y comunicarse con los dos AP con dos canales en el mismo tiempo. Este diseño es típico de las redes WLAN 802.11b, con cada célula funcionando a una velocidad de datos máxima de 11 Mbps[12].

2.4.3. Multiplexacion por División de Frecuencias Ortogonales

Multiplexacion por División de Frecuencias Ortogonales, en inglés ***Orthogonal Frequency Division Multiplexing*** (OFDM), también llamada modulación por multitono discreto, en inglés **Discrete Multitone Modulation** (DMT), es una modulación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias donde cada una transporta información la cual es modulada en QAM o en PSK.

12 (Cisco Systems, 2008)

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

Debido al problema técnico que supone la generación y la detección en tiempo continuo de los cientos, o incluso miles, de portadoras espaciadas que forman una modulación OFDM, los procesos de modulación y demodulación se realizan en tiempo discreto mediante la IDFT y la DFT respectivamente.

La modulación OFDM es muy robusta frente al multi trayecto (multi-path), que es muy habitual en los canales de radiodifusión, frente a las atenuaciones selectivas en frecuencia y frente a las interferencias de RF.

Debido a las características de esta modulación, es capaz de recuperar la información de entre las distintas señales con distintos retardos y amplitudes (fading) que llegan al receptor, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia.

Si se compara a las técnicas de banda ancha como CDMA, la modulación OFDM genera una alta tasa de transmisión al dividir el flujo de datos en muchos canales paralelos que se transmiten en igual número de portadores *s* de banda angosta y con tiempos de símbolo (uno o varios bits) mayores al caso de usar banda ancha donde para lograr la misma tasa de transmisión los tiempos de símbolo son más cortos[13].

Los canales de banda angosta de OFDM son ortogonales entre si, lo que evita el uso de bandas de guardas y así un eficiente uso del espectro. Ya que los desvanecimientos (fading) afectan selectivamente a uno o un grupo de canales, es relativamente simple

13 (IEEE, 2004; Cisco Systems, 2008)
(Wikipedia, 2009)

ecualizarlos en forma individual lo que también se contrapone a la ecualización de un sistema de banda ancha.

2.5. ÁREA DE COBERTURA Y VELOCIDAD EN LAS REDES INALÁMBRICAS DE ÁREA LOCAL.

Un área de cobertura WLAN es el espacio en el que dos dispositivos WLAN pueden enviar datos con éxito. El área de cobertura creada por un AP depende de muchos factores.

En primer lugar, la potencia de transmisión de un AP o NIC WLAN no puede superar un nivel determinado sobre la base de los reglamentos de los organismos reguladores, como la FCC. La FCC limita la potencia de transmisión para asegurar la equidad en las bandas sin licencia. Por ejemplo, si dos vecinos compran un AP y lo instalan en sus casas para crear una WLAN, estos equipos se ajustan a las regulaciones de la FCC. Sin embargo, si una persona compra e instala antenas de alta ganancia para su AP, y supera la potencia regulada por la FCC, se puede obtener una mayor área de cobertura incluso en toda la manzana. Sin embargo, podría evitar que la otra persona que tiene otro AP pueda trabajar en absoluto debido a la injerencia del AP dominante.

Los materiales y la ubicación de los AP también son un impacto para el área de cobertura. Por ejemplo, poner el AP cerca de un archivador de metal aumenta la reflexión y dispersión, lo que reduce el área de cobertura. Ciertamente, la construcción de hormigón con barras de acero típica de un moderno edificio de oficinas reduce el área de cobertura. De hecho, cuando el diseño de un edificio hace que se produzcan interferencias en algunas zonas, los AP pueden usar diferentes tipos de antenas que cambiar la forma del área de cobertura de un círculo con otro tipo de forma.

Como resultado, las señales inalámbricas más débiles no pueden transmitir datos a velocidades más altas, pero pueden transmitir datos a velocidades más bajas. Por lo tanto, los estándares WLAN son diseñados para soportar múltiples velocidades. Un dispositivo

cerca de un AP puede tener una señal fuerte, por lo que puede transmitir y recibir datos a tasas más altas. Un dispositivo en el borde del área de cobertura, donde las señales son débiles, aún puede ser capaz de enviar y recibir datos, aunque a una velocidad menor[14].

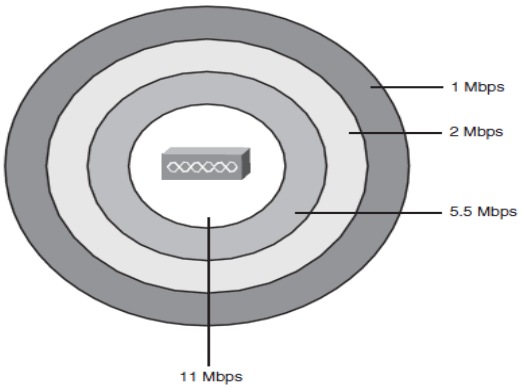


Ilustración 2-5 Demostración de cambios en la tasa de transferencia dependiendo de la distancia al AP[15]

El tamaño real del área de cobertura depende de un gran número de factores, los cuales incluyen la banda de frecuencias utilizadas por el estándar de WLAN, y los obstáculos entre los dispositivos cerca de la WLAN, la interferencia de otras fuentes de energía de radiofrecuencia, las antenas utilizadas en los clientes y los AP, y las opciones utilizadas por OFDM y DSSS. En términos generales, los estándares WLAN que usan frecuencias altas pueden enviar datos más rápidamente, pero esto trae como consecuencia que el área de cobertura se vuelve más corta.

Tabla 2-3 Comparación los diferentes estándares, variación de velocidades y superposición de canales.

Estándar IEEE	Velocidad Máxima (Mbps)	Variación de velocidades (Mbps)	Frecuencia	Canales en los cuales no existe superposición
802.11b	11 Mbps	1,2,5.5	2.4Ghz	3
802.11a	54 Mbps	6,9,12,18,24,36,48	5 GHz	12
802.11g	54 Mbps	6,9,12,18,24,36,48	2.4 GHz	3

14 (IEEE, 2004)
15 (BookSprint, 2007)

Hay que tomar en cuenta que el número de canales sin superposición soportados por un estándar, como se muestra en la ilustración 2-5, afecta a la combinación de ancho de banda disponible. Por ejemplo, una cliente en una WLAN 802.11g que utiliza exclusivamente la transmisión puede trabajar a 54 Mbps, Pero tres dispositivos podrían sentarse al lado de uno al otro y enviar al mismo tiempo, usando tres diferentes canales, a tres diferentes AP. Teóricamente, las WLAN pueden soportar un *throughput*[16] de 3 * 54 Mbps o 162 Mbps, para estos dispositivos.

2.5.1. Sistema de Distribución Inalámbrico

Un sistema de distribución inalámbrico (WDS Wireless Distribution System) permite la interconexión inalámbrica de puntos de acceso en una red IEEE 802.11. Está diseñada para autorizar que la red inalámbrica pueda ser ampliada mediante múltiples puntos de acceso sin la necesidad de un cable troncal que los conecte. La ventaja de WDS sobre otras soluciones es que conserva las direcciones MAC de los paquetes de los clientes a través de los distintos puntos de acceso.

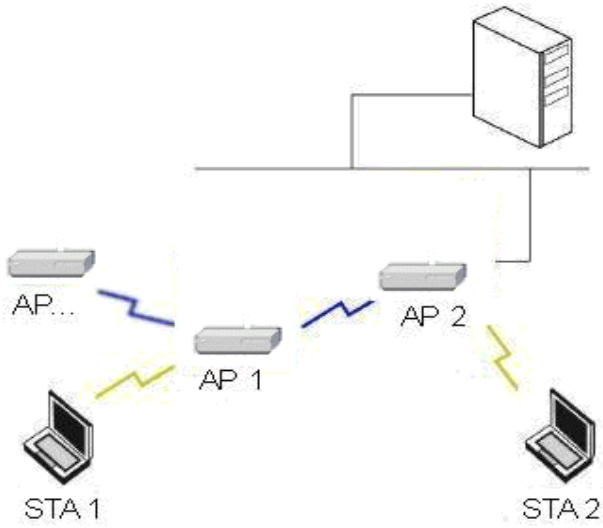


Ilustración 2-6 Ejemplo de una implementación de WDS utilizando varios AP.

16 Capacidad de carga que puede procesar el equipo.

Todos los puntos de acceso en un sistema de distribución inalámbrico deben estar configurados para utilizar el mismo canal de radio, y compartir las claves WEP o WPA si se utilizan. WDS también requiere que cada punto de acceso sea configurado de forma que pueda conectarse con los demás.

WDS puede ser también denominado modo repetidor porque parece hacer de puente entre distintos puntos de acceso, pero a diferencia de un simple repetidor, con WDS se consigue más del doble de velocidad.

2.6. SEGURIDAD EN REDES INALÁMBRICAS.

Hoy en día todas las redes necesitan una buena seguridad, pero las WLAN tienen requisitos de seguridad únicos.

Las WLAN introdujeron un numero de vulnerabilidades que no existían en la red cableada Ethernet, algunas de estas vulnerabilidades les dieron a los hackers una oportunidad de causar daño robando información, accediendo a equipos dentro de la red cableada que sucede a la WLAN, o sacando del aire a un servicio causando un ataque de denegación del servicio (Denial-of-Service “DoS”). Otro tipo de vulnerabilidades pueden ser causadas por la no utilización de ningún mecanismo de seguridad.

Las siguientes son algunas de las amenazas severas que pueden existir en una WLAN.

- WarDriving: El atacante solamente busca tener acceso a internet gratuitamente, esta persona maneja su auto o camina por varios lugares, intentando encontrar puntos de acceso que tengan una seguridad débil o que carezcan de ella. El atacante puede usar herramientas que se pueden encontrar en internet para hacer este tipo de ataque.

- Hackers: La motivación de los Hackers es obtener información o causar una denegación del servicio. El objetivo puede ser obtener acceso a redes empresariales sin necesidad de acceder desde el internet o pasar a través de un firewall.

- Puntos de Acceso Falsos: el atacante puede capturar los paquetes de una WLAN, encontrando el SSID y rompiendo las seguridades si es que se usan, luego el atacante puede configurar su propio AP, con las mismas configuraciones, y obtener a los usuarios que no detectan que este es un AP falso, esto puede causar que los usuarios ingresen sus nombres de usuario y contraseñas.

Para reducir el riesgo de un ataque, se puede utilizar tres tipos de herramientas en una WLAN.

- Autentificación mutua.
- Encriptación.
- Herramientas de detección de intrusos.

La autentificación mutua puede ser usada a través del cliente y el AP. El proceso de autenticación usa una clave secreta, llamada “Llave” en ambos equipos, y usando algún algoritmo matemático, el AP puede confirmar que ese cliente tiene derechos de autenticación, además, el cliente puede confirmar que el AP también posee la llave correcta. El proceso nunca envía la llave por las ondas de radio si es que no se establece una conexión segura, por lo tanto un atacante que esté utilizando un software para análisis de redes y que capture todos los frames que viajen por el aire no podrá ver el valor de la llave. Este proceso ayuda mucho para la mitigación de AP falsos.

La encriptación usa una llave secreta y una fórmula matemática para encriptar los contenidos de los frames de la WLAN. El equipo receptor después usa otra fórmula para desencriptar los datos. Nuevamente utilizando este método un atacante puede interceptar los frames enviados en las ondas de radio pero no podrá leer su contenido.

Las otras herramientas incluyen varias opciones las cuales son llamadas herramientas de intrusión, estas herramientas incluyen Sistema de detección de Intrusos (*IDS, Intrusion Detection Systems*) y los Sistemas de Prevención de Intrusos (*IPS, Intrusion Prevention Systems*).

2.6.1. Estándares de Seguridad en redes inalámbricas

El primer estándar de seguridad para redes WLAN, denominado *Wired Equivalent Privacy* (WEP) tuvo muchos problemas de seguridad, razón por la cual las siguientes normas fueron diseñadas con el objetivo de solucionar los problemas creados por WEP. La Wi-Fi Alliance, una asociación industrial, ayudó a solucionar el problema mediante la definición del estándar WI-FI. Por último, el IEEE concluyó su labor sobre un estándar oficial 802.11i.

Tabla 2-4 Revisiones del estándar 802.11 y sus estándares de seguridad.

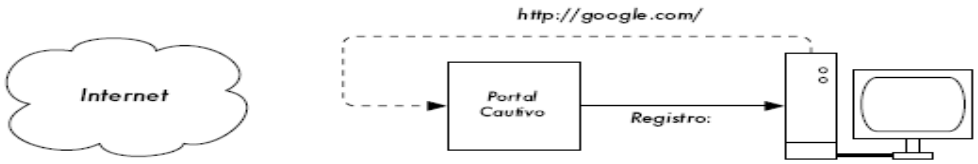
Nombre	**Año**	**Definido Por**
Wired Equivalent Privacy (WEP)	1997	IEEE
Extensible Authentication Protocol (EAP)	2001	Cisco, IEEE
Wi-Fi Protected Access	2003	Wi-Fi Alliance
802.11i (WPA2)	2005	IEEE

2.6.2. Portal Cautivo

Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo. Este utiliza un navegador web para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso) a los usuarios antes de permitirles el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente en todas los equipos móviles y sistemas operativos.

Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar la comunicación con el portal cautivo, el usuario selecciona la red y establece una conexión inalámbrica; a continuación, cuando se solicita una página web utilizando cualquier navegador, en lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página de registro o de bienvenida puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña o ingresar cualquier otra credencial que solicite el administrador de red. El punto de acceso u otro servidor en la red verifica los datos. Cualquier otro tipo de acceso a la red se bloquea hasta que se verifiquen las credenciales.



17

Ilustración 2-7 Ejemplo del funcionamiento de un Portal Cautivo dentro de una LAN

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es re direccionado al sitio web que solicitó originalmente

Los portales cautivos no proveen cifrado de datos para las redes inalámbricas, al contrario de esto para la autentificación se utiliza a las direcciones MAC e IP del cliente como identificadores únicas y periódicamente se solicita que el usuario se re-autentique.

En redes públicas o semipúblicas, las técnicas de encriptación como WEP y WPA son difíciles de manejar, debido a que no hay forma de distribuir claves públicas o compartidas para el público en general sin comprometer la seguridad de esas claves. En esas

17 http:// dev.wifidog.org/wiki/doc

instalaciones, una simple aplicación como un portal cautivo provee un nivel de servicio intermedio entre completamente abierto y completamente cerrado.

2.6.3. Wired Equivalent Privacy (WEP)

Wired Equivalente Privacy (WEP) fue el estándar original 802.11 desarrollado por IEEE, proveyendo servicios de autenticación y encriptación. Como resultado de ser el primer estándar de seguridad, WEP solamente proveía una débil autentificación y encriptación, llevándolo al punto que hoy en día sus servicios son fácilmente vulnerados por un atacante usando herramientas que pueden ser descargadas desde internet.

A continuación se detallan sus principales debilidades:

- ***Static Preshared Keys*** **(PSK)**: El valor de clave que se configura en cada cliente y en cada AP, sin poseer ninguna forma dinámica para el intercambio de las llaves sin la intervención humana. Como resultado, muchas personas no se molestaron en cambiar las claves configuradas por defecto, especialmente en las empresas con un gran número de conexiones móviles inalámbricas.

- **Llaves muy fáciles de romper**: Los principales de las llaves tienen una longitud en bits muy corta (64 bits, de los cuales sólo 40 fueron la clave única). Esto hizo más fácil predecir el valor de la clave sobre la base de los frames copiados de la WLAN. Además, el hecho de que la clave no cambia normalmente significa que el hacker podría reunir suficientes frames que contenían datos vulnerables sobre los 24 bits restantes, lo que hace una vía más fácil romper la contraseña.

Debido a los problemas con WEP, y a la mejora de los estándares que aparecieron a continuación, se ha descontinuado el uso de ese estándar, sin embargo hay todavía personas que lo utilizan ya que todavía está presente su disponibilidad en algunos AP y Enrutadores inalámbricos[18].

2.6.4. Encubrimiento del Nombre de la Red y filtrado de direcciones MAC

Debido a los problemas de WEP, muchos vendedores incluyeron nuevas funciones relacionadas con la seguridad que no son parte de WEP. Sin embargo, muchas personas relacionan estas funciones con WEP solo por el tiempo en que estas características se anunciaron al público. Estas características descritas no proveen una gran seguridad, y no son parte de ningún estándar, pero su uso es bastante amplio hasta el día de hoy.

La primera característica descrita, encubrimiento del SSID cambia el proceso de cómo los clientes se asocian con el AP. Antes de que el cliente pueda comunicarse con el AP el debe saber un dato muy importante, el cual es el SSID del AP que particularmente se le conoce como el nombre de la red.

Existen 4 pasos que los clientes siguen para asociarse a un AP, los cuales son:

- El AP envía una transmisión periódica (Periodic Beacon frame), generalmente cada 100ms y que contiene el SSID del AP y las configuraciones requeridas para la asociación.
- El cliente escucha las transmisiones de los AP en todos los canales y guarda la información de todos los AP en el rango de alcance.
- El cliente se asocia con el AP que tenga la señal más fuerte y que provenga del SSID preferido.

18 (IEEE, 2004)

- La autenticación ocurre tan pronto el cliente se asocie con el AP.

Básicamente, el cliente aprende acerca de cada AP y su SSID a través del proceso de trasmisión periódica. Este proceso es fundamental cuando se necesita movilizarse físicamente de un lugar a otro permitiéndole al cliente moverse y re asociarse con un nuevo AP cuando el antiguo pierde señal, la tecnología WDS puede ser utilizada en estos casos. Sin embargo, los las transmisiones periódicas permiten a un atacante encontrar información acerca del AP para intentar asociarse a él y tener acceso a la red.

El encubrimiento del SSID es una característica que hace que el AP deje de enviar transmisiones de frames periódicas. Esto parece resolver el problema con los atacantes ya que les hace difícil de encontrar los AP. Sin embargo, los clientes aún tienen que ser capaces de encontrar el AP. Por lo tanto, si el cliente se ha configurado con una SSID nula o sin SSID, el cliente envía un mensaje de prueba para encontrarlo, lo que provoca que el AP responderá a ese llamado enviando su SSID. En pocas palabras, es simple hacer que todos los APs respondan para anunciar su SSID, incluso con el encubrimiento habilitado en el AP, por lo que los atacantes todavía pueden encontrar todos los APs.

La segunda característica extra que a menudo se la utiliza con WEP es el filtrado de direcciones MAC. El AP puede ser configurado con una lista de direcciones MAC permitidas de los clientes en la WLAN, filtrando frames enviados por los clientes WLAN cuya dirección MAC no está en la lista. Los clientes permitidos son guardados en una lista, el número de direcciones MAC que pueden ser guardadas en un AP depende de la marca y modelo del dispositivo. Al igual que con el encubrimiento SSID, el filtrado de MAC puede prevenir el acceso a la red a personas no autorizadas, pero no detiene un ataque real. El atacante puede utilizar un adaptador WLAN que permita modificar la dirección MAC de

su tarjeta de red, cambiando la dirección verdadera por una capturada con un analizador de tráfico inalámbrico.[19]

2.6.5. Wi-Fi Protected Access (WPA)

WPA es la abreviatura de "*Wifi Protected Access"*, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (*Transition Security Network*).

WPA utiliza TKIP (*Temporal Key Integrity Protocol*) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

2.6.6. Wi-Fi Protected Access PSK (WPA-PSK)

WPA-PSK Es el sistema más simple de control de acceso tras WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de *PreShared* Key y viene a significar clave compartida

19 (IEEE, 2004)

previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida.

WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red.

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuerza bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Este diálogo va cifrado con las claves compartidas. La debilidad consiste en que se puede obtener el contenido del paquete de autenticación y su valor de cifrado; entonces, mediante un proceso de ataque de diccionario o de fuerza bruta, se puede obtener la contraseña.

2.6.7. Wi-Fi Protected Access Enterprise (WPA Enterprise)

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo el usuario de un sistema identificados con nombre/contraseña o la posesión de un certificado digital. Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un cliente se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red, parece el problema del huevo y la gallina. En este punto es donde entra en juego el IEEE

802.1X, que describimos a continuación, para permitir el tráfico de validación entre un cliente y una máquina de la de local. Una vez que se ha validado a un cliente es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los clientes WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS que se describe más adelante.

2.6.8. Remote Authentication Dial-In User Service (RADIUS)

RADIUS es un servicio de seguridad para la autenticación y la autorización de los usuarios. Soporta cualquier tipo de transmisión de datos, desde *dial-up*[20] hasta redes inalámbricas Wi-Fi, y por lo tanto se puede utilizar junto con un servidor RADIUS para proporcionar servicios de autenticación. Luego de establecer la conexión, el servidor de acceso envía las peticiones de autenticación para el servidor RADIUS. El servidor RADIUS autentica a los usuarios y autoriza el acceso a los recursos de la red interna. Es un protocolo abierto y es distribuido en código de fuente, como puede revisarse en los RFCs que lo definen[21].

Gracias a que el servicio es abierto, puede ser adaptado para trabajar con terceros. Cualquier servidor de acceso que admita el protocolo de cliente de RADIUS puede comunicarse con el Servidor.

20 (DIAL UP) Conexión por línea conmutada es una forma de acceso a Internet en la que el cliente utiliza un módem para llamar a través de la Red Telefónica.
20 RFC 2139 (RADIUS Accounting, Abril 1997)
RFC 2865 (Remote Authentication Dial In User Service (RADIUS), June 2000)

2.6.9. 802.1X

Debido a las carencias de 802.11 ha sido necesario establecer una nueva normativa estándar que permita tanto la autenticación como el intercambio dinámico de contraseñas, de forma fácil y segura.

El estándar IEEE 802.1X proporciona un sistema de control de dispositivos de red, de admisión, de tráfico y gestión de claves para dispositivos tos en una red inalámbrica. 802.1X se basa en puertos, para cada cliente dispone de un puerto que utiliza para establecer una conexión punto a punto. Mientras el cliente no se ha validado este puerto permanece cerrado. Cada una de estas funcionalidades se puede utilizar por separado, permitiendo a WPA, por ejemplo, utilizar 802.1X para aceptar a una estación cliente.

Para el control de admisión 802.1X utiliza un protocolo de autenticación denominado EAP y para el cifrado de datos CCMP y esto es lo que se conoce como RSN (Robust Secure Network) o también WPA2. No todo el hardware admite CCMP.

2.6.10. EAP

802.1X utiliza un protocolo de autenticación llamado EAP (*Extensible Authentication Protocol*) que admite distintos métodos de autenticación como certificados, tarjetas inteligentes, Kerberos, LDAP, etc. En realidad EAP actúa como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos.

El proceso de validación está conformado por tres elementos, un solicitante que quiere ser validado mediante credenciales, un punto de acceso y un sistema de validación situado en la parte cableada de la red. Para conectarse a la red, el solicitante se identifica mediante credenciales que pueden ser un certificado digital, una pareja nombre/usuario u otros datos. Junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de

validación tiene que utilizar. Evidentemente no podemos pretender que el punto de acceso disponga del sistema de validación. Por ejemplo, si queremos utilizar como credenciales los usuarios de un sistema, será el punto de acceso el que tendrá que preguntar al sistema si las credenciales son correctas. En general EAP actúa de esta forma, recibe una solicitud de validación y la remite a otro sistema que sepa cómo resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se he identificado, salvo aquéllas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPOL (*EAP over LAN*). Una vez validado, el punto de acceso admite todo el tráfico del cliente.

Los pasos que sigue el sistema de autenticación 802.1X son:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

El protocolo 802.1X posee un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se manda tras el mensaje de aceptación. El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables. En los casos prácticos de aplicación del protocolo 802.1X, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP están:

2.6.11. EAP-TLS

Es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (Transport Layer Security).

2.6.12. EAP-TTLS

El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor[22].

22 (Joseph Davies. Microsoft Corparation, 2004)

2.6.13. Wi-Fi Protected Access v2 (WPA2)

Wi-Fi Protected Access versión 2 (WPA2) es un sistema creado para corregir las vulnerabilidades detectadas en WPA. Está basado en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

Wifi Alliance denomina a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

WPA2-Personal también es compatible con versiones anteriores como WPA original. Tanto en los Enrutadores inalámbricos como los puntos de acceso se pueden optar por tipos de configuraciones diferentes ya sea solo para WPA2-Personal o para un modo mixto lo que supone que puede ejecutar dispositivos inalámbricos compatibles con WPA2 y WPA en la misma red. La mayoría de los usuarios necesitan seleccionar una configuración mixta si disponen de equipos o dispositivos que no son compatibles con WPA2-Personal.

Los sistemas equipados con tarjetas inalámbricas compatibles con WPA2-Personal usarán el cifrado de AES (Advanced Encryption Standard) de WPA2 que es más potente, mientras que los dispositivos solo compatibles con WPA seguirán el WPA[23].

23 (VLADIMIROV, 2004)

CAPITULO III

3. ANÁLISIS DEL HARDWARE PARA LA IMPLEMENTACIÓN DEL PROYECTO

3.1. HISTORIA DE LA MODIFICACIÓN DE HARDWARE.

Las modificaciones y mejores en el hardware no son nuevos conceptos, las razones para hacer una modificación de hardware son diferentes, pero siempre buscando un mismo resultado, el perfeccionamiento del equipo y además con la gratificante recompensa de saber que se lo ha hecho manualmente y se ha mejorado la entrada produciendo una salida mucho mas enriquecida.

En los últimos años, las modificaciones de hardware se han acentuado en el mercado. Las tiendas de computadoras venden accesorios para personalizar los computadores de escritorio, las tiendas en línea muestran los últimos avances y además mejoras a los productos que ya están en el mercado. Se puede pensar que cualquier equipo de hardware puede ser un candidato para ser modificado. La creatividad y determinación pueden realizar cosas inimaginables y producir equipos o modificarlos según nuestras necesidades.

Sin embargo, al igual que los artistas, los hackers a veces colaboran y forman comunidades de personas que trabajan hacia una meta similar. El uso del término hacker es un arma de doble filo, y a menudo lleva a una mítica. Contrariamente a la forma en que grandes

medios de comunicación gozan de la utilización de la palabra para describir a los criminales que rompen los sistemas de computación, un hacker puede ser definido simplemente como alguien que participa en la exploración de la tecnología. Y un hack en el mundo de la tecnología define un nuevo y novedoso método de creación o una forma nueva de resolver un problema, generalmente en una manera poco ortodoxa. La filosofía de la mayoría hackers de hardware es sencilla:

- Hacer algo con una pieza de hardware que nunca se ha hecho antes.
- Crear algo extraordinario.
- No dañar nada en el proceso.

A mediados del siglo 20 se desarrollaron, el ENIAC, UNIVAC, y mainframes de IBM, las personas de las instituciones académicas tuvieron la suerte de que los equipos fueron diseñados para su experimentación, pero no eran accesibles al público. Con el desarrollo y lanzamiento del primer microprocesador (Intel 4004), en noviembre de 1971, finalmente el público en general pudo probar a la computación. El potencial del hardware hacking ha crecido enormemente en la última década, como las computadoras y la tecnología se han convertido en más entrelazados con las actividades principales y la vida cotidiana[24].

Las modificaciones de hardware o hardware hacks se clasifican en 4 diferentes categorías.

- **Personalización y adaptación**. Incluye cosas tales como modificaciones a los teléfonos celulares, temas personalizados y tonos de timbre, y proyectos de arte como la creación de un acuario de un PC de escritorio.

- **Añadir funcionalidad**. Lograr que un sistema o equipo realice funciones que no eran para lo que estaban creados originalmente. Esto incluye cosas tales como la modificación del iPod para ejecutar Linux, la transformación del enrutador

24 (Russell, 2004)

inalámbrico instalando Linux y agregándole más funcionalidad de hardware y software o la modificación de la Atari 2600 para soportar sonido estéreo y salida de vídeo compuesto.

- **Aumentar la capacidad de rendimiento**. Mejora o actualización de un producto. Esto incluye cosas tales como añadir memoria a un asistente digital personal (PDA), modificación de las tarjetas de red inalámbrica para agregar una antena externa, o aumentar la velocidad del reloj (overclocking) de las tarjetas madre.

- **Eliminar los mecanismos de seguridad y de protección**. Esto incluye cosas como remover protecciones para los teléfonos celulares y que permitan la conectividad en bandas internacionales, liberar nuevas opciones secretas escondidas en equipos por ejemplo, la instalación de puertos seriales, o cambio de firmware a pesar de estar bloqueado para su uso.

Es importante señalar que las modificaciones de hardware requiere al menos un conocimiento básico de las técnicas de hacking, ingeniería inversa, habilidades y experiencia en la electrónica y la codificación.

3.2. ENRUTADOR INALÁMBRICO LINKSYS Y LA SERIE WRT54GX

Linksys empezó a vender la versión 1.0 del WRT54G a finales de 2002 como un equipo inalambrico casero que tenia las capacidades de *firewall* y enrutador. En un principio, fue una iniciativa destinada a apoyar las redes inalámbricas, con la inclusión de características adicionales para complementar las capacidades inalámbricas. En ese momento, el dispositivo era relativamente común, incluyendo en su equipo un puerto para la conectividad hacia el internet (WAN), cuatro puertos 10/100, y soporte para el estándar 802.11b. El dispositivo se diseñó con una interfaz Web para la configuración que había de convertirse en popular entre los dispositivos de consumo en años posteriores.

Desde el lanzamiento inicial en el año 2002, Linksys ha revisado el hardware del WRT54G varias veces para proporcionar actualizaciones al equipo. Este dispositivo fue tan exitoso que Linksys liberó varios modelos similares en la serie WRT54G para ofrecer diversas características.

Ilustración 3-1 LinkSys WRT54G V 2.0

Esta línea de productos ha sido destacada para LinkSys, aunque las cifras de ventas para el dispositivo no suelen romperse en comparación con todos sus productos. Esta popularidad puede deberse, en parte, a la facilidad con la que puede modificarse el dispositivo, y como tal, una comunidad dedicada a desarrollar software libre para el equipo y también la posibilidad para los hardware hackers, que tienen en este dispositivo miles de opciones para modificar y añadir.

Con el reciente apoyo hacia el firmware de terceros a través de la liberación del modelo WRT54GL, Linksys está lista para vender aún más unidades.

3.3.LIBERACIÓN DEL FIRMWARE DEL WRT54G

En el año 2003, Andrew Miklas envió varias veces mensajes de advertencia a la lista de correo del Kernel de Linux[25] acerca de su descubrimiento de que Linksys estaba usando Software en el Firmware bajo General Public License (GPL) [26] para el Linksys WRT54G. Como parte de la GPL, cualquiera que modifica el código abierto necesariamente tiene que ponerlo a disposición de la comunidad; sin embargo, Andrew no pudo localizar el origen de las modificaciones.

Entusiastas de Linux se hicieron conscientes del uso del software de código abierto por parte de LinkSys publicando varios anuncios en Slashdot[27] en junio de 2003. Slashdot y las comunidades Linux, hicieron llegar sus opiniones a Linksys protestando sobre el uso de software bajo licencia GPL. Con una gran presión por parte de la comunidad, y un grupo de ejecutivos de Linksys, se libera por fin el código de los enrutadores inalámbricos WRT54G sobre la Licencia Publica General GPL.

En junio de 2003, Rob Flickenger publica en su blog sobre el trabajo que había venido desempeñando durante las sesiones llamadas *Hack Night* con *Seattle Wireless*. En estos anuncios, Rob vincula al inicio del desarrollo de herramientas para la construcción de su propio firmware. Además, Andrew hizo algunos anuncios adicionales para la lista de correo del Kernel de Linux sobre los métodos y los temas de cambio de plataforma con la compilación de código para el Linksys WRT54G.

A partir de este punto, se ha logrado el desarrollo de *firmwares* completamente libres, y nuevas herramientas para el WRT54G y, a partir del lanzamiento del WRT54G con Linux como Firmware, muchas empresas comenzaron a desarrollar enrutadores inalámbricos de bajo costo con similares características. Todo esto produjo una serie de diferentes

25 Fuente: http://lkml.org/lkml/2003/6/7/164
26 Fuente: http://www.opensource.org/licenses/gpl-license.php
27 www.slashdot.org es un sitio de noticias orientado a la tecnología.

versiones del firmware, todos con diferentes complementos. En el año 2005 Linksys desarrolló un nuevo modelo del enrutador inalámbrico (WRT54GL) dirigido a la comunidad de software libre, que mantiene todas las características principales de los primeros modelos, pero además los componentes para modificación de hardware y firmware son más accesibles y mantiene un bajo costo.

3.4. VERSIONES DE LA SERIE WRT54G

El WRT54G original fue equipado con una CPU MIPS a 125 MHz con 16 MB de memoria RAM y 4 MB de memoria flash para almacenar el firmware. En revisiones posteriores, se aumentó la velocidad de la CPU a 200 MHz y se doblaron tanto la memoria RAM como flash a 32 y 8 MB, respectivamente. Todos los modelos vienen con un switch de 5 puertos (el puerto para internet está en el mismo switch pero en una VLAN diferente) y con un chipset inalámbrico de Broadcom[28].

3.5. CARACTERÍSTICAS DE HARDWARE WRT54G

En el desarrollo de este proyecto se han utilizado diferentes versiones del enrutador inalámbrico Wrt54g, los cuales se utilizaron para realizar pruebas de escalabilidad y estabilidad, además de comprobar las modificaciones de hardware necesarias para la mejora del equipo.

Los componentes de hardware del enrutador inalámbrico WRT54GL son presentados en la siguiente ilustración.

28 (Asadoorian, 2007)

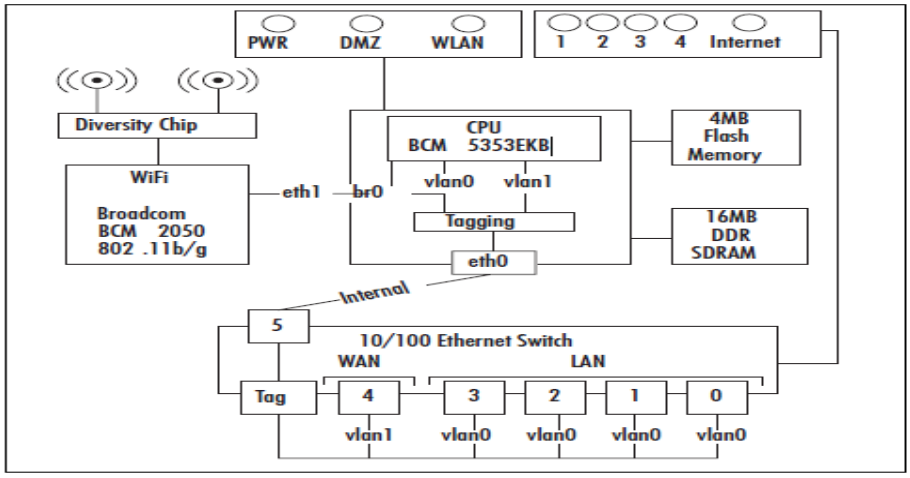


Ilustración 3-2 Diagrama de bloques de un WRT54GL[29]

Existen en el mercado diversas versiones del enrutador inalámbrico WRT54GL, sin embargo no todas ellas tienen la capacidad de ser modificadas con *firmware* de terceros. A continuación en la Tabla 3-1 se listan las versiones de la gama WRT54G compatibles para ser embebidos.

Tabla 3-1 Versiones del LinkSys WRT54G con capacidad de ser embebido

Versión	**CPU**	**RAM**	**Memoria Flash**	**Más información**
1.0	125 MHz	16 MB	4 MB	Presenta 20 diodos LED en el panel frontal, la conexión inalámbrica la proporciona una tarjeta MiniPCI insertada en la placa base.
1.1	125 MHz	16 MB	4 MB	Los LEDs fueron reducidos a 8. El chipset inalámbrico se integró en la placa base.
2.0	216 MHz	16 MB	4 MB	Igual que la versión 1.1 con una actualización de la CPU y más integración del transmisor inalámbrico (transmisor menos complejo con menos componentes).
3.0	216 MHz	16 MB	4 MB	Incluye un switch no documentado detrás del panel frontal izquierdo pensado para su uso con una característica conocida como "Secure EZ Setup" para configurar una conexión inalámbrica segura.
3.1	216 MHz	16 MB	4 MB	La versión 3.1 del hardware incluye un nuevo botón iluminado con el logo de Cisco a la izquierda del panel frontal del enrutador. Este botón se usa para configurar la conexión inalámbrica segura ("Secure EZ Setup") de LinkSys.
WRT54GL	**CPU**	**RAM**	**Memoria Flash**	**Más información.**
1.0	200 MHz	16 MB	16 MB	Se lanzó en el año 2005 para soportar firmware de terceros, esencialmente es igual al WRT54GS v4.0 en cuanto a hardware. No viene con SpeedBooster, sin embargo se puede tener esta característica con firmwares de terceros.
1.1	200MHz	16MB	16 MB	Números de serie comienzan con CL7B,

29 (Asadoorian, 2007)

Aunque existen muchos modelos y variantes de los Linksys WRT54G, la mayoría de los modelos tienen las mismas características básicas. Es necesario explorar estas características comunes a fin de comprender las diferencias entre versiones.

3.5.1. Corriente Eléctrica.

Aparte de la versión 1.0 del WRT54G, todos los requisitos de corriente eléctrica son los mismos para todos los dispositivos, es decir 12V DC 1.0A. Estos requerimientos de conexión a la corriente son estándar para los Enrutadores inalámbricos y los AP. Gracias a esto se logra la compatibilidad con PoE (Power over Ethernet).

3.5.2. El Botón de Reset

Este botón hace que el dispositivo se restablezca a los valores predeterminados de fábrica. Es programable y tiene muchos usos diferentes, dependiendo de cuándo y durante cuánto tiempo se presione. Se debe tener cuidado de no presionar por accidente, ya que hacerlo podría causar que el dispositivo se reinicie o puede restablecerse a la configuración de fabrica. Se encuentra ubicado en la parte posterior del dispositivo a un lado de la interfaz WAN.

3.5.3. Luces LED

Las luces de LED difieren en los diversos modelos, y las combinaciones de la luz indican diferentes condiciones del dispositivo.

Ilustración 3-3 Luces LED del WRT54GL

La luz de "*Power*" indica cuando el dispositivo está recibiendo corriente eléctrico. Esta luz se pone en verde cuando el dispositivo esta encendido y funcionando, cuando el dispositivo está iniciando o cuando este tiene algún error la luz empieza a parpadear. La luz de la DMZ (*Demilitarized zone*) se usa de diferentes formas dependiendo del firmware instalado, por ejemplo, en la distribución de GNU/LINUX OpenWrt se lo utiliza para indicar que se está iniciando el sistema operativo. Las siguientes luces, se las utiliza independientemente de la distribución de firmware para indicar que existe conexión, por ejemplo cuando se ilumina el LED de WLAN, significa que existe uno o más clientes conectados por este medio, de igual forma los LEDS 1,2,3,4 monitorean la actividad de los puertos LAN, que están conectados en modo SWITCH. Y por último el LED que indica la conexión a internet.

3.5.4. Botón y LEDS Secure Easy Setup

Este botón está detrás del logo de Cisco Systems, es llamado Secure Easy Setup (SES por sus siglas en ingles). Este botón apareció por primera vez en el WRT54G versión 1.1, y fue diseñado originalmente para permitir a usuarios sin experiencia configurar una red inalámbrica encriptada. En los firmware de terceros como OpenWrt se puede configurar las acciones que este botón realiza, por ejemplo se lo puede emplear para enviar el comando reboot, y de esta manera reiniciar el dispositivo de manera segura.

3.5.5. Arquitectura del Procesador.

Todos los procesadores que se venden con los modelos WRT54G utilizan el procesador Broadcom MIPS (*Microprocessor without Interlocket Pipeline Stages*). Son basados en RISC (*Reduced Instruction Set Computer*), lo cual significa que se tiene un set de instrucciones pequeño, a comparación de otros procesadores como los Intel. Estos procesadores son comunes en dispositivos embebidos como consolas de video juegos y dispositivos portátiles como Palms, Pocket PC y en los Enrutadores y switches Cisco Systems. La mayoría de distribuciones de Linux son compiladas para la arquitectura Intelx86 la cual es completamente diferente a la MIPS. Esto significa que es necesario portar o re compilar el software para permitir la ejecución de los programas o saber que el software ha sido desarrollado o se ha portado a esta arquitectura.

Existen dos familias principales de los procesadores Broadcom que se usan los modelos LinkSys WRT54G.

- **BCM47XX.** Los BCM47XX se dividen en dos modelos diferentes, los BCM4704 que fueron desarrollados para ser utilizados en dispositivos AP pequeños. Este procesador provee solamente funciones de CPU y se necesitan otros chips para manejar las interfaces de red Ethernet y las Inalámbricas. Se lo puede encontrar en versiones antiguas de la gama WRT54G por ejemplo la versión 1.0 y 1.1 los cuales contienen chips separados para las otras funciones. El procesador BCM4712 no solamente contiene las funciones de CPU sino que además maneja las interfaces Ethernet y las Inalámbricas. La última versión de este procesador fue utilizada en el WRT54G versión 2.0, el cual tenía un incremento en la velocidad del CPU de 125Mhz a 200Mhz.

- **BCM5352.** La familia de procesadores BCM5352 es la próxima generación de procesadores SoC (System on Chip) Utilizan chips integrados para controlar las interfaces de red Ethernet y las Inalámbricas. Es utilizado en los WRT54G versión 3,4 y L.

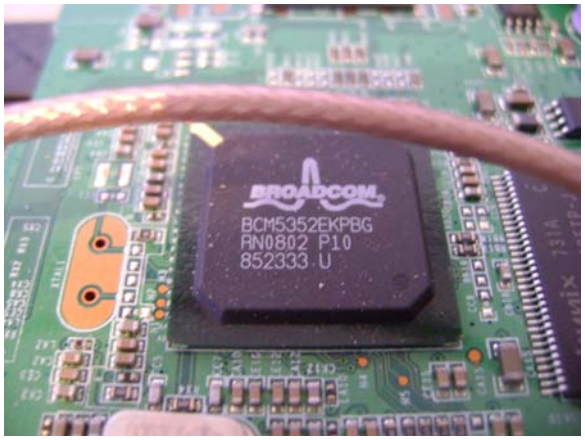


Ilustración 3-4 Procesador BCM5352 de un WRT54GL

3.5.6. Almacenamiento

El almacenamiento en los dispositivos WRT54G se basa en memorias FLASH NVRAM, un tipo de memoria no volátil comúnmente utilizada en equipos electrónicos pequeños como una cámara digital. Uno de los limitantes es el límite de almacenamiento, lo que define cuanto software se va a poder instalar en el dispositivo. Sin embargo esta limitante puede resolverse agregando una memoria SD o MMC[30] debido a que algunas versiones de los Enrutadores WRT54G están provistos de puertos llamados GPIO (General Purpose Input Output) los cuales sirven de entrada y salida para instalar nuevos dispositivos de almacenamiento entre otras cosas.

Ilustración 3-5 Memoria Flash de 8MB WRT54GL

30 Dispositivos de almacenamiento de bajo costo disponibles en cámaras digitales y PDAS.

3.5.7. Memoria RAM

La serie de Enrutadores inalámbricos WRT54G utilizan SDRAM[31] como memoria principal del sistema, sin embargo esta memoria va soldada directamente al *"Printed Circuit Board (PCB)"* en vez de utilizar una memoria general como las DIMM de los PC.

La serie WRT54GL tiene incorporada una memoria RAM de 16MB sin embargo existen métodos para ampliar esta memoria removiendo las sueldas que van hacia la PCB y utilizar partes de una memoria SDRAM de un PC o computador portátil. Este método es sumamente complejo ya que las soldaduras son muy compactas y existe el riesgo de dañar el PCB y dejarlo inservible.

Ilustración 3-6 Memoria RAM de 16MB de un WRT54GL

3.5.8. Red Inalámbrica y Ethernet

Las capacidades de red en la plataforma WRT54G son amplias, las cuales incluyen un Switch Ethernet, habilidad para configurar *Virtual LANs* (VLAN) entre otras. Este dispositivo provee 5 puertos FastEthernet con capacidades de switch. La configuración original del enrutador tiene dos VLANs, la primera es usada para la interfaz inalámbrica la cual hace puente con las interfaces Ethernet, la segunda VLAN conecta al puerto de la WAN, lo que permite separar las redes para luego unirlas por rutas. Estas VLANs pueden

31 Dynamic Random Access Memory

ser modificadas para por ejemplo aislar la red inalámbrica de la red cableada o separar los puertos Ethernet según los requerimientos.

