# “RED DE ACCESO INALÁMBRICO PARA LA ZONA CENTRO DE LA CIUDAD DE IBARRA”

*Autor-Javier ESPINOSA[1], Tutor-Jaime MICHILENA[2]*

Carrera de Ingeniería en Electrónica de Redes y de Comunicación de la Universidad Técnica del Norte, Avenida 17 de Julio, Ibarra, Imbabura

javiem06@gmail.com, jrmichilena@utn.edu.ec

**Resumen.** *En este trabajo se realizara un diseño para una red de acceso inalámbrico utilizando la tecnología WIFI en la zona centro de la ciudad de Ibarra. Este trabajo esta dividido en 5 capítulos q nos llevaran a tener el diseño deseado*

*El objetivo por el cual se realiza este proyecto es para poder integrar Tecnologías de Información y Comunicación en la ciudad tal y como nos indica el Plan Nacional de Desarrollo de las Comunicaciones impulsado por el Gobierno Nacional y mejorar la calidad de vida de los habitantes de la ciudad, además que con este proyecto estaremos sacando provecho a los anillos de fibra óptica que se encuentran en la ciudad de Ibarra.*

## Palabras Claves

Integrar, Tecnologías, Información, Desarrollo, Comunicaciones.

**Abstract.** *In this paper we conduct a design for a wireless network using WiFi technology in the center area of the Ibarra´s city. This work is divided into 5 chapters that take us to +have the desired design*

*The purpose for which this project is done is to integrate Information and Communication Technologies in the city as it indicates the NDP Communications driven by the national government and improve the quality of life of the inhabitants of the city, and that with this project we will be taking advantage of the fiber optic rings that are in the city of Ibarra.*

## Keywords

Integrate, Technologies, Information, Communication, Quality.

## Introducción

El primer capítulo incluirá toda la fundamentación teórica necesaria sobre tecnologías y términos que se utilizará en el diseño.

En el segundo capitulo se realizará un levantamiento de información geográfica donde estará incluido todos los estudios de la zona de cobertura para poder tener la información necesaria que ayudara a comenzar con nuestro diseño.

Una vez obtenida la información geográfica, comenzaremos con la planeación de la red donde se detallará los nodos y los equipos necesarios para que el diseño sea adecuadamente realizado, también se detallaran la ubicación de los mismos.

Con los datos obtenidos en los capítulos anteriores ya podremos diseñar nuestra red y será necesario detallar una topología de red, las zonas de cobertura y los servicios necesarios para dar una correcta utilización a nuestra red.

Finalmente se hará un análisis costo beneficio sobre nuestro proyecto y se incluirán manuales de configuración, usuarios y todos los anexos necesarios que sirvan para justificar este proyecto.

## Materiales y Métodos

Este proyecto está enfocado en toda la zona centro de la ciudad de Ibarra cuyo perímetro estará limitado por las calles:

• Sánchez y Cifuentes

• García Moreno

• Vicente Rocafuerte

• Cristóbal Colón

Se realizará un levantamiento de información de la situación actual de la ciudad en nuestra zona de cobertura, para determinar obstáculos físicos que puedan causar interferencia a la red, además de información correspondiente a los usuarios que van a tener acceso a esta red mediante observación de campo se contara el numero de usuarios promedio que se tendrá en determinados sectores de nuestra zona de cobertura durante una semana tomando en cuenta los días lunes, martes, miércoles, jueves, viernes y los horarios de 8h00 a 10h00, de 12h00 a 14h00 y de 17h00 a 18h00.

Se determinará los nodos que serán necesarios para cubrir toda el área con la utilización de Access Point analizando marcas de quipos de diferentes proveedores cuyas características puedan satisfacer los requerimientos de nuestra red, teniendo en cuenta que estos se deberán integrar a los tres anillos de fibra óptica que cubren toda esta zona y también se deberá ver todos los equipos necesarios para interconectar esta red atreves de los anillos de fibra óptica.

Con la información anterior se procederá al diseño de red que cumpla con los requerimientos de cobertura y acceso a los usuarios en el área especificada sin problemas de corte o desconexión, para lo cual se hará una estudio de hand-off que permita reducir estos problemas de manera que sea imperceptible la asociación de un AP a otro para el usuario.