3.6. MODELOS DEL DISPOSITIVO WRT54G DISPONIBLES PARA EL ESTUDIO.

3.6.1. LinkSys WRT54G Versión 1.0

Lanzado a finales del 2002 la versión 1.0 del enrutador inalámbrico LinkSys WRT54G es el primer equipo de la gama WRT54G, el cual incorpora la más alta tecnología inalámbrica de esos años. Es fácilmente reconocible de las siguientes versiones, en parte debido a que en el panel frontal tiene 20 luces LED en los puertos WLAN, LAN Y WAN, estos LEDs son utilizados para indicar la actividad y advertir de colisiones entre paquetes; por otro lado, es el único modelo que en la parte frontal tiene un logotipo llamado "InstantWireless". Esto se debe a que la compañía fabricante del enrutador (LinkSys) fue adquirida por el gigante de la computación Cisco Systems en marzo del 2003, por 500 millones de dólares. Sin embargo Cisco decidió mantener la marca "LinkSys" para los futuros dispositivos pero se incluyo el logotipo de Cisco para recordarle al consumidor que el equipo está respaldado por la tecnología altamente comprobada de Cisco.

Ilustración 3-7 Panel Frontal WRT54G Versión 1.0

El dispositivo inalámbrico utiliza el BCM2050 de Broadcom; sin embargo, se puede instalar cualquier otra tarjeta inalámbrica miniPCI[32], brindando la posibilidad de instalar

32 Puerto de expansión, comúnmente utilizado en computadoras portátiles.

drivers apropiados para diferentes distribuciones de firmware o desarrollar uno propio. Otra diferencia de este modelo es la utilización de una fuente de poder de corriente continua de 5V y 2.0A en comparación con los 12V y 1.0A de los siguientes modelos. Esto fue desarrollado debido a que ofrecía compatibilidad con otros equipos de LinkSys como el WAPPOE, el cual provee capacidades de PoE[33] utilizando los pares sin usar del cable Ethernet. Las características principales del LinkSys WRT54G 1.0 son las siguientes:

Tabla 3-2 Tabla de especificaciones técnicas del WRT54G Versión 1.0

Velocidad del Procesador	125Mhz
RAM	16MB
Flash	4Mb
Prefijo en el numero serial	CDF0-CDF1

3.6.2. LinkSys WRT54G Versión 2.0

La versión 2.0 del WRT54G fue la última en utilizar los dispositivos Ethernet de la empresa ADMTec como chips separados, además la velocidad del procesador se incrementa a 200Mhz.

Ilustración 3-8 Panel Frontal WRT54G Versión 2.0

El panel frontal de este dispositivo es muy diferente a la versión 1.0 debido a que se reducen las luces LED a 8 y además incorpora el logotipo “Cisco Systems”. Las características principales del LinkSys WRT54G 1.0 son las siguientes:

33 Power Over Ethernet es una tecnología que permite suministrar corriente eléctrica utilizando el cableado UTP

Tabla 3-3 Tabla de especificaciones técnicas del WRT54G Versión 2.0

Velocidad del Procesador	200Mhz
RAM	16MB
Flash	4Mb
Prefijo en el numero serial	CDF5

3.6.3. LinkSys WRT54GL Versión 1.0 y 1.1

El modelo WRT54GL 1.0 es casi idéntico a la versión 4.0 del WRT54G que fue dejada de fabricar en el año 2005. La única diferencia es el cambio de fabricante de la memoria Flash y de la SDRAM. En el año 2007 se liberó el modelo WRT54GL 1.1 el cual tiene diferencias menores respecto a la versión 1.0, uno de los principales cambios la mejora del procesador y sus características internas, sin embargo la velocidad sigue siendo la misma.

Ilustración 3-9 Panel Frontal WRT54GL Versión 1.1

Uno de los propósitos por los cuales el modelo WRT54GL fue liberado es para apoyar a la comunidad hacker, El costo de este dispositivo varía entre 59$ y 79$. Las principales características que tiene este modelo son las capacidades de instalar lectores de tarjetas MMC/SD, puertos JTAG para modificación del firmware y un puerto serial que puede ser utilizado para un sin número de utilidades por ejemplo conectar un GPS al dispositivo para utilizarlo en WarDriving[34]. Las características principales del LinkSys WRT54G 1.0 son las siguientes:

34 Wardriving es la búsqueda de redes inalámbricas Wi-Fi en movimiento, utilizando un auto o a pie.

Tabla 3-4 Tabla de especificaciones técnicas del WRT54GL Versión 1.0

Velocidad del Procesador	200Mhz
RAM	16MB
Flash	4Mb
Prefijo en el numero serial	Versión 1.0:CL7A Versión 1.1:cl7B

3.7. SERVIDOR DE AUTENTIFICACIÓN

3.7.1. Introducción al Servidor de Autentificación

A diferencia de los sistemas operativos de los consumidores finales como Microsoft Windows, el sistema operativo GNU / Linux le da un administrador de red la posibilidad de acceso a la manipulación y configuración de los protocolos y servicios. Gracias a esto se puede acceder y manipular paquetes de red en cualquier nivel del modelo OSI[35] desde el data-link hasta la capa de aplicación. Las configuraciones de enrutamiento pueden ser basadas en cualquier información contenida en un paquete de red, desde la dirección de enrutamiento, los puertos y el contenido que estos envían.

Antes de tener acceso a los recursos de la red, los usuarios deben ser autenticados. En un mundo ideal, cada usuario inalámbrico debería tener un identificador personal que fuera único, inmodificable e imposible de suplantar por otros usuarios. Este es un problema muy difícil de resolver en el mundo real.

La función principal del servidor de autentificación basado en GNU / LINUX es proveer de conectividad continua las 24 horas, y permitir a los usuarios que se conectan a las redes inalámbricas abiertas (Hotspots) puedan iniciar sesión utilizando un nombre de usuario previamente registrado, o comprar tiempo de navegación. Además de esto el servidor de autentificación es centralizado y permite que los usuarios puedan utilizar el mismo nombre

35 El Modelo OSI es un lineamiento funcional para tareas de comunicaciones, consta de 7 capas.

de usuario en cualquier locación que esté disponible y conectada a la red de portales cautivos.

3.7.2. Requerimientos de Hardware para el servidor de autentificación.

Los requerimientos de hardware para instalar un servidor de autentificación de portal cautivo varían dependiendo de la cantidad de usuarios que se vaya a tener en la red, por lo tanto para la implementación de este proyecto y en modo de demostración, se puede instalar el servidor en un PC de bajo costo que pueda cargar un sistema operativo GNU / LINUX y que tenga la capacidad de procesamiento para poder tener los servicios de Web y Base de Datos. Además de los requerimientos de hardware es indispensable que el servidor de autentificación pueda ser accedido por las puertas de enlace del portal cautivo, en este caso los enrutadores inalámbricos, por lo que para la implementación de este proyecto es necesario una IP publica, que permita la conexión desde cualquier parte del mundo.

Otra forma de solventar la implementación del servidor de autentificación y que mantenga conectividad 24 horas al día es el alquiler de un servicio de *Hosting Dedicado,* el cual permite configurar el equipo como si estuviera físicamente conectado en la misma oficina o habitacion, accediendo desde una consola de administración por medio del protocolo SSH. Por otra parte existen servidores web que ofrecen alojamiento de páginas web, base de datos y acceso a los pre compiladores por ejemplo PHP, pero para la implementación de este proyecto necesario realizar configuraciones extra al servidor lo cual implica tener acceso directo a la línea de comandos y tener permisos de súper usuario, por lo que no es posible instalar el servidor de autentificación en un servidor de páginas web (Hosting).

CAPITULO IV

4. SELECCIÓN DE SOFTWARE NECESARIO PARA LA IMPLEMENTACIÓN DEL PROYECTO

4.1.INTRODUCCIÓN AL SISTEMA OPERATIVO GNU / LINUX

GNU/Linux es uno de los términos empleados para referirse al sistema operativo libre similar a Unix que utiliza como base las herramientas de sistema de GNU y el núcleo Linux. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL de GNU (Licencia Pública General de GNU) y otras licencias libres.

La historia del núcleo Linux está fuertemente vinculada a la del proyecto GNU. El proyecto GNU, iniciado en 1983 por Richard Stallman, tiene como objetivo el desarrollo de un sistema operativo Unix completo compuesto enteramente de software libre. Cuando la primera versión del núcleo Linux fue liberada en 1991, el proyecto GNU ya había producido varios de los componentes fundamentales del sistema operativo, incluyendo un intérprete de comandos, una biblioteca C y un compilador, pero aún no contaba con el

núcleo que permitiera completar el sistema operativo. Finalmente el núcleo o Kernel creado por Linus Torvalds[36] en 1991, fue el que completo el sistema operativo.

4.2. DISTRIBUCIONES GNU / LINUX

Una distribución es una variante del sistema GNU/Linux que se enfoca a satisfacer las necesidades de un grupo especifico de usuarios. De este modo hay distribuciones para hogares, empresas y servidores. Algunas distribuciones son completamente libres, pero muchas no lo son.

Las distribuciones son desarrolladas por individuos, empresas u otros organismos. Cada distribución puede incluir cualquier número de software adicional, incluyendo software que facilite la instalación del sistema. La base del software incluido con cada distribución incluye el núcleo Linux y las herramientas GNU, al que suelen añadirse también varios paquetes de software.

Las herramientas que suelen incluirse en la distribución de este sistema operativo se obtienen de diversas fuentes, y en especial de proyectos de software libre. Casi todas con licencia GPL o compatibles con ésta (LGPL, MPL). Usualmente se utiliza la plataforma X.Org Server, basada en la antigua XFree86, para sostener la interfaz gráfica.

4.3. FIRMWARE GNU / LINUX

El Firmware o programación en firme, es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de

36 (Schroder, 2005)

un dispositivo de cualquier tipo. Al estar integrado en la electrónica del dispositivo es en parte hardware, pero también es software, ya que proporciona lógica y se dispone en algún tipo de lenguaje de programación. Funcionalmente, el firmware es el intermediario (interfaz) entre las órdenes externas que recibe el dispositivo y su electrónica, ya que es el encargado de controlar a ésta última para ejecutar correctamente dichas órdenes externas[37].

Se puede encontrar firmwares en memorias ROM de los sistemas de diversos dispositivos periféricos, como en monitores de video, unidades de disco, impresoras, etc., pero también en los propios microprocesadores, chips de memoria principal y en general en cualquier circuito integrado. En un microprocesador el firmware es el que recibe las instrucciones de los programas y las ejecuta en la compleja circuitería del mismo, emitiendo órdenes a otros dispositivos del sistema.

Debido a la libración a la comunidad de software libre del firmware original del WRT54G por parte de LinkSys, se han creado varias distribuciones de Linux basadas en el firmware original. Las primeras distribuciones basadas en dicho firmware se valían esencialmente del todo el software original, pero al pasar de los años se ha seguido desarrollando nuevas herramientas y portando las existentes, y es así como el día de hoy las nuevas distribuciones contienen el Kernel de Linux en sus últimas versiones, permitiendo así una mejora considerable de rendimiento y de funcionalidad, además se han portado a esta plataforma la mayoría de herramientas de red de el sistema operativo GNU / LINUX.

4.4. FIRMWARE ORIGINAL DEL LINKSYS WRT54G

El firmware original de LinkSys fue la versión que despertó a la creatividad del movimiento hacking del WRT54G. Este firmware está basado en Linux, y gran parte de los componentes han sido liberados bajo la licencia GNU General Public License (GPL). Aunque este firmware no es modificable o extensible directamente, ha servido como la

37 (Russell, 2004)

base de muchas de las otras soluciones de firmware de terceros en términos de código o de diseño.

A pesar de ser el firmware original y estar diseñado explícitamente para el dispositivo, en sus primeras versiones no agregaba tantas características como las versiones de terceros, debido a que cada versión del firmware se guiaba directamente de la versión del dispositivo, y las actualizaciones eran menores. Sin embargo, las versiones posteriores son compatibles con WPA-PSK y WPA2-PSK, por lo que ofrece una protección adecuada para la mayoría de *Small Office Home Office* (SOHO). Muchas de las versiones originales del firmware no contenían soporte para Wi-Fi Protected Access (WPA)[38].

Es importante señalar que este firmware es perfectamente adecuado para su uso por el usuario domestico, que está satisfecho con el funcionamiento del WRT54G. Este ofrecerá muchas de las características requeridas por el usuario promedio, que incluye la traducción de direcciones de red (NAT[39]) seguridad inalámbrica y un firewall básico.

A partir de la versión 5 del Wrt54g salió un nuevo firmware que no está basado en Linux, sino más bien en un Unix propietario como sistema en tiempo real diseñado para dispositivos embebidos, llamado VxWorks[40] y por lo tanto se limito las funcionalidades de este dispositivo, disminuyendo la memoria flash a solo 2MB y la memoria RAM a 4 MB, pero a pesar de esto existe una distribución de Linux para el Wrt54G que permite su instalación en el dispositivo, sin embargo su funcionalidad es limitada debido a que no contiene todos los paquetes pueden ser instalados por falta de espacio de almacenamiento[41].

38 (Asadoorian, 2007)
39 NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes
40 www.windriver.com/VxWorks
41 (Asadoorian, 2007)

4.5. FIRMWARE GNU / LINUX DE TERCEROS PARA EL WRT54GL

4.5.1. OpenWrt

El desarrollo de OpenWrt fue inducido inicialmente gracias a la licencia GPL, que impulsaba a todos aquellos fabricantes que modificaban y mejoraban el código, a liberar éste y contribuir cada vez más al proyecto en general. Poco a poco el software ha ido creciendo y en la actualidad se encuentra características implementadas que convierten al enrutador inalámbrico en un completo servidor de red, apto para administrar cientos de usuarios simultáneos y brindar de servicios como: VPN, Servidor de archivos, Portal Cautivo, Servidor Web, VLAN. Además de la portabilidad de software que brinda de herramientas y servicios, los desarrolladores de OpenWrt han creado drivers para diversos dispositivos que pueden ser conectados en el equipo para mejorar su desempeño o agregar nuevas características como puede ser: almacenamiento externo mediante tarjetas Secure Digital, cámaras web, GPS, Módems.

Ilustración 4-1 Consola de administración OpenWrt 8.04

El Firmware basado en GNU / LINUX OpenWrt fue liberado en enero de 2004 por un grupo de desarrolladores en respuesta al gran numero de firmware de terceros basados en el firmware original de LinkSys y que proveían solo unas pocas herramientas extras o se enfocaban en un nicho del mercado. La propuesta del grupo OpenWrt fue desarrollar una distribución que no dependa del firmware original de LinkSys, portando los paquetes existentes de GNU / LINUX a la arquitectura MIPS, y permitiendo así su instalación en otras plataformas embebidas como por ejemplo Belkin, D-Link, NETGEAR, y Motorola.

Este firmware está pensado para usuarios con experiencia en el sistema operativo GNU / LINUX ya que solamente las configuraciones básicas como por ejemplo configurar la red LAN y WAN, instalar software y revisar el estado del servidor se pueden realizar mediante el GUI[42], sin embargo es el que mayor capacidades de expansión provee, lo que lo convierte en el mejor candidato para este proyecto[43].

Ilustración 4-2 Interfaz Grafica por web del OpenWrt

En posteriores versiones se incorpora un manejador de paquetes que permite la instalación de software pre compilado utilizando la línea de comandos o la interfaz grafica, estos paquetes están disponibles desde internet en repositorios que manejan distintas versiones de compilación dependiendo de la versión de OpenWrt. Entre el software portado a la plataforma MIPS que está disponible en los repositorios se encuentra:

- Asterisk: Software de Voz Sobre IP (VOIP)
- Apache: Servidor Web
- MySql: Servidor de Base de Datos relacionadas.
- WifiDog: Servidor de Portal Cautivo
- Snort: Sistema de Detección de Intrusos.
- Samba: Servidor de archivos del protocolo SMB.

42 Graphic User Interface
43 Fuente: http://wiki.openwrt.org/

4.5.1.1. Sistema de archivos OpenWrt

Los sistemas de archivos (filesystem en inglés), estructuran la información guardada en una unidad de almacenamiento, que luego será representada ya sea textual o gráficamente utilizando un gestor de archivos. La mayoría de los sistemas operativos poseen su propio sistema de archivos. OpenWrt incorpora 2 sistemas de archivos: SQUASHFS y JFFS2 los cuales manejan las particiones de la memoria Flash y la memoria RAM del dispositivo. Estos sistemas de archivos son configurados automáticamente al momento de instalar el firmware.

```
root@Cautivame:~# df
Filesystem           1k-blocks      Used Available Use% Mounted on
rootfs                    1600      1600         0 100% /
/dev/root                 1600      1600         0 100% /rom
tmpfs                     7172       376      6796   5% /tmp
/dev/mtdblock/4           1728      1332       396  77% /jffs
mini_fo:/jffs             1600      1600         0 100% /
```

Ilustración 4-3 Puntos de montaje del OpenWrt 8.04

- **SQUASHFS**. Es un sistema de archivos basado en software libre comprimido de sólo lectura, que reduce archivos, nodos y directorios, y soporta tamaños de bloque de hasta 1024 KB para mayor compresión.

  Este sistema de archivos está pensado para su uso como sistema de archivos genérico de sólo lectura y en dispositivos de bloques/sistemas de memoria limitados donde se requiere poca sobrecarga. La versión estándar de SquashFS utiliza compresión mediante gzip.

  También se lo utiliza en las versiones en Live CD de Linux. A menudo se combina con un sistema de archivos de unión de otros sistemas de archivos, como UnionFS o aufs, para proveer un entorno de lectura-escritura para distribuciones Live CD de Linux. De este modo se combinan las ventajas de la alta velocidad de compresión de SquashFS con la posibilidad de alterar la distribución mientras se ejecuta.

- **JFSS2**: Journalling Flash File System versión 2 o JFFS2 es un sistema de archivos de registro estructurado para el uso en dispositivos de memoria flash. Es el sucesor de JFFS. JFFS2 se ha incluido en el Kernel de Linux desde la versión 2.4.10. Este sistema de archivos no está comprimido, lo que implica la utilización de mayor espacio en la memoria flash, sin embargo, sus capacidades de lectura y escritura le permiten al usuario modificar al dispositivo y guardar archivos, instalar software y grabar configuraciones temporales.

4.5.2. DD-WRT

DD-WRT es un firmware no-oficial para Linksys WRT54G/GS/GL y otros enrutadores 802.11g basados en un diseño de referencia similar o igual al Broadcom. Las primeras versiones de DD-WRT se basaron en el firmware "Alchemy" de Sveasoft Inc, que a su vez se basa en el firmware original GPL de Linksys y en otros proyectos. DD-WRT se creó debido a que Sveasoft comenzó a cobrar 20$ por descargar su software.

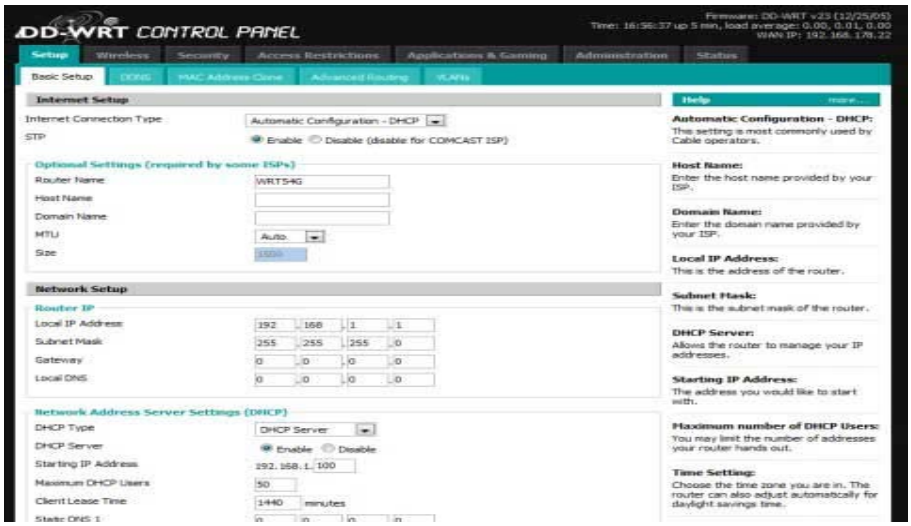


Ilustración 4-4 Pantalla de administración web del DD-WRT

Entre otras características que el firmware oficial de LinkSys no incluye, DD-WRT añade el Kai Console Gaming network, WDS Puente de red/repetidor, Autenticación RADIUS

para comunicaciones Wireless más seguras, avanzado control de balanceo de cargas o Calidad de servicio (QoS), y software para que funcionen las tarjetas SD/MMC que se le pueden instalar haciendo algunas modificaciones al dispositivo.[44]

Al estar basado en OpenWrt el DD-WRT ofrece características similares como por ejemplo su sistema de archivos y manejadores de paquetes, y una de sus principales características es la facilidad de configuración, ya que tiene una interfaz web muy amigable para los usuarios comunes además que incorpora software pre instalado para la mayoría de requerimientos de los usuarios. Este firmware a comparación con OpenWrt está diseñado para usuarios con poca experiencia en GNU / LINUX, por lo que no incluye características avanzadas de administración y configuración de red.

4.6. SERVIDOR DE PORTAL CAUTIVO WIFIDOG

El proyecto WifiDog fue iniciado por la empresa canadiense Île sans fil[45], y se encuentra actualmente en producción. Está desarrollado como contraparte a otras soluciones de portales cautivos las cuales son difíciles de implementar en equipos embebidos ya que para su funcionamiento necesitan de espacio de almacenamiento extra y procesadores más potentes. Está diseñado para tener control de acceso centralizado, control de estado del nodo y el manejo de contenido local específico para cada punto de acceso.

A diferencia de otras soluciones de portal cautivo, Wifidog no necesita que una ventana del explorador web esté siempre activa, por lo que funciona con cualquier plataforma con un navegador web, incluyendo PDAs y teléfonos celulares. Esta desarrollado en el lenguaje de programación “C” para que sea fácil de incluir en los sistemas embebidos (Se ha diseñado para el Linksys WRT54G, pero corre en cualquier plataforma de GNU / Linux). Además su tamaño reducido hace la mejor opción para un portal cautivo embebido, por ejemplo:

44 Fuente: http://www.dd-wrt.com/wiki/index.php/%C2%BFQu%C3%A9_es_%22DD-WRT%22%3F
45 www.ilesansfil.org

una instalación típica sólo necesita de 30kb, y una instalación funcional podría hacerse en menos de 10kb si es necesario.

El conjunto de herramientas del portal cautivo Wifidog, es principalmente un servidor de autenticación desarrollada en PHP usando una base de datos PostgreSQL. La puerta de enlace Wifidog maneja las reglas del Firewall, denegando el acceso a la red a los usuarios que no han sido autentificados, y establece los puertos y protocolos permitidos a los usuarios registrados. Esta puerta de enlace se conecta con el servidor de autenticación el cual compara con la base de datos para permitir o denegar el acceso a los usuarios y dependiendo de las configuraciones aplica las restricciones de uso por ejemplo el límite de tiempo o la cantidad de ancho de banda disponible para cada usuario.

A continuación se detallan algunas de sus características:

- Posee ayuda multilingüe para usuarios (con la detección del navegador y la selección del usuario) con la capacidad de agregar más idiomas usando un redactor y disponible en los siguientes idiomas: Inglés, Francés, Alemán, Español , Italiano, Griego, Portugués, Sueco, Búlgaro y Japonés.
- Informes y estadística incluyendo: 10 consumidores más altos del ancho de banda , 10 usuarios más frecuentes, 10 usuarios más móviles, exportación de los datos a SQL, informe de cuántos usuarios utilizan realmente la red , registro de la conexión , gráfico de uso de la red (por hora, día laborable y mes) , informe individual del usuario, información de los nodos más populares (por visita), información del estado de la red , estado del nodo , registro interno e informe del registro del usuario.
- Validación de usuario: Los usuarios pueden crear y activar cuentas utilizando el email como validador de identidad, sin la intervención del administrador. WifiDog concede al usuario un período de gracia de algunos minutos después de registrase

en el portal para validar su email. Los usuarios pueden solicitar que el servidor vuelva a enviar el email de la validación[46].

4.6.1. Diagrama de Flujo del proceso de autentificación de WifiDog

El siguiente diagrama de flujo de datos describe las fases que ocurren en el proceso de autentificación de un usuario en una red de portales cautivos.

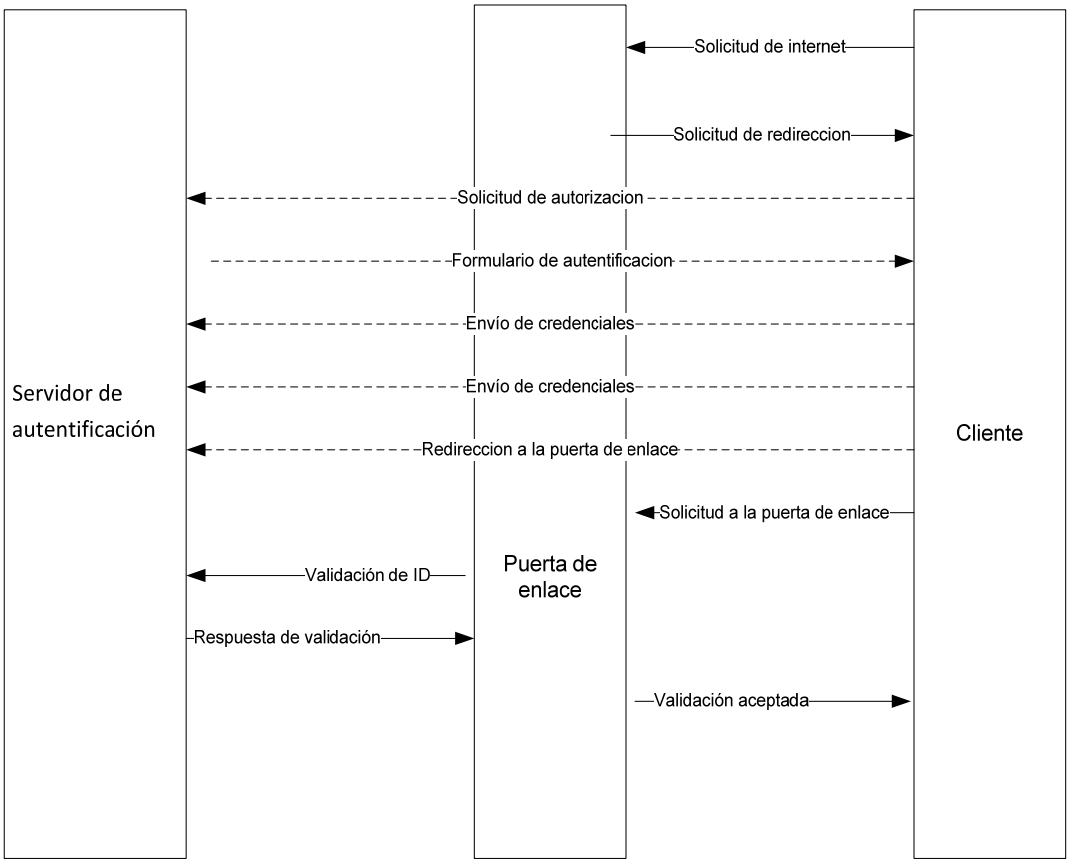


Ilustración 4-5 Diagrama de flujo de datos en el proceso de autenticación WifiDog

46 Fuente: http://dev.wifidog.org/wiki/About

Descripción del Diagrama de Flujo de Datos.

1. El cliente hace su petición inicial, como si ya estuviera conectado, (por ejemplo: http://www.google.com)

2. Reglas de firewall. El portal de envía la solicitud para redirigir a un puerto local en el Portal, Seguido a esto, el Portal proporciona una respuesta de redirección HTTP que contiene el ID de Gateway.

3. El cliente hace su solicitud al servidor de autenticación.

4. El portal de acceso responde con una página que tiene un formulario de acceso para usuarios.

5. El cliente proporciona su información de identificación (nombre de usuario y contraseña)

6. Después de una autenticación exitosa, el cliente obtiene una redirección HTTP al servidor web de la propia puerta de enlace con su prueba de autenticación (token), http://GatewayIP:GatewayPort/wifidog/auth?token=[auth token].

7. El cliente se conecta a la puerta de enlace y permite su acceso al internet

8. El servidor de autenticación notifica al cliente que su solicitud se ha realizado correctamente

4.7. COMPONENTES DE SOFTWARE NECESARIOS PARA EL SERVIDOR DE AUTENTIFICACIÓN DEL PORTAL CAUTIVO

4.7.1. Ubuntu Linux

El 8 de julio de 2004, Mark Shuttleworth y la empresa Canonical Ltd. anunciaron la creación de la distribución Ubuntu. Ésta tuvo una financiación inicial de 10 millones de dólares (US$). El proyecto nació por iniciativa de algunos programadores de los proyectos Debian, Gnome porque se encontraban decepcionados con la manera de operar del Proyecto Debian, la distribución Linux sin ánimo de lucro más popular del mundo.

De acuerdo con sus fundadores, Debian se trataba de un proyecto demasiado burocrático donde no existían responsabilidades definidas y donde cualquier propuesta interesante se ahogaba en un mar de discusiones. Asimismo, Debian no ponía énfasis en estabilizar el desarrollo de sus versiones de prueba y sólo proporcionaba auditorías de seguridad a su versión estable, la cual era utilizada sólo por una minoría debido a la poca o nula vigencia que poseía en términos de la tecnología Linux actual.

Ubuntu está basado en la distribución Debian GNU/Linux y soporta oficialmente dos arquitecturas de hardware: Intel x86, AMD64. Sin embargo ha sido portada extraoficialmente a cinco arquitecturas más: PowerPC, SPARC (versión "alternate"), IA-64, Playstation 3[47] y HP PA-RISC.

Al igual que casi cualquier distribución basada en Linux, Ubuntu es capaz de actualizar a la vez todas las aplicaciones instaladas en la máquina a través de repositorios, a diferencia de otros sistemas operativos comerciales, donde esto no es posible. Esta distribución ha sido y está siendo traducida a numerosos idiomas, y cada usuario es capaz de colaborar voluntariamente a esta causa, a través de Internet. Los desarrolladores de Ubuntu se basan en gran medida en el trabajo de las comunidades de Debian, GNOME y KDE (como es el caso de las traducciones)[48].

4.7.2. Servidor Web Apache

El servidor Apache es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, Windows, Macintosh entre otras, que implementa el protocolo HTTP/1.1. Está basado inicialmente en el código del NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que sus desarrolladores querían que tuviese la vinculación de algo que es firme y enérgico pero no agresivo, y la tribu Apache

47 Consola de Juegos de video.
48 Fuente: http://ubuntu.com.es/

fue la última en rendirse al que pronto se convertiría en gobierno de EEUU. En sus inicios Apache consistía solamente en un conjunto de parches para ser aplicados al servidor de NCSA. Apache tiene amplia aceptación en la red y desde 1996, Apache es el servidor HTTP más usado en el mundo. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años[49].

Es utilizado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web. Muchas aplicaciones web están diseñadas asumiendo como ambiente de implementación a Apache, o que utilizarán características propias de este servidor web. En una distribución Linux para servidores, Apache es el componente de servidor web en la popular plataforma de aplicaciones LAMP, junto a MySQL y los lenguajes de programación PHP/Perl/Python[50].

Este servidor web es redistribuido como parte de varios paquetes propietarios de software, incluyendo la base de datos Oracle. Mac OS X [51]integra Apache como parte de su propio servidor web y como soporte de su servidor de aplicaciones WebObjects. Es soportado por Borland en las herramientas de desarrollo Kylix y Delphi. Apache es incluido con Novell NetWare 6.5[52], donde es el servidor web por defecto, y en muchas distribuciones Linux. Es utilizado para muchas otras tareas donde el contenido necesita ser puesto a disposición en una forma segura y confiable. Un ejemplo es al momento de compartir archivos desde una computadora personal hacia Internet[53].

El principal competidor de Apache es Microsoft Internet Information Services (IIS), algunos de los sitios web más grandes del mundo están ejecutándose sobre Apache. La capa frontal (front-end) del motor de búsqueda Google está basada en una versión modificada de Apache, denominada Google Web Server (GWS).

49 Estadísticas históricas y de uso diario proporcionadas por Netcraft: http://www.netrcraft.com.
50 Lenguajes de programación orientadas a la web, que compilan el software bajo demanda.
51 Sistema Operativo de Apple Computer.
52 Sistema Operativo de Red de la empresa Novell.
53 (Schroder, 2005)

4.7.3. Servidor de Base de Datos Relacionadas PostgreSQL

PostgreSQL es una base de datos relacional[54], distribuida bajo licencia BSD y con su código fuente disponible libremente. Es el motor de bases de datos de código abierto más potente en los últimos tiempos.

Sus características técnicas la hacen una de las bases de datos más potentes y robustas del mercado. Su desarrollo comenzó hace más de 15 años, y durante este tiempo, estabilidad, potencia, robustez, facilidad de administración e implementación de estándares han sido las características que más se han tenido en cuenta durante su desarrollo. En los últimos años se han concentrado mucho en la velocidad de proceso y en características demandadas en el mundo empresarial.

PostgreSQL se puede ejecutar en la gran mayoría de sistemas operativos existentes en la actualidad, entre ellos Linux y UNIX en todas sus variantes (AIX, BSD, HP-UX, SGI IRIX, Mac OS X, Solaris, y Windows. Las características más importantes y soportadas son[55]:

- Llaves ajenas (foreign keys)
- Joins
- Vistas (views)
- Disparadores (triggers)
- Reglas (Rules)
- Funciones/procedimientos almacenados (stored procedures) en numerosos lenguajes de programación, entre otros PL/pgSQL (similar al PL/SQL de Oracle)
- Herencia de tablas (Inheritance)
- PITR - point in time recovery
- Tablespaces
- Replicación asíncrona

[54] En una base de datos relacional, todos los datos se almacenan y se acceden a ellos por medio de relaciones.
[55] (Schroder, 2005)

4.7.4. Firewall de Linux – NETFILTER IPTABLES

Un Firewall es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

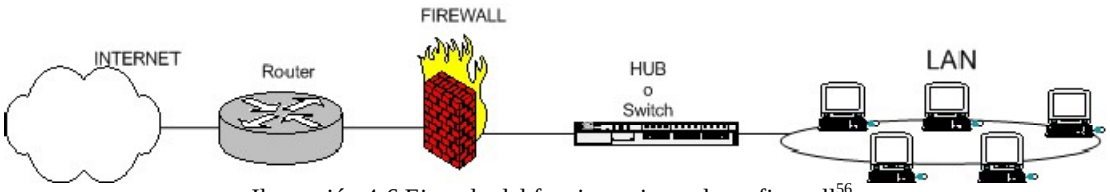


Ilustración 4-6 Ejemplo del funcionamiento de un firewall[56]

Los *Firewall* pueden ser implementados en hardware o software, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del Firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar un Firewall a una tercera red (NIC), llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para Firewall basados en Linux.

56 Fuente: http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/

El componente más popular construido sobre Netfilter es IPTables, una herramienta de Firewall que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.

IPTables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre IPTables se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter. Sin embargo, el proyecto ofrece otros subsistemas independientes de IPTables tales como "*connection tracking system*" o sistema de seguimiento de conexiones, o que, que permite encolar paquetes para que sean tratados desde espacio de usuario. IPTables es un software disponible en prácticamente todas las distribuciones de Linux actuales.

IPTables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Cada regla especifica qué paquetes la cumplen (match) y un destino que indica qué hacer con el paquete si éste cumple la regla. Cada paquete de red que llega a una computadora o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete. Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la política de destino de la cadena dicta qué hacer con el paquete. Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada (lo que se denomina implicit target RETURN o RETORNO de destino implícito). Solo las cadenas predefinidas tienen políticas.

En IPTables, las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes IP, que determinan lo que se debe hacer con ellos. Cada regla puede desechar el paquete de la cadena (cortocircuito), con lo cual otras cadenas no serán consideradas. Una cadena puede contener un enlace a otra cadena: si el paquete pasa a través de esa cadena entera o si cumple una regla de destino de retorno, va a continuar en la primera cadena. No hay un límite respecto de cuán anidadas pueden estar las cadenas.[57]

A continuación se detalla el diagrama de procesos de IPTABLES.

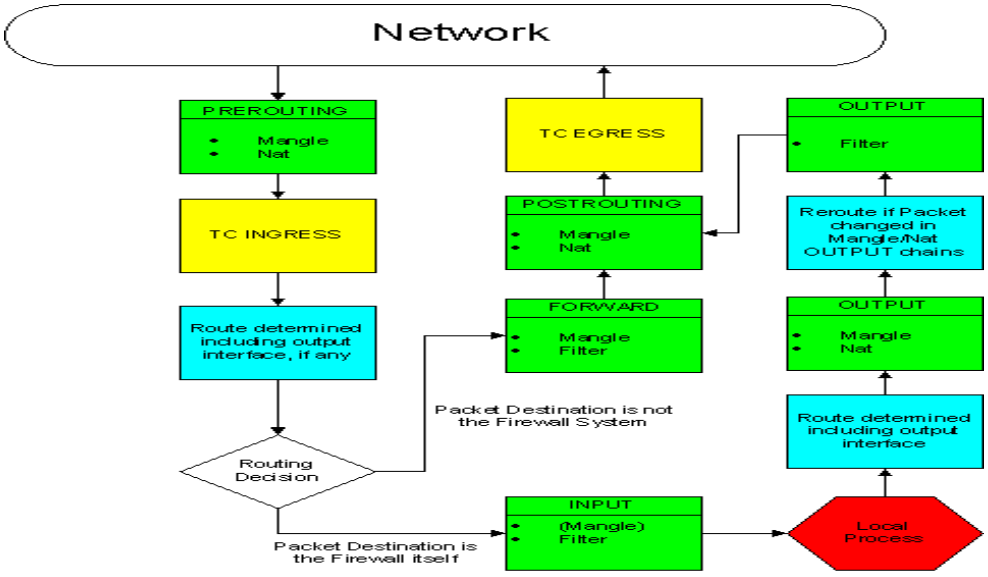


Ilustración 4-7 Diagrama de flujo de datos de IPTABLES[58]

Antes de IPTables, los programas más usados para crear Firewall en Linux eran ipchains en el núcleo Linux 2.2 e ipfwadm en el núcleo Linux 2.0, que a su vez se basaba en ipfw de BSD. Tanto ipchains como ipfwadm alteran el código de red para poder manipular los paquetes, ya que no existía un framework general para el manejo de paquetes hasta la aparición de IPTables. IPTables mantiene la idea básica introducida en Linux con ipfwadm: listas de reglas en las que se especifica qué buscar dentro de un paquete y qué

58 Fuente: http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall-html/

hacer con ese paquete. Ipchains agrega el concepto de cadenas de reglas (chains) e IPTables extendió esto a la idea de tablas: se consultaba una tabla para decidir si había que NAT-ear un paquete, y se consultaba otra para decidir como filtrar un paquete. Adicionalmente, se modificaron los tres puntos en los que se realiza el filtrado en el viaje de un paquete, de modo que un paquete pase solo por un punto de filtrado[59].

4.8. **TFTP**

TFTP (Trivial File Transfer Protocol) es un protocolo de transferencia de archivos sencillo, similar al FTP, definido por primera vez en 1980. Suele utilizarse en la transferencia de archivos pequeños entre computadoras de una red. Utiliza el puerto UDP 69 (puerto 69) como protocolo de transporte a diferencia de FTP que utiliza el puerto 21 TCP. Es utilizado generalmente para transferir archivos pequeños dentro de una red.

Algunas de las características de este protocolo son:

- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor. Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

59 Fuente: http://www.netfilter.org/documentation/index.html

A continuación se muestra el ejemplo de la transferencia de un archivo por TFTP

1. La máquina A, que inicia la comunicación, envía un paquete RRQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.

2. responde con un paquete ACK (acknowledgement/confirmación), que también sirve para informar del puerto de la máquina B al que tendrá que enviar los paquetes restantes.

3. La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.

4. El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

CAPITULO V

5. IMPLEMENTACIÓN DE LAS HERRAMIENTAS GNU / GPL EN EL ENRUTADOR E INSTALACIÓN DEL SERVIDOR DE AUTENTIFICACIÓN.

5.1. INSTALACIÓN DEL FIRMWARE GNU / LINUX OPENWRT EN EL ENRUTADOR WRT54GL.

Existen diferentes tipos de Firmware para el WRT54G los cuales proveen de diversas funcionalidades como se puede observar en el Capítulo 4 Pagina 61. Para el desarrollo de este proyecto se eligió la utilización de OpenWrt como Firmware los enrutadores inalámbricos WRT54G V 2.0 y WRT54GL V 1.1; debido a que, es la distribución que mantiene un desarrollo más acelerado y tiene una amplia gama de software que ha sido portado a la arquitectura del enrutador.

Las instrucciones de instalación del firmware para los modelos WRT54G pueden variar dependiendo del tipo de firmware y modelo del enrutador, lo que implica la comprobación y revisión de todos sus procedimientos para la instalación. A continuación se describirán 3 formas de instalación del firmware de terceros, a partir de la experiencia adquirida en el proceso de instalación y de los diferentes casos que pueden presentarse cuando se modifica el hardware.

5.2.INSTALACIÓN DE OPENWRT UTILIZANDO TFTP

La instalación del firmware de terceros utilizando el protocolo TFTP es fiable y segura, debido a que tiene métodos de comprobación y recuperación de daños. Sin embargo resulta compleja por la cantidad de procedimientos previos para preparar el dispositivo. A continuación se detalla el proceso de instalación.

Al momento de encender el dispositivo WRT54G desde la versión 2 en adelante se inicia un proceso llamado CFE (*Common Firmware Environment*) que es el encargado de ejecutar las instrucciones básicas del proceso de encendido para iniciar el sistema operativo. Una de las primeras funciones que realiza el CFE es chequear si existe una partición en la memoria no volátil NVRAM[60], en caso de no existir, el CFE crea una nueva partición utilizando las instrucciones grabadas. Independientemente de que sea una nueva partición o una existente, el proceso de encendido revisa obligatoriamente el parámetro *boot_wait* y en caso de que esté activado inicia un servidor TFTP el cual espera por una conexión por unos segundos; a continuación, se ejecuta un control de redundancia cíclica (CRC) para comprobar que el firmware no esté corrupto. En caso de que el firmware tenga algún daño el CFE mantendrá el servidor TFTP activo para que se pueda transferir un nuevo firmware además de los siguientes procesos:

Al encender el enrutador el CFE inicia un conjunto de utilidades IP, que permiten realizar dos acciones, la primera es responder a solicitudes ARP[61] para la dirección IP 192.168.1.1 y escucha el trafico Broadcast ARP. Una vez que el sistema ha iniciado normalmente, el contenido de la partición NVRAM es copiado a la memoria RAM, este proceso se ejecuta automáticamente.

60 Léase Almacenamiento en la página 59
61 ARP (Address Resolution Protocol) Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

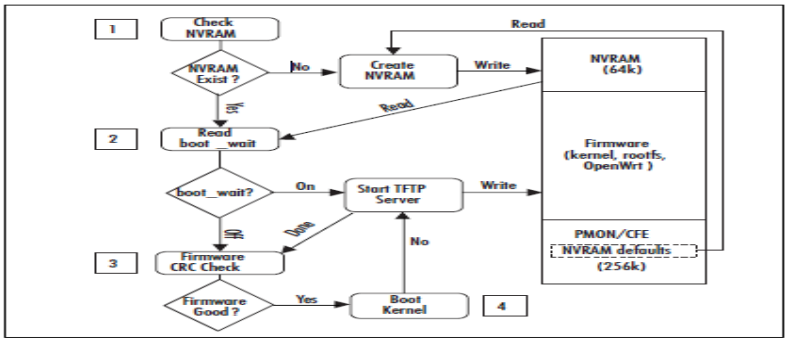


Ilustración 5-1 Diagrama de flujo de datos del sistema de encendido del WRT54G[62]

Una vez que el comando *boot_wait* este encendido, se puede realizar la instalación vía TFTP la cual es más segura que todos los demás tipos de instalación, debido a que el firmware es instalado sin que el sistema operativo del enrutador se haya cargado, lo que disminuye el riesgo de que se corrompa. A continuación se describen los pasos a seguir para realizar una instalación TFTP.

- Es necesario descargar la imagen pre compilada del firmware que se instalará en el WRT54GL, para las pruebas de este proyecto se ha utilizado OpenWrt Kamikaze 8.04.
- A continuación se configura la dirección IP en la interfaz de red en la computadora que servirá para transferir el firmware, dicha dirección tiene que estar en la misma red que el enrutador, la cual el CFE configura automáticamente en 192.168.1.1. entonces conociendo estos parámetros se configura la interfaz de la computadora cliente como 192.168.1.1 y la máscara de subred 255.255.255.0[63] como se puede observar en la figura 5-2. Una vez configurada la dirección IP en la computadora, es necesario conectar el cable de red.
- El proceso *boot_wait* tiene un límite máximo de espera que por defecto es de 5 segundo; sabiendo esto, es importante tener el comando TFTP con todas las instrucciones listo para su ejecución. El uso del comando TFTP en Windows con

62 (Asadoorian, 2007)
63 La máscara de subred se utiliza para dividir grandes redes en redes menores, facilitando la administración y reduciendo el tráfico inútil, de tal manera que será la misma para ordenadores de una misma subred.

las instrucciones necesarias para enviar el firmware del enrutador es el siguiente: *tftp -i 192.168.1.1 put c:\openwrt-wrt54g-squashfs.bin*[64]

- Luego de haber configurado el comando correctamente en el símbolo de sistema de Windows o en la ventana de consola, se debe encender el enrutador y al mismo tiempo ejecutar el comando.
- Una vez que se haya ejecutado el comando correctamente, el enrutador se reiniciará algunas veces, esto se puede observar cuando el LED de Poder titila constantemente, al cabo de unos segundos dejará de titilar y eso significa que el firmware fue cargado con éxito.
- Al término del proceso de la instalación del firmware por TFTP se puede acceder a la interfaz web del firmware en la dirección 192.168.1.1 para continuar con la configuración de las redes cableadas e inalámbricas.

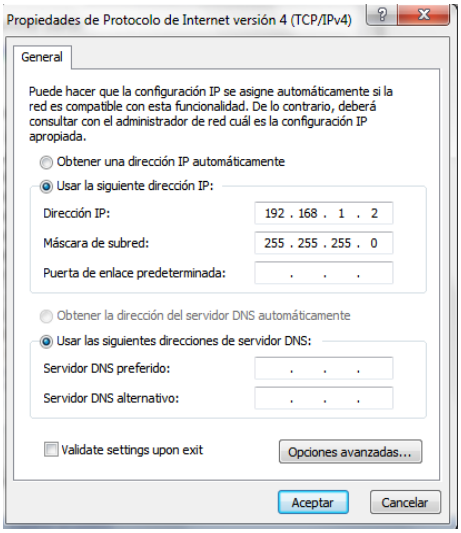


Ilustración 5-2 Configuración de dirección IP en Windows 7

64 La IP 192.168.1.1 es la dirección remota del enrutador y c:\openwrt-wrt54g-squashfs.bin es la ubicación del firmware que se enviara.

5.3. INSTALACIÓN DE OPENWRT POR MEDIO DE LA INTERFAZ WEB

La instalación de un nuevo firmware utilizando la interfaz web, es sin lugar a dudas la más fácil en comparación con la instalación por medio de TFTP, debido a que solo es necesario subir al enrutador inalámbrico la imagen del firmware, y además de esto es una instalación segura, debido a que la configuración de fabrica del sistema operativo original valida la imagen antes de empezar con la instalación.

En primer lugar es necesario descargar la imagen pre compilada del firmware que se instalara en el WRT54GL, para las pruebas de este proyecto se ha utilizado OpenWrt Kamikaze 8.04[65].

Una vez obtenida la imagen del nuevo firmware que se va a instalar es necesario realizar algunos cambios al enrutador inalámbrico, el primer paso es restaurarlo a su configuración de fabrica, este proceso se lo puede realizar manteniendo el botón apretado por 25 segundos, esto es importante debido a que las configuraciones del enrutador pueden afectar el proceso de actualización, y puede resultar en la corrupción del firmware cargado.

En seguida de haber restaurado el enrutador a su configuración original se puede acceder a la consola de administración web en la dirección IP 192.168.1.1 y utilizar el nombre de usuario por defecto "*admin*" y contraseña "*admin*".

65 Fuente: http://downloads.openwrt.org/kamikaze/8.09/brcm-2.4/openwrt-wrt54g-squashfs.bin

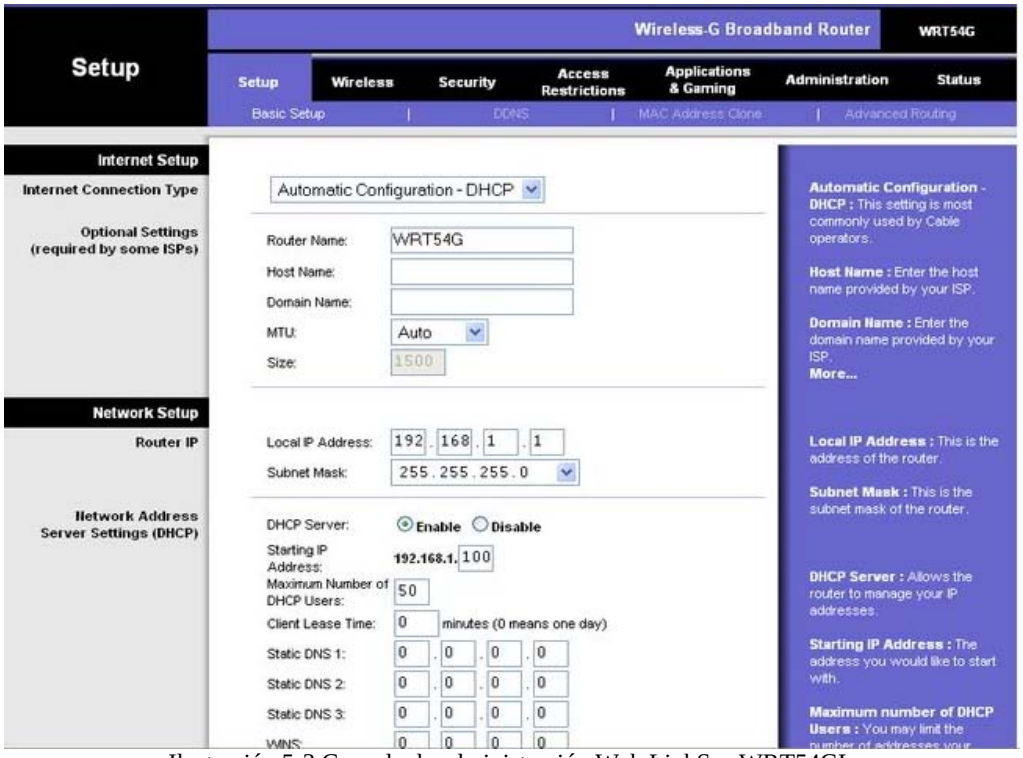


Ilustración 5-3 Consola de administración Web LinkSys WRT54GL

Ejecutados estos pasos previos se puede cargar el firmware utilizando la consola de administración web. Es necesario ingresar a esta interfaz escribiendo en el navegador web http://192.168.1.1. Debido a que en el proceso de configuración de un nuevo firmware el servicio de DHCP está deshabilitado, es necesario configurar una dirección IP estática dentro de la red por defecto del enrutador, en este caso se configura la dirección IP 192.168.1.2 con máscara de red 255.255.255.0. A continuación se detallan los pasos para la actualización del firmware utilizando la interfaz web en un WRT54GL:

Una vez realizados los pasos anteriores, se ingresa a la consola de administración web y se navega hasta el apartado llamado Firmware Upgrade que se encuentra localizado en "Administration | Firmware Upgrade".

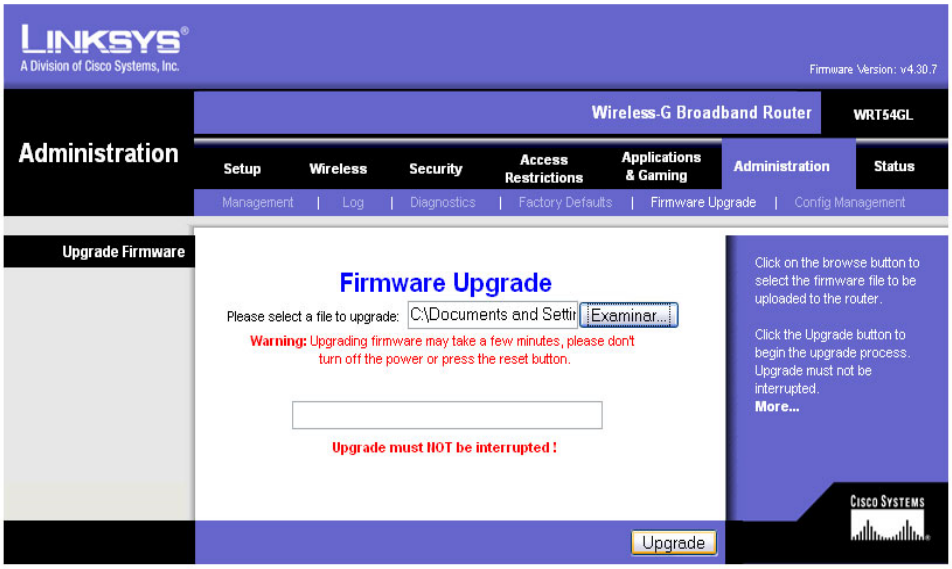


Ilustración 5-4 Consola de administración Web del LinkSys WRT54GL

Como se puede observar en la ilustración 5-4, en la sección “Firmware Upgrade”, se debe seleccionar el botón “Examinar” para localizar el archivo que contiene el firmware pre compilado. Una vez que se haya seleccionado la imagen apropiada para este dispositivo se selecciona el botón “Upgrade”.

Después de enviar el firmware al equipo, este se encarga de verificar la imagen previamente adjuntada para detectar el tipo de instalación que llevara a cabo. Cuando la carga del firmware comience aparecerá un mensaje en letras rojas que indica “*Upgrade must NOT be interrupted*” que en inglés significa “La actualización no debe ser interrumpida”. En este punto del proceso de actualización es extremadamente importante que la conexión de red, la corriente eléctrica del enrutador y la computadora que envía la imagen estén disponibles. De darse una falla de comunicación el enrutador podría quedar con el firmware dañado, lo que implicaría la necesidad de una instalación por JTAG para recuperar el enrutador.

Una vez realizados estos pasos, aparecerá un mensaje indicando que la actualización tuvo éxito “*Upgrade is Successful*”. A continuación solo basta con presionar el botón “*Continue*” para que el equipo se reinicie con el nuevo sistema operativo.

5.4. INSTALACIÓN DE OPENWRT POR MEDIO DE CABLE JTAG

La instalación del firmware de terceros utilizando el Cable JTAG es la instalación más complicada y lenta, pero a su vez es la más limpia debido a que en el proceso de instalación toda la memoria NVRAM y sus particiones son borradas y creadas nuevamente, lo que permite manipular de mejor manera al enrutador. Asimismo este tipo de instalación es útil para restaurar enrutadores con firmware defectuoso los cuales no permiten ninguna de los anteriores tipos de instalación por varias razones como por ejemplo que el parámetro *boot_wait* no está activado y en consecuencia el servicio de TFTP no puede arrancar.

Para realizar una instalación por medio del cable JTAG se necesita una computadora con un puerto de impresora paralelo LPT (*Line PrinTer*) en donde se conecta el cable JTAG se lo debe construir utilizando un cable de impresora paralela bidireccional.

En el mercado ecuatoriano es difícil de encontrar cables JTAG; pero, ventajosamente su construcción no es demasiado compleja debido a que existe bastante documentación en libros e internet y herramientas de software diseñadas para transferir imágenes de firmware.

5.4.1. Construcción de un cable JTAG.

Los dispositivos WRT54G poseen un grupo de puertos multipropósito los cuales pueden proveer de corriente eléctrica, puertos de entrada, salida, sincronización de reloj y tierra.

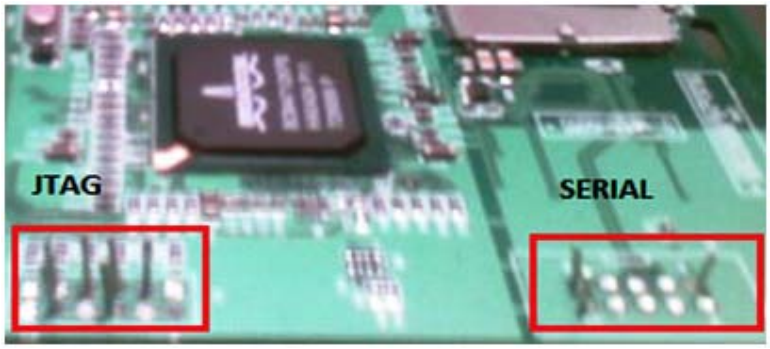


Ilustración 5-5 Puerto JTAG de un LinkSys WRT54G V 2.0

Para la implementación del cable JTAG en el enrutador inalámbrico se ha tomado como ejemplo el modelo WRT54G V2.0 el cual al igual que los otros modelos tiene un puerto JTAG y SERIAL como se puede observar en la ilustración 5-5. Dicho enrutador puede retirarse de su carcasa quitando las antenas y presionando los extremos inferiores con cuidado para desprender la parte anterior. Para mas referencias obsérvese la ilustración 5-6.


Ilustración 5-6 Manera en la que se destapa un enrutador inalámbrico WRT54G

La mejor forma para poder adaptar el cable JTAG en el enrutador inalámbrico, es colocar pines en los puntos que van conectados a la computadora, esto permite la reconexión del cable de ser necesario y se mitiga el riesgo de dañar el equipo por una suelda defectuosa.

Además de la construcción de un cable JTAG, es necesario contar con un conjunto de utilidades llamadas "*WRT54G EJTAG DeBrick*". Este conjunto de utilidades traen consigo el driver para controlar el cable JTAG utilizando el puerto de impresora LPT y las

herramientas para cargar nuevamente el CFE, formatear la NVRAM y reinstalar el firmware.

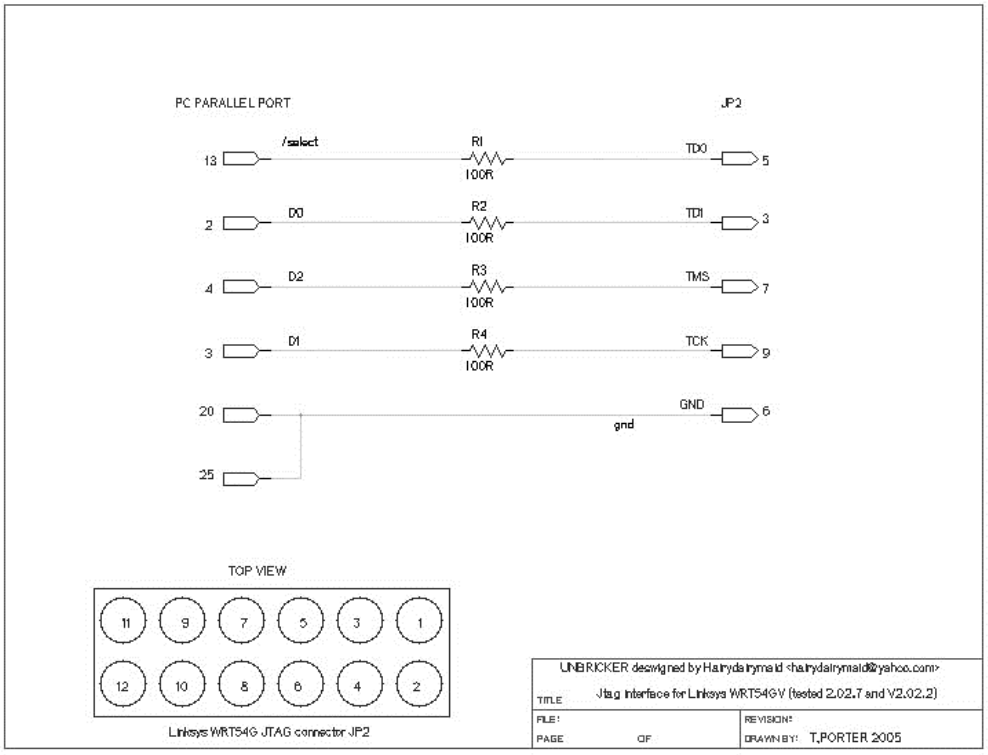


Ilustración 5-7 Diagrama de circuitos eléctricos para construir un cable JTAG[66]

Los requerimientos de hardware para construir el cable JTAG son los siguientes:

- Cable de impresora paralelo bidireccional
- 4 resistencias de 100 Ohm
- Soldador y Estaño
- Pistola de Silicón, con una placa de silicón.
- 6 pines para conectar a los puertos de conexión.
- 1 cinta aislante.

66 Fuente: http://alwar.mainfri.com/Downloads/tjtagv2/tjtagv2-1-4.zip

Para la construcción del cable JTAG se tienen que seguir las instrucciones del diagrama de circuitos que viene adjunto con el paquete de utilidades "*WRT54G EJTAG DeBrick"* en la figura 5-8, en este se detallan los puntos en donde debe ir conectado cada cable, las resistencias, los puentes y los puntos donde se conectan en el puerto del enrutador.

En primer lugar se debe abrir un cable de impresora antiguo de 1 metro de longitud y cortarlo en la mitad, debido a que la longitud del cable aumenta la resistencia lo que puede generar pérdida de información o que el proceso de instalación demore más. Una buena práctica para poder reconectar el cable JTAG al enrutador es unir conectores hembra que se los encuentra en cualquier tienda de electrónica o en una placa madre de un computador antiguo como muestra la ilustración 5-8.

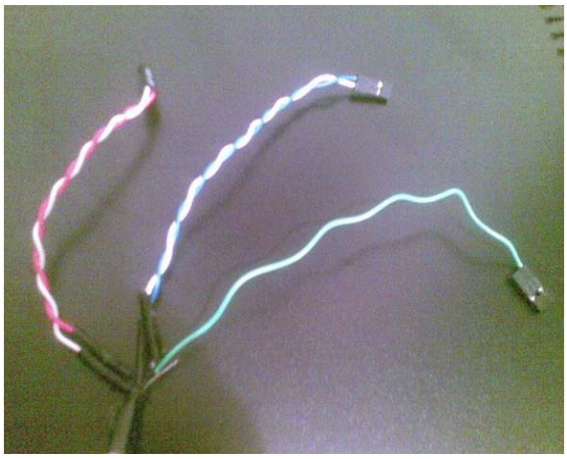


Ilustración 5-8 Cable Impresora con conectores hembra

Una vez cortado el cable de impresora y conectado los cables hembra que irán al puerto JTAG, se debe abrir el conector macho del cable de impresora para poder unir los cables necesarios como muestra la ilustración 5-7. Para el funcionamiento del cable JTAG solo son necesarios 5 cables, por lo que se debe elegir cuales cables serán los que vayan conectados al enrutador ya que el cable de impresora contiene 17 líneas de señal y 8 líneas de tierra. Es recomendable elegir colores distintos que sean distinguibles para evitar confusiones.

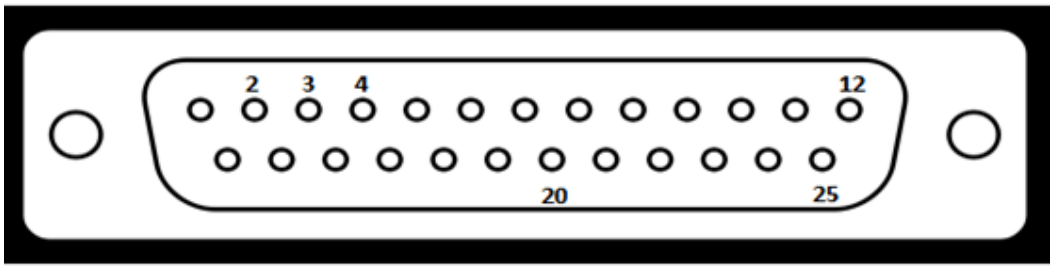


Ilustración 5-9 Puntos utilizados en el conector de Impresora LPT macho

Después de haber identificado los cables que se utilizarán, se debe soldar cada punto siguiendo la ilustración 5-7, en donde se puede observar que cada punto del conector de impresora LPT esta numerado y se pueden observar en que cable van las resistencias de 100 Ohm, además del puente que se debe conectar entre los puntos 20 y 25 que ira conectado a tierra. En la ilustración 5-9 se puede observar la numeración de los puntos del puerto de impresora LPT

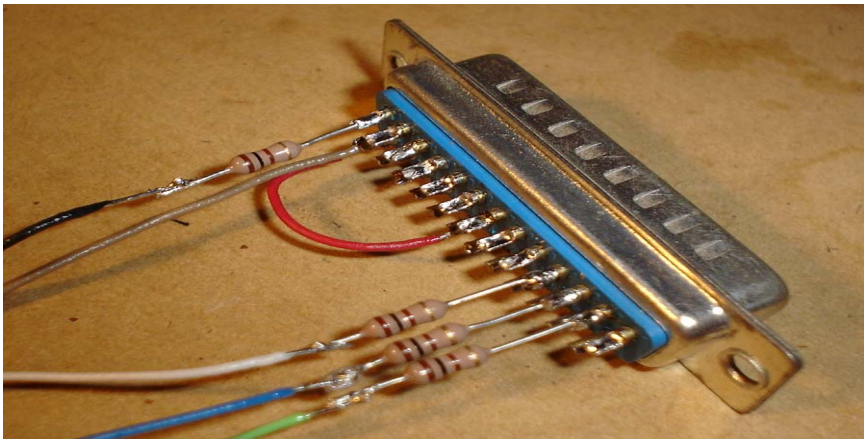


Ilustración 5-10 Conexión del puerto de impresora macho

Al finalizar la construcción del conector JTAG y haber soldado los puntos y resistencias. Es necesario realizar las pruebas de conectividad, para ello se puede utilizar un multímetro. Después de comprobar que todos los puntos funcionan y que las resistencias están trabajando se puede colocar silicón en los puntos soldados para evitar interferencia.

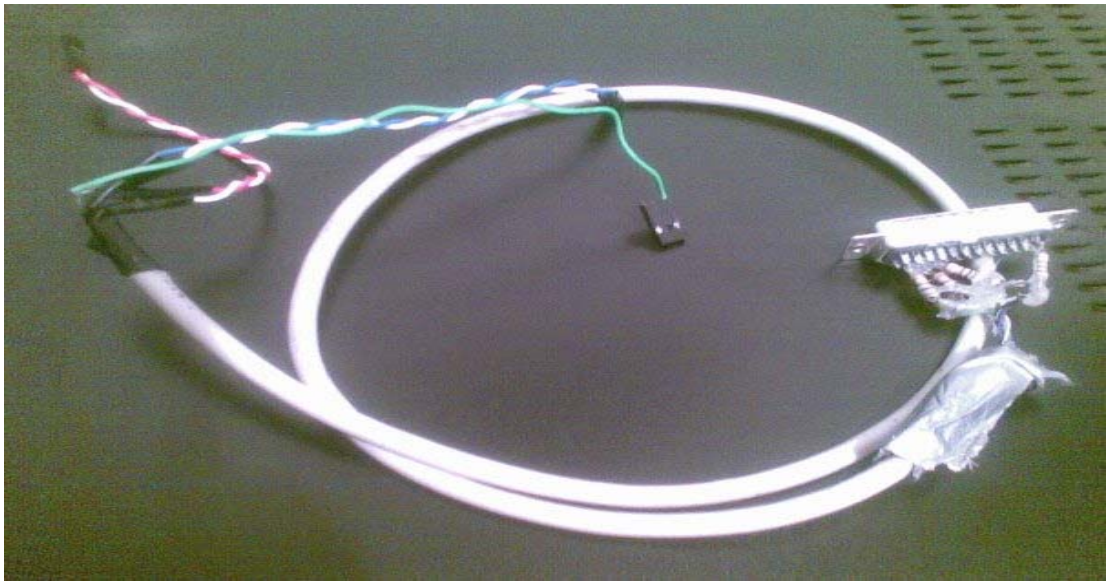


Ilustración 5-11 Cable JTAG

El siguiente paso es colocar el cable JTAG en el puerto del mismo nombre en el enrutador, para esto se debe de soldar los pines en los puntos de enrutador, para referenciar que puntos son los que funcionaran en el dispositivo es necesario utilizar el diagrama de circuitos de JTAG que se puede observar en la ilustración 5-7. Los puntos en el puerto JTAG están referenciados por dos números los cuales empiezan de derecha hacia izquierda como se puede ver en la ilustración 5-12.

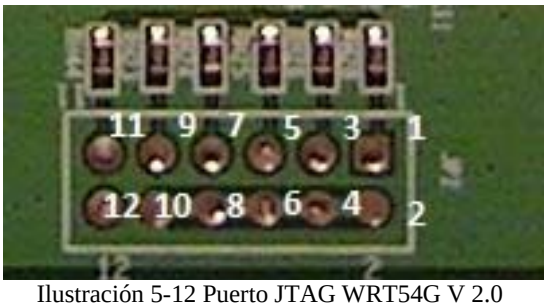


Ilustración 5-12 Puerto JTAG WRT54G V 2.0

Cada punto en el puerto JTAG del enrutador tiene una función específica como se muestra en la siguiente tabla.

Tabla 5-1 Especificación de las funciones de cada punto en el puerto JTAG del WRT54G V 2.0[67]

Punto JTAG	Señal que se transmite o recibe
1	JTAG_TRST_L
3	JTAG_TDI
5	JTAG_TDO
7	JTAG_TMS
9	JTAG_TCK
11	SW1 RESET
2,4,6,8,10,12	TIERRA

Cuando el cable JTAG esté terminado, se lo conecta en el puerto paralelo LPT de la computadora y se unen los puntos al enrutador.

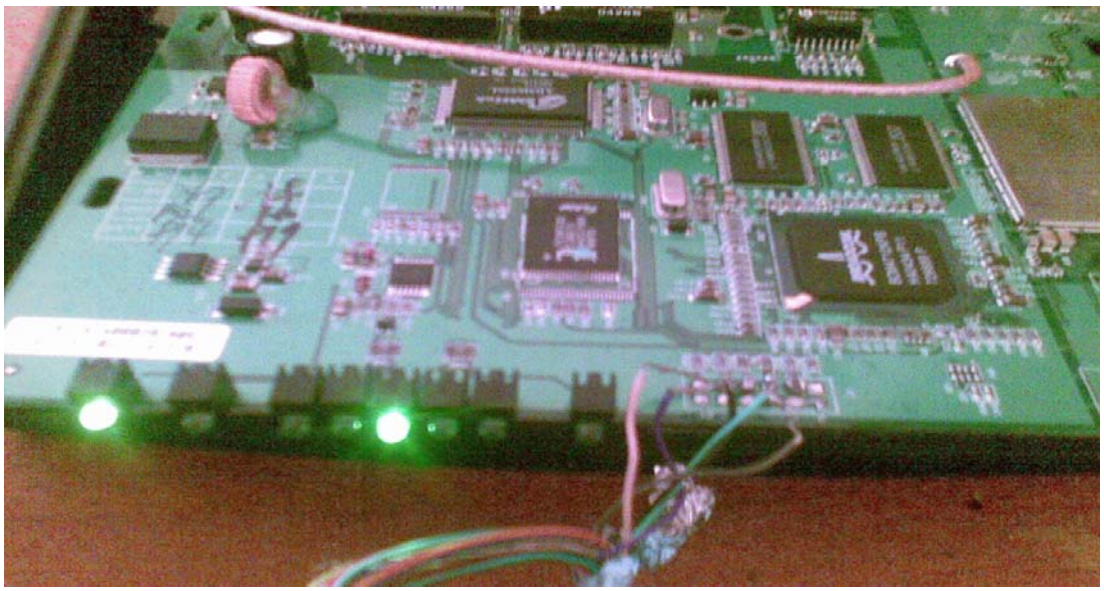


Ilustración 5-13 Cable JTAG conectado a WRT54G V2.0

67 Tomado del Broadcom BCM47XX Reference Guide

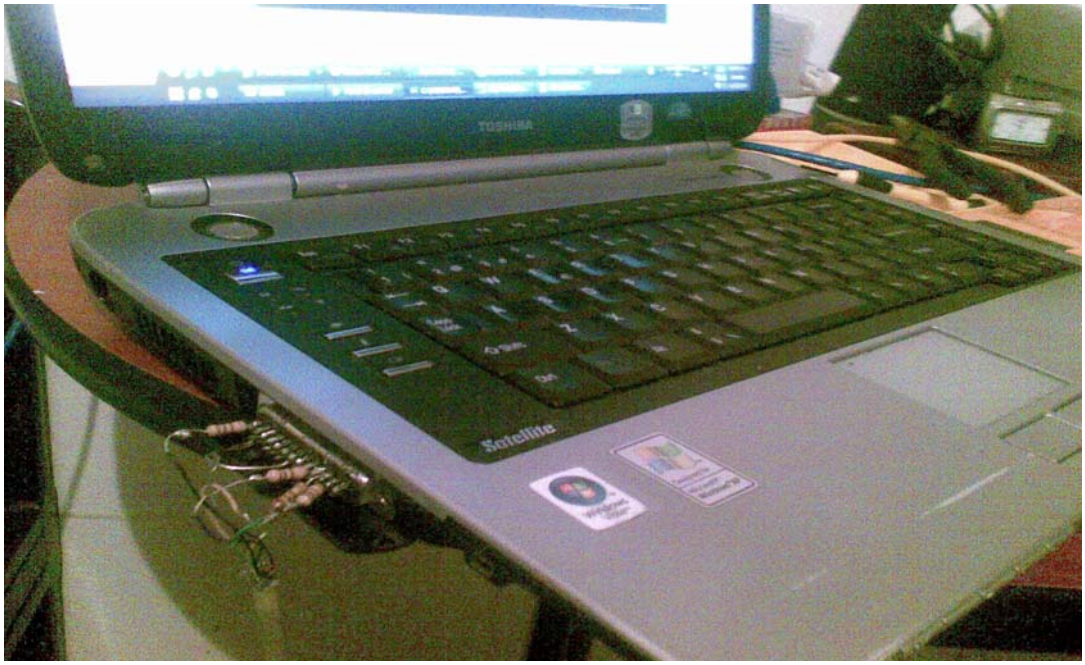


Ilustración 5-14 Cable JTAG conectado al puerto paralelo LPT de la computadora.

5.4.2. Instalación de Firmware utilizando cable JTAG.

Una vez que la construcción del cable concluyó y de realizarse las pruebas de comunicación con el multímetro, es necesario instalar el driver del cable para que la computadora pueda trabajar con el enrutador directamente conectado por el cable JTAG. Cabe señalar que el cable JTAG puede hacer que la transferencia de la imagen demore bastante.

Para la implementación del firmware por medio del cable JTAG se utilizarán dos tipos de software: WDU (WRT54G Debrick Utility) especialmente desarrollado para controlar la comunicación entre el enrutador inalámbrico WRT54G y la computadora, formatear y particionar la memoria NVRAM; y por otro lado, Skynet Repair Kit für Linksys que genera nuevamente el CFE para el equipo. Dicho software puede ser descargado desde la página web: http://www.wlan-skynet.de/download/index.shtml.

Antes de iniciar el proceso de transferencia de firmware, también conocido como "*Flasheo*" es importante saber que el momento de conectar el cable JTAG en el puerto paralelo en la computadora, el enrutador debe de estar apagado.

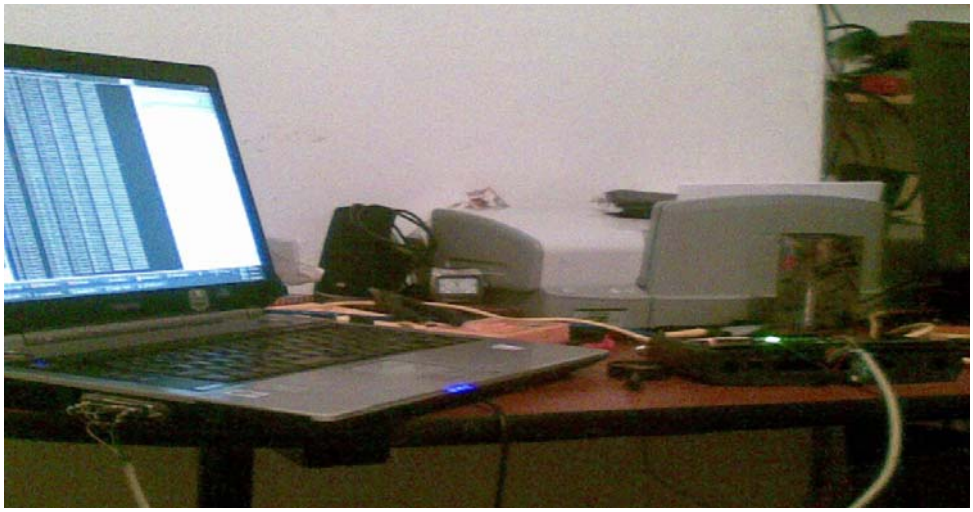


Ilustración 5-15 Computadora conectada por medio del cable JTAG con el WRT54G V2.0

Lo primero que se tiene que realizar para empezar el proceso de flasheo del enrutador es descomprimir los archivos que contienen el software "Debrick Utility". En esta carpeta se encuentran los archivos "wrt54g.exe" el cual se utiliza para la transferencia del CFE. El "giveio.sys" que contiene el driver para el cable JTAG, dicho archivo se lo debe de copiar en la carpeta C:\WINDOWS\system32\drivers, realizado este paso se ejecuta el programa "loaddrv.exe" en donde se debe seleccionar la ubicación del driver previamente copiado, luego seleccionar la ubicación, se debe dar clic en el botón "*Install*". Hecho esto el driver estará instalado permanentemente en la computadora y se podrá utilizar la herramienta para transferir el nuevo CFE.

Al finalizar el paso anterior se debe instalar el programa Skynet Repair Kit für Linksys, una vez instalado se ejecuta el programa llamado "Bootloader Creator". Luego de ejecutarlo es necesaria una conexión a internet para que el programa descargue las actualizaciones de firmware, pasados unos minutos aparecerá una pantalla indicando que el proceso de actualización concluyo exitosamente.

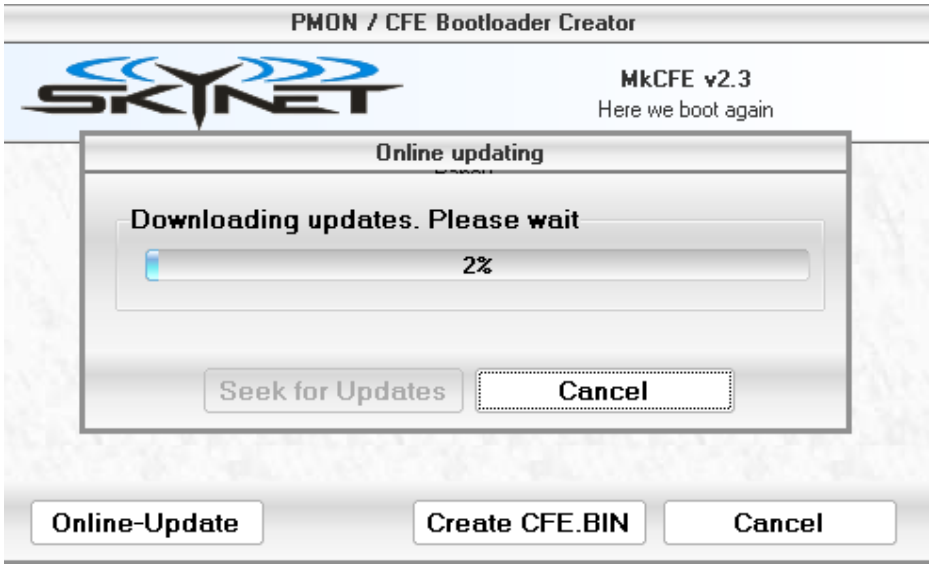


Ilustración 5-16 Actualización del software SkyNet Repair Kit

El siguiente paso es seleccionar el modelo, versión y la dirección MAC del enrutador, es importante seleccionar el modelo y versión exacta ya que en caso contrario el enrutador podría quedar inservible. La dirección MAC puede localizarse en la base del enrutador como se observa en la ilustración 5-17.

Ilustración 5-17 Dirección MAC de WRT54G V2.0 localizada en la base del dispositivo.

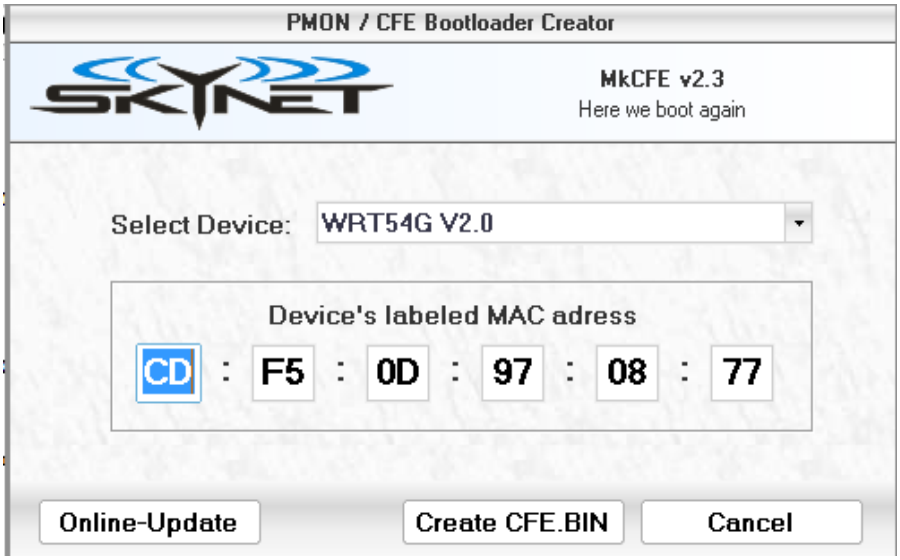


Ilustración 5-18 Selección de modelo, versión y dirección MAC del enrutador inalámbrico WRT54G V2.O

En seguida de haber ingresado los parámetros correctos, se debe dar clic en el botón llamado "*Create CFE.BIN*", esto generara un nuevo archivo llamado "CFE.bin" que tiene que guardarse en la misma carpeta en donde se descomprimió el software Debrick Utility.

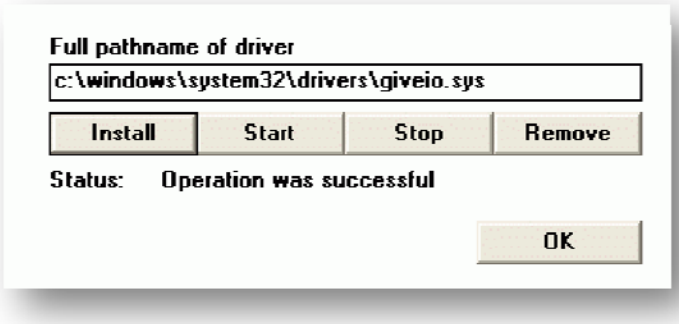


Ilustración 5-19 Programa instalador del driver para el cable JTAG "LoadDrv"

Con todos los pasos anteriores, la comunicación entre el enrutador inalámbrico y la computadora esta correctamente configurada, por lo cual se puede ejecutar el "WRT54G Debrick Utility". Este software tiene algunos parámetros que sirven para realizar test de conectividad, transferir y sobre escribir el CFE o formatear la memoria completamente y luego transferir el CFE. Para lo cual utilizaremos la opción de formatear y luego escribir el nuevo CFE debido a que esto permite realizar una instalación limpia y así evitar futuros problemas de incompatibilidad.

En este punto de la instalación, el enrutador debe de estar conectado a la computadora con el cable JTAG y encendido. Para comenzar la instalación, hay que iniciar la consola de comandos de Windows, ubicarse en la carpeta que se descomprimió y que contiene el archivo “wrt54g.exe”. Una vez ubicada la carpeta se debe ejecutar el siguiente comando: “**wrt54g.exe –erase:wholeflash /noreset /nobreak /fc:16**”, con el cual se borrara toda la memoria FLASH “-erase:wholeflash”, se impide el reinicio automático y previene de un corte de comunicación si es que existe algún error “/noreset /nobreak /fc:16”.

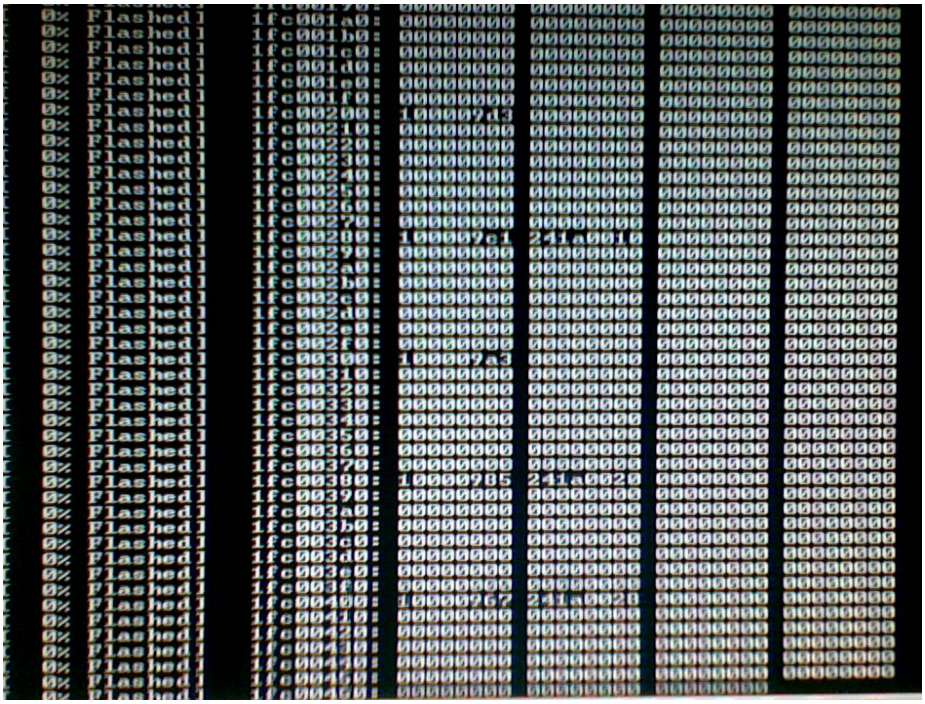


Ilustración 5-20 Proceso de borrado de la memoria FLASH.

Al finalizar el borrado de la memoria flash, es probable que el enrutador quede con el LED de encendido parpadeando, esto es normal. Ahora que el enrutador tiene formateada la memoria flash se ejecuta el comando: “**wrt54g.exe flash:cfe**” el cual utiliza el archivo CFE.bin previamente generado con Skynet Repair Kit y lo transfiere al enrutador. Este proceso tarda alrededor de 20 minutos debido a que la velocidad del cable JTAG es bastante lenta. En la pantalla se puede observar el porcentaje de la transferencia del CFE.

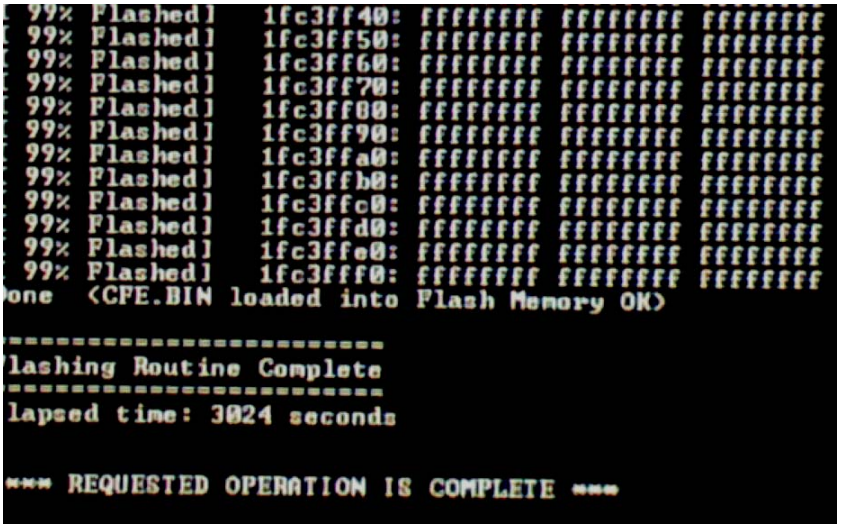


Ilustración 5-21 Finalización exitosa de la transferencia del CFE por medio del cable JTAG.

Terminado el proceso de borrado y transferencia del nuevo CFE, el enrutador tendrá las funciones básicas nuevamente en actividad, con una memoria NVRAM formateada y lista para el nuevo firmware OpenWrt. En este punto se puede utilizar el comando “ping” a la dirección 192.168.1.1 para comprobar la disponibilidad del enrutador. Si se recibe una respuesta positiva, quiere decir que es posible realizar la transferencia del firmware OpenWrt por medio de TFTP.

Ilustración 5-22 Respuesta exitosa del enrutador luego de formatear memoria NVRAM.

Al haber finalizado correctamente el proceso de transferencia de un nuevo CFE y formateado la memoria NVRAM, se puede apagar el equipo, desconectar los cables del JTAG y volverlo a insertar en su carcasa.