Para brindar administración a la red utilizaremos una solución bajo software libre que nos permita controlar el tiempo de sesión de los usuarios, esto se lo realizará con la utilización de un portal cautivo el cual será configurado según las necesidades determinadas en el proceso de levantamiento de información, además es necesario instalar un servidor que nos permita realizar una autentificación por dirección MAC, esto nos garantizara tener una buena administración de nuestros puntos de acceso.

También se va analizar los servicios y proponer políticas de acceso adecuadas para los usuarios que utilicen la red, Es necesario también realizar restricciones para el acceso al Internet esto se lo hará con la utilización de un Firewall Proxy.

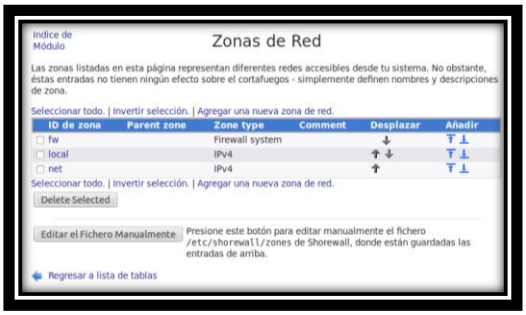
Se realizara un estudio de mercado y características de los equipos que están disponibles en el mercado para así poder realizar una lista detallada de los equipos más idóneos para que estos se puedan adquirir mediante el proceso de compras públicas.

Con el desarrollo de nuestro diseño iremos probando las políticas de acceso en un servidor de prueba.

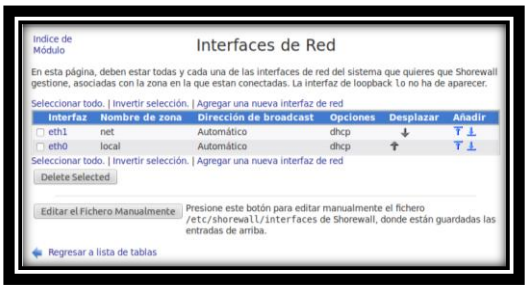
Se realizarán las conclusiones y recomendaciones necesarias y un análisis de las lecciones aprendidas en el transcurso de proyecto.

# 1. Resultados

Para comenzar debemos configurar nuestro Firewall Shorewall, para esto deberemos definir tres zonas: nuestra zona local, zona de net, y nuestra zona firewall, además de asociar con las interfaces de red por las cuales se van a conectar.




Zonas de Red




Interfaces de Red

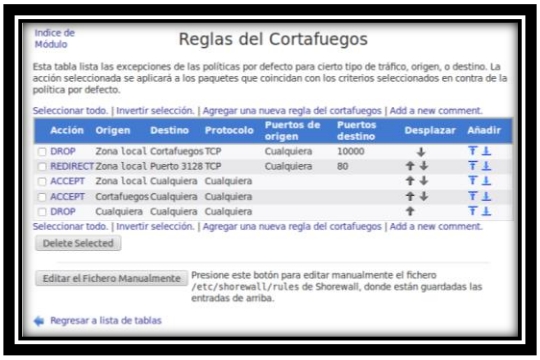
También es importante hacer en enmascaramiento para que nuestra red local salga a la red net (internet) a través de la eth1.


Enmascaramiento

Una vez definidas las interfaces y las zonas daremos las políticas por defecto donde negaremos el tráfico por defecto, y las reglas del firewall, estas reglas no serán muchas ya que necesitamos las siguientes:

- Denegar el tráfico de la red local hacia el firewall proxy en el puerto de Webmin para evitar las conexiones que permitan el ingreso a la configuración de nuestro firewall.
- Re direccionar todo el tráfico de nuestra red local hacia el puerto 3128 que es el puerto en el que trabaja nuestro proxy para que nuestro proxy sea transparente.
- Permitimos el tráfico de la red local hacia el internet.
- Permitimos el tráfico de la zona de firewall hacia cualquier parte.
- Denegamos el tráfico del internet hacia nuestra zona firewall y loca.
- Dejar un rango de IPs de Administrador con permisos para configuración remota.


Políticas por Defecto.