5.5. CONFIGURACIÓN DE OPENWRT 8.04 KAMIKAZE EN WRT54GL.

Una de las ventajas de la instalación de firmware de terceros en el WRT54G es la adición de nuevas tecnologías y herramientas que no están disponibles en el firmware original del LinkSys como se lo puede observar en el capítulo 4.5, 5.1, 5.2, 5.3 y 5.4 existen diferentes maneras de transferir el nuevo firmware que se basan en las necesidades que se tengan para la nueva instalación y además del estado del enrutador. En este caso si es que el enrutador es nuevo se puede instalar directamente el firmware utilizando la Consola de Administración Web, o el cable JTAG para después enviar el firmware utilizando TFTP. Una vez que se haya transferido el firmware al enrutador es necesario continuar con la configuración e instalación del software necesario.

En todos los modelos de enrutadores LinkSys la dirección IP es la 192.168.1.1 con máscara de subred 255.255.255.0, este estándar lo respetan los desarrolladores de firmware de terceros, por lo que luego de que se haya transferido la imagen del firmware se puede acceder al enrutador desde la consola SSH[68] o desde el navegador WEB a la dirección 192.168.1.1, Para esto es necesario que la interfaz LAN de la computadora cliente esté dentro de la misma red como se lo indica en el capítulo 5.2.

Para el diseño de este proyecto y como se lo ha mencionado anteriormente, se ha utilizado el firmware de terceros OpenWrt 8.04 Kamikaze el cual provee de una sencilla pero poderosa consola de administración web a la cual además se le pueden agregar complementos.

68 SSH son las siglas en ingles de Secure Shell. Es el sucesor de Telnet y permite establecer comunicaciones seguras creando túneles cifrados entre dos equipos.

OpenWrt 8.04 configura por default un máximo de 100 usuarios simultáneos, lo que para la mayoría de lugares que distribuyen internet gratuito suficiente, sin embargo esta configuración puede ser modificada para permitir mas conexiones simultaneas.

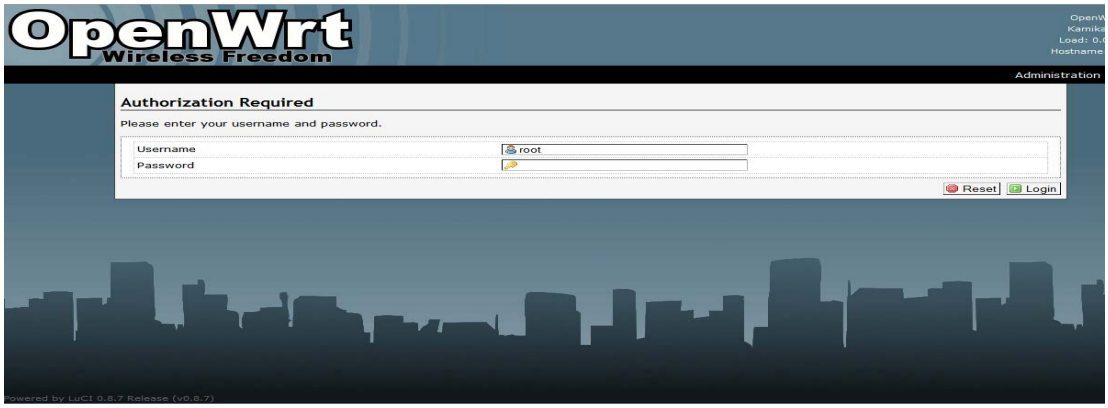


Ilustración 5-23 Primera pantalla de configuración en la consola web del OpenWrt 8.04

En el momento de la configuración inicial del OpenWrt se tiene que ingresar a la dirección http://192.168.1.1 utilizando cualquier navegador web. La primera vez que se accede a la consola de administración web se debe escribir una nueva contraseña la cual se utilizara a futuro para volver a ingresar al enrutador, después de escribir la contraseña se da clic en el botón "*Login*".

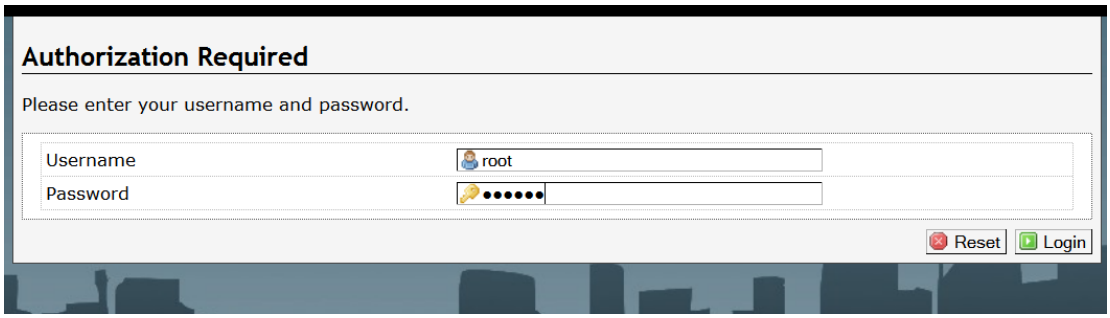


Ilustración 5-24 Selección de nueva contraseña para el OpenWrt

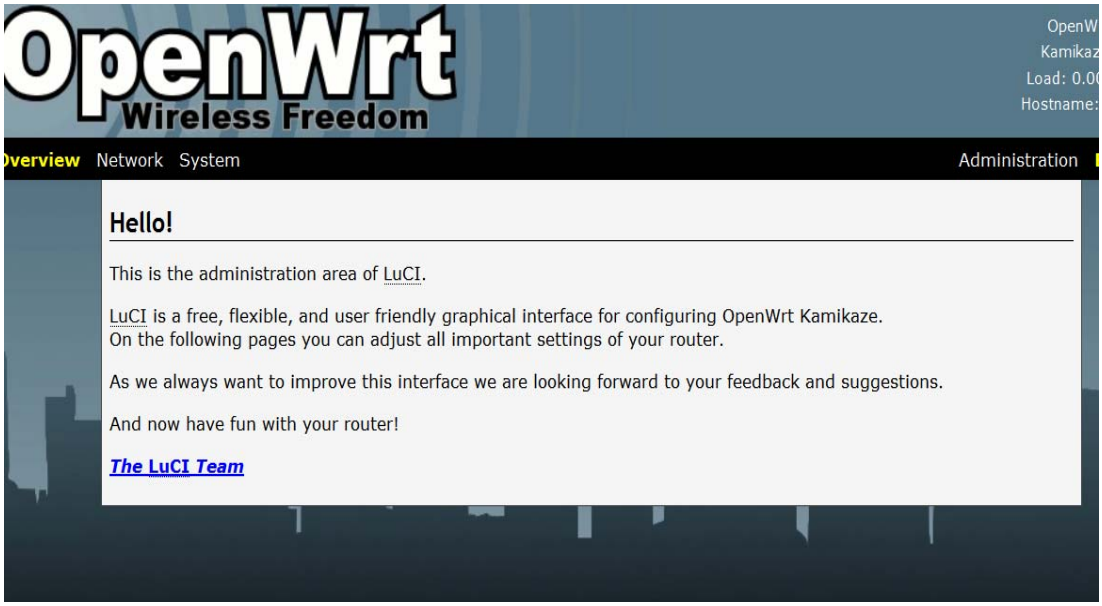


Ilustración 5-25 Pantalla de bienvenida del OpenWrt

Una vez se haya ingresado al enrutador aparecerá la pantalla de bienvenida en donde se describe las funciones de la consola de administración web llamada "*LUCI*", el cual se ejecuta utilizando un servidor web liviano de código libre llamado "*BusyBox HTTPd*" el cual permite ejecutar *CGI´S*[69] directamente desde la web.

5.5.1. Configuración de la red utilizando la consola de administración web del OpenWrt 8.04

La consola de administración web tiene dos módulos "*Administration & Essentials*", en los cuales están distribuidas las configuraciones básicas y las avanzadas, sin embargo se puede modificar las configuraciones básicas utilizando el modulo avanzado. En este modulo lo primero que se necesita configurar son los parámetros de las redes LAN y WAN para lo cual hay que dar clic en "Administration", luego de esto aparecerán nuevos menús que contienen las páginas de configuración para las diferentes funciones básicas del enrutador.

69 Interfaz de entrada común (en inglés Common Gateway Interface, abreviado CGI) es una tecnología de la Web que permite a un cliente solicitar datos de un programa ejecutado en un servidor web.

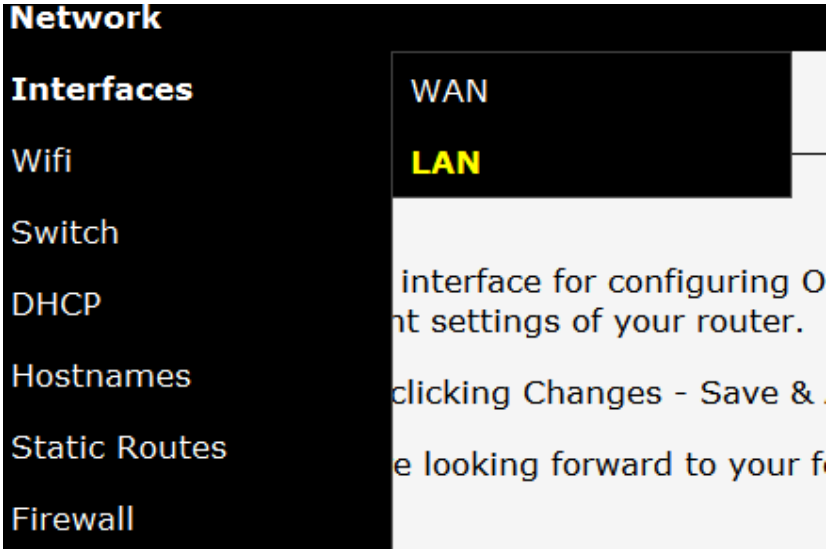


Ilustración 5-26 Menú de configuración de la red en la consola de administración web del OpenWrt

El menú de configuración de la red “Network” contiene los siguientes submenús como se muestra en la siguiente tabla.

Tabla 5-2 Menú de configuración de la Red

Menú	Submenú	Descripción
Interfaces	WAN	Configura las interfaces WAN y LAN.
	LAN	
Wifi	WLO	Habilita el adaptador de red inalámbrica y configura el SSID y los parámetros de seguridad.
Switch		Configuración de VLANS
DHCP	Leases	Administra el servidor DHCP
Hostnames		Hostnames definidos por el usuario.
Static Routes		Rutas estáticas definidas por el usuario.
Firewall	Zones	Configuración del firewall, re direccionamiento de tráfico, control de puertos de entrada y salida.
	Traffic Control	
	Traffic Redirection	

Primero se debe configurar la red de área local LAN y el servicio DHCP para que el trabajo sea más fácil[70].

Para este proyecto la red original se la ha sustituido por la 192.168.3.1 con máscara de subred 255.255.255.0. Una vez que se realizan los cambios se debe dar clic en el botón llamado "*Save & Apply*"[71] que guarda la configuración y posteriormente la escribe en la memoria no volátil NVRAM.

Tabla 5-3 Parámetros de la configuración LAN.

Dirección IP	192.168.3.1
Mascara de subred	255.255.255.0

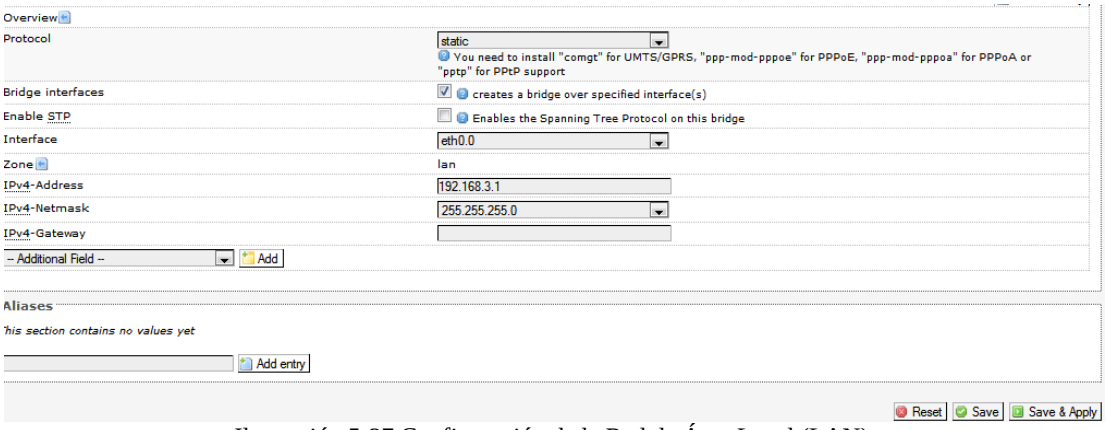


Ilustración 5-27 Configuración de la Red de Área Local (LAN)

Como se puede observar en la ilustración 5-28 el servicio DHCP comenzara a proveer direcciones IP en la red LAN desde el rango 192.168.3.100 hasta el rango 192.168.3.150 con un periodo de renovación de 12 horas. Los parámetros de "Puerta de enlace" y DNS los toma automáticamente de la configuración WAN.

70 Hasta este punto la red inalámbrica continúa deshabilitada.
71 En la actualidad no existe una traducción al idioma español de la consola de administración web "LUCI"

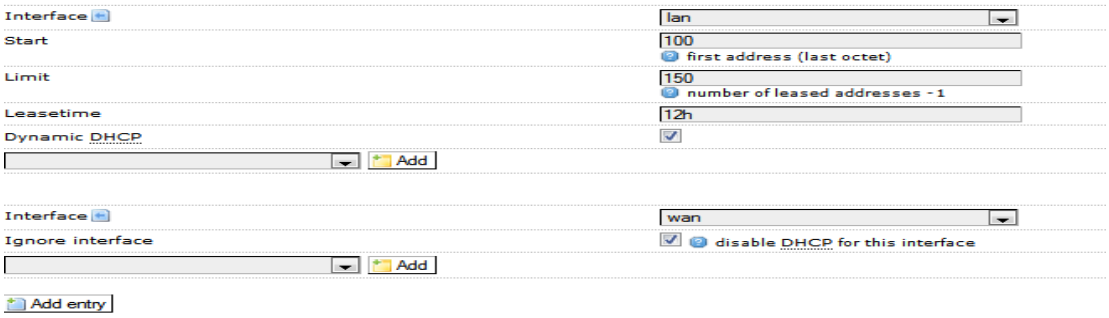


Ilustración 5-28 Configuración del servicio DHCP

En configuración original del OpenWrt 8.04 los parámetros de la red WAN están establecidos para obtener la dirección IP, puerta de enlace y DNS automáticamente con DHCP, por lo que es necesario cambiar estos parámetros a direcciones estáticas.

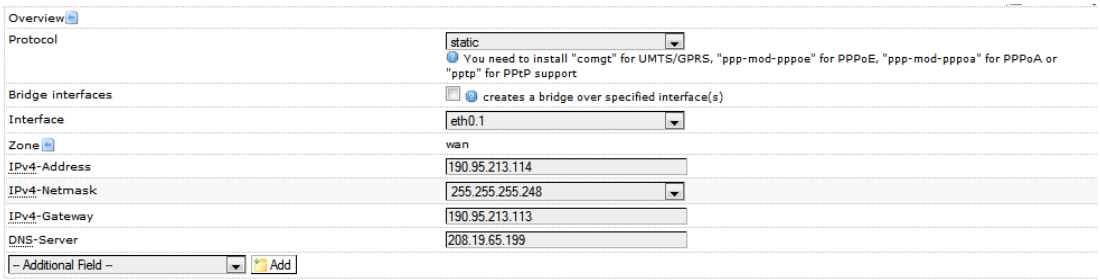


Ilustración 5-29 Configuración de la red WAN en el OpenWrt 8.04

Como se observa en la Ilustración 5-29 se establecen los siguientes parámetros para la red WAN para la configuración de la IP pública contratada con el ISP[72] Trans-Telco.

Tabla 5-4 Parámetros de la configuración WAN.

Dirección IP	190.95.213.114
Mascara de subred	255.255.255.248
Puerta de enlace	190.95.213.113
Servidor DNS primario	208.19.65.199

72 ISP Proveedor de servicios de Internet, en ingles (Internet Service Provider)

Después de completar las configuraciones de la red cableada se puede configurar la red inalámbrica, para este proyecto la red inalámbrica no utilizara ningún tipo de cifrado de datos ni credenciales de acceso debido a que esto se manejara con el portal cautivo "WifiDog".

OpenWrt tiene la capacidad de dividir redes inalámbricas creando nuevas redes virtuales con diferentes SSID y configuraciones de seguridad, por lo que el dispositivo de la red inalámbrica original se llama WL0 (Wireless LAN 0).

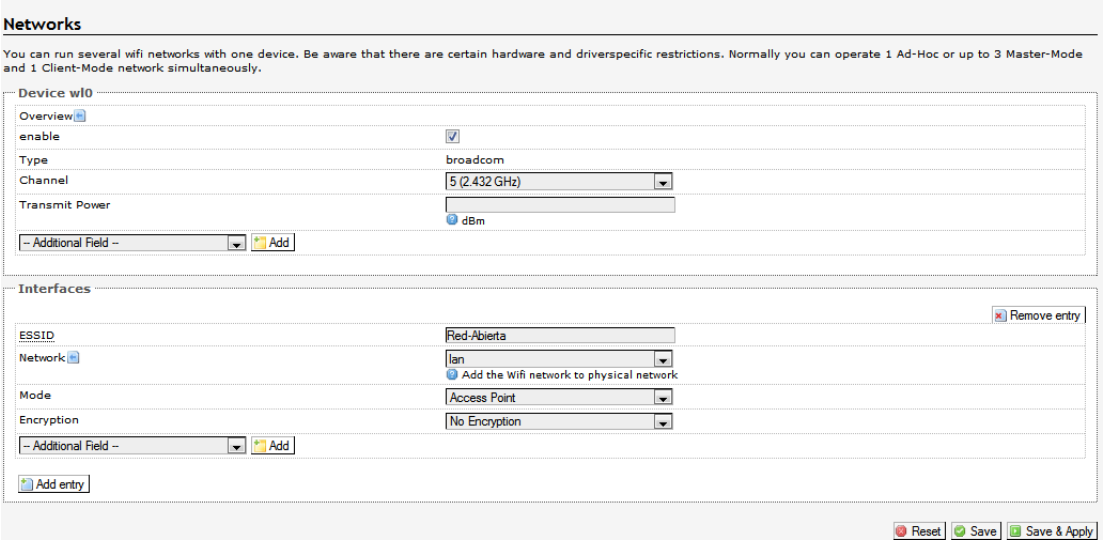


Ilustración 5-30 Configuración de la red inalámbrica en OpenWrt 8.04

En la ilustración 5.30, se puede observar que se ha configurado la red inalámbrica sin protección, con un SSID llamado "**Red-Abierta**" y trabaja en el canal 5 del 802.11g.

5.6. CONSOLA DE ADMINISTRACIÓN POR INTERPRETE DE COMANDOS

La consola de administración por interprete de comandos es otra forma de configurar el enrutador inalámbrico, y al igual que todas las distribuciones de GNU / LINUX, esta característica está disponible en el OpenWrt. Esta herramienta resulta muy útil ya que

permite la conexión directa con el intérprete de comandos, el cual posee las mismas funcionalidades que un intérprete de comandos de una distribución grande como por ejemplo UBUNTU.

El protocolo SSH trabaja de forma similar a telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Los sistemas operativos GNU / LINUX son conocidos por sus poderosos intérpretes de comandos, los cuales independientemente de la distribución, funcionan de manera similar. A diferencia de las interfaces graficas las cuales difieren en sus aplicaciones, configuración y funcionamiento. Es por esto que cuando se conoce el funcionamiento de una línea de comandos en GNU / LINUX, se puede manejar cualquier distribución. OpenWrt utiliza un intérprete de comandos llamado ASH, que es una versión simplificada y reducida del comúnmente conocido BASH.

Para poder establecer una comunicación SSH desde el Sistema Operativo Windows, es necesario instalar un cliente SSH debido a que este Sistema Operativo no posee este software. Para ello se instalara el cliente de SSH "*PuTTY*", el cual es muy conocido, fácil de usar[73].

Una vez descargado, se debe ejecutar el archivo llamado "putty.exe. Al ejecutarlo aparecerá una ventana en donde se puede escribir la dirección IP del enrutador, y además se puede guardar los datos para futuras conexiones.

73 Fuente: http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

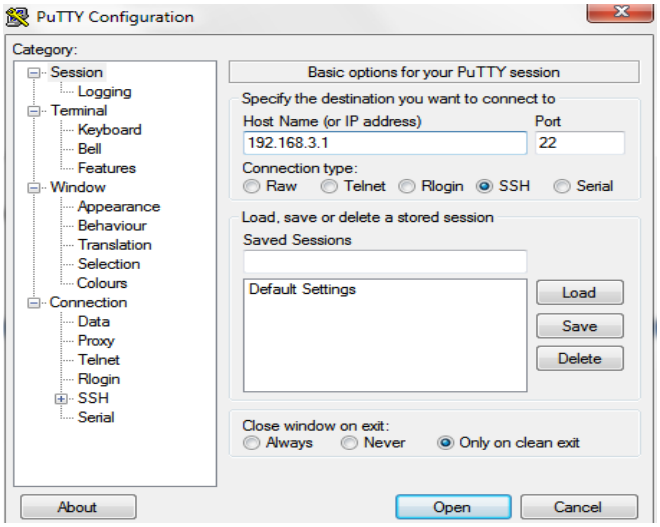


Ilustración 5-31 Pantalla principal de PuTTY

Después de escribir la dirección IP del enrutador, se tiene que dar clic en “Open” y aparecerá una pantalla en la cual solicitara confirmación para la clave publica que está transmitiendo el enrutador, después de aceptar esa clave se podrá iniciar sesión con el nombre de usuario root y la contraseña que previamente se había guardado en la consola de administración web.

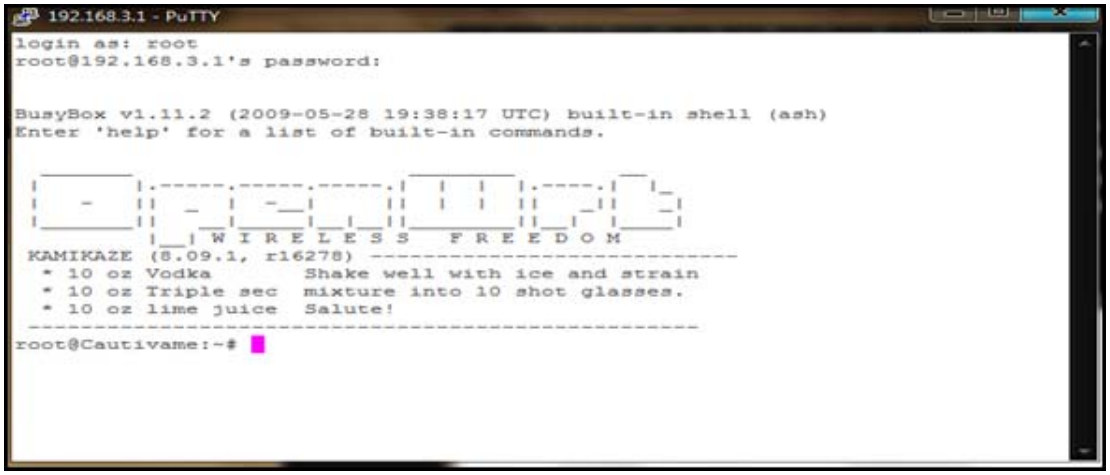


Ilustración 5-32 Pantalla principal de la consola de administración por línea de comandos y SSH

Como se muestra en la ilustración 5-32 después de iniciar sesión se tiene completo acceso a las funcionalidades de GNU / LINUX utilizando el interprete de comandos. Una vez se

haya ingresado correctamente al enrutador por medio de SSH se podrá iniciar el proceso de configuración del WIFIDOG y las herramientas necesarias.

5.7.INSTALACIÓN DE MEMORIA NO VOLÁTIL ADICIONAL.

El enrutador inalámbrico WRT54GL es fabricado con una memoria no volátil de 4MB y una memoria RAM de 16 MB, las cuales se utilizan para cargar el firmware y otro software que necesita el equipo. Sin embargo OpenWrt maneja a la memoria RAM como almacenamiento no volátil, emulando particiones en donde se descomprimen los archivos del sistema operativo.

Una de las ventajas de los enrutadores inalámbricos LinkSys WRT54G en sus versiones 1, 2, 3,4 y GL es la de tener en su placa madre, puertos de propósito general GPIO (*General Purpose Input Output*) que pueden aportar en gran medida a la ampliación del equipo. Con estos puertos es posible agregar memorias no volátiles SD, puertos USB, GPS, tarjetas Bluetooth, y módems GSM. El puerto GPIO es una interfaz disponible en algunos dispositivos, sus puertos pueden actuar como entrada o salida, para leer las señales digitales de otras partes de un circuito. Un puerto GPIO suele tener pines individuales, ya sea como entrada o salida. Cada pin puede ser de configuración flexible para aceptar o enviar a diferentes dispositivos. Los voltajes de entrada y de salida son por lo general, de 3.3 voltios[74].

La comunidad de desarrolladores de OpenWRT han creado *drivers*[75] para diversos dispositivos externos que pueden ser acoplados al equipo utilizando los puertos auxiliares (JTAG, SERIAL, GPIO). Gracias a esto es posible la implementación de una tarjeta SD, pero debido a que no existe una documentación oficial sobre los puertos GPIO la

74 (Asadoorian, 2007)
75 Controlador de hardware que permite la comunicación entre el hardware y software.

comunidad de software libre y *hardware hacking* es la principal responsable de la documentación y soporte para la modificación del enrutador inalámbrico.

El tamaño de almacenamiento original del enrutador inalámbrico WRT54GL, no es una limitante para poder instalar las aplicaciones necesarias para el desarrollo de este proyecto, sin embargo con fines de investigación y para implementar herramientas adicionales, se agregara una memoria no volátil Secure Digital (SD) en el enrutador inalámbrico LinkSys WRT54GL.

Los requerimientos de hardware que se utilizaran para agregar una memoria no volátil externa al dispositivo son los siguientes:

Tabla 5-5 Componentes de Hardware necesarios para agregar una memoria no volátil SD

Hardware	**Descripción**
Memoria MicroSD 2GB y Adaptador SD	Memoria para ser añadida al enrutador
Cable IDE	Para utilizar algunos cables blindados.
Soldador Cautín	Necesario para unir la memoria

Para comenzar la instalación de la tarjeta de memoria adiciona es necesario abrir el enrutador para poder identificar los puertos GPIO. Véase el capitulo 5.4.2.

La Figura 5-33 muestra al enrutador inalámbrico WRT43GL sin la protección de plástico que la recubre.

Ilustración 5-33 Componentes internos del enrutador inalámbrico LinkSys WRT54GL

En la siguiente figura se muestran los puertos GPIO que irán conectados desde el enrutador inalámbrico LinkSys WRT54GL hacia la memoria SD.

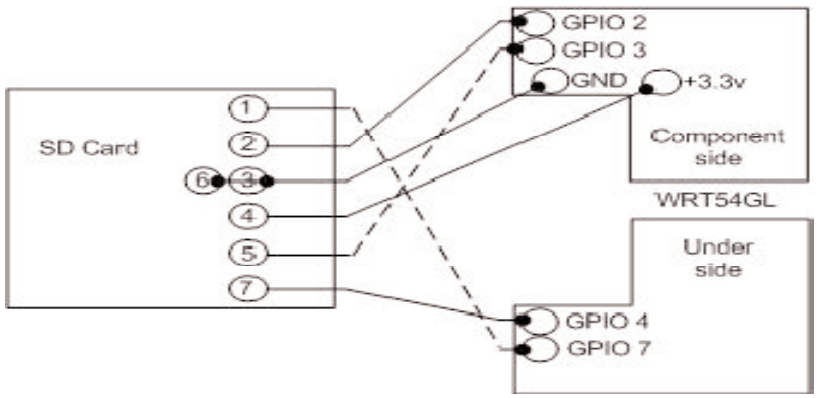


Ilustración 5-34 Diagrama de circuitos eléctricos para conectar una memoria SD al enrutador inalámbrico Wrt54GL[76]

76 (Asadoorian, 2007)

Al momento de identificar los puertos GPIO es recomendable señalarlos con algún tipo de marcador, para tener una referencia y no dañar al dispositivo al momento de soldar los cables. Los dos puertos necesarios para la conexión a tierra y el puerto de voltaje se encuentran en la parte superior del dispositivo.

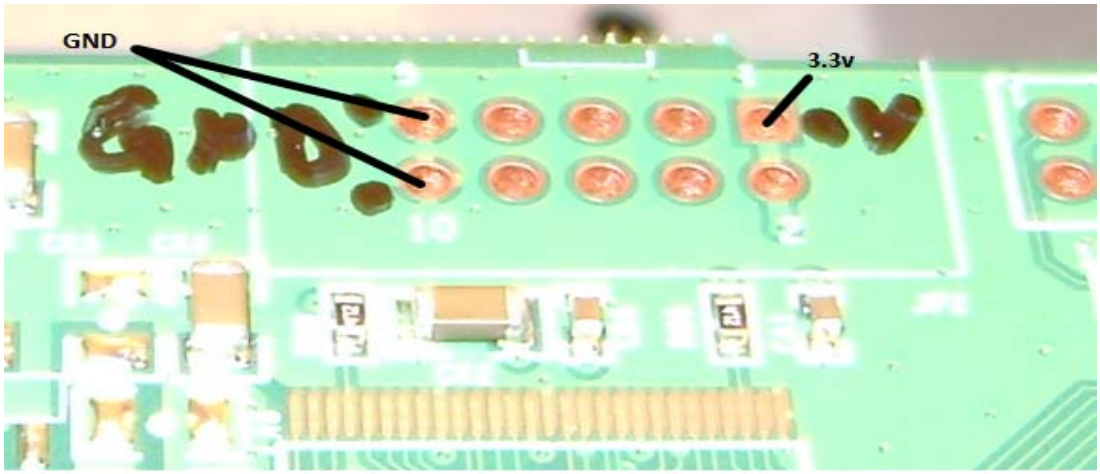


Ilustración 5-35 GPIO de tierra GND y el GPIO de voltaje en el enrutador inalámbrico WRT54GL

Los puertos GPIO 2, 3, 4 y 7 están localizados en la parte inferior de las luces LED y del Botón "*SES*".

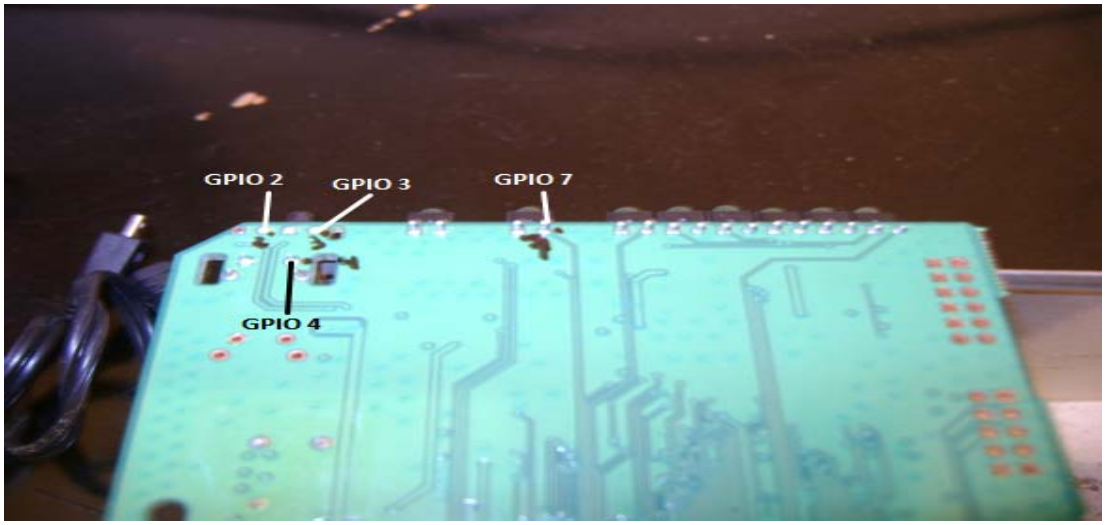


Ilustración 5-36 Puertos GPIO 2, 3, 4 y 7 localizados debajo de las luces LED.

Una vez que se hayan identificado los puertos GPIO del enrutador como se puede observar en la ilustración 5-36, es necesario soldar los cables, para ello se necesitara extraer 7 cables del puerto IDE y soldarlos con mucha precaución de no dañar las soldaduras originales del dispositivo, en caso contrario podría dañarse permanente.

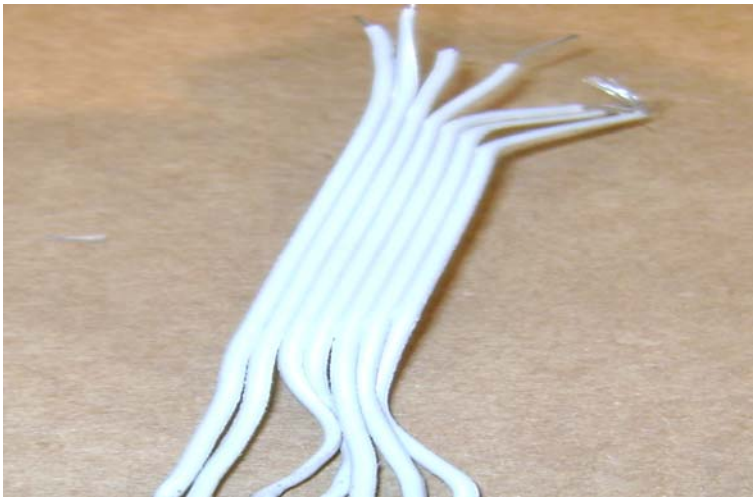


Ilustración 5-37 Cable IDE utilizado para la conexión hacia la tarjeta SD.

En la figura 5-38 se puede observar la soldadura a los cables de Tierra (GND) y el de Voltaje.

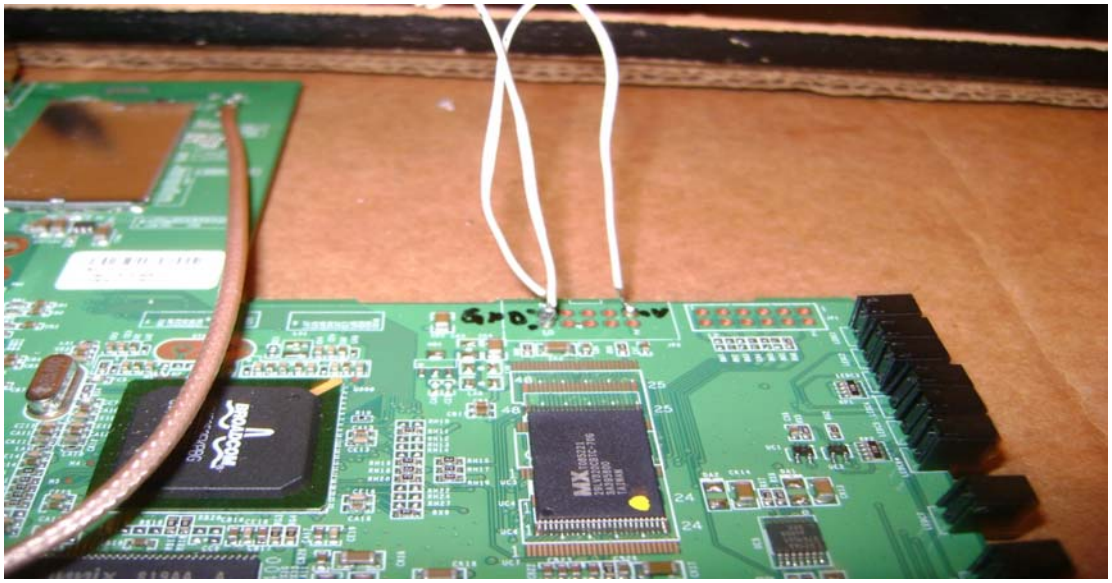


Ilustración 5-38 Puertos GND y de Voltaje soldados al dispositivo.

Los puertos GPIO 2, 3, 5 y 7 son algo difícil de soldar debido a que sus puntos están en uso por otros componentes como las luces LED, por lo que su soldadura debe de ser de lo más cuidadosa para no dañar el equipo. En la siguiente ilustración se puede ver la soldadura de dichos cables.

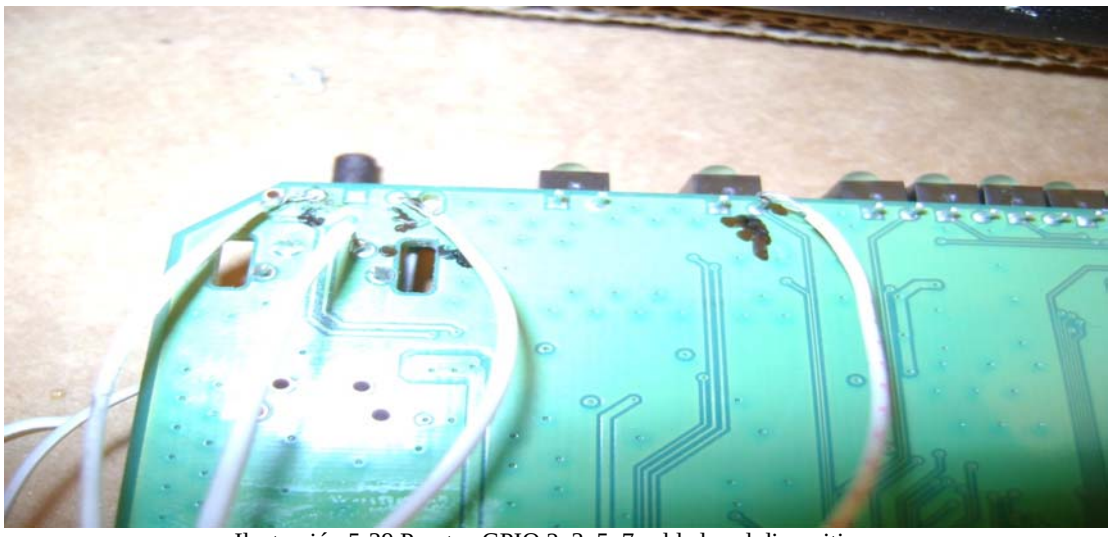


Ilustración 5-39 Puertos GPIO 2, 3, 5, 7 soldados al dispositivo

El siguiente paso es soldar los puntos que van conectados a la memoria SD, para este proceso se soldaron aparte estos cables con el fin de evitar desconectar los puertos GPIO que se habían soldado al enrutador.

Para soldar los cables a la memoria SD se debe de seguir la referencia de la figura 5-37 en donde esta detallado el diagrama de circuitos para la conexión de la memoria. Los puertos a soldar están numerados a continuación en la ilustración 5-40.

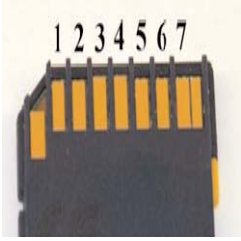


Ilustración 5-40 Numeración correspondiente a los puertos en la memoria SD[77].

77 (Asadoorian, 2007)

Se pueden conectar los cables previamente soldados con los que están unidos al enrutador como muestra la siguiente figura.

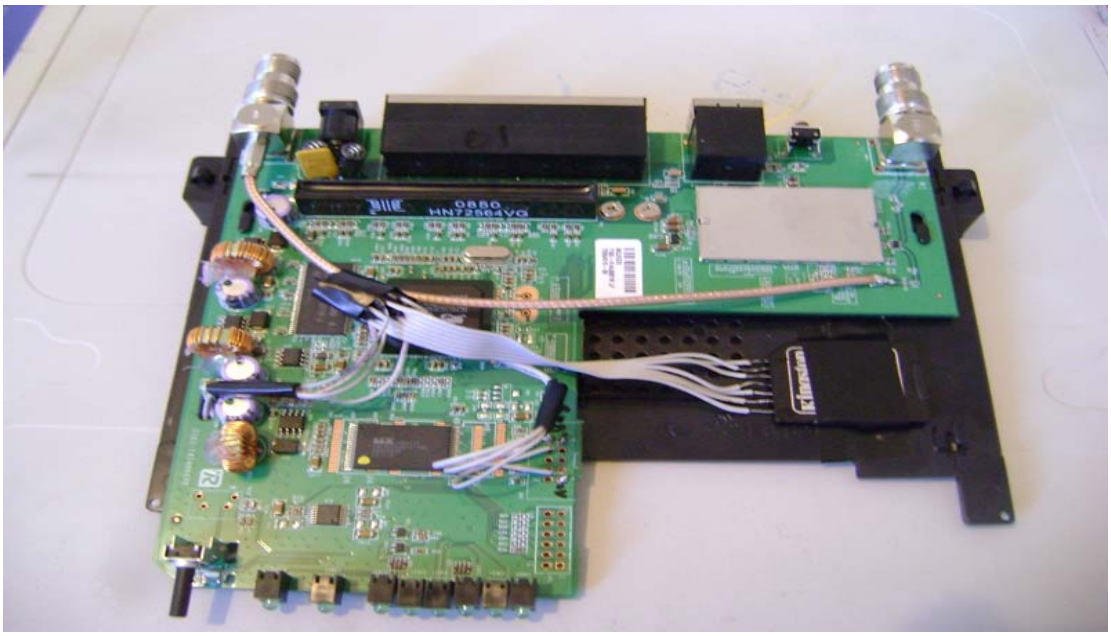


Ilustración 5-41 Memoria SD de 2GB añadida al enrutador inalámbrico WRT54GL por medio de los puertos GPIO.

Luego de conectar los cables entre la memoria SD y el enrutador, se debe de pegar la memoria con cinta aislante en la parte de la carcasa inferior que no está utilizada para evitar un corto circuito. Al terminar el proceso de soldado de la memoria SD, es necesario volver a cerrar el equipo en su carcasa y encenderlo

5.7.1. Configuración de la tarjeta Secure Digital en el enrutador.

Además de las mejoras y portaciones que se han creado para el sistema operativo OPENWRT, la comunidad de desarrolladores se ha dedicado buscar nuevas funcionalidades para el equipo, como lo es la adición de memorias, cámaras y módems, es por esto que el firmware OPENWRT 8.04 Kamikaze tiene la capacidad de instalar en su Kernel nuevos módulos que contienen los drivers necesarios para dichos dispositivos.

Para iniciar la instalación de la memoria adicional en el enrutador, se debe iniciar sesión por la consola de comandos estableciendo una conexión con el programa PuTTY, como se lo explica en el capítulo 5.6.

Cuando se haya iniciado sesión por medio de SSH se procederá con la instalación de los paquetes necesarios para que el enrutador reconozca a la tarjeta de memoria. El primer paso es actualizar los repositorios de software. OpenWrt tiene un manejador de software llamado Opkg, que funciona de manera parecida al de sistemas operativos grande como "Aptitude" para Ubuntu o "Yum" para RedHat. El comando que se ejecutara es: "**opkg update**" el cual actualiza la lista de software disponible para el sistema operativo.

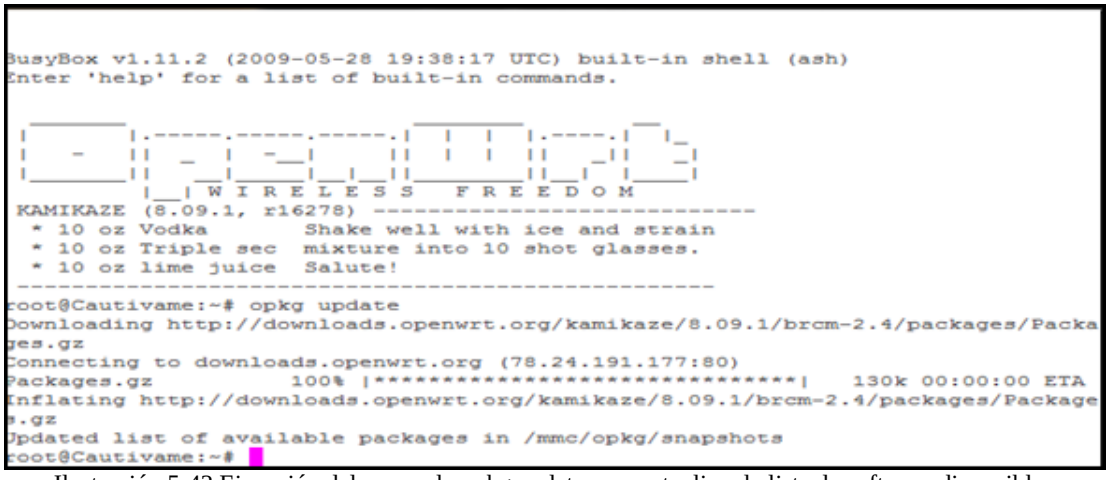


Ilustración 5-42 Ejecución del comando opkg update para actualizar la lista de software disponible.

Después de realizar la actualización de la lista de software disponible es necesario dirigirse a la carpeta donde están los drivers del dispositivo utilizando el comando: "**cd /lib/modules/2.4.35.4/**". Al finalizar la ejecución de este comando, se debe descargar el driver para la tarjeta SD utilizando el comando "wget" desde la URL http://download.tcsoft.net/mmc.o. El comando resultante es el siguiente: "wget http://download.tcsoft.net/mmc.o".

Cuando la descarga haya finalizado se puede ejecutar el comando "ls" para comprobar la ubicación del archivo.

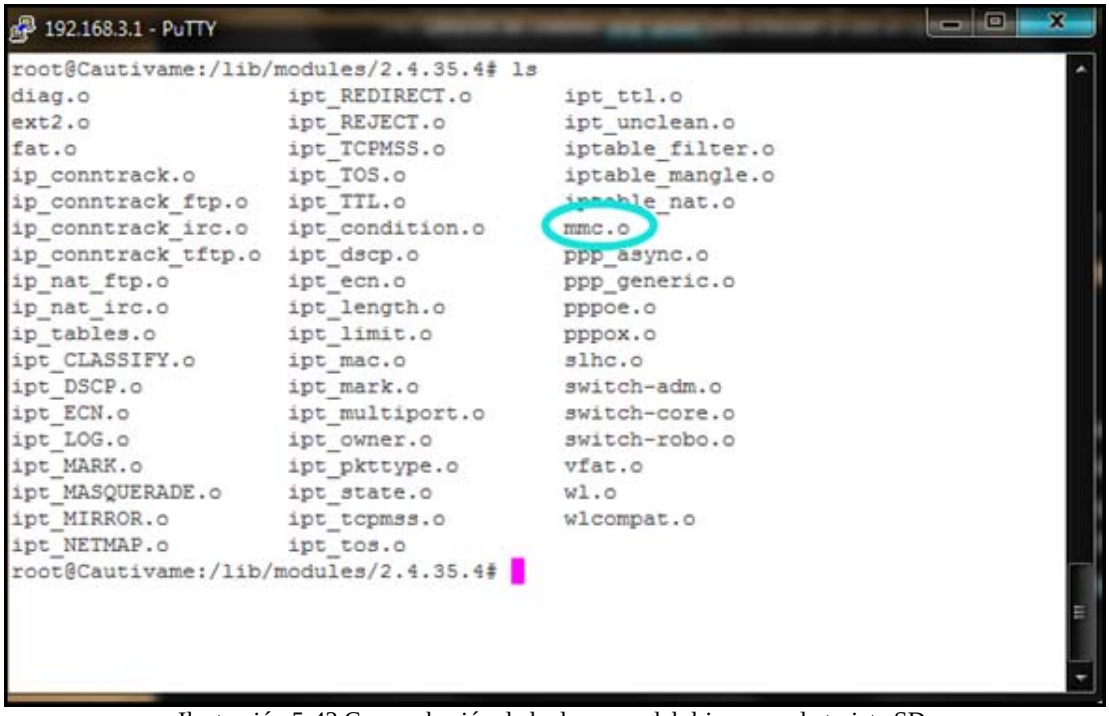


Ilustración 5-43 Comprobación de la descarga del driver para la tarjeta SD

Lo siguiente es enmascarar los puertos GPIO que no están utilizándose en el enrutador ejecutando el siguiente comando: "**echo "0x9c" > /proc/diag/gpiom**ask" e iniciar el driver de la tarjetita de memoria con el comando "**insmod mmc**". Luego de esto se puede comprobar el funcionamiento de la memoria SD revisando los logs del Kernel con el comando: "**dmesg**".

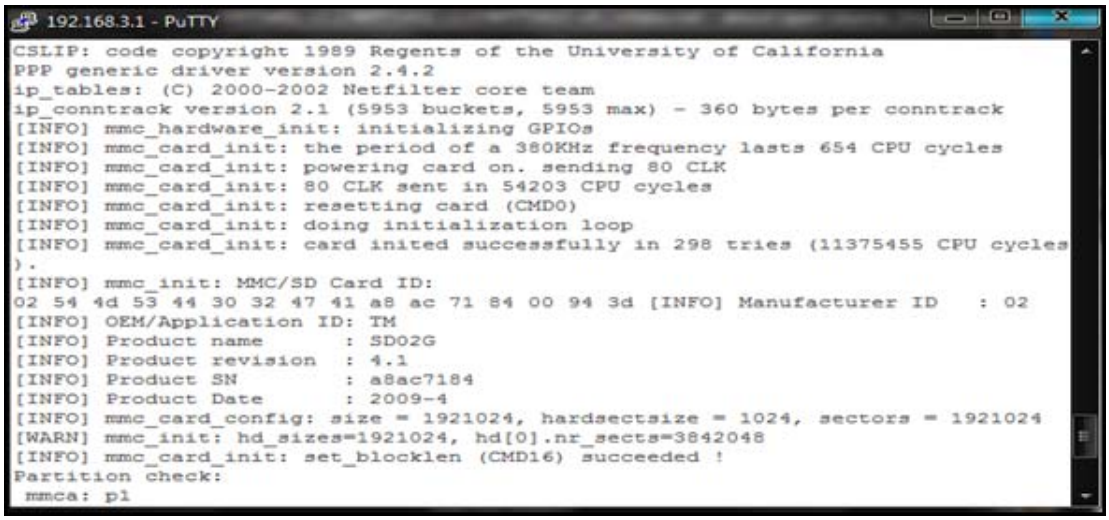


Ilustración 5-44 Comprobación de la carga del driver de la tarjeta de memoria SD.

Como se puede observar en la ilustración 5-44 la carga del driver tuvo éxito, y aparece la información de la tarjeta SD.

Ahora que la conexión de la tarjeta SD hacia el enrutador ha sido comprobada, es necesario instalar el software para formatear la tarjeta a un sistema de archivos compatible con GNU / LINUX y además montar la tarjeta en la tabla de particiones para lo cual se ejecutaran lo siguientes comandos: "**opkg install kmod-fs-ext2 e2fsprogs**".

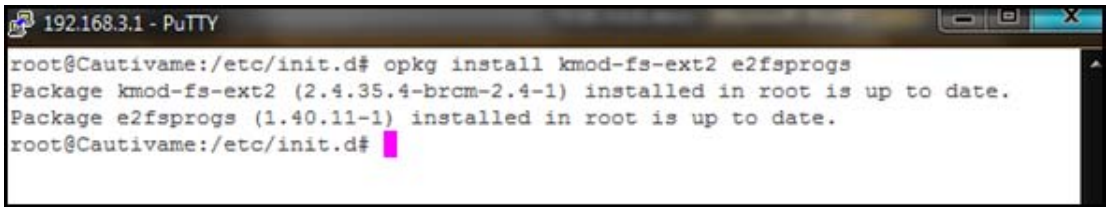


Ilustración 5-45 Instalación del software necesario para formatear la tarjeta y montar el sistema de archivos.

El siguiente paso es formatear la tarjeta al sistema de archivos ext2[78].

Ilustración 5-46 Formato de la tarjeta de memoria SD al sistema de archivos SD.

El proceso de formateo de la memoria SD durará dependiendo del tamaño de la misma, en este caso al ser de 2GB este proceso tarda alrededor de 10 minutos. Una vez que la tarjeta fue formateada con éxito es necesario agregarla en la tabla de particiones para lo cual, en primer lugar se debe crear una carpeta en donde se montara la tarjeta con el comando "**mkdir /mmc**"[79] y después se debe modificar el archivo "**/etc/fstab**" y añadir la siguiente

78 Ext2 (second extended filesystem o "segundo sistema de archivos extendido") es un sistema de archivos con registro por diario (journaling). Es el sistema de archivo más usado en distribuciones Linux
79 La carpeta se la llama "mmc" debido al nombre del driver en referencia a MultiMedia Card (mmc)

instrucción al final:"**/dev/mmc /mmc ext2 defaults 0 0**", lo que hará que al iniciar el sistema operativo se monte la tarjeta en la capeta "**/mmc**".

Al finalizar estos procesos, se debe crear un script de línea de comandos que automatizará todo este proceso cada vez que el enrutador se reinicie, para ello se debe crear un archivo llamado "**mmc**" en la carpeta de inicio del sistema "**/etc/init.d/**" con los siguientes parámetros[80]:

```
#!/bin/sh /etc/rc.common #importa las librerías del sistema
# MMC Script
START=20 # prioridad de ejecución
start() {
echo "0x9c" > /proc/diag/gpiomask # se enmascara los GPIO sin uso
insmod /lib/modules/2.4.35.4/mmc.o # se carga el driver de la tarjeta SD
mount /dev/mmc/disc0/part1 /mmc # se monta la tarjeta SD en la carpeta /mmc
}
```

Al archivo creado se le debe de dar permisos de lectura y ejecución, para lo cual se utiliza el comando "**chmod 755 /etc/init.d/mmc**" y después hay que habilitarlo para su ejecución automática con el comando "/etc/init.d/mmc load". Una vez ejecutados todos estos comandos y creado el archivo de configuración automática, se deberá reiniciar el equipo para comprobar el funcionamiento de la tarjeta.

Hecho esto se comprueba que la tarjeta este montada en la carpeta "**/mmc**" con el siguiente comando: "**df –h**".

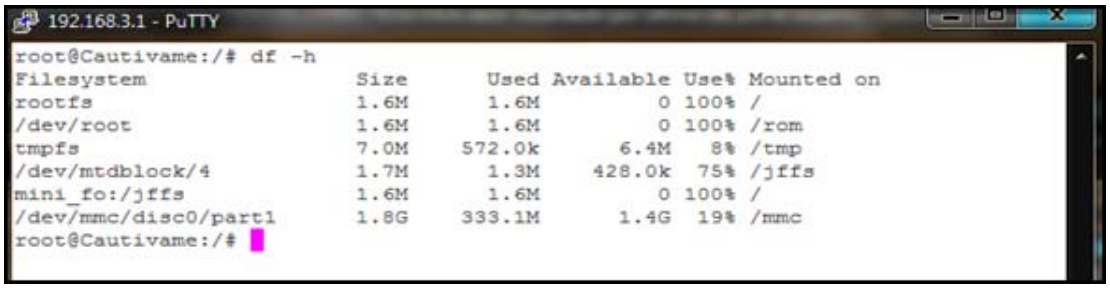


Ilustración 5-47 Comprobación del montaje exitoso de la tarjeta SD en la carpeta /MMC

80 (Asadoorian, 2007)

Como se puede ver en la figura anterior, se ha montado exitosamente la tarjeta SD con el sistema de archivos ext2 en la carpeta /mmc.

Luego de esto se puede leer y escribir en la tarjeta SD utilizando el punto de montaje de la carpeta /mmc, pero todavía hace falta indicarle al sistema operativo de esa nueva ubicación para posteriormente poder instalar paquetes en dicha ubicación con los siguientes comandos:

```
export PATH=$PATH:/mmc/bin:/mmc/sbin:/mmc/usr/bin:/mmc/usr/sbin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/mmc/lib:/mmc/usr/lib
```

La última modificación del sistema operativo para establecer las nuevas ubicaciones es modificar el archivo "**/etc/opkg.conf**" el cual configura al manejador de software "OPKG" en el cual se establecerá un nuevo destino para la instalación de software, además de implantar la nueva ubicación para los archivos temporales descargados y la memoria virtual que se utiliza en el momento de la instalación como se puede observar en la siguiente figura.

Ilustración 5-48 Configuración de OPKG para permitir instalaciones en la tarjeta SD.

Finalizados todos los procesos anteriores el sistema operativo será capaz de instalar software o grabar cualquier archivo en la tarjeta de memoria SD. Para indicarle al manejador de paquetes en que ubicación se debe instalar el software es necesario agregar la opción "**–mmc**" que hace referencia al destino configurado en el archivo "**/etc/opkg.conf**".

Para comprobar el nuevo proceso de instalación se instalara el programa de edición de texto “NANO” con el comando “**opkg install -d mmc nano**”.

Es importante señalar que el proceso de lectura y escritura en la tarjeta de memoria SD produce un destello en las luces LED del botón “SES” debido al uso del GPIO 2.

Ilustración 5-49 Instalación del programa de edición de texto "NANO" en la tarjeta SD

5.8. INSTALACIÓN DE LA PUERTA DE ENLACE WIFIDOG EN EL ENRUTADOR INALÁMBRICO.

Una vez que se ha instalado y configurado la tarjeta de memoria no volátil en el enrutador inalámbrico LinkSys WRT54GL, es factible instalar las aplicaciones necesarias para la implementación del portal cautivo, ya que dicho software ocupa alrededor de 5 MB que podría saturar al dispositivo de ser instalado directamente en la memoria Flash.

Wifidog es el software de Portal Cautivo para plataforma GNU / LINUX más aceptado en el mercado y está compuesto por dos módulos: Servidor de autenticación y la puerta de enlace. Como se puede revisar en el capitulo 2.6.2 se detallo a profundidad las ventajas del portal cautivo y en el capítulo 4.6 se habló específicamente del funcionamiento de Wifidog.

Para comenzar la instalación de Wifidog en el enrutador inalámbrico, es necesario descargarlo desde el repositorio de software de OpenWrt y direccionar su instalación a la memoria SD, para esto se utilizara el comando: "**opkg install –d mmc wifidog**". Cuando el proceso de instalación comienza se puede observar que el manejador de paquetes OPKG instala las dependencias del Wifidog.

Ilustración 5-50 Instalación de Wifidog en la tarjeta SD

Después de terminar la instalación es necesario mover el archivo "**/mmc/etc/init.d/wifidog**" hacia la ubicación: "**/etc/init.d/wifidog**", debido a que OpenWrt solamente lee los scripts de inicio en la ubicación origina. Al finalizar la copia se debe modificar el archivo "**/etc/init.d/wifidog**" con la herramienta de edición de textos previamente instalada "NANO" y añadir la carpeta en donde se ubican los binarios del programa "**/mmc/**"como se puede ver en la siguiente ilustración.

Ilustración 5-51 Modificación del script de inicio de Wifidog

Luego de hacer estos cambios en la configuración de arranque de Wifidog, se debe modificar el archivo de configuración de Wifidog que se encuentra en "**/etc/wifidog.conf**", dicho archivo tiene algunos parámetros usables, pero para fines demostrativos se modificarán solamente los parámetros más comunes.

Tabla 5-6 Descripción de parámetros para la configuración de Wifidog en el archivo /etc/wifidog.conf

Parámetro	Configuración	Descripción
GatewayID	cautivame2h	Nombre de la puerta de enlace en donde se instala el enrutador.
GatewayInterface	br-lan	Interfaz de red que se conecta al internet.
AuthServer { Hostname 192.168.3.100 Path /	- 192.168.3.100 - /	Dirección Ip del servidor Wifidog de autentificación y la ruta hacia la página web de inicio de sesión.
Daemon	1	Especifica si es que Wifidog inicia como servicio del sistema.
CheckInterval	300	Tiempo en segundos en que la puerta de enlace espera para establecer conexión con el servidor de autentificación de Wifidog.
ClientTimeout	5	Tiempo de espera para eliminar al cliente de la lista de usuarios conectados.
TrustedMACList	00:10:b5:87:d2:6c,00:1E:68:8A:BB:9A	Direcciones MAC que no necesitan pasar atreves del servidor de autentificación. Estas direcciones pueden ser utilizadas para las maquinas de la red LAN.

FirewallRuleSet validating-users {
FirewallRule allow udp to 0.0.0.0/0
FirewallRule allow tcp port 80 to 0.0.0.0/0
FirewallRule allow tcp port 443 to 0.0.0.0/0
}
	Puerto http 80
	- Puerto https 443
		Regla de Firewall para los usuarios que están en periodo de validación. Solo permite la navegación por páginas web.

FirewallRuleSet known-users {
FirewallRule allow udp to 0.0.0.0/0
FirewallRule allow tcp port 80 to 0.0.0.0/0
FirewallRule allow tcp port 443 to 0.0.0.0/0
FirewallRule allow icmp to 0.0.0.0/0
FirewallRule allow tcp port 50451 to 0.0.0.0/0
FirewallRule allow tcp port 587 to 0.0.0.0/0
FirewallRule allow tcp port 25 to 0.0.0.0/0
FirewallRule allow tcp port 110 to 0.0.0.0/0
FirewallRule allow tcp port 21 to 0.0.0.0/0
FirewallRule allow to 0.0.0.0/0
}
	Puerto http 80
	Puerto https 443
	Puerto VoIP 50451
	Puerto SMTP 25
	Puerto POP3 110
	Puerto FTP 21
		Regla de Firewall para los usuarios que iniciaron sesión en la red de portales cautivos. Con esta regla los usuarios pueden navegar y trabajar con clientes de correo POP3 Y SMTP.

FirewallRuleSet unknown-users { FirewallRule allow udp port 53 FirewallRule allow tcp port 53 FirewallRule allow udp port 67 FirewallRule allow tcp port 67	Puerto DNS 53 Puerto DHCP 67	Regla de firewall para los usuarios que no presentan ninguna condición especifica. En general esta regla bloquea todo el tráfico.

Terminados los procedimientos señalados anteriormente se puede probar el funcionamiento de Wifidog ejecutando el script de inicio con el comando "**/etc/init.d/wifidog start**".

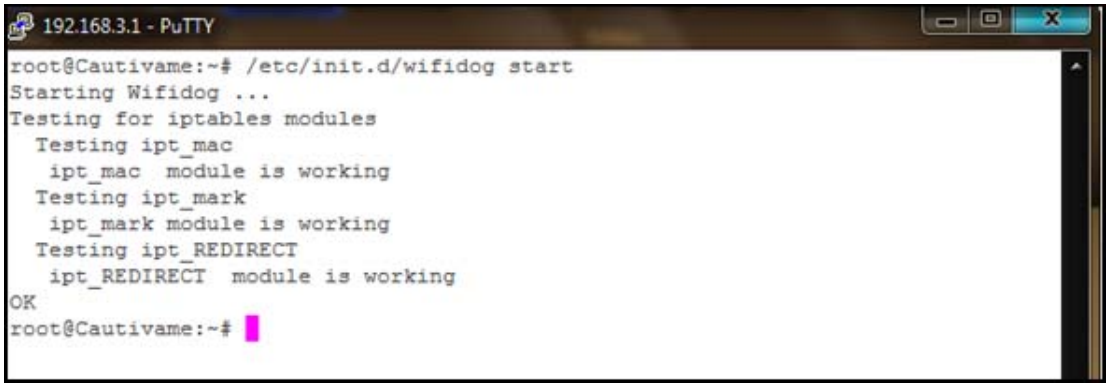


Ilustración 5-52 Ejecución exitosa de Wifidog

Cuando se haya comprobado que Wifidog está funcionando, se lo habilitara para su inicio automático con el sistema operativo "**/etc/init.d/wifidog enable**", con esto cada vez que se reinicie el enrutador Wifidog se iniciara automáticamente.

5.9.INSTALACIÓN DE SERVIDOR DE AUTENTICACIÓN.

El servidor de autentificación, como su nombre lo indica está encargado de realizar las tareas de manejo y autentificación de usuarios

Al iniciar la instalación y configuración del servidor de autentificación, se utilizara Ubuntu 9.04 "**Jaunty Jackalope**"[81], una distribución del Sistema Operativo GNU / LINUX, sin embargo las configuraciones y las herramientas de software que son necesarias para el funcionamiento del servidor de autentificación Wifidog, pueden ser instaladas en cualquier distribución de GNU / LINUX con capacidades de servidor como por ejemplo: Red-Hat, Centos y Debian.

81 Fuente: http://www.ubuntu.com/getubuntu/download

El sistema operativo será instalado[82] en una PC de escritorio con los siguientes componentes de Hardware:

Tabla 5-7 Componentes de Hardware del servidor de Autentificación

Componente	**Características.**
Procesador	Intel(R) Celeron(R) CPU 2.40GHz
Memoria RAM	759036 KB
Disco Duro	120 GB
Interfaz de Red.	Realtek 10/100 Fast Ethernet

5.9.1. Instalación y Configuración de pre requisitos del Servidor de Autentificación WifiDog.

Una vez que se ha instalado el sistema operativo Ubuntu, se trabajará mediante consola de línea de comandos con una conexión SSH, esto es debido a que la versión de Ubuntu Server no instala la interfaz grafica por defecto para ahorrar recursos del sistema y también para excluir software probablemente innecesario, pero es posible instalar la interfaz grafica más adelante de ser necesario.

La configuración de la red en el servidor de autentificación es la siguiente:

Tabla 5-8 Datos de la red del Servidor de Autentificación

Dirección IP del Servidor	192.168.3.100
Mascara de subred	255.255.255.0

82 Véase Anexo “Instalación de Ubuntu Server” http://www.debianadmin.com/ubuntu-lamp-server-installation-with-screenshots.html

Ubuntu Server, al igual que OpenWrt tiene un manejador de paquetes llamado “Aptitude” que almacena en repositorios el software pre compilado disponible para la arquitectura de hardware y la distribución. Además que permite la instalación, modificación y desinstalación del software con unas pocas instrucciones en línea de comandos o desde la interfaz grafica.

Para comenzar la instalación del servidor web Apache y PHP5[83] es necesario actualizar la lista de repositorios y de software utilizando la consola de comandos, para lo cual se establecerá conexión SSH por medio de “PuTTY” a la dirección 192.168.3.100.

Para iniciar sesión en el servidor de autentificación se utilizara el nombre de usuario y la contraseña configurados en la instalación.

En Ubuntu Server, al momento de iniciar sesión, el usuario no cuenta con los privilegios de administración requeridos para modificar el sistema, por lo que se ejecuta el comando “*sudo –s*” el cual luego de ingresar la contraseña concederá permisos de Súper Usuario.

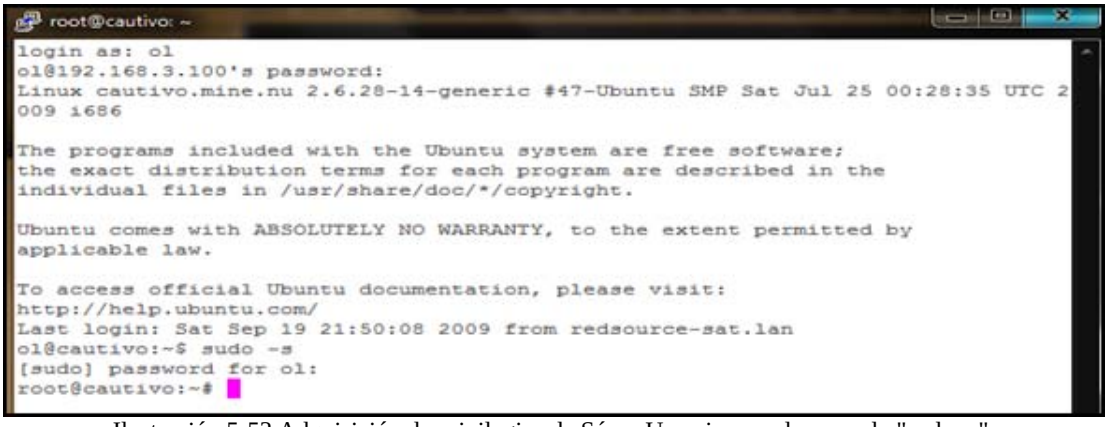


Ilustración 5-53 Adquisición de privilegios de Súper Usuario con el comando "sudo -s"

83 PHP es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.

Con los privilegios de Súper Usuario se actualizan los repositorios de software con el comando "*aptitude update*".

Ilustración 5-54 Actualización de repositorios de software

5.9.1.1. Instalación y configuración del servidor Web Apache y el lenguaje de programación Pre Interpretado PHP.

Después de actualizar los repositorios de software se puede iniciar la instalación de Apache conjuntamente con PHP5, para lo cual se ejecuta el comando "*Aptitude install apache2 php5*".

Además instalan los componentes requeridos para PHP5 que complementan la instalación de Apache permitiendo que pueda interactuar directamente con PHP y PostgreSQL con el comando: "*aptitude install php5-mhash php5-pgsql php-pear php5-xmlrpc php5-curl php5-mcrypt*".

Cuando se hayan instalado estos paquetes de software, será necesario modificar el archivo de configuración de Apache2 indicando la ubicación del directorio WEB, la cual se establecerá a "*/var/www/wifidog-auth/wifidog/*". Para esto se modifica el archivo

"*/etc/apache2/sites-available/default*" con el editor de textos NANO como se puede observar en la siguiente figura.

Ilustración 5-55 Configuración de directorios en Apache

Al finalizar estas configuraciones se debe reiniciar el servidor Apache con el comando *"/etc/init.d/apache2 reload*".

5.9.1.2. Instalación y configuración de el servidor de Base de Datos Relacionadas PostgreSQL

Después de la instalación de Apache y Php con todos sus componentes se debe instalar el servidor de base de datos relacionadas PostgreSQL con el comando *"aptitude install postgresql"*.

Una vez instalado PostgreSQL es necesario crear una base de datos y un usuario relacionado para Wifidog.

PostgreSQL tiene un usuario especifico el cual puede manejar por completo el servidor de base de datos, para iniciar sesión con este usuario se ejecuta el comando "sudo su – postgres" y para crear un usuario "createuser wifidog –pwprompt".

Ilustración 5-56 Creación de usuario wifidog

Se crea una base de datos llamada “wifidog” con el comando “createdb wifidog --encoding=UTF-8 --owner=wifidog”.

Ilustración 5-57 Creación de base de datos "wifidog"

Hecho esto se tendrá una base de datos llamada “wifidog” relacionada al usuario “wifidog”.

5.9.1.3. Instalación y configuración del servidor de Correo Electrónico Postfix

Wifidog utiliza un sistema de registro para los nuevos usuarios el cual envía un correo electrónico solicitando la confirmación de la cuenta de correo, para lo cual es necesaria la instalación de un servidor de Correo Electrónico. Para este proyecto se ha escogido como servidor de Correo Electrónico al Agente de Transporte de Correo Postfix.

Postfix es un Servidor de Correos Electrónicos de software libre el cual en los últimos años se ha convertido en una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail.

Para instalar Postfix con todos sus complementos se ejecutara el siguiente comando “aptitude install postfix libsasl2-modules sasl2-bin”.

En los últimos años la publicidad y el correo no deseado en internet se han convertido en un gran problema para las compañías proveedoras de servicios de internet, por lo cual en la mayoría de servidores de correo las políticas de seguridad impiden establecer conexiones sin autentificación. Una alternativa para esto es el reenvió SMTP[84], con lo cual se puede establecer una conexión entre dos servidores que reenvíen correos. Para lo cual se configurara una cuenta de correo gratuito para que acepte conexiones de reenvió de SMTP.

El servicio de correo electrónico gratuito GMAIL, es una alternativa viable para reenvió de SMTP, debido a que GMAIL admite conexiones SMTP seguras. El funcionamiento de esta configuración se explica en la siguiente ilustración.

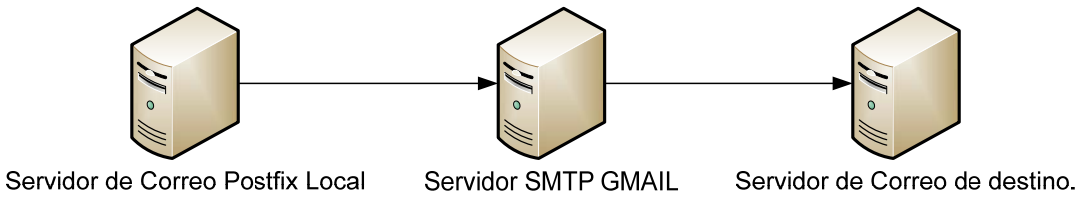


Ilustración 5-58 Ejemplo de reenvió de SMTP

Para configuración del reenvió de SMTP es necesario contar con una cuenta de el correo electrónico gratuito GMAIL, en este caso olbapcrazy@gmail.com. Esta cuenta será la que enviara el correo electrónico a todos los destinatarios.

El primer paso de la configuración de reenvío de SMTP es modificar el archivo "*/etc/postfix/main.cf*" de configuración en el servidor local Postfix y agregar las siguientes líneas al final como se puede observar en la siguiente tabla.

84 Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos

Tabla 5-9 Configuración del reenvío SMTP de Postfix

smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
relayhost = [smtp.gmail.com]:587
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
smtp_use_tls = yes

Después se modifica el archivo "/etc/postfix/sasl/passwd" de la siguiente manera:

[smtp.gmail.com]:587 olbapcrazy@gmail.com:clave

Luego de esto se cambian los permisos de Postfix para que se pueda leer el archivo con el comando "*chmod 600 /etc/postfix/sasl/passwd*". Y finalmente se reinicia el servicio "/etc/init.d/postfix restart". Con estas configuraciones, el servidor local de correo electrónico Posftix tiene la capacidad de reenviar todos los correos que entran por la interfaz local en el puerto SMTP 25 hacia GMAIL.

5.9.1.4. Instalación del Servicio de Control de Versiones SubVersion.

Subversion (SVN) es un sistema de control de versiones iniciado en 1999 por CollabNet Inc. Se utiliza para mantener las versiones actuales y los archivos históricos, como por ejemplo el código fuente, páginas web, y la documentación.

Wifidog utiliza para la instalación de su servidor de autentificación el sistema de control de versiones Subversion, por lo cual es necesario su instalación, esto se lo realiza con el comando "aptitude install subversión".

5.9.2. Instalación del Servidor de Autentificación Wifidog

Para iniciar la instalación del Servidor de Autentificación Wifidog se descargaran los archivos que contienen el sistema de autentificación en la carpeta /tmp con el comando *"svn checkout https://dev.wifidog.org/svn/trunk/wifidog-auth", acto seguido se moverá la carpeta descargada a la ubicación "/var/www/" con el comando "mv wifidog-auth/ /var/www/"*.

Ilustración 5-59 Descarga de los archivos necesarios para la instalación de Wifidog.

Al haber copiado los archivos de instalación de Wifidog a la carpeta en donde se alojan las páginas web del servidor Apache, se puede ingresar al instalador grafico mediante Web en la dirección http://192.168.3.100/.

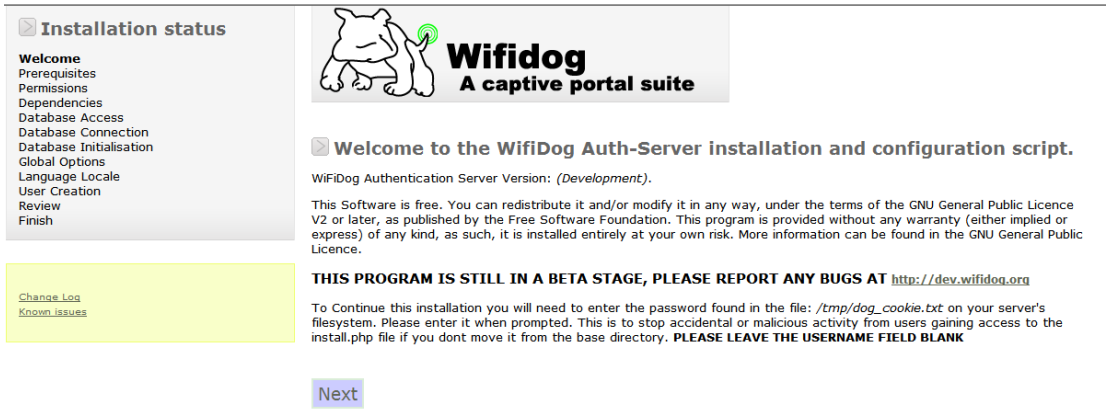


Ilustración 5-60 Pagina principal del instalador Wifidog

Al abrir la página de instalación aparecerá una ventana solicitando el nombre de usuario y contraseña para continuar. Esta contraseña es generada automáticamente y se guarda en la carpeta *"/tmp/"*del servidor con el nombre "dog_cookie.txt", dentro de este archivo se encuentra la contraseña. No es necesario ingresar un nombre de usuario como se puede ver en la siguiente ilustración.

Ilustración 5-61 Inicio de sesión en la instalación de Wifidog

Aparece una ventana indicando que los permisos de los archivos y carpetas no son los correctos, y en la parte inferior de la misma se encuentran los comandos que se debe de copiar en la consola de comandos para solucionar estos requerimientos.

Ilustración 5-62 Permisos insuficientes para las carpetas y archivos de instalación

Se copia y se pega en la consola SSH los comandos descritos por el instalador, acto siguiente se da clic en el botón "*Refresh*" y se puede observar que se ha corregido el error.

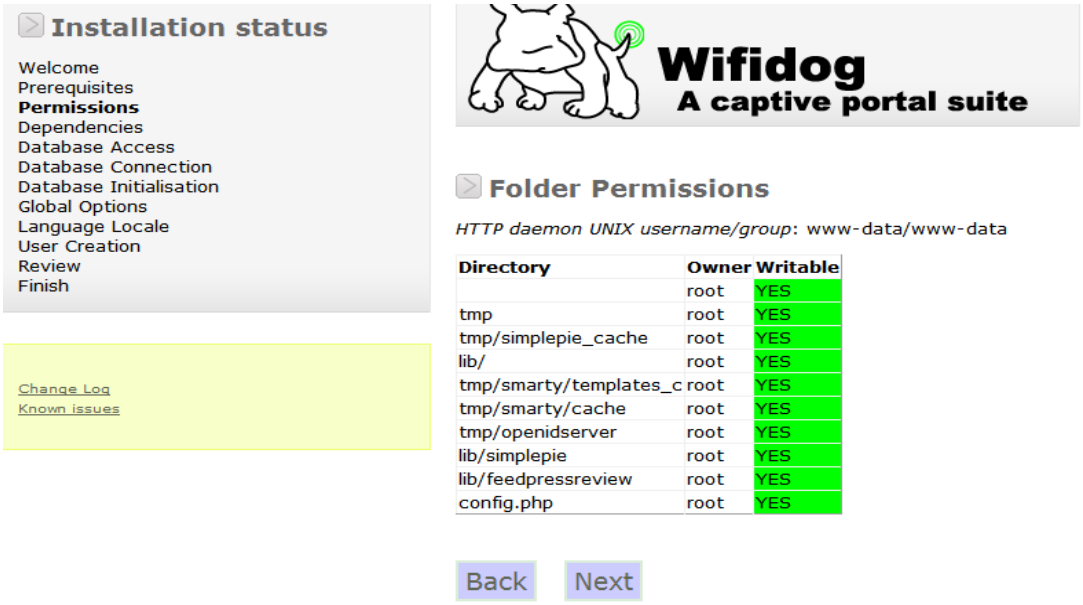


Ilustración 5-63 Corrección de permisos en archivos de instalación

Al haber corregido los errores y dar clic en el botón "*Next*" aparece otra lista de requerimientos incompletos, solo es necesario corregir los requerimientos en rojo, para hacerlo se debe dar clic en "Install".

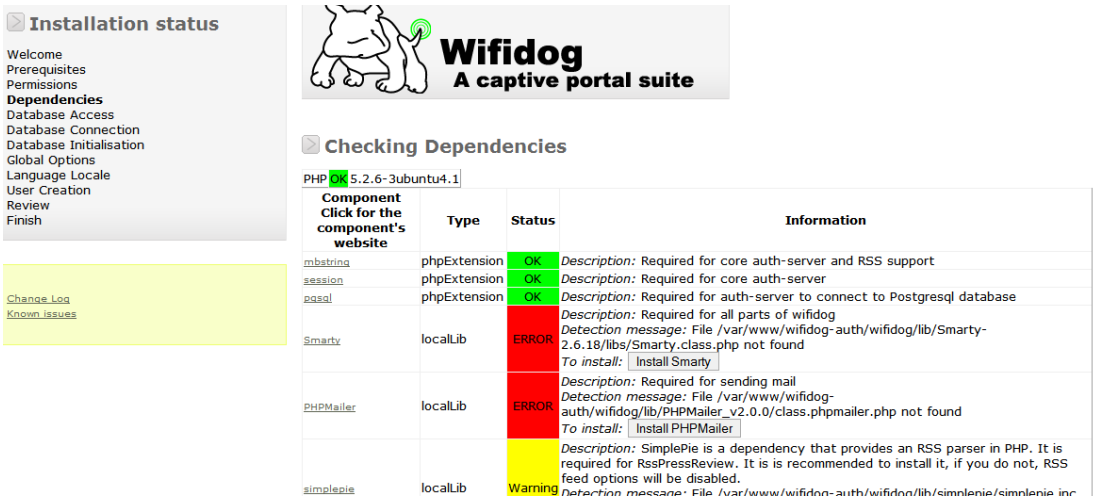


Ilustración 5-64 Error al revisar las dependencias de Wifidog.

Al haber corregido la dependencia incompleta el color de la advertencia cambia a verde y se puede dar clic en siguiente.

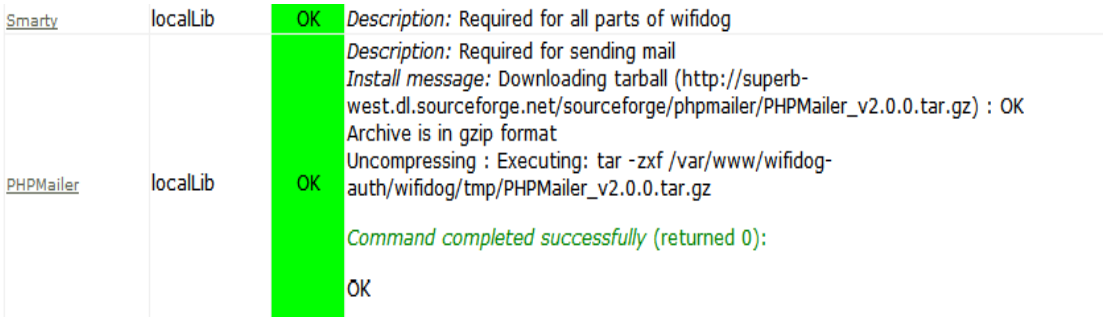


Ilustración 5-65 Corrección de dependencias

La siguiente ventana solicita la información para conectarse con la base de datos previamente configurada. Se escribe el nombre de la base de datos, el usuario, la contraseña, la dirección del servidor y el puerto.

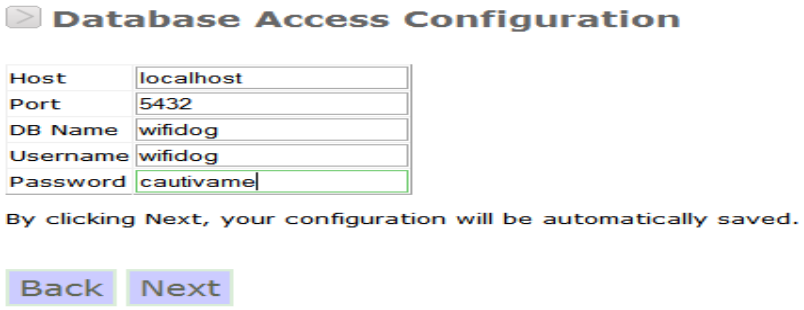


Ilustración 5-66 Solicitud de credenciales para conexión con la base de datos.

Se configura si la base de datos deberá ser revisada con una tarea del sistema y además se habilita o no el soporte para Google Maps. Es importante señalar que este servicio para páginas Web no está disponible en el Ecuador, y después de varias pruebas se recomienda su inhabilitación.

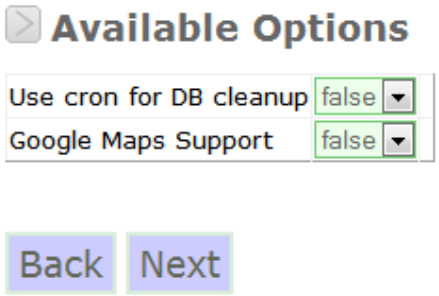


Ilustración 5-67 Inhabilitación de Google Maps

Wifidog está traducido a varios idiomas. Se debe seleccionar el idioma “Español”.

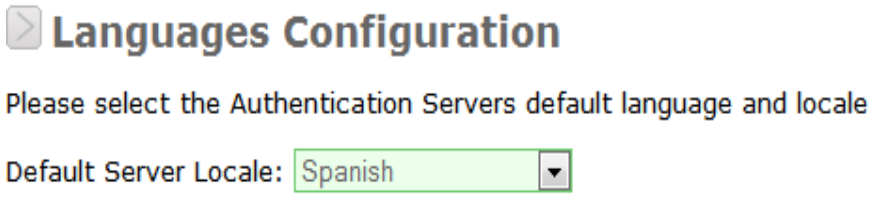


Ilustración 5-68 Selección del lenguaje.

Ingreso de información para la cuenta de administrador “admin”.

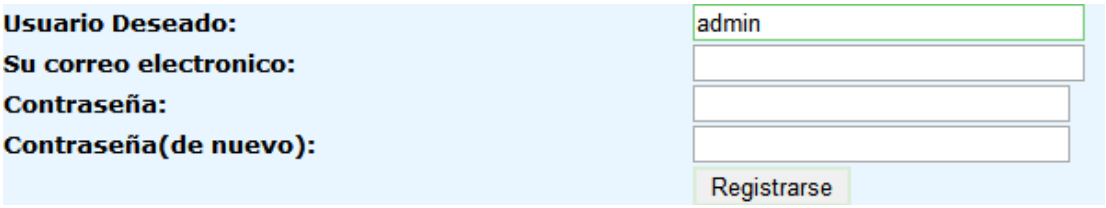


Ilustración 5-69 Registro de la cuenta de administrador

5.9.3. Configuración del Servidor de Autentificación Wifidog.

Wifidog administra las redes de portales cautivos creando un contenedor principal llamado “Network” (Redes) y dentro de este contenedor se encuentran los “Nodos”, que son las puertas de enlace del portal cautivo. Esto es de utilidad, debido a que todas las redes manejan una configuración única, por lo cual, las llamadas Redes pueden referirse a diferentes empresas o instituciones, las cuales requieran de una configuración especifica. La siguiente ilustración explica su funcionamiento.

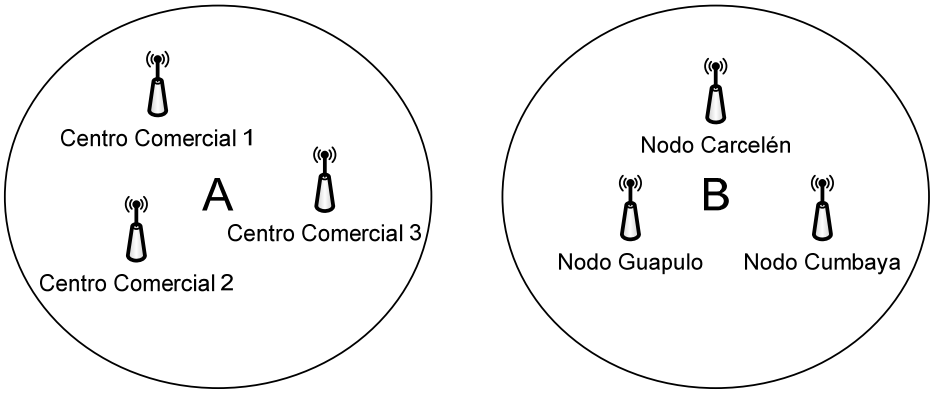


Ilustración 5-70 Ejemplo de Nodos y Redes en una red Wifidog

Luego de haber instalado satisfactoriamente WifiDog se re direccionara a la página web de inicio de sesión, en donde se debe de llenar los campos registrados en el momento de la instalación. Nombre de usuario “admin” contraseña “cautívame”

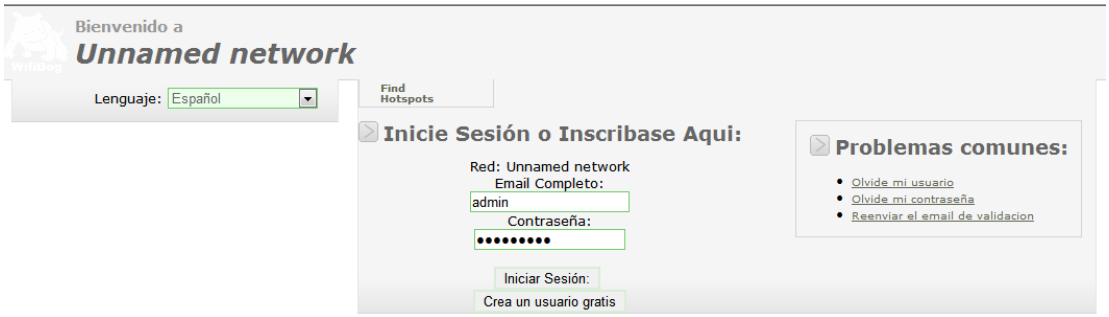


Ilustración 5-71 Primer inicio de sesión en el servidor de autentificación.

La primera página que aparecerá después del inicio de sesión solicitara ingresar el nombre del Nodo y sus detalles de ubicación, este nodo se guarda en la red que se crea al momento de la instalación llamada “Default Network” sin embargo este nombre se puede modificar posteriormente.

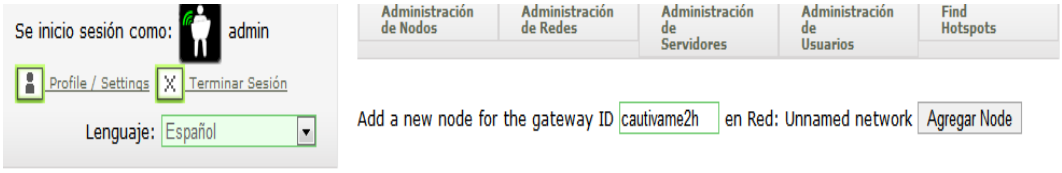


Ilustración 5-72 Ingreso del nombre de la primera puerta de enlace Wifidog

El nombre del primer nodo se llamara “cautivame2h” debido a su ubicación, como se muestra en la Ilustración 5-72

Ilustración 5-73 Información adicional para el primer nodo configurado.

Como se puede observar en el capítulo 5.8, el nombre de nodo se lo guarda previamente en el enrutador inalámbrico, en el archivo *“/etc/wifidog”*.

El servidor de autentificación, en su consola de administración web, utiliza un menú en el cual se encuentran todas las utilidades necesarias para administrar una red. Es importante señalar que no todo el menú se encuentra traducido al español.

Tabla 5-10 Menú de configuración Wifidog

Menú principal	**Menú secundario**	**Descripción.**
Administración de Nodos	Agregar un nuevo Nodo	Agrega y edita los nodos de una red específica.
	Edit nodes	
Administración de Redes	*Add a network on this server*	Agrega y edita las redes del servidor y sus configuraciones personalizadas.
	Edit network	
Administración de Servidores	*Content type filters*	Edita las configuraciones del servidor, como sus tipos de contenido, las dependencias necesarias, las plantillas para redes que pueden ser reusadas, el contenido de las redes que puede ser reusado, los roles de usuarios y los host virtuales que manejan los nombres de los dominios, en caso de que el servidor sea compartido con diferentes nombres de dominio.
	Dependencies	
	Profile templates	
	Reusable content library	
	Server Configuration	
	User roles	
	Virtual hosts	
Administración de usuarios	Estadísticas	Control de usuarios, estadísticas de acceso y además puede importar usuarios desde el software de portal cautivo NoCat.
	Importar base de datos de *NoCat*[85]	
	User manager	
	Usuarios en línea	
Find Hotspots	List in HTML format	Busca los nodos activos de todas las redes configuradas en el servidor.

Después de editar el primer nodo en el servidor, es necesario modificar el perfil del administrador en el menú "Administración de servidores/User Roles" y habilitar la opción "NETWORK_PERM_EDIT_DYNAMIC_ABUSE_CONTROL" para que pueda modificar las configuraciones de control de abuso y saturación de red.

[85] NoCat Auth es un software de portal cautivo de software libre.

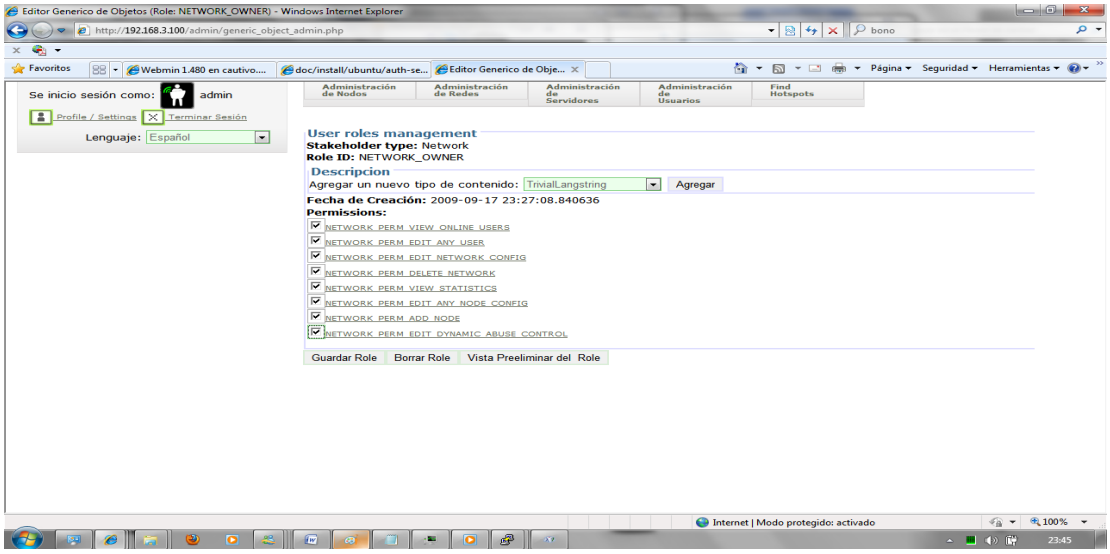


Ilustración 5-74 Configuración de roles de usuario

Con los roles de administrador correctamente establecidos, se configura la red por defecto de WifiDog.

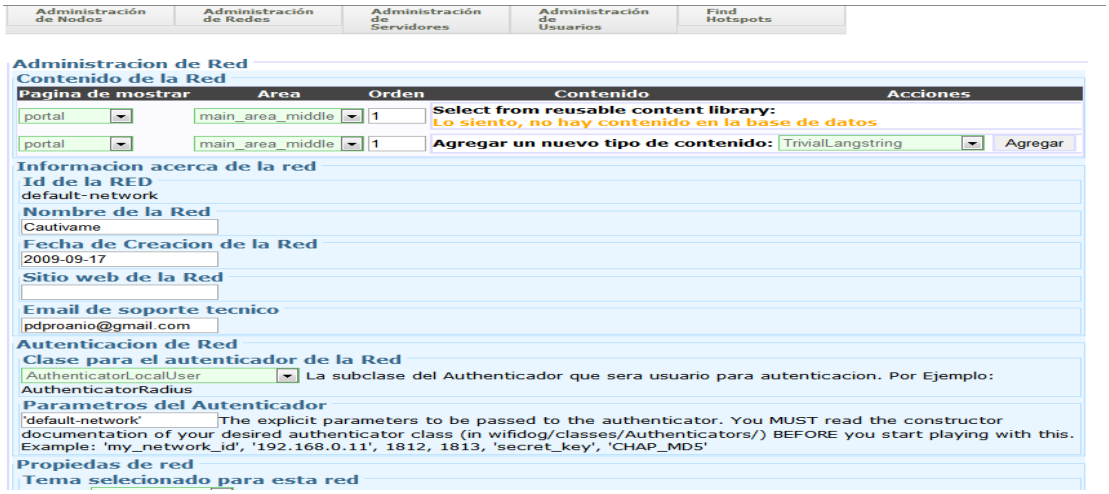


Ilustración 5-75 Configuración del nombre de la red y la información de su administrador.

El nombre de la red original del portal cautivo se la ha cambiado a “Cautívame”, por hacer referencia al portal cautivo. La información básica de los administradores de la red servirá para todos los nodos que se encuentren dentro de la misma.

Wifidog provee algunas formas de establecer una autentificación del usuario. Para este proyecto se ha utilizado la autentificación interna, que utiliza información guardada en la base de datos PostgreSQL para registrar nuevos usuarios o para identificar usuarios existentes. Además de este tipo de autentificación, Wifidog permite establecer comunicación con servidores LDAP y Radius que pueden estar configurados en el mismo servidor o en uno externo. Con la configuración básica se puede denegar el registro de nuevos usuarios, permitiendo así solamente el uso de usuarios internos o simplemente manejar el ancho de banda de los usuarios sin necesidad de que inicien sesión en el servidor.

Cuando un usuario crea una nueva cuenta para el portal cautivo, se le da un periodo de gracia, en el cual puede usar el internet para revisar el correo electrónico y confirmar la cuenta. El tiempo del periodo de gracia se lo configura en segundos en el campo de "Tiempo de gracia para validación".

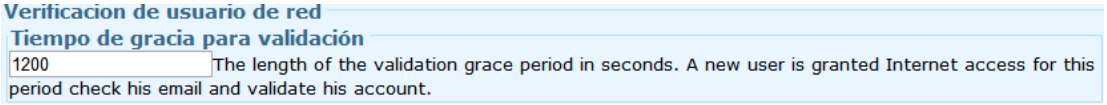


Ilustración 5-76 Periodo de gracia para usuarios nuevos contado en segundos (1200 = 20 Minutos)

El control de ancho de banda y el tiempo de navegación es una de las características más importantes del sistema de Portal Cautivo Wifidog, ya que con esta característica se puede controlar la cantidad de ancho de banda que un usuario puede utilizar en un nodo y en una red en general, además permite definir el tiempo máximo de duración de una conexión. Si un usuario sobrepasa el límite de alguna de estas características se le denegara el uso de la red automáticamente. Otra característica es que pasado el tiempo definido por el administrador los contadores volverán a estar en 0 y el usuario podrá volver a trabajar con la red. Esta característica se llama "*Abuse Control*" y se configura de la siguiente manera.

Tabla 5-11 Control de conexiones en la red Wifidog "Abuse Control"

Tipo de control	**Parámetro**	**Descripción.**
Abuse control window	1 day	Lapso de tiempo para que los contadores se reinicien en 0.
Network max total bytes transfered	300000000	Máximo de ancho de banda permitido para enviar y recibir en la RED en Bytes (300 MB)
Network max connection duration	08:00:00	Duración máxima permitida de una conexión en la RED, hasta que los contadores se reinicien en 0. (8 Horas)
Node max total bytes transfered	80000000	Máximo de ancho de banda permitido para enviar y recibir en el Nodo en que se conecta el cliente. (80MB)
Node max connection duration	02:00:00	Duración máxima permitida de una conexión en un Nodo, hasta que los contadores se reinicien en 0. (2 Horas)

Cada vez que un usuario se conecte a la red tendrá un máximo de 80MB disponibles de ancho de banda en el nodo que se conecte, y de ser el caso si el usuario cambia de nodos tendrá 300MB en toda la red. Además tendrá un máximo de conexión de 2 horas en cada nodo y 8 horas en toda la red. Estos contadores se reiniciaran diariamente.

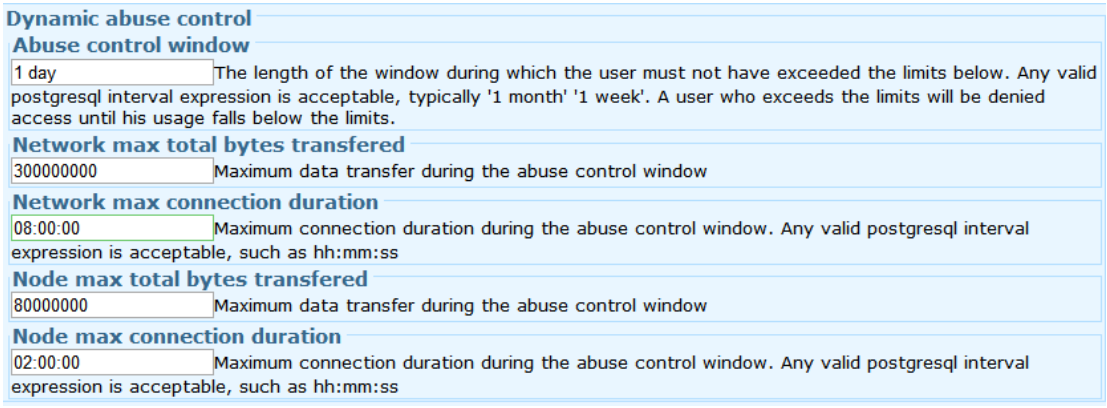


Ilustración 5-77 Configuración de "Abuse Control" para administrar el ancho de banda y el tiempo de la conexión de cada usuario.

Para finalizar la configuración del “Abuse Control” es necesario insertar un aviso para que cuando el usuario se conecte a la red sea informado del ancho de banda disponible y el

utilizado así como el tiempo que lleva conectado en la red. Para esto se debe agregar el tipo de contenido "*UIAllowedBandwidth*" en la página de configuración de la RED.

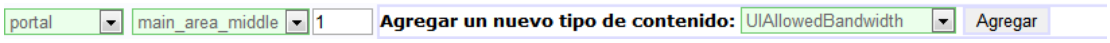


Ilustración 5-78 Menú para agregar una nueva ventana de "Abuse Control"

Al igual que la ventana de "Abuse Control" es posible agregar diferentes tipos de contenido y publicarlos en la página principal del portal cautivo o en la página que aparece después de haber iniciado sesión.

Al finalizar las configuraciones anteriormente descritas, el Servidor de Autentificación del Portal Cautivo Wifidog estará listo para ser utilizado.

5.10. INSTALACIÓN DE SERVIDOR DE ARCHIVOS SAMBA EN ENRUTADOR INALÁMBRICO WRT54G.

Como se lo detalla en el capítulo 5.7, el enrutador inalámbrico LinkSys Wrt54GL que se utiliza para este proyecto ha sido modificado para montar como un disco duro adicional una memoria SD de 2GB. Esta memoria es utilizada para almacenar gran parte de los sistemas utilizados para el portal cautivo Wifidog y otras herramientas de red necesarias. Sin embargo existe un espacio de memoria libre que ha quedado disponible, y puede ser utilizado para otros propósitos.

El objetivo principal de este proyecto es brindar a los propietarios y administradores de las organizaciones una manera fácil y económica de administrar la red, con un enrutador de bajo costo que funcione como servidor de red, proveyéndoles de herramientas fáciles de utilizar. Una vez instalado la puerta de enlace del portal cautivo Wifidog con todas sus herramientas y haberlo enlazado al servidor de autentificación, es de gran utilidad añadir un servidor de archivos, el cual podría ser utilizado según las necesidades, pero para este proyecto se ha pensado la necesidad de un repositorio de parches y herramientas de

seguridad para proveer a los usuarios finales de una manera fácil. Para esto es necesaria la instalación del servidor de archivos SAMBA.

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que las computadoras con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory[86] para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autentificar con su propio archivo de usuarios[87].

Para instalar SAMBA en el enrutador inalámbrico WRT54GL es necesario establecer una conexión por medio de SSH, una vez establecida esta conexión se instalará el paquete con todas sus dependencias en la memoria SD con el comando “opkg install –d mmc samba3”.

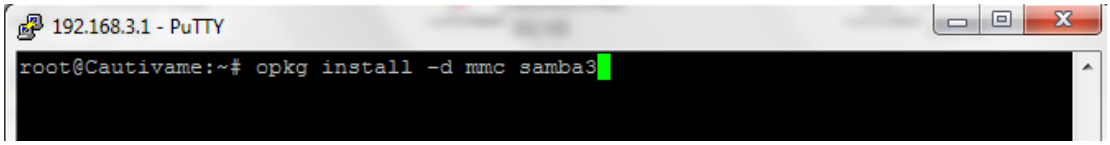


Ilustración 5-79 Instalación del sistema de compartición de archivos SAMBA en la memoria SD del WRT54GL

Después de descargar los archivos es necesario editar la configuración de este servicio en el archivo modificando los parámetros de autentificación para que los usuarios anónimos puedan acceder a la carpeta compartida.

86 Active Directory es un servicio de directorio que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red.
87 (Schroder, 2005)

Tabla 5-12 Configuración de SAMBA, parámetros globales

Parámetro	**Descripción.**
[global]	Configuración general de SAMBA
security = share	Permiso para compartir sin contraseña
guest account = nobody	Cuenta de los usuarios anónimos.

Hecho esto se necesita crear una carpeta compartida que estará situada en una carpeta creada más adelante en la memoria SD.

Tabla 5-13 Configuración de una nueva carpeta compartida en SAMBA

Parámetro	**Descripción**
[compartida]	Nombre de la carpeta a compartir.
path = /mmc/compartida	Ubicación de la carpeta compartida
read only = no	Permiso de lectura y escritura
guest ok = yes	Permiso para los usuarios anónimos
create mask = 0700	Permisos de los nuevos archivos creadas
directory mask = 0700	Permisos de las nuevas carpetas creadas

Se crea la carpeta ubicada en la memoria SD que se compartirá mediante el protocolo SMB con el siguiente comando: "*mkdir /mmc/compartida*"

Al terminar la configuración de SAMBA es necesario habilitar el servicio, para su ejecución en el arranque del sistema con el comando "*/etc/init.d/samba3 enable*" y después iniciar el servicio para comprobar su funcionamiento con el comando "*/etc/init.d/samba3 start*".

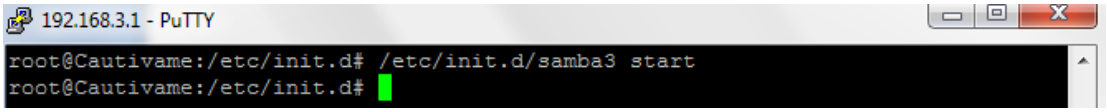


Ilustración 5-80 Ejecución de SAMBA en el enrutador LinkSys WRT54GL

Una vez ejecutado el servicio de SAMBA es posible ingresar a la carpeta compartida mediante el explorador de Windows a la dirección \\192.168.3.1.

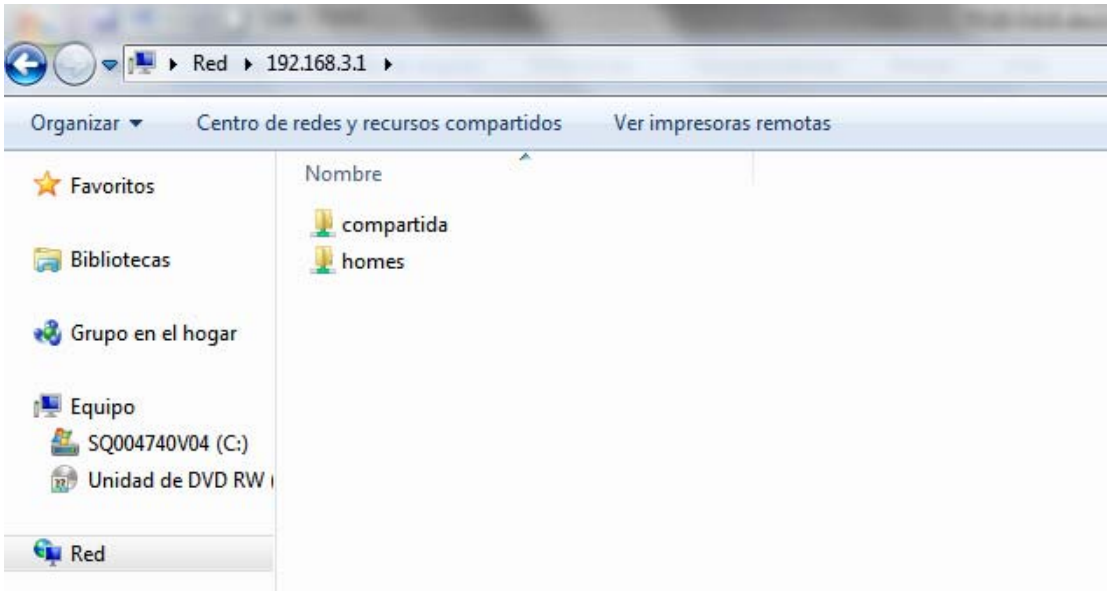


Ilustración 5-81 Carpetas compartidas de SAMBA vistas desde el explorador de Windows.

Como se puede observar en la figura anterior, en el explorador de Windows aparece la carpeta "compartida" la misma que ha sido configurada anteriormente, por lo que se puede saber que la configuración de SAMBA ha sido exitosa. Hecho esto se copiara el software de seguridad que será compartido a los usuarios de la red.

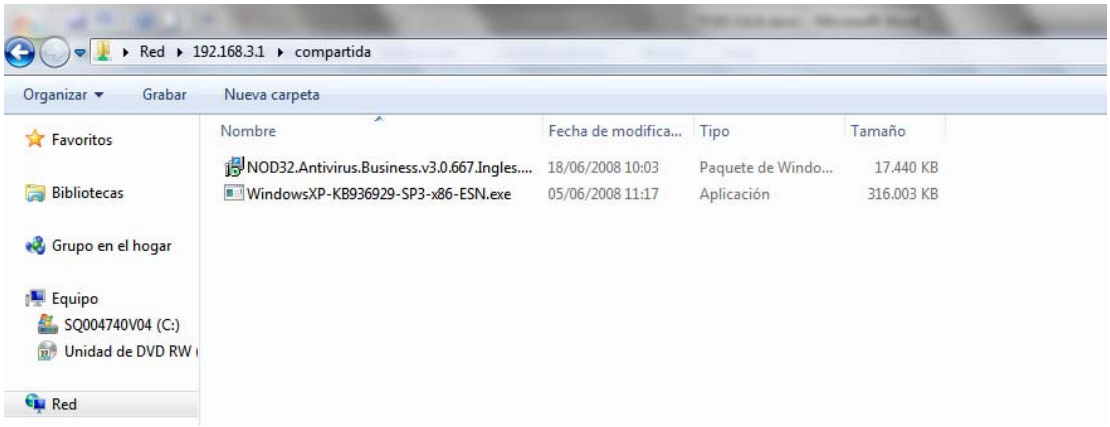


Ilustración 5-82 Archivos copiados exitosamente en la nueva carpeta compartida en SAMBA.

Se han copiado a la carpeta compartida dos utilidades: una copia de demostración del antivirus NOD32 V3.0 y Windows XP Service Pack 3, este software es de gran popularidad y puede ayudar a mejorar las condiciones de seguridad de los equipos cliente.

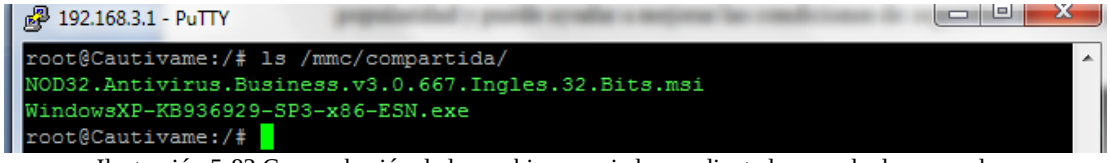


Ilustración 5-83 Comprobación de los archivos copiados mediante la consola de comandos

Como se puede observar en la ilustración 5-83, se ha comprobado la existencia de los archivos copiados a la carpeta compartida desde la consola de comandos y con el comando *"ls /mmc/compartida"*.

Para difundir esta carpeta compartida dentro del nodo de Wifidog es necesario iniciar sesión en el servidor de autentificación, dirigirse a la ubicación: "*Administración de nodos/Edit node*" y agregar una entrada llamada "SimpleString". Además de esto se agregaran las condiciones de uso del nodo.

Ilustración 5-84 Nueva entrada para publicar la carpeta compartida y las condiciones de uso en el Nodo.

Wifidog acepta etiquetas HTML que pueden ser utilizadas para resaltar u ordenar la información como se muestra en la siguiente ilustración.

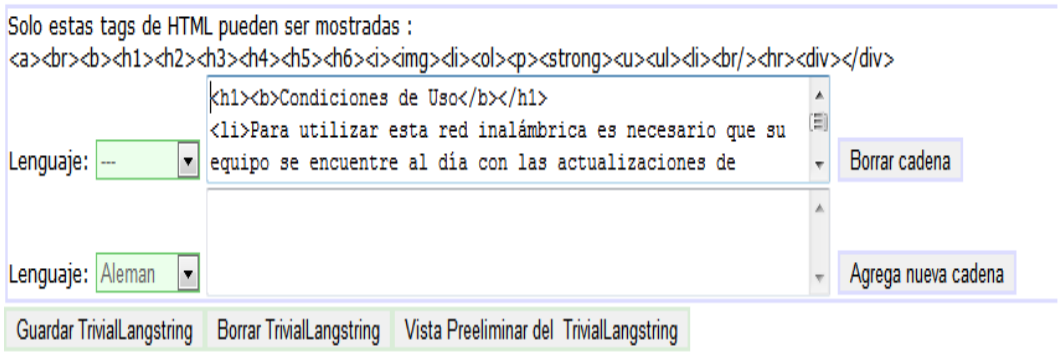


Ilustración 5-85 Edición de la entrada que contiene las condiciones de uso del nodo y la publicación de la carpeta compartida.

Se podrá observar la siguiente información en el servidor de autentificación luego de haber grabado los datos.

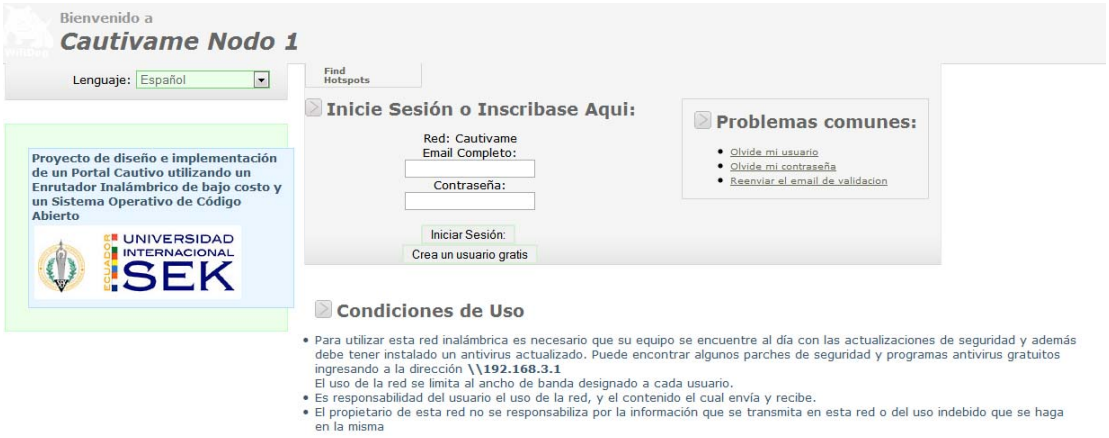


Ilustración 5-86 Condiciones de uso y carpeta compartida publicados exitosamente.

5.11. VERIFICACIÓN DE RESULTADOS

Después de finalizar todos los procesos de instalación y configuración en el enrutador inalámbrico Wrt54GL y en el servidor de autentificación Ubuntu 9.04 descritos anteriormente, se ha completado el proceso de instalación y configuración de la Puerta de enlace y Servidor de autentificación Wifidog, para lo cual se comprobará su funcionamiento.

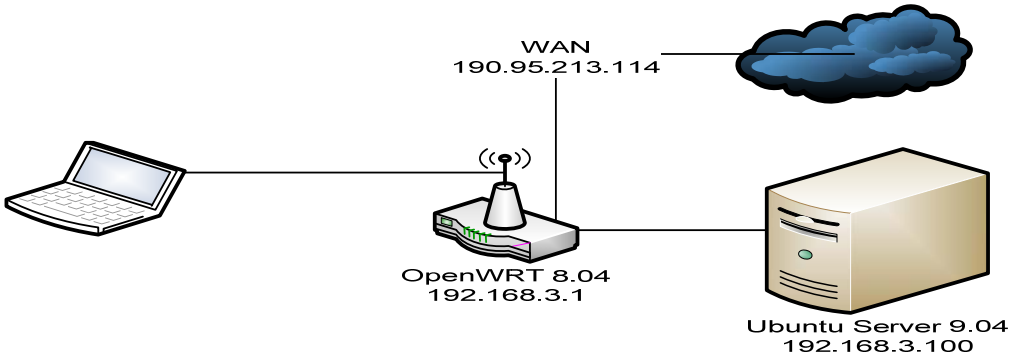


Ilustración 5-87 Configuración de la red LAN y WAN para la demostración del proyecto.

La configuración establecida para la red de prueba y demostración del proyecto de Portal Cautivo Embebido y Servidor de Autentificación utiliza al mismo enrutador para dar acceso a internet, y el servidor de autentificación y los clientes están dentro de la red LAN. Sin embargo el enrutador posee una dirección IP pública para poder acceder desde internet a la red interna de ser necesario.

5.11.1. Pruebas del funcionamiento del Portal Cautivo Wifidog.

El SSID de la red WLAN se lo ha establecido como “Red-Abierta”, ya que con este nombre es posible llamar la atención de usuarios externos para que se conecten a la red por medio del enrutador inalámbrico y aporten a generar estadísticas y revisión de configuraciones; además de esto, Dentro de la red del portal cautivo, se han creado usuarios locales para hacer pruebas y registrar sucesos.

El primer paso para establecer una conexión de red es buscar la WLAN “Red Abierta” y unirse a ella.

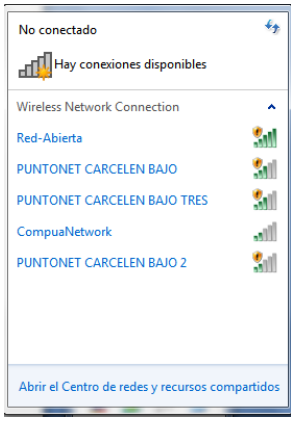


Ilustración 5-88 Conexión a la red WLAN "Red-Abierta

Una vez que se ha realizado la conexión, el servidor DHCP envía la configuración de red necesaria a los clientes. Esto se lo puede comprobar con el comando "*ipconfig /all*"[88] en Windows.

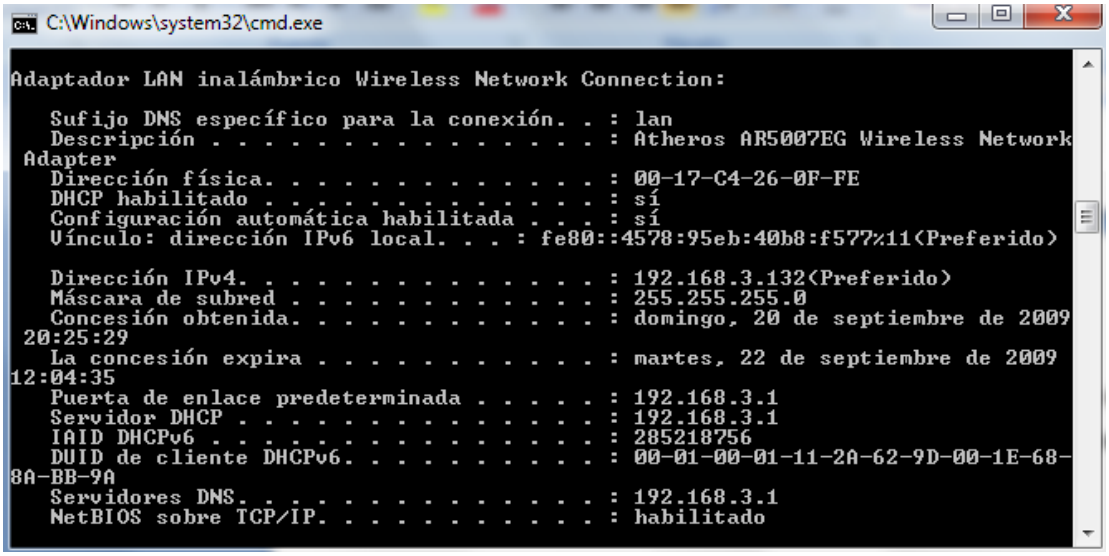


Ilustración 5-89 Adquisición de parámetros de la red por medio de DHCP

Cuando se establece una conexión entre un cliente y la puerta de enlace, se genera un ID único de la conexión llamado "TOKEN" que permite a Wifidog mantener el seguimiento al usuario, independientemente de la computadora, dirección IP o Nodo en el cual trabaje.

Según las configuraciones establecida por DHCP, en este momento se tiene acceso a la red y se debería también tener acceso a internet, para lo cual se abre un navegador web.

88 En GNU / LINUX se utiliza el comando "ifconfig"

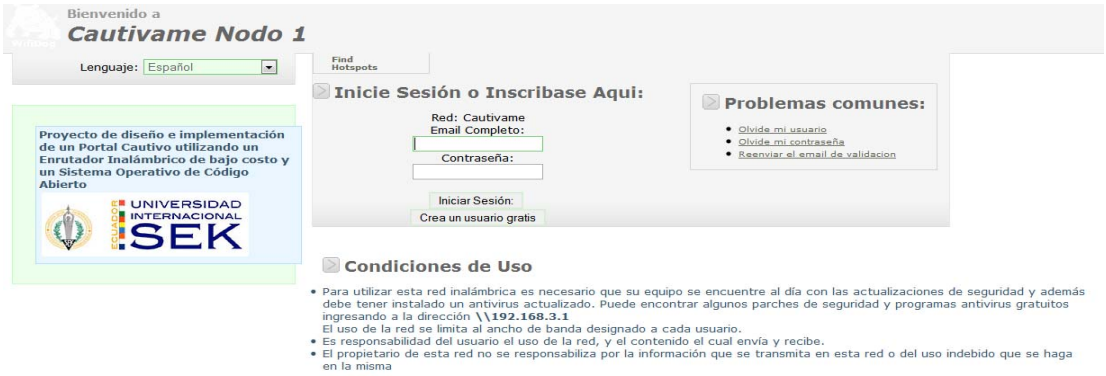


Ilustración 5-90 Portal cautivo solicitando credenciales para iniciar sesión en la red.

Al momento de abrir el navegador web e intentar abrir la pagina web “google.com” se redirige la consulta hacia la pagina web del portal cautivo, en donde se debe ingresar el nombre de usuario y contraseña de un usuario existente o crear una nueva cuenta, para lo cual se da clic en el botón “Crea un usuario gratis”. En el formulario de registro se deben llenar todos los campos.

Tabla 5-14 Campos del formulario para crear un nuevo usuario en el nodo del portal cautivo.

Usuario Deseado:
Su correo electrónico:
Contraseña:
Contraseña(de nuevo):

Luego de llenar los campos obligatorios, se da clic en el boton “Registrarse”. Si los campos llenados son correctos una nueva pagina aparecera indicando que el usuario tiene 20 minutos de gracia para poder entrar al internet para revisar el correo electronico enviado y confirmar la cuenta.

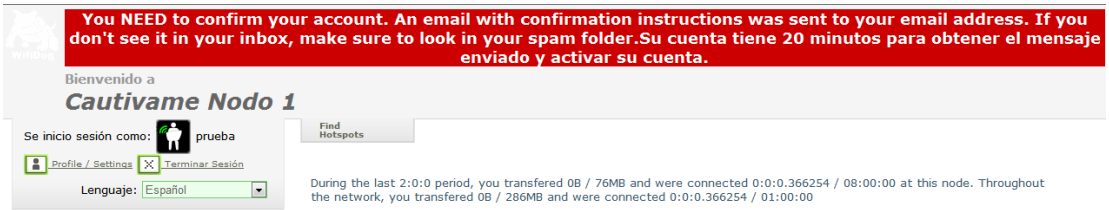


Ilustración 5-91 Mensaje de advertencia de periodo de gracia en la red.

Con este periodo de gracia se puede revisar el correo de confirmación. Se da clic en el enlace y se activa la cuenta.

Ilustración 5-92 Correo electrónico de confirmación de la cuenta

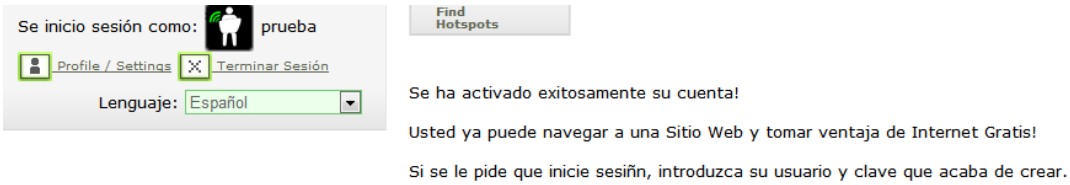


Ilustración 5-93 Activación exitosa de la cuenta.

El usuario puede cambiar sus datos ingresando en el menú "*Profile / Settings*".

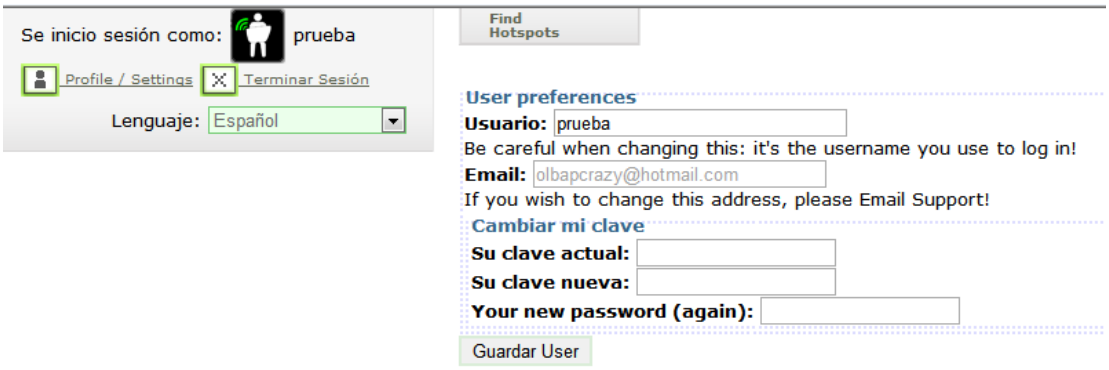


Ilustración 5-94 Cambio de contraseña del usuario "prueba"

Al momento de activar la cuenta se puede utilizar el internet, sujetándose a la configuración del firewall de la puerta de enlace de Wifidog, y a las políticas de uso de la red descritas en el capítulo 5.8 y 5.9.3.

Cuando un usuario registrado inicia sesión nuevamente en la red de portales cautivos, aparecerá una página en donde se informa la cantidad de ancho de banda que le queda por consumir, y el tiempo total utilizado.

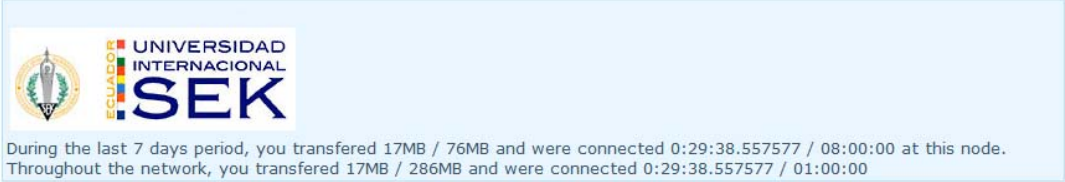


Ilustración 5-95 Mensaje de aviso sobre la cantidad de ancho de banda consumido hasta el momento, y el tiempo restante de la conexión.

En caso de que el usuario exceda el límite de tiempo permitido para una conexión o el ancho de banda asignado al nodo, las políticas de firewall cambiaran automáticamente, por lo que perderá la conexión a internet y la navegación será redirigida al portal cautivo que contendrá un mensaje indicando las razones por las que ha sobrepasado el límite.

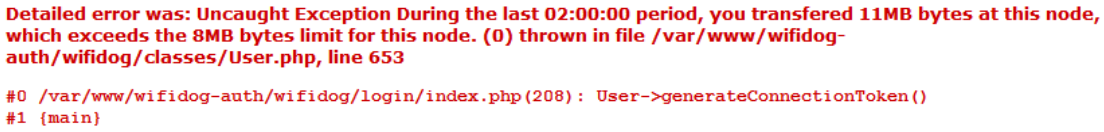


Ilustración 5-96 Mensaje de error por haber excedido el límite de ancho de banda asignado al nodo.

Esta forma de controlar el ancho de banda en lugar del contenido por parte de Wifidog, da lugar a que un usuario tenga una navegación libre, hasta que exceda el ancho de banda asignado o el tiempo, permitiendo así controlar a los usuarios que abusan de la red, descargando cantidades grandes de información, o permaneciendo por un tiempo mayor al establecido.

5.11.2. Estadísticas de uso del Portal Cautivo Wifidog.

Wifidog provee de estadísticas que se generan de los registros en la base de datos mediante el seguimiento a los usuarios, esto permite que el administrador pueda revisar el uso de la

red, los usuarios registrados y los más frecuentes. Para poder acceder a esta característica es necesario iniciar sesión en el Servidor de Autentificación del Portal Cautivo Wifidog y dirigirse al menú “Administración de Usuarios”. En dicho menú se puede escoger dos tipos de consultas para buscar estadísticas, la primera opción es generar estadísticas por cada usuario.

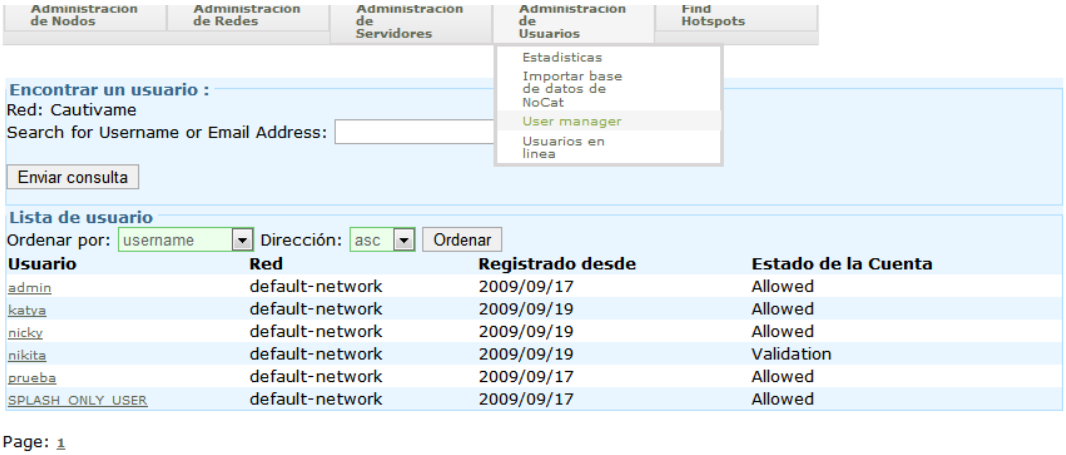


Ilustración 5-97 Usuarios Registrados en el portal cautivo

Como se puede observar en la figura anterior, Wifidog provee de una lista de usuarios registrados en la red, además de la fecha de su registro y el estado de la cuenta. Las cuéntas en estado “Allowed” están activas ya que fueron confirmadas con el correo de activación, por otro lado las cuentas en estado “Validation” no han sido comprobadas, por lo que no proveen acceso a internet.

En la siguiente tabla se puede observar las consultas que están disponibles en el servidor de autentificación. Cabe señalar que al igual que algunas características de Wifidog, el modulo de estadísticas no está traducido al español por completo.

Tabla 5-15 Tipos de estadísticas disponibles en Wifidog

10 usuarios más frecuentes
Anonymised SQL data export (for academic research)
Breakdown of how many users actually use the network
Content display and clickthrough report
Grafico de uso de la red por hora, semana y mes
Información del estado del Nodo
Información del Estado de la Red
Log de Registro (Primera conexión de usuarios nuevos)
Log de conexiones
Los 10 más altos consumidores de banda ancha
Los 10 usuarios mas móviles
Nodos más populares, según visita
Reporte de número de usuarios registrados
Reporte individual por usuario

Para generar reportes individuales, es necesario dar clic sobre su usuario, esto redirigirá a la página de edición de las cuentas, luego se debe de dar clic en el link "*Get user statistics*". Esto genera un detalle del uso de la red por parte del usuario seleccionado.

Reporte individual por usuario

Perfil

Usuario:	prueba
Email:	olbapcrazy@hotmail.com
Red:	default-network
Id Unico:	69da136cfb809346f260da65e72a22d4
Miembre Desde:	jue 17 sep 2009 23:58:50 EDT
Estado de la Cuenta:	Allowed
Localidad Preferidad:	

6 Conexiones

Sesión Iniciada	Tiempo Utilizado	Estado del Token	Nodo	IP	D	U
sáb 19 sep 2009 17:07:18 EDT	2m 39s	USED	Cautivame Nodo 1	192.168.3.132	1,7M	314,4K
sáb 19 sep 2009 14:43:47 EDT	53m 5s	USED	Cautivame Nodo 1	192.168.3.132	7M	5,4M
sáb 19 sep 2009 11:59:34 EDT	35s	USED	Cautivame Nodo 1	192.168.3.132	431,7K	391,2K
sáb 19 sep 2009 11:32:51 EDT	3m 35s	USED	Cautivame Nodo 1	192.168.3.132	1M	338,6K
vie 18 sep 2009 00:13:47 EDT	4m 15s	USED	Cautivame Nodo 1	192.168.3.132	4M	310,5K
jue 17 sep 2009 23:58:50 EDT	14m 57s	USED	Cautivame Nodo 1	192.168.3.132	5,4M	1,2M
Total:	**1h 19m 6s**				**19,7M**	**7,9M**

1 direcciones MAC

MAC	Contado
00:17:C4:26:0F:FE	6

Ilustración 5-98 Estadísticas del usuario "prueba"

La opción de generar estadísticas manualmente, es mucho más funcional que la anteriormente descrita, ya que con ella se puede obtener información que puede ser de utilidad para los administradores o propietarios de la red. A continuación se muestra las estadísticas más importantes.

- 10 usuarios más frecuentes

10 usuarios mas frecuentes

Usuario (usuario)	Dias diferentes conectados
prueba	3
admin	3
katya	2
nicky	1
nikita	1

Ilustración 5-99 Estadísticas de los 10 usuarios más frecuentes en la red

- Promedio de visitas por día.

Estadisticas

Promedio de visitas por dia:	2.46 (por el periodo seleccionado)
Trafico:	Entrante: 126,6M Saliente: 26M (por el periodo seleccionado)

Ilustración 5-100 Estadísticas del promedio de visitas por día.

- Log de Registro (Primera conexión de usuarios nuevos)

Log de Registro (Primera conexión de usuarios nuevos)

Usuarios que se inscribierón aqui

Nodo	Usuario	Fecha de Registro
Cautivame Nodo 1	nicky	sáb 19 sep 2009 12:30:24 EDT
Cautivame Nodo 1	nikita	sáb 19 sep 2009 12:25:28 EDT
Cautivame Nodo 1	katya	sáb 19 sep 2009 11:15:07 EDT
Cautivame Nodo 1	prueba	jue 17 sep 2009 23:58:50 EDT
Cautivame Nodo 1	admin	jue 17 sep 2009 23:31:22 EDT
Total:	**5**	

Ilustración 5-101 Registro de creación de nuevas cuentas.

- Log de conexiones

Log de conexiones

Numero de usuarios unicos:5

Usuario	Acumolado de MAC	Acumulado e Cx	Ultima Vez visto
admin	2	11	2009-09-21 17:48:20
nicky	1	10	2009-09-19 13:54:42
prueba	1	6	2009-09-19 17:07:18
katya	1	4	2009-09-21 17:48:34
nikita	1	2	2009-09-19 12:27:50

Ilustración 5-102 Estadísticas del total de las conexiones, en donde se puede ver la dirección MAC del equipo del cliente.

- Los 10 más altos consumidores de banda ancha.

Los 10 mas altos consumidores de banda ancha

Usuario (usuario)	Entrante	Saliente	Total
admin	49,7M	9,1M	58,8M
katya	44,1M	7,5M	51,7M
prueba	19,7M	7,9M	27,6M
nicky	12,3M	1,3M	13,6M
nikita	742,5K	274,3K	1016,8K

Ilustración 5-103 Estadísticas de los usuarios que consumen más ancho de banda. Se puede observar la cantidad de bytes enviados y recibidos.

Como se puede observar en las figuras anteriores, Wifidog provee de herramientas poderosas para controlar la red inalámbrica con seguridad y definir las políticas de uso de la red para los usuarios.

CAPITULO VI

6. ANÁLISIS DE FACTIBILIDAD DEL PROYECTO DE UN ENRUTADOR INALÁMBRICO EMBEBIDO Y UN SERVIDOR DE AUTENTIFICACIÓN COMPARTIDO.

En el capítulo 1.4, se nombra al Servidor de Autentificación como “Universal” o “General”, refiriéndose a la forma de trabajar de este servidor. Uno de los inconvenientes para implementar un Portal Cautivo, es el costo de instalación y de los componentes de hardware, debido a que es necesario un equipo con capacidades altas de procesamiento, memoria y almacenamiento para implementar el Sistema Operativo Ubuntu, en donde estén almacenadas las utilidades necesarias para la comunicación con los enrutadores inalámbricos y el software de portal cautivo. Los desarrolladores de Wifidog hasta la fecha no han logrado portar correctamente el servidor de base de datos relacionadas PostgreSQL, el cual es necesario para instalar el servidor de autentificación de Wifidog; debido a esto, no es posible instalarlo en el enrutador inalámbrico, por lo tanto se necesita un servidor extra.

El costo de implementación de un servidor de autentificación es relativamente alto, debido a que se requiere tener un equipo con capacidades para instalar un sistema operativo de servidor como Ubuntu, y el costo que implica contratar a un profesional en el área de sistemas,

La solución a esta problemática, es la implementación de un único Servidor de Autentificación Wifidog, con todas las herramientas de red necesarias, al cual los enrutadores inalámbricos tengan acceso dirigiéndose a una IP publica. Esto permite ahorrar costos al administrador de la red o al propietario que corresponden a la contratación de un profesional de sistemas para que configure el servidor de autentificación y el costo del equipo servidor.

Si una organización adquiere el servicio de portal cautivo embebido, se le entrega el enrutador inalámbrico con las modificaciones de hardware y software necesarios, y configurados para enlazarse directamente con el servidor de autentificación Wifidog.

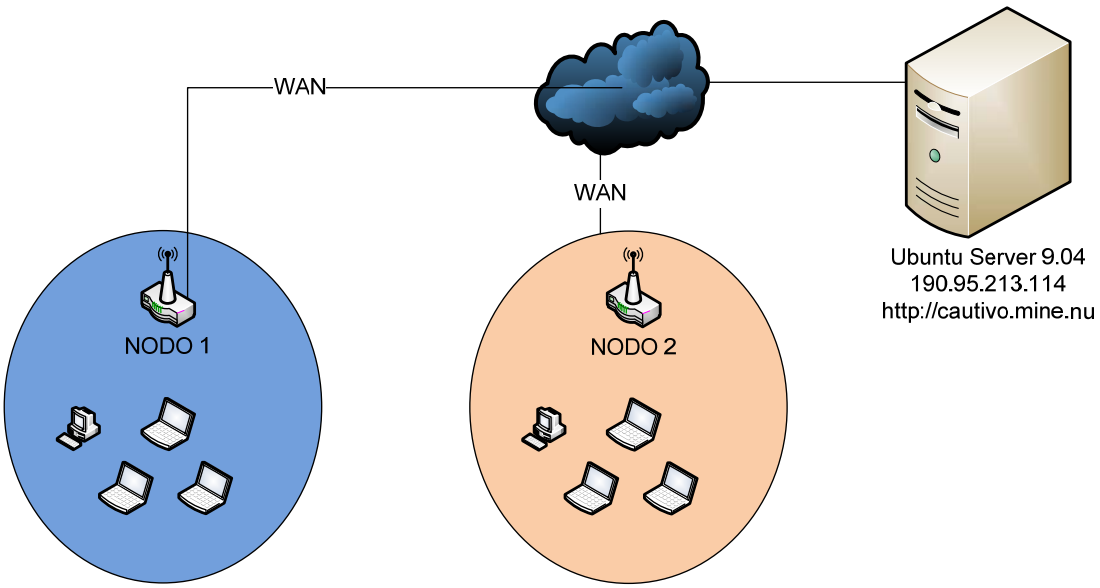


Ilustración 6-1 Diseño de la red de internet para los nodos externos que podrían utilizar los servicios de Portal Cautivo

En la figura anterior, la configuración de la red está diseñada para aceptar conexiones externas para que el servidor de autentificación de portal cautivo Wifidog maneje otros nodos además de los internos.

6.1. ANÁLISIS DE LAS CARACTERÍSTICAS TÉCNICAS DEL ENRUTADOR INALÁMBRICO WRT54GL MODIFICADO

Cuando un enrutador LinkSys WRT54G es adquirido, las funcionalidades de fábrica van de acuerdo a su costo, y son útiles para la mayoría de los que utilizan estos equipos en sus casas u oficinas como un enrutador inalámbrico que provea internet y comunicación LAN. Sin embargo, una vez que el enrutador ha sido modificado en hardware y software provee de nuevas herramientas de software y de medios de almacenamiento extra, cambiando por completo el objetivo por el cual fue creado.

Tabla 6-1 Algunas de las nuevas funcionalidades del enrutador inalámbrico WRT54GL frente a las originales.

EQUIPO	**VLAN**	**SSH**	**WIFIDOG**	**FIREWALL**	**SAMBA**	**ALMACENAMIENTO**	**INSTALA NUEVO SOFTWARE**
Modificado	SI	SI	SI	SI	SI	2GB	SI
Sin Modificar	SI	NO	NO	SI	NO	4MB	NO

En la tabla anterior, la mejora del equipo modificado es notable frente a su configuración original. Cabe mencionar que para este proyecto no se aplicaron todas las mejoras de hardware y software que pueden implementarse en el enrutador inalámbrico, quedando pendiente servicios como: Asterisk, Apache, Php, MySQL, LDAP y modificaciones de hardware como: Modem GSM.

Con todas las mejoras mencionadas anteriormente, se podría decir que el enrutador inalámbrico WRT54GL se ha convertido en un completo servidor de red, que provee de las herramientas necesarias para la administración y manejo de una red LAN.

6.2. ANÁLISIS DEL COSTO DE LA IMPLEMENTACIÓN DE PORTAL CAUTIVO EMBEBIDO Y SERVIDOR DE AUTENTIFICACIÓN.

En el desarrollo de este proyecto se ha mencionado las veces que se ha utilizado algún material o accesorio de hardware para la modificación del enrutador inalámbrico. El costo de modificación del enrutador inalámbrico LinkSys WRT54G está sin duda muy debajo en relación al aporte de servicios y capacidades que brinda una vez modificado. Sin embargo el tiempo empleado para el estudio, la modificación de las partes y las pruebas realizadas supera en gran medida al costo.

A continuación se agruparan todos los gastos de fabricación y de mantenimiento del enrutador inalámbrico.

Tabla 6-2 Costos de materiales y servicios necesarios para la modificación de Hardware y Software del LinkSys WRT54GL

Material o Servicio	**Descripción o Función.**	**Costo**
Enrutador Inalámbrico LinkSys WRT54GL	Enrutador inalámbrico.	69.99 $
Tarjeta SD 2GB	Conectada al equipo por medio de los puertos GPIO para proveer de almacenamiento extra.	11.00 $
Cable LPT Paralelo	Parte esencial del cable JTAG utilizado para formatear la memoria NVRAM.	5.00 $
Resistencias 100 Ohm	Utilizadas para la fabricación del cable JTAG.	1.00 $
Cable IDE.	Utilizado para soldar la memoria SD al enrutador.	3.00 $
		Total: 89,99 $

Para el diseño y la implementación de este proyecto se han consumido alrededor de 100 horas, si se establece un valor a la hora de trabajo equivaldría a 20 dólares, el costo de fabricación del enrutador es la suma del costo de modificación mas el tiempo utilizado.

Tabla 6-3 Costo total del proyecto de modificación del enrutador inalámbrico Wrt54GL

Costo de modificación	89.99 $
Costo del tiempo utilizado.	2000 $
Costo total de modificación.	2089,99 $ Dólares

El tiempo que se refiere la tabla anterior, fue el requerido para la investigación y modificación del enrutador inalámbrico Wrt54G, sin embargo, una vez finalizada la investigación y habiendo obtenido todos los conocimientos, experiencia y herramientas para dicho trabajo, se ha reducido el tiempo total a 5 horas.

Para obtener rentabilidad de este servicio, sería necesario vender el enrutador inalámbrico LinkSys WRT54G modificado en 2089,99 dólares cada uno, sin embargo esto desorientaría el objetivo de este proyecto; el cual, está concebido para ofrecer una herramienta poderosa a un bajo precio. Es por esto que la solución para obtener rentabilidad sin que afecte al costo general, es la distribución masiva de enrutadores inalámbricos embebidos, con capacidad de conectarse al servidor de autentificación.

La siguiente tabla muestra los posibles clientes del enrutador inalámbrico embebido con conexión al Servidor de Autentificación.

Tabla 6-4 Mercado Objetivo para la difusión y venta del enrutador modificado y la conexión al servidor de autentificación[89]

Razón Social	**Cantidad de establecimientos**
Cafeterías	80
Restaurantes	512
Hoteles	63
Centros Comerciales de gran concurrencia.	7
Centros de Educación Superior	124
Instituciones Educativas de educación media.	134
Total	920

89 Fuente: Cámara de Comercio de Quito
Consejo Nacional de Educación Superior (CONESUP)

Se ha tomado como referencia para el mercado objetivo, organizaciones, establecimientos o lugares públicos en donde generalmente se provee internet inalámbrico gratuito. Es común encontrar en estos lugares puntos de acceso inalámbrico sin autentificación[90], o con clave de red compartida, utilizando un punto de acceso inalámbrico conectado al proveedor de internet. Si se toma como referencia un porcentaje del total de posibles clientes obtendríamos lo siguiente:

Tabla 6-5 Porcentaje mínimo de posibles clientes.

Posibles Clientes	**Porcentaje**	**Total.**
920	10%	92 Clientes.

Se ha tomado como referencia el 10% del total de establecimientos, lo que genera a 92 posibles clientes. En la tabla 6.2 se obtiene el costo total de inversión de hardware para la modificación del enrutador inalámbrico que es de 89,99 $.

Tabla 6-6 Costo mínimo de un enrutador inalámbrico modificado y el funcionamiento de el servidor de autentificación por un año

Costo en hardware de la modificación del enrutador inalámbrico WRT54GL.	89,99 $
Pago Anual de internet para el Servidor de Autentificación.	672.00 $
Total.	761,99

Entonces se obtiene un requerimiento mínimo de 761,99 dólares para implementar un enrutador inalámbrico embebido con OPENWRT y un Servidor de Autentificación conectado a internet con una IP publica por un año para un solo cliente.

90 Metro Café Quito, Coffee Tree Quito, Crepes and Waffles Quito, Hotel Colón.

Tabla 6-7 Calculo de ingreso bruto para la instalación de un enrutador embebido y un servidor de autentificación para cada cliente.

Posibles Clientes	**Costo mínimo del proyecto**	**Ingreso Bruto.**
96	761,99	73151,04 $ Dólares.

Si el 10% del total de posibles clientes es 96, y tomando como hipótesis que todos adquirieran los servicios de un enrutador inalámbrico embebido conectado a un servidor de autentificación, el costo total de inversión decrecería en gran medida, debido a que la sumatoria de todos esos posibles clientes, que pagarían el costo mínimo anual aumentaría en un gran porcentaje a la utilidad del proyecto. Esto permite que se pueda reducir el costo total del proyecto, para que cubra en su totalidad la inversión en horas de investigación, costo de hardware y otros servicios requeridos por un año a 300$ Dólares si se penetra en el mercado objetivo vendiendo el enrutador en mediana escala.

Tabla 6-8 Calculo estimado de ventas de 10% del total de clientes objetivos por un año

Posibles Clientes	**Costo de Servicio a cada Cliente (Anual)**	**Ingreso Bruto**
96	300$ Dólares.	28800 $ Dólares

Después de haber transcurrido el año de servicio con el Servidor de Autentificación WifiDog, los propietarios de los equipos embebidos, pueden optar por renovar la licencia, para lo cual deberán pagar la suma de 105,01 Dólares, que es el equivalente a la resta del costo de fabricación del equipo menos el costo 65% total del servicio.

Tabla 6-9 Costo de renovación de licencias

Costo del equipo modificado	**65% del costo total del servicio**	**Costo de renovación**
89,99 $	105,01 $	110,01 $

En el mercado existen equipos de enrutamiento de altas capacidades de procesamiento, sin embargo no ofrecen los servicios que el enrutador inalámbrico LinkSys WRT54GL modificado puede ofrecer. Algunos de los equipos no cuentan con servicio de red

inalámbrica integrada, por lo que para su funcionamiento se requiere un Access Point externo.

Tabla 6-10 Equipos de enrutamiento de altas prestaciones, algunos no llevan WLAN[91]

Marca y Modelo	**Precio**
Readylink Wireless Access Point 2.4/5ghz 802.11a+b+g – Isp	1160.00$
Engenius Senao De 600 W Con Antena De 32 Dbi	300$
Cisco 1750 48 Dram 8 Flash Ccna Ccnp Voz, (Sin WLAN)	415$
Cisco 1751v 96 Dram 32 Flash Ccna Ccnp Ccvp Central De Voz (Sin WLAN)	505$

Se puede realizar el cálculo de rentabilidad del proyecto tomando los valores del costo de la modificación, el número de posibles clientes en el mercado objetivo y el costo de investigación, para este cálculo se utilizan todos los factores de inversión posibles, y se toma en cuenta la contratación de un empleado al cual se le da todos los beneficios de ley.

Tabla 6-11 Cálculo de la rentabilidad estimada anual

Factor de Inversión Anual	**Cantidad**	**V. Unitario**	**V. Total**
Inversión e investigación	100 horas	20,00	2.000,00
Conexión de internet anual. (56$ mensuales)	12 meses	56,00	672,00
Costo de servicios (Luz, teléfono)	12 meses	25,00	300,00
Costo de administrador del servicio (225 x 14)	14	300,00	4.200,00
Costos totales de servicios			**7172,00**
Imprevistos (10%)			717,20
Costo hardware (96 equipos)	96	89,90	8.630,40
Costo total (servicios + fabricación)			**16519,60**
INGRESOS BRUTOS	**96**	**300,00**	**28800,00**
UTILIDAD BRUTA (Ingresos brutos - costo total)			**12281,00**

91 Fuente: mercadolibre.com.ec

Como se puede evidenciar en la tabla 6-11, la Utilidad anual frente a la inversión necesaria para la venta de los equipos y del servicio, es muy superior.

La siguiente tabla representa un flujo de caja estimado de demostración entre los meses Junio 2009 y Mayo 2010, para poder analizar la factibilidad del proyecto frente a los costos de fabricación y operación.

Tabla 6-12 Flujo de caja estimado anual.

	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo
Fuentes de efectivo												
Ventas de equipos	0	1	3	5	8	9	5	4	8	13	14	10
Fuentes totales de efectivo	0	300	900	1500	2400	2700	1500	1200	2400	3900	4200	3000
Usos del Efectivo												
Compras de hardware	0,00	89,90	269,70	449,50	719,20	809,10	449,50	359,60	719,20	1168,70	1258,60	899,00
Gastos generales y Operativos												
Sueldo del empleado	300,00	300,00	300,00	300,00	300,00	300,00	300,00	300,00	300,00	300,00	300,00	300,00
Servicios												
Luz y Teléfono	23,00	25,00	22,00	25,00	25,00	25,00	25,00	25,00	25,00	25,00	25,00	25,00
Internet	56,00	56,00	56,00	56,00	56,00	56,00	56,00	56,00	56,00	56,00	56,00	56,00
Otros	21,00	14,00	21,00	12,00	12,00	12,00	12,00	12,00	12,00	12,00	12,00	12,00
Usos Totales del Efectivo	400,00	484,90	668,70	842,50	1112,20	1202,10	842,50	752,60	1112,20	1561,70	1651,60	1292,00
Saldos Finales de Efectivo (Superávit, Déficit)	**-400,00**	**-184,90**	**231,30**	**657,50**	**1287,80**	**1497,90**	**657,50**	**447,40**	**1287,80**	**2338,30**	**2548,40**	**1708,00**

En la tabla 6-12 del cálculo de flujo de caja estimado de los meses junio 2009 y mayo 2010, se toma un valor de 300 dólares mensuales para el pago de un empleado, por lo que los superávit pueden ser utilizados para capital.

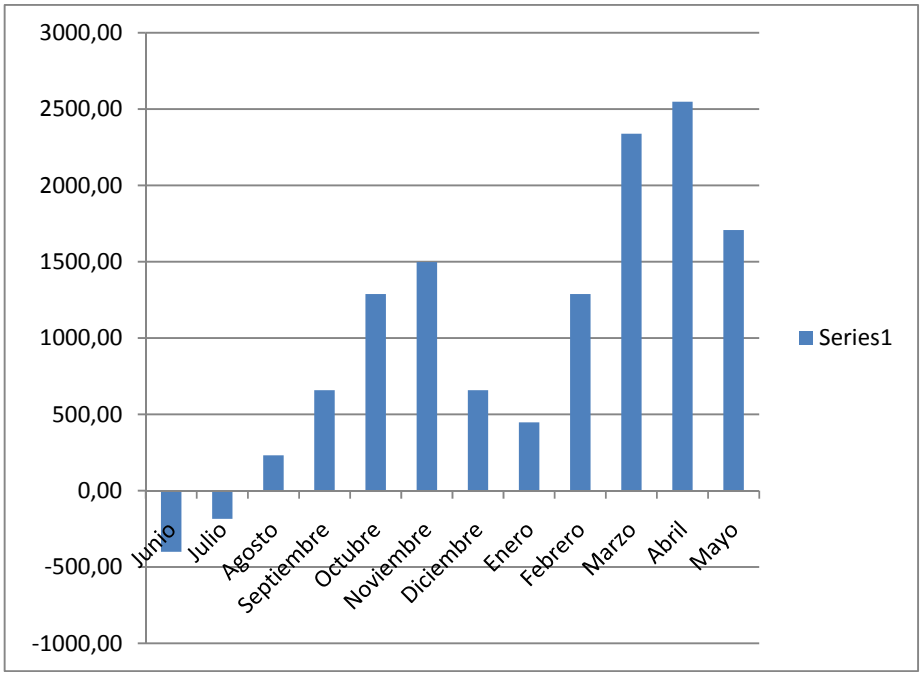


Ilustración 6-2 Diagrama de Flujo de Caja Anual

En la ilustración 6-2 se puede observar gráficamente y con más detalle el flujo de caja anual.

CAPITULO VII

7. CONCLUSIONES Y RECOMENDACIONES

7.1.CONCLUSIONES.

- Después de las pruebas se observó que el enrutador inalámbrico LinkSys WRT54GL es el mejor equipo para la modificación de Hardware y la implementación de firmware de terceros, debido a su capacidad de ampliación de memoria, puertos seriales y JTAG.
- A pesar de existir otro firmware de terceros para los enrutadores inalámbricos WRT54G, OPENWRT 8.04 Kamikaze es la herramienta que se adapta mejor a la modificación de estos equipos, debido a que cuenta con más portaciones de software y una comunidad de usuarios, foros de discusión y blogs
- La instalación por medio de la interfaz web es el método más fácil y seguro para instalar OpenWrt, debido a que solamente es necesario subir la imagen del firmware por medio del navegador web.
- Se pueden implementar herramientas más sofisticadas de administración de red en el enrutador, como por ejemplo IPTRAF, Dansguardian, SQUID, para acrecentar la potencia del equipo y dar mayores prestaciones.
- La versión más reciente del firmware de terceros OpenWrt, está compilada con una de las últimas versiones del Kernel de Linux, sin embargo esta versión tiene dificultades con los controladores para la interfaz WLAN.
- Wifidog es la mejor herramienta para portales cautivos de software libre, sin embargo, tiene deficiencia en el manejo de usuarios y su interfaz todavía no está bien traducida al español.
- Uno de los principales inconvenientes de Wifidog es su integración con PostgreSQL, debido a que no es compatible con OpenWrt y exige la instalación de otro servidor.
- En caso de que la carga del firmware sea defectuosa, es posible restaurar el equipo a su configuración original mediante el cable JTAG.
- La venta del servicio de un enrutador inalámbrico modificado, con funciones de servidor y con una memoria de 2GB, conectado por internet a un Servidor de Autentificación por 1 año tiene una rentabilidad estimada de 4088,96 $ Dólares.

7.2. RECOMENDACIONES

- Se recomienda la implementación de Portales Cautivos en la Universidad Internacional SEK, ya que cualquier persona, ya sea estudiante o no de la universidad puede conectarse a la red inalámbrica para acceder a información privada o causar daños.
- Todos los modelos del WRT54G tienen la misma forma y diseño de su carcasa por lo que es fácil de confundirse de modelo, se recomienda siempre revisar el número de serie y consultarlo en internet antes de adquirirlo.
- Es posible modificar la velocidad del procesador del WRT54GL hasta los 250Mhz pero no es recomendable debido a que produce un recalentamiento del dispositivo.
- Los enrutadores inalámbricos modificados WRT54GL podrían ser utilizados como servidores en zonas rurales, y áreas marginales, en donde no se tienen las capacidades económicas para adquirir un servidor y armar una topología de red, por ejemplo escuelas y colegios.
- LinkSys ha publicado recientemente el enrutador inalámbrico 802.11n WRT160n, el cual tiene las mismas prestaciones que el WRT54GL y en los últimos días los desarrolladores de OpenWrt han logrado portar el sistema operativo a la nueva arquitectura de procesador. Por lo que se recomienda su estudio para nuevos proyectos.
- No se recomienda la implementación de una interfaz grafica para el sistema operativo Ubuntu Server, debido a que consume demasiados recursos innecesarios.
- Es recomendable hacer copia de seguridad de la base de datos PostgreSQL que administra el Servidor de Autentificación Wifidog utilizando la herramienta web “PhpPgMyadmin”.
- La compra de los enrutadores inalámbricos es más barata en internet, debido a los impuestos que recaen sobre los equipos.
- En Brasil existe un proyecto ecológico para el equipo WRT54GL el cual es implementado en zonas rurales para ofrecer conectividad, el equipo es alimentado por paneles solares y utiliza baterías de celular para dar corriente en las noches o días nublados. Este proyecto podría ser tomado para la estación científica de Limoncocha.

CAPITULO VIII

BIBLIOGRAFÍA

Asadoorian Paul LinkSys WRT54G Ultimate Hacking. [Libro]. - United States of America : SYNGRESS, 2007.

BookSprint Redes Inalámbricas en los Paises en Desarrollo [Libro]. - Londres : 2007, Limehouse Book Sprint Team , 2007.

Cisco Systems CCENT/CCNA ICND1 [Libro]. - Indianapolis, Indiana 46240 USA : Cisco Press, 2008.

Comptia Secure Certification + [Libro]. - United States of America : Microsoft Press, 2004.

IEEE IEEE 802.11 Handbook A Designer´s Companion [Libro]. - [s.l.] : IEEE Press, 2004.

Joseph Davies. Microsoft Corparation Deploying SECURE 802.11 Wireless Networks with Microsoft Windows. [Libro]. - Redmond, Washington : Microsoft Press, 2004.

Miller, Stewart S. Seguridad en WiFi [Libro]. - España : Mc Graw-Hill, 2003.

Russell Joe Grand - Ryan HARDWARE HACKING - Have Fun While Voiding Your Warranty [Libro]. - Rockland, MA 02370 : Syngress Publishing, Inc., 2004.

Schroder Carla Curso de Linux [Libro]. - España : ANAYA, 2005.

VLADIMIROV ANDREW A. Hacking Wireless Seguridad de Redes Inalambricas [Libro]. - Madrid : ANAYA, 2004.

Wikipedia Wikipedia en español [En línea]. - 2009. - es.wikipedia.org.

CAPITULO IX

GLOSARIO DE TÉRMINOS

Aberdeen Group: Organización dedicada a la investigación y análisis de productos y compañías dedicadas al mercado de Tecnologías de la Información (IT)

AP (Access Point): Punto de Acceso inalámbrico a una red WLAN.

CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, es un protocolo de encriptación desarrollado por IEEE.

CSMA / CA: Carrier Sense, Multiple Access, Collision Avoidance (acceso múltiple por detección de portadora con evasión de colisiones) es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos

DHCP: (Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Servidor) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

GPL: La Licencia Pública General (GPL) es una licencia creada por la Free Software Foundation a mediados de los 80, y está orientada principalmente a proteger la libre distribución, modificación y uso de software.

Hacker: Los términos hacker y hack tienen significados positivos y también negativos. Se suelen usar los términos hacking y hacker para expresar admiración por el trabajo de un desarrollador de software calificado, o de una modificación o mejora de un hardware, pero también se puede utilizar en un sentido negativo para describir una solución rápida pero poco elegante a un problema. Algunos desaprueban el uso del hacking como un sinónimo de cracker, en marcado contraste con el resto del mundo, en el que la palabra hacker se

utiliza normalmente para describir a alguien que "hackea" un sistema con el fin de eludir o desactivar las medidas de seguridad.

Hotspot*:* Los Hotspots son los lugares que ofrecen acceso Wifi, que pueden ser aprovechados especialmente por dispositivos móviles.

IDC: *International Data Corporation*. Compañía que se dedica a investigar sobre las nuevas tendencias del mercado de tecnología.

Kernel: En computación el Kernel es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora

LED: Light-Emitting Diode es un dispositivo semiconductor (diodo) que emite luz incoherente de espectro reducido cuando se polariza de forma directa la unión del diodo en forma Positiva-negativa.

MAC: Media Access Control o control de acceso al medio (MAC) es un identificador de 48 bits que corresponde de forma interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE

PDA: Personal Digital Assistant (Asistente Digital Personal), es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

PoE: Es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como,

por ejemplo, un teléfono IP o una cámara de red, usando el mismo cable que se utiliza para una conexión de red.

Portabilidad: La portabilidad es uno de los conceptos clave en la programación de alto nivel. Se define como la característica que posee un software para ejecutarse en diferentes plataformas, el código fuente del software es capaz de reutilizarse en vez de crearse un nuevo código cuando el software pasa de una plataforma a otra. A mayor portabilidad menor es la dependencia del software con respecto a la plataforma.

Reset: Se conoce como reset (reiniciar) a la puesta en condiciones iniciales de un sistema. Este puede ser mecánico, electrónico o de otro tipo.

RFC: Request For Comments (Petición De Comentarios) son una serie de notas sobre Internet que comenzaron a publicarse en 1969[1]. Se abrevian como RFC. Cada una es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET).

Software Libre: Es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente

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

UNIX: Unix es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T

Wardriving: Se llama wardriving a la búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un coche o camioneta y una computadora equipada con Wifi.

WLAN: (Wireless Local Area Network) es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas.

XFREE86: XFree86 provee una interfaz gráfica cliente/servidor entre el hardware (sistemas gráficos y dispositivos de entrada, como el mouse o el teclado) y un entorno de escritorio que provee un sistema de ventanas así como una interfaz estandarizada de aplicación (API por sus siglas en inglés).

CAPITULO X

ANEXOS

ANEXO 1

INSTALACIÓN DE UBUNTU SERVER 9.04 CON HERRAMIENTAS LAMP

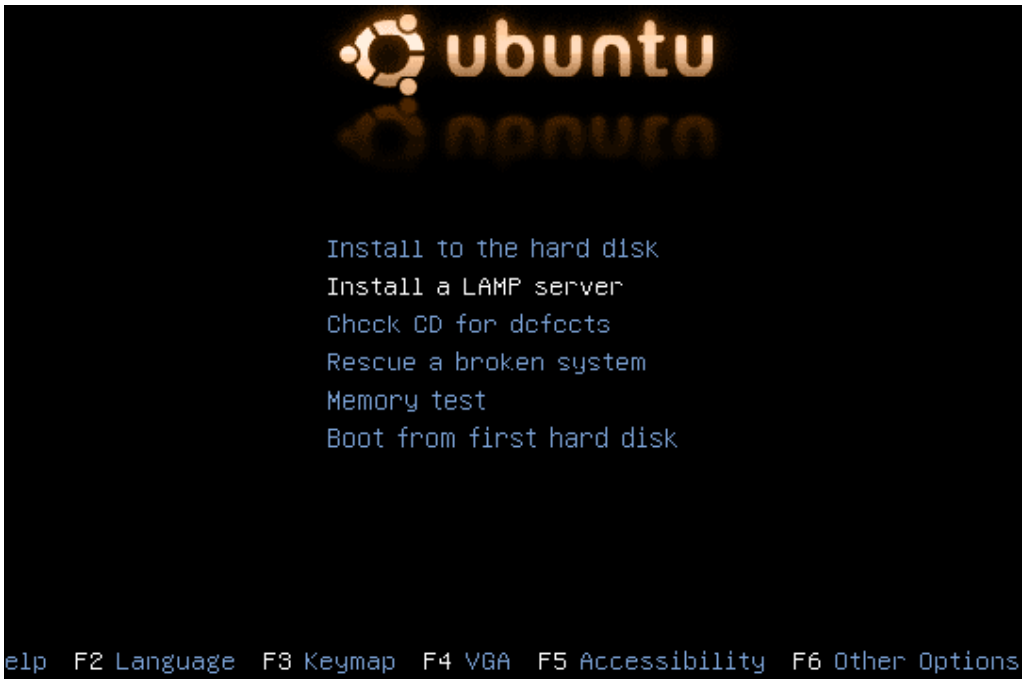
Instalación de Ubuntu Server 9.04.
Fuente: http://www.debianadmin.com/ubuntu-lamp-server-installation-with-screenshots.html

La opción de LAMP ahorra el trabajo de instalación y la integración de cada uno de los cuatro componentes de carcasas diferentes, un proceso que puede llevar horas y requiere de alguien que es experto en la instalación y configuración de las aplicaciones individuales. Usted obtiene una mayor seguridad, menor tiempo de instalación, y un menor riesgo de una mala configuración, todo lo cual resulta en un menor costo de propiedad.

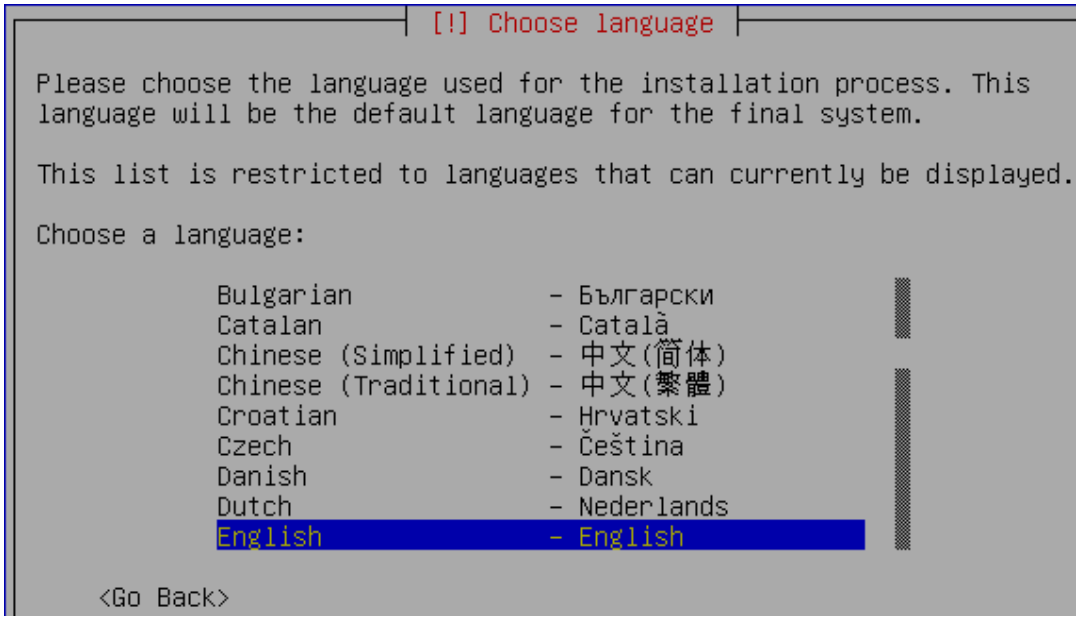
Ubuntu LAMP servidor de instalar las versiones siguientes

Linux
Apache2
MySQL5
PHP5

Primero se necesita descargar una versión de Ubuntu. Después de que se crea un CD y arrancar con el CD de inicio Una vez que se arranca debería ver la siguiente pantalla en el presente es necesario seleccionar la segunda opción "Instalar una opción de servidor LAMP" y, presione ENTRAR

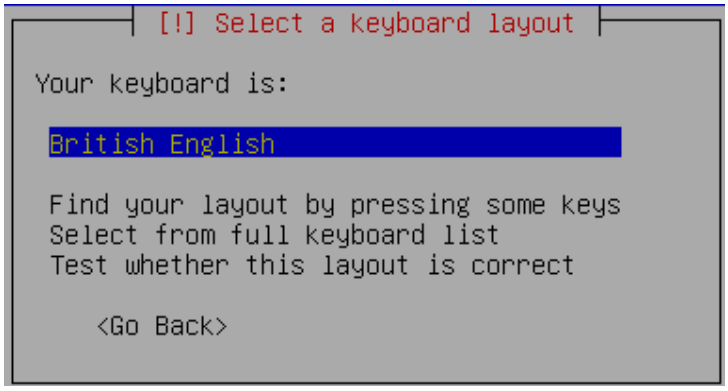


Selecciona el idioma y pulse enter usted puede ver que hemos seleccionado Inglés en la pantalla de following

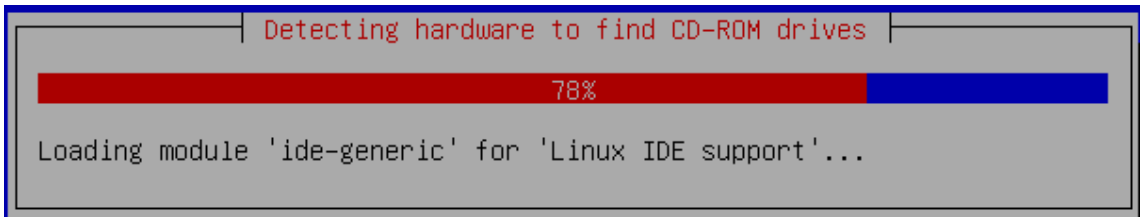


Elija su ubicación y pulse Intro se puede ver que hemos seleccionado del Reino Unido en la pantalla following

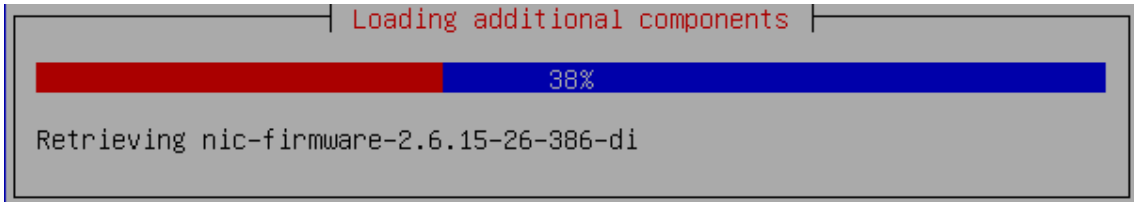
Seleccionar y distribución de teclado, presione ENTRAR



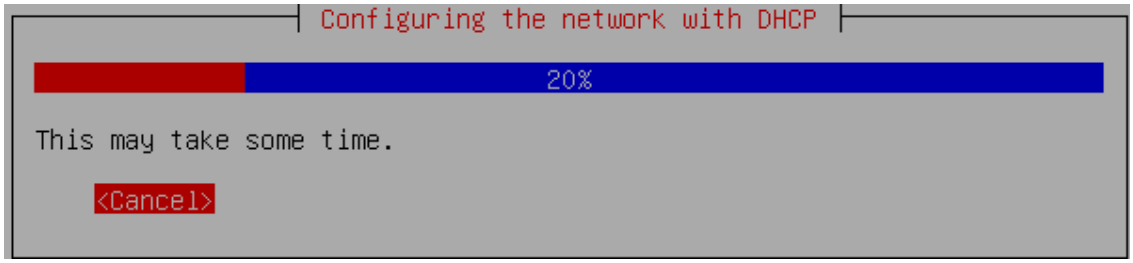
Detección de hardware para encontrar controladores de CD-ROM en el progreso



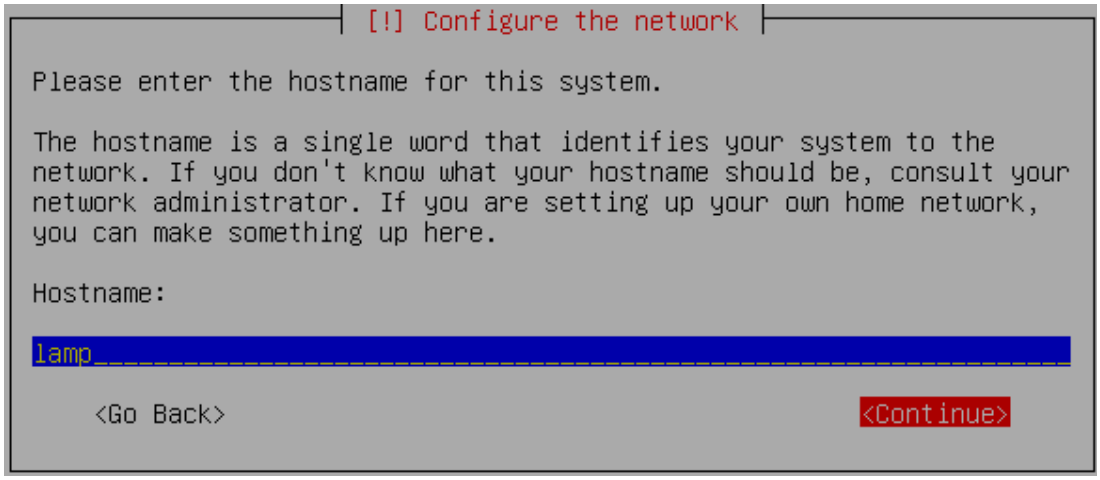
Cargar componentes adicionales de la barra de progreso



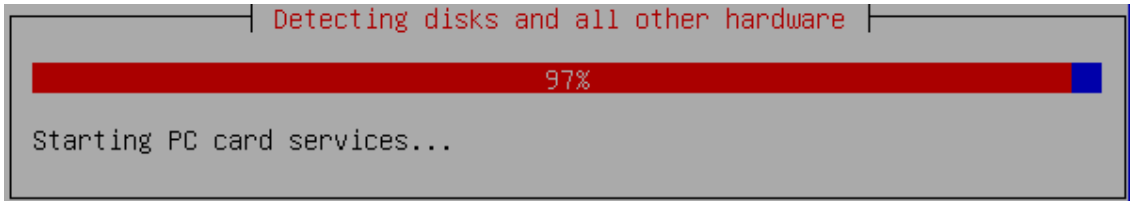
Configura la red con DHCP si hay un servidor DHCP en la red



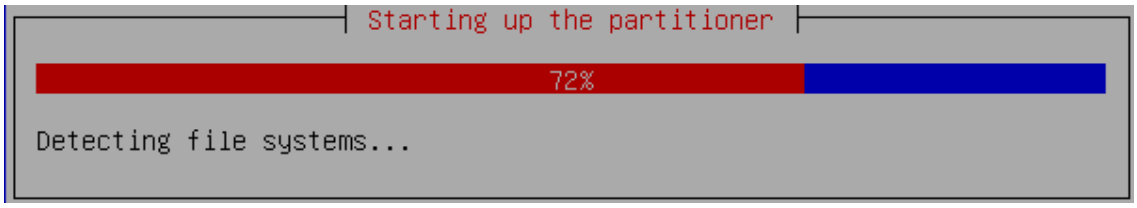
Introduzca el nombre de host del sistema de modo que en este ejemplo que entrar aquí como la lámpara



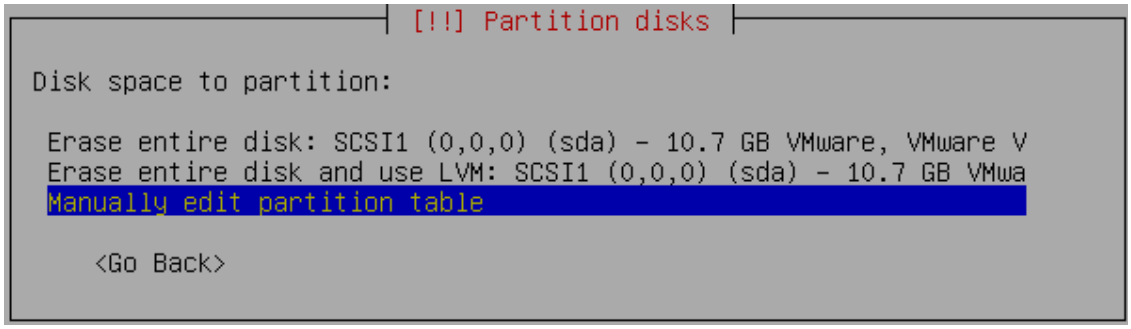
La detección de los discos y hardware en el progreso

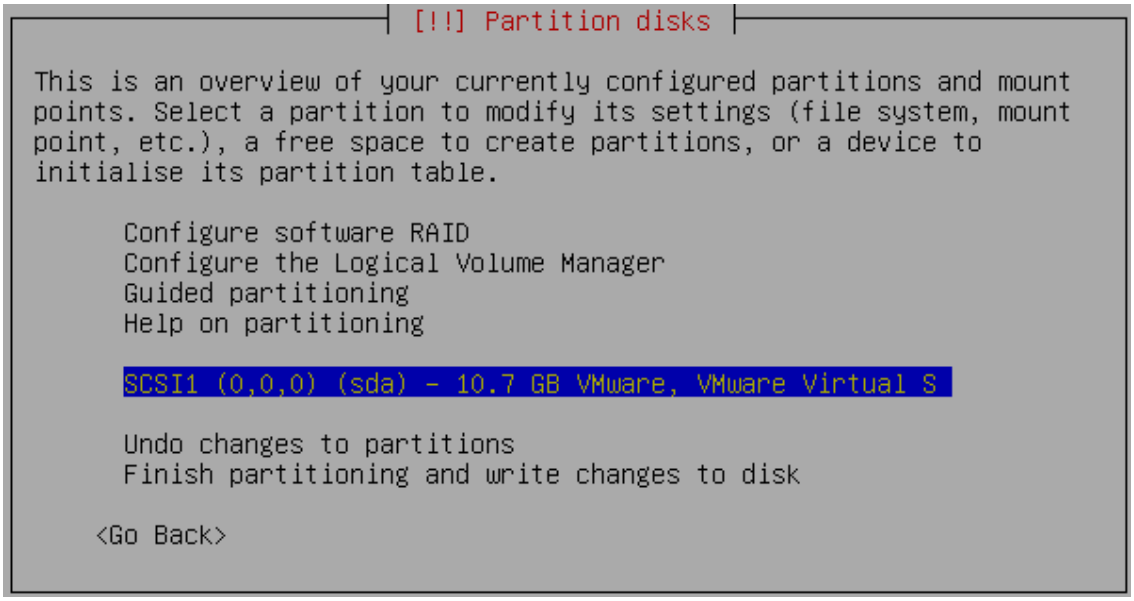


Iniciando el particionado en curso

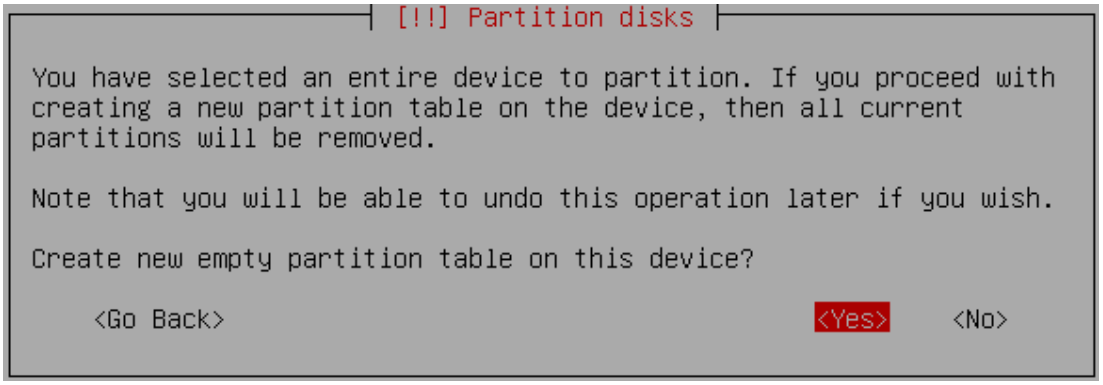


Usted tiene que particionar su disco duro en el que he seleccionado manualmente editar la tabla de partición y presione ENTRAR

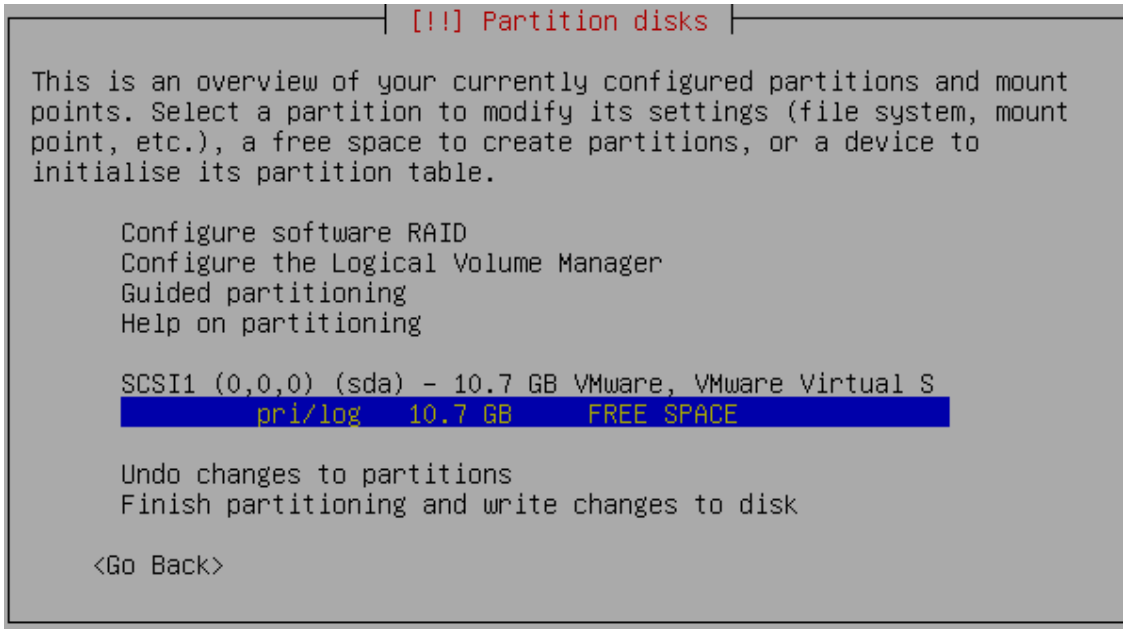




Crear una nueva tabla de particiones en el dispositivo, seleccione Sí y pulse Enter

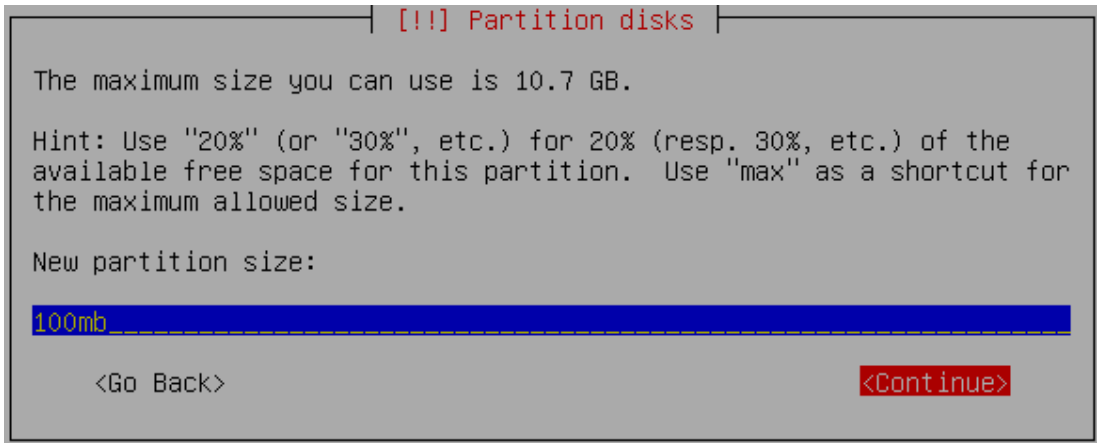


Ahora usted puede ver el espacio libre y pulse Enter

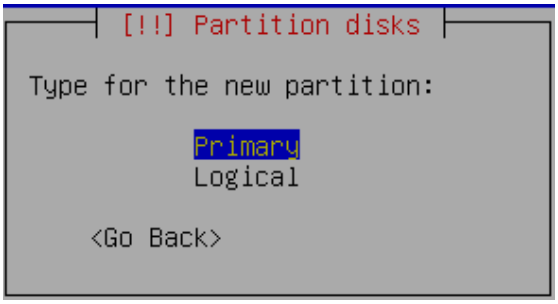


Cómo usar este espacio libre, seleccione Crear una nueva partición y presione ENTRAR

Introduzca el tamaño partition y pulse continuar he entrado 100mb en este ejemplo

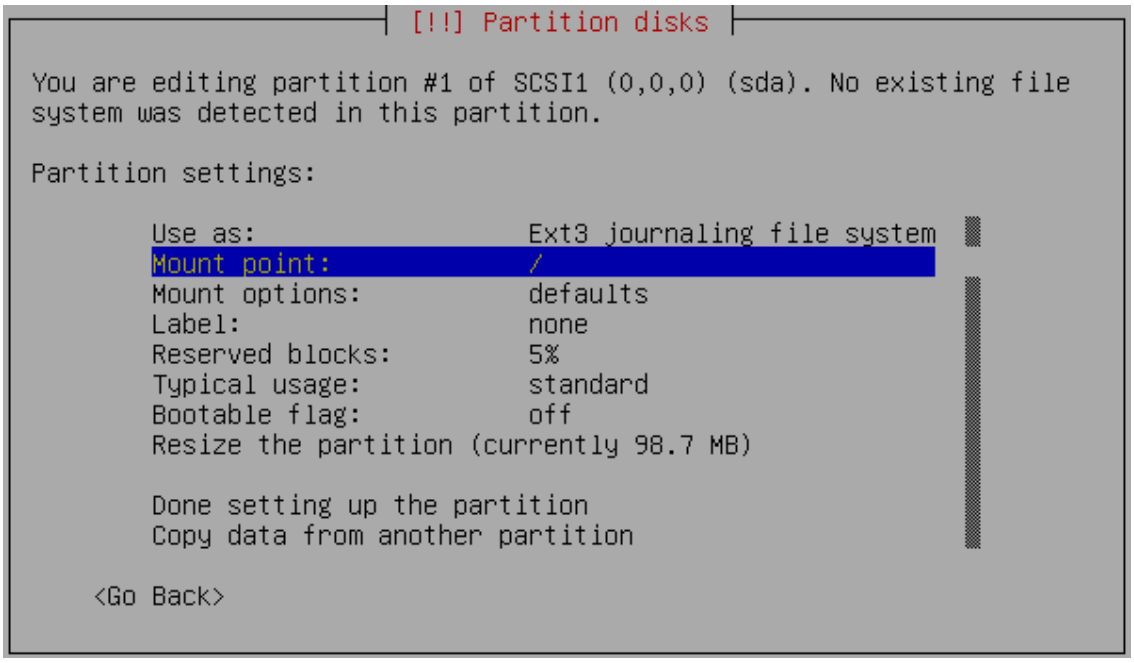


Seleccione el tipo de la partición y presione ENTRAR en este ejemplo que ha seleccionado primaria

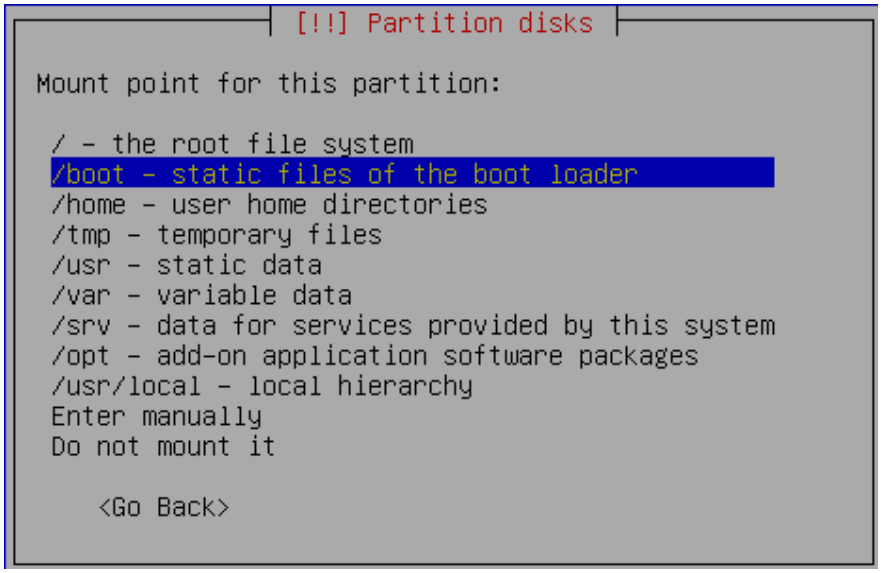


Ubicación para la nueva partición como principio y presione ENTRAR

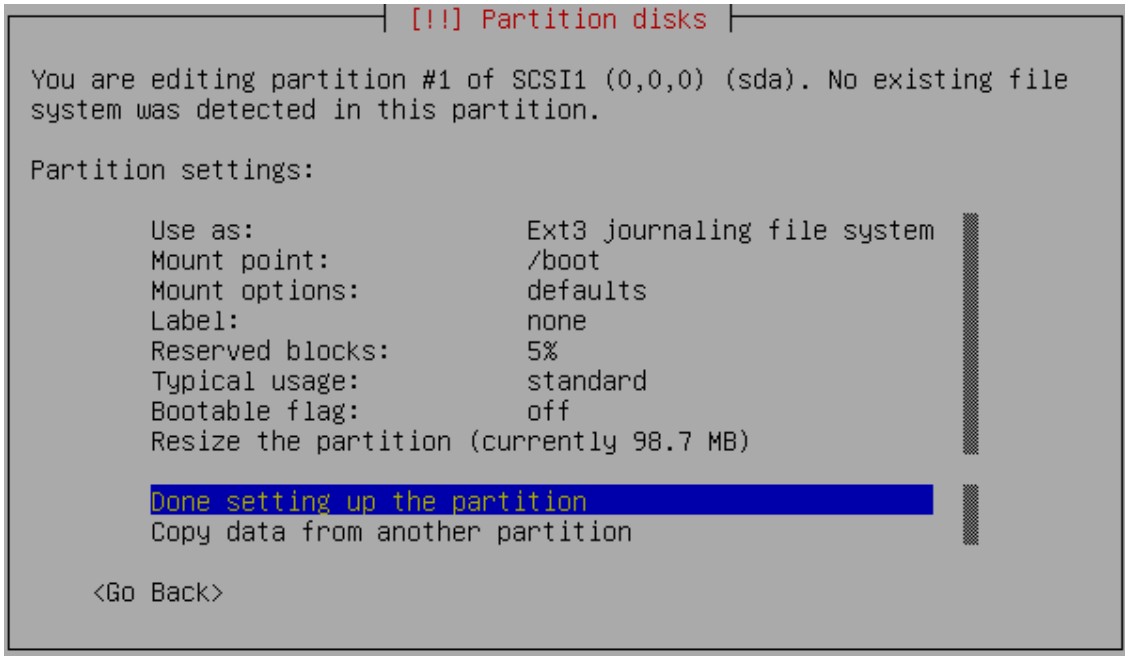
Ahora tiene que seleccionar el punto de montaje con la pantalla siguiente y presione ENTRAR para cambiar el punto de montaje



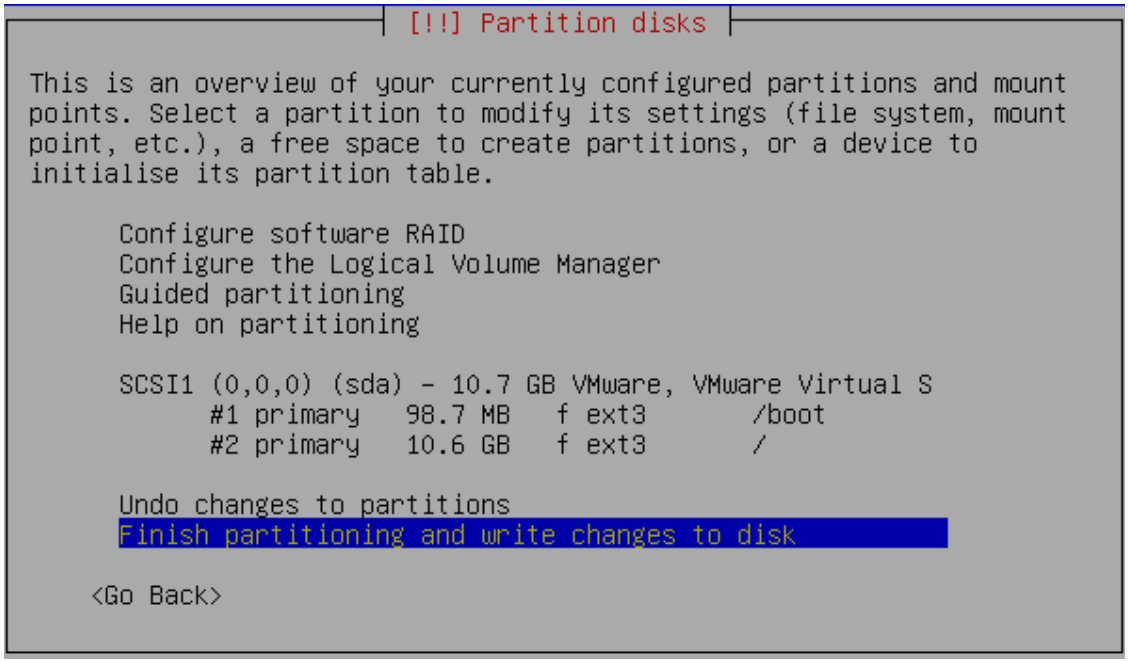
Ahora puedes ver las disponibles los puntos de montaje y aquí he seleccionado / boot punto de montaje y pulse enter



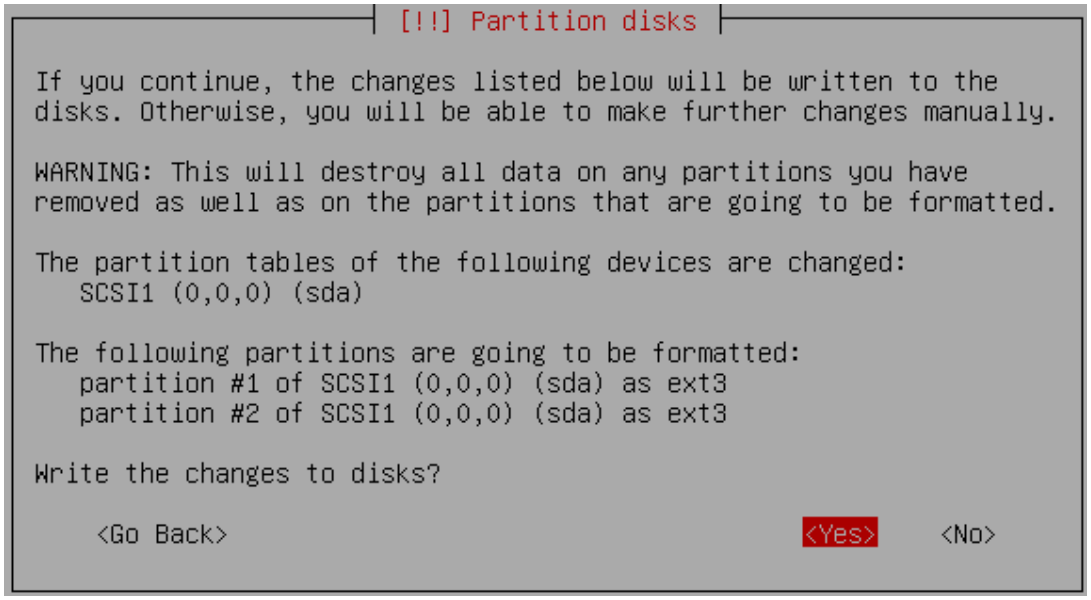
Ahora usted debería ver la siguiente pantalla, y aquí es necesario seleccionar "Hecho de definir la partición" y presiona Enter Esto creará el fichero / boot punto de montaje con 100 MB de espacio y puede crear el punto de montaje / de la misma manera con los el espacio existente.



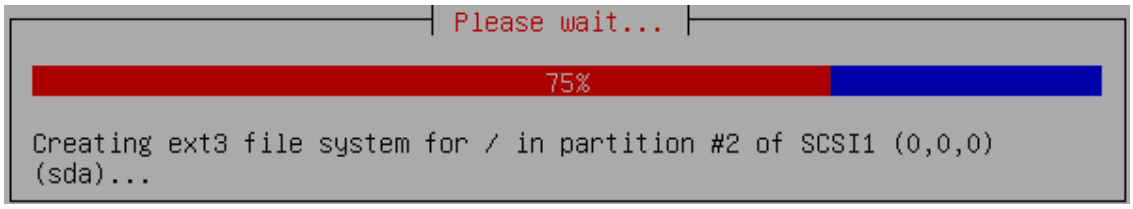
Usted puede ver esto en la siguiente pantalla, aquí tienes que seleccionar "Finalizar el particionado y escribir los cambios en disco" y presione Enter



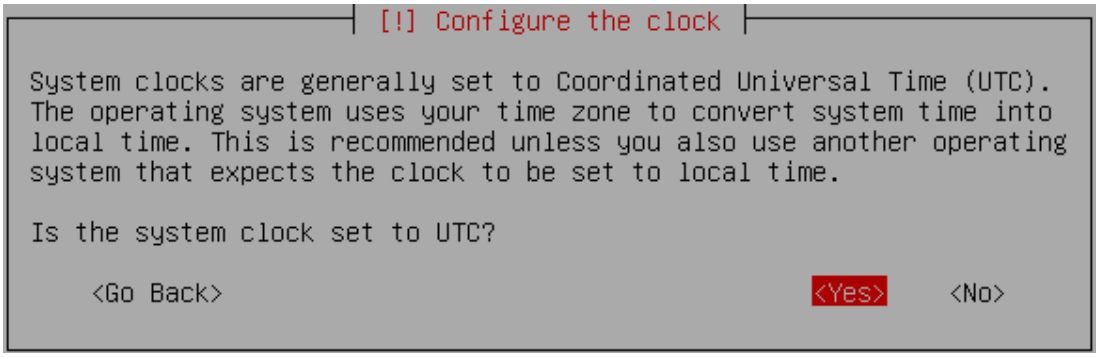
Escribir los cambios en esta opción de disco que usted necesita para seleccionar Sí y pulse Enter



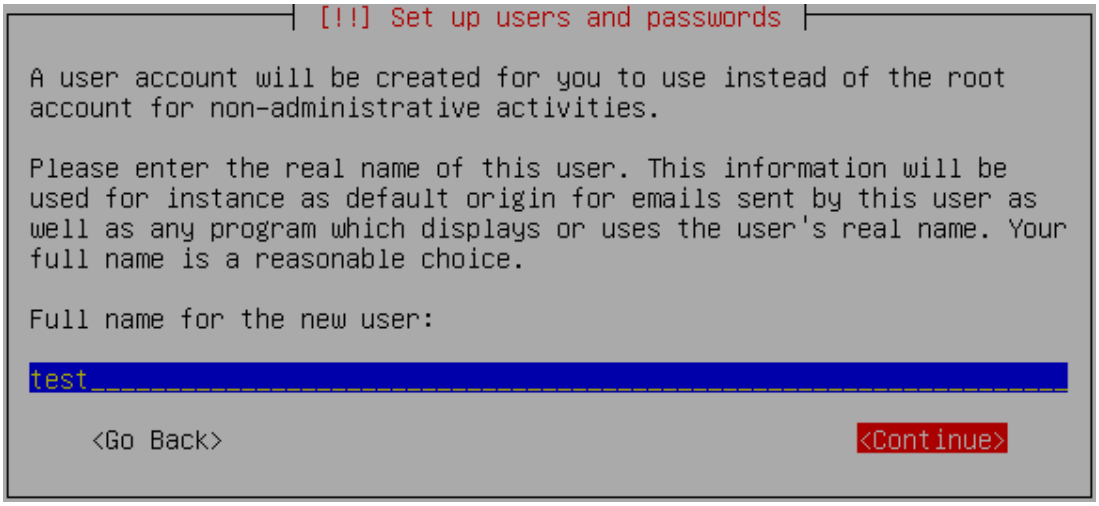
Creación de sistema de archivos ext3 en el progreso



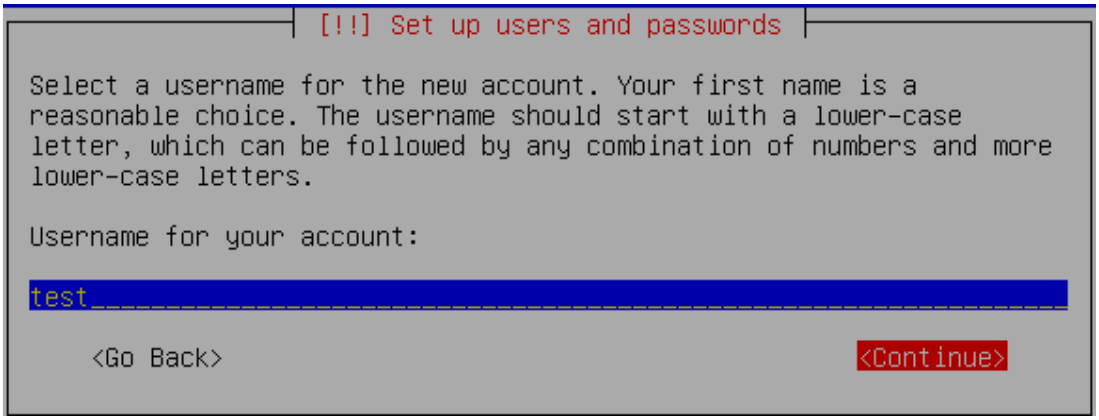
Configuración de la opción de reloj aquí si quieres dejar UTC Seleccione Sí y no lo contrario, presione ENTRAR



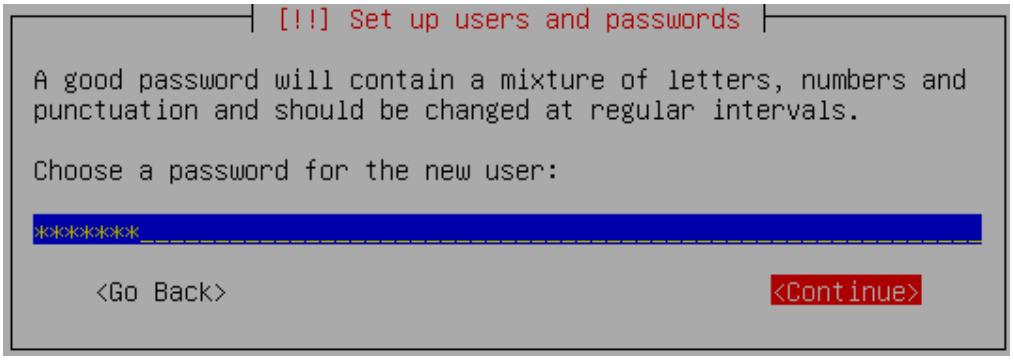
Es necesario introducir el nombre completo del usuario que desea crear para su servidor en este ejemplo que ha creado el usuario de prueba Seleccione Continuar y presione ENTRAR



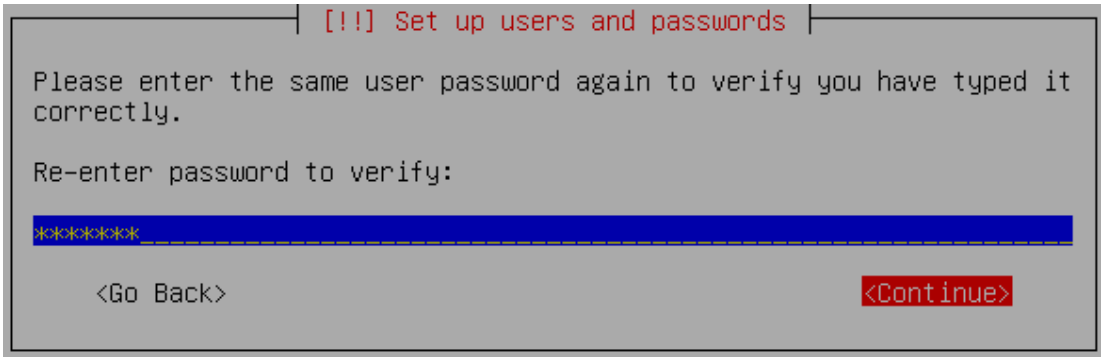
Nombre de usuario de tu cuenta en este he entrado en la prueba Seleccione Continuar y presione ENTRAR



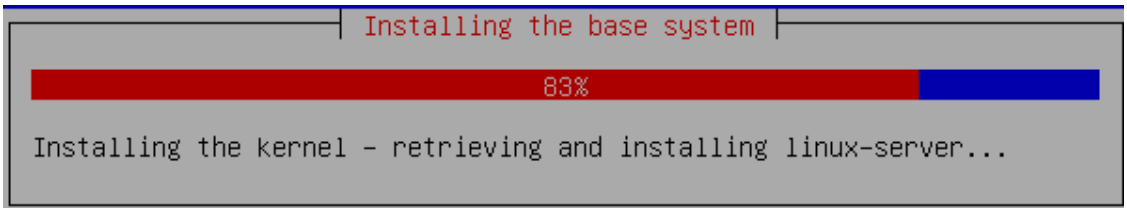
Introduce la contraseña de usuario de prueba Seleccione Continuar y presione ENTRAR



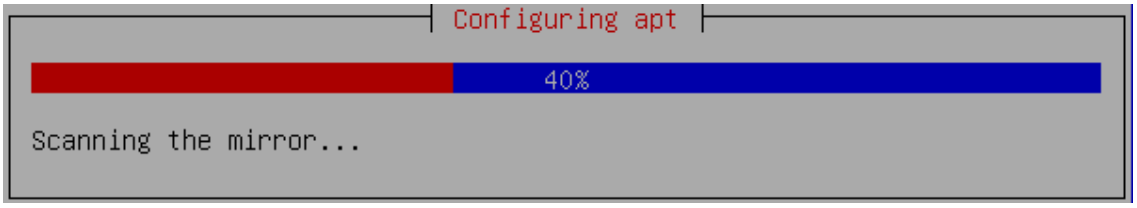
Confirme la contraseña de usuario de prueba Seleccione Continuar y presione ENTRAR



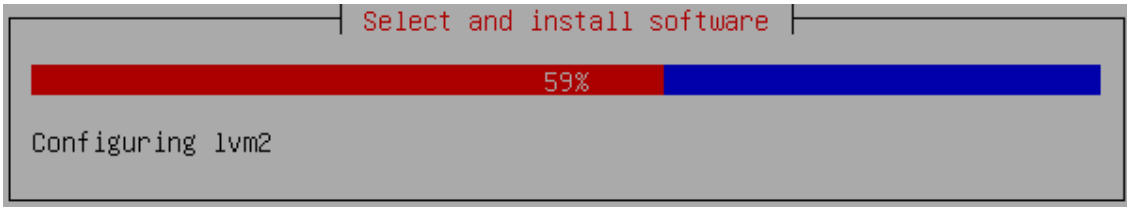
Instalar el sistema base en el progreso



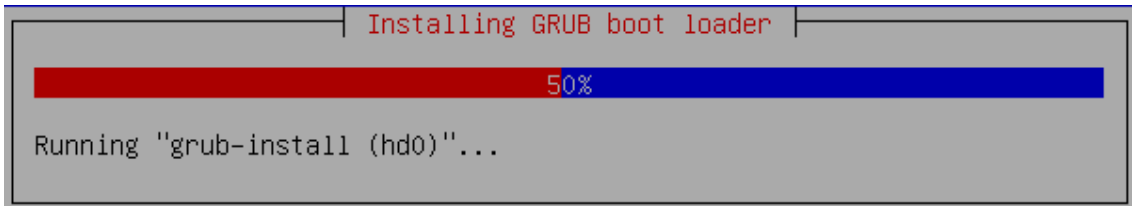
Configuración de espejo de este paquete estarán relacionados con la opción de país



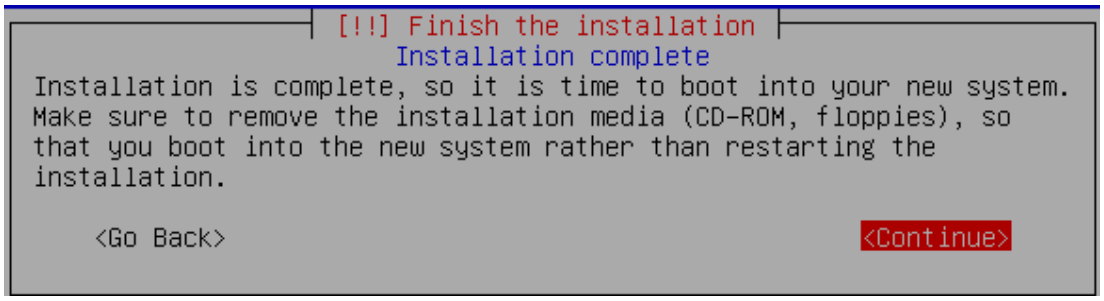
Elegir e instalar programas en curso



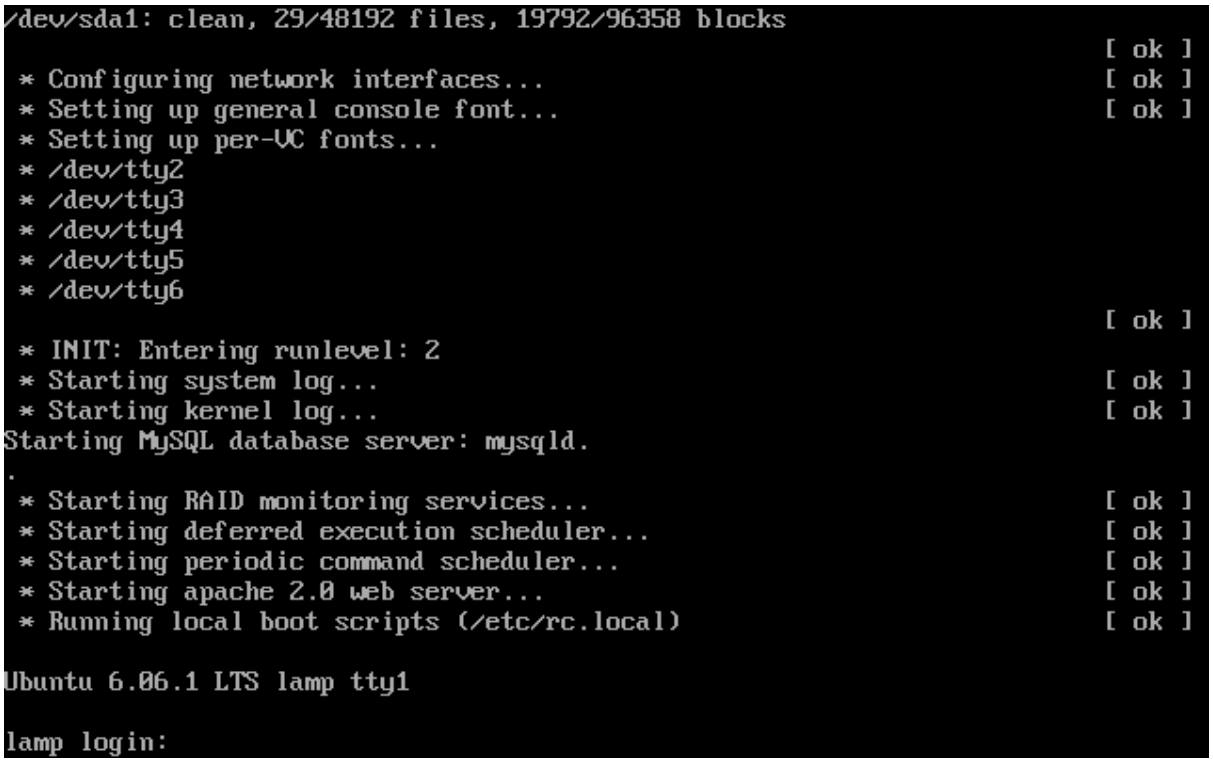
Instalación de GRUB gestor de arranque en el progreso



Mensaje de instalación completa aquí tiene que quitar la unidad de CD Seleccione Continuar y pulse Enter se reinicie el servidor de



Después de reiniciar puede ver la siguiente pantalla del sistema de nombre de usuario



Esto completará la instalación LAMP Ubuntu Server y el servidor está listo para la instalación de aplicaciones que soporta Apache, MySQL y PHP.

ANEXO 2

SCRIPT DE CONFIGURACIÓN DE WIFIDOG EN ENRUTADOR INALÁMBRICO

Script de configuración para Wifidog en Enrutador Inalámbrico
Fuente: /etc/wifidog.conf

```
# $Id: wifidog.conf 11656 2008-07-05 13:07:12Z florian $
# WiFiDog Configuration file

# Parameter: GatewayID
# Default: default
# Optional
#
# Set this to the node ID on the auth server
# this is used to give a customized login page to the clients and for
# monitoring/statistics purpose
# If none is supplied, the mac address of the GatewayInterface interface will be used,
# without the : separators

GatewayID cautivame2h

# Parameter: ExternalInterface
# Default: NONE
# Optional
#
# Set this to the external interface (the one going out to the Inernet or your larger LAN).
# Typically vlan1 for OpenWrt, and eth0 or ppp0 otherwise,
# Normally autodetected

# ExternalInterface eth0

# Parameter: GatewayInterface
# Default: NONE
# Mandatory
#
# Set this to the internal interface (typically your wifi interface).
# Typically br-lan for OpenWrt, and eth1, wlan0, ath0, etc. otherwise

GatewayInterface br-lan
#GatewayInterface wlan0

# Parameter: GatewayAddress
# Default: Find it from GatewayInterface
# Optional
#
# Set this to the internal IP address of the gateway.  Not normally required.
#GatewayAddress 192.168.3.1

# Parameter: AuthServer
# Default: NONE
# Mandatory, repeatable
#
```

```
# This allows you to configure your auth server(s).  Each one will be tried in order, untill one responds.
# Set this to the hostname or IP of your auth server(s), the path where
# WiFiDog-auth resides in and the port it listens on.
#AuthServer {
#       Hostname                (Mandatory; Default: NONE)
#       SSLAvailable            (Optional; Default: no; Possible values: yes, no)
#       SSLPort                 (Optional; Default: 443)
#       HTTPPort                (Optional; Default: 80)
#       Path                    (Optional; Default: /wifidog/ Note:  The path must be both prefixed and suffixed by /.  Use a single / for server root.)
#   LoginScriptPathFragment  (Optional; Default: login/? Note:  This is the script the user will be sent to for login.)
#   PortalScriptPathFragment (Optional; Default: portal/? Note:  This is the script the user will be sent to after a successfull login.)
#    MsgScriptPathFragment     (Optional; Default: gw_message.php? Note:  This is the script the user will be sent to upon error to read a readable message.)
#   PingScriptPathFragment    (Optional; Default: ping/? Note:  This is the script the user will be sent to upon error to read a readable message.)
#   AuthScriptPathFragment    (Optional; Default: auth/? Note:  This is the script the user will be sent to upon error to read a readable message.)
#}

#AuthServer {
#    Hostname auth.ilesansfil.org
#    SSLAvailable yes
#    Path /
#}

AuthServer {
    Hostname 192.168.3.100
    SSLAvailable no
    Path /
  #  PingScriptPathFragment https://192.168.3.100/ping/?
  # LoginScriptPathFragment https://192.168.3.100/login/?
  # PortalScriptPathFragment https://192.168.3.100/portal/?
  # MsgScriptPathFragment https://192.168.3.100/gw_message.php?
  # AuthScriptPathFragment https://192.168.3.100/auth/?
}

# Parameter: Daemon
#   AuthScriptPathFragment    (Optional; Default: auth/? Note:  This is the script the user will be sent to upon error to read a readable message.)
#}

#AuthServer {
#    Hostname auth.ilesansfil.org
#    SSLAvailable yes
#    Path /
#}
```

```
AuthServer {
    Hostname 192.168.3.100
    SSLAvailable no
    Path /
  #  PingScriptPathFragment https://192.168.3.100/ping/?
  # LoginScriptPathFragment https://192.168.3.100/login/?
  # PortalScriptPathFragment https://192.168.3.100/portal/?
  # MsgScriptPathFragment https://192.168.3.100/gw_message.php?
  # AuthScriptPathFragment https://192.168.3.100/auth/?
}

# Parameter: Daemon
# Default: 1
# Optional
#
# Set this to true if you want to run as a daemon
Daemon 1

# Parameter: GatewayPort
# Default: 2060
# Default: 2060
# Optional
#
# Listen on this port
# GatewayPort 2060

# Parameter: HTTPDName
# Default: WiFiDog
# Optional
#
# Define what name the HTTPD server will respond
# HTTPDName WiFiDog
# Parameter: HTTPDMaxConn
# Default: 10
# Optional
#
# How many sockets to listen to
# HTTPDMaxConn 10

# Parameter: CheckInterval
# Default: 60
# Optional
#
# How many seconds should we wait between timeout checks.  This is also
# how often the gateway will ping the auth server and how often it will
# update the traffic counters on the auth server.  Setting this too low
# wastes bandwidth, setting this too high will cause the gateway to take
# a long time to switch to it's backup auth server(s).
```

```
CheckInterval 300

# Parameter: ClientTimeout
# Default: 5
# Optional
#
# Set this to the desired of number of CheckInterval of inactivity before a client is logged
out
# The timeout will be INTERVAL * TIMEOUT
ClientTimeout 5

# Parameter: TrustedMACList
# Default: none
# Optional
#
# Comma separated list of MAC addresses who are allowed to pass
# through without authentication
TrustedMACList 00:10:b5:87:d2:6c,00:1E:68:8A:BB:9A,00:1A:DC:BD:3B:19

# Parameter: FirewallRuleSet
# Default: none
# Mandatory
# Parameter: FirewallRule
# Default: none
#
# Define one firewall rule in a rule set.

# Rule Set: global
#
# Used for rules to be applied to all other rulesets except locked.
FirewallRuleSet global {
   ## To block SMTP out, as it's a tech support nightmare, and a legal liability
   #FirewallRule block tcp port 25
   ## Use the following if you don't want clients to be able to access machines on
   ## the private LAN that gives internet access to wifidog.  Note that this is not
   ## client isolation;  The laptops will still be able to talk to one another, as
   ## well as to any machine bridged to the wifi of the enrutador.
   # FirewallRule block to 192.168.0.0/16
   # FirewallRule block to 172.16.0.0/12
   # FirewallRule block to 10.0.0.0/8
   ## This is an example ruleset for the Teliphone service.
   #FirewallRule allow udp to 69.90.89.192/27
   #FirewallRule allow udp to 69.90.85.0/27
   #FirewallRule allow tcp port 80 to 69.90.89.2
}

# Rule Set: validating-users
#
# Used for new users validating their account
FirewallRuleSet validating-users {
```

```
        FirewallRule allow udp to 0.0.0.0/0
        FirewallRule allow tcp port 80 to 0.0.0.0/0
        FirewallRule allow tcp port 443 to 0.0.0.0/0
        FirewallRule allow tcp port 2060 to 0.0.0.0/0
}

# Rule Set: known-users
#
# Used for normal validated users.
FirewallRuleSet known-users {
        FirewallRule allow udp to 0.0.0.0/0
        FirewallRule allow tcp port 80 to 0.0.0.0/0
        FirewallRule allow tcp port 443 to 0.0.0.0/0
        FirewallRule allow icmp to 0.0.0.0/0
        FirewallRule allow tcp port 50451 to 0.0.0.0/0
        FirewallRule allow tcp port 587 to 0.0.0.0/0
        FirewallRule allow tcp port 25 to 0.0.0.0/0
        FirewallRule allow tcp port 110 to 0.0.0.0/0
        FirewallRule allow tcp port 21 to 0.0.0.0/0
        FirewallRule allow to 0.0.0.0/0

}

# Rule Set: unknown-users
#
# Used for unvalidated users, this is the ruleset that gets redirected.
#
# XXX The redirect code adds the Default DROP clause.
FirewallRuleSet unknown-users {
    FirewallRule allow udp port 53
    FirewallRule allow tcp port 53
    FirewallRule allow udp port 67
    FirewallRule allow tcp port 67
}

# Rule Set: locked-users
#
# Not currently used
FirewallRuleSet locked-users {
    FirewallRule block to 0.0.0.0/0
}
```

ANEXO 3

SCRIPT DE CONFIGURACIÓN DEL SERVIDOR SAMBA 3 EN EL ENRUTADOR INALÁMBRICO.

Script de configuración del servidor samba 3 en el enrutador inalámbrico.
Fuente: /etc/samba/smb.conf

```
[global]
        netbios name = openwrt
        workgroup = REDSOURCE
        server string = openwrt
        syslog = 10
        encrypt passwords = true
        passdb backend = smbpasswd
        obey pam restrictions = yes
        socket options = TCP_NODELAY
        unix charset = ISO-8859-1
        preferred master = yes
        os level = 20
        security = share
        guest account = nobody
        invalid users = root
        smb passwd file = /etc/samba/smbpasswd

[homes]
        comment = Home Directories
        browseable = yes
        read only = no
        create mode = 0750

[compartida]
        path = /mmc/compartida
        read only = no
        guest ok = yes
        create mask = 0700
        directory mask = 0700
```