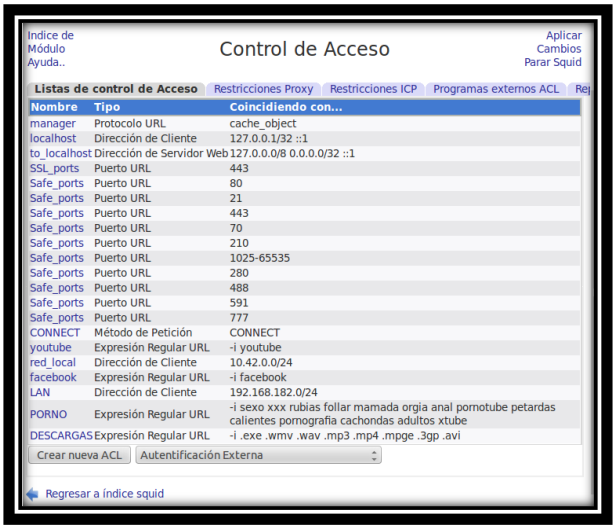



Reglas del Cortafuegos

Después de tener nuestro Firewall Shorewall listo y corriendo configuraremos nuestro proxy, es importante definir el puerto de trabajo que es el 3128 y que trabaje de forma transparente, deberemos crear las siguientes reglas que rechazaran las solicitudes web de nuestros usuarios, las reglas del proxy son las siguientes:

- Prohibir todas las páginas con contenido sexual.
- Prohibir páginas de gran tráfico de datos como son YouTube y Facebook.
- Prohibir las descargas de música y videos.
- Dejar un rango de IPs de Administrador con permisos para configuración remota.


Puertos y Trabajo de Red



Listas de Control de Acceso


Restricciones Proxy

Una vez configurado nuestro servidor Firewall Proxy y corriendo configuramos nuestro portal cautivo, es esencial que nuestro Portal Cautivo nos permita autentificación para usuarios que pueden tener acceso a internet y debe permitir libre acceso a paginas gubernamentales como el SRI, el GAD de San Miguel de Ibarra, el Gobierno Provincial, etc.

Hemos utilizado EasyHotSpot para poder cumplir con estos requerimientos, ya que en este sistema ya se encuentran configurados y corriendo tanto Free Radius como Chillispot.

Con UniFi software podemos monitorear todos nuestros APs y ver el número de usuarios que están conectados a nuestra red, esta es un software que nos proporciona una fácil administración de nuestra red inalámbrica

## PRUEBAS

En esta sección definiremos pruebas que nos garantizaran el correcto funcionamiento de nuestra red, esto lo haremos probando cada servidor y comprobando que las reglas que hemos definido funcionen correctamente

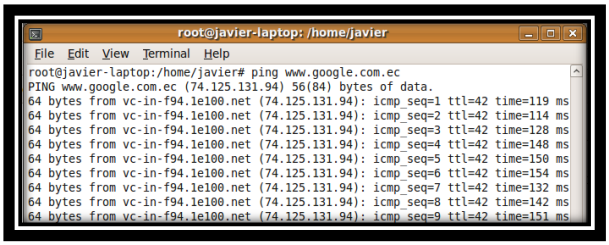
- Pruebas de conectividad del Firewall Proxy.- esta prueba consiste en verificar que el Firewall Proxy tenga salida a internet, para comprobar esto realizaremos un ping al servidor de google y entraremos en esta pagina a través del navegador web.


Ping de Firewall Proxy a Google


Google desde Firewall Proxy

Con esta prueba podemos comprobar que nuestro Firewall Proxy tiene conexión con Internet y que funciona la regla del Shorewall que nos permite desde firewall tener acceso a todo.

- Pruebas de Conectividad del el Portal Cautivo.- en esta prueba realizaremos un ping desde el Portal Cautivo hasta Google y nos entramos desde el navegador web a Google.




Ping de Portal Cautivo a Google


Google desde el Portal Cautivo

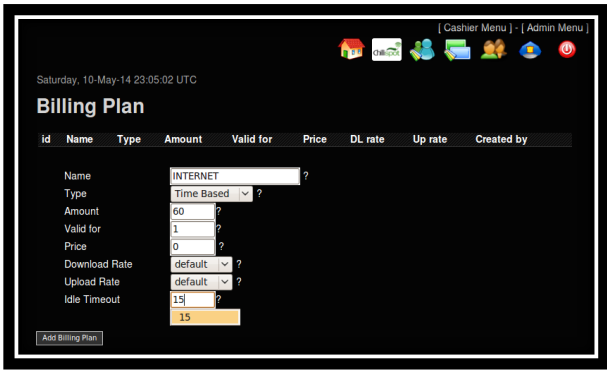
Con esta prueba comprobamos que nuestro Portal Cautivo tiene salida a Internet y también nos dice que el Firewall esta realizando correctamente el nateo y el enmascaramiento.

- Conexión del Usuario.- en esta prueba nos conectaremos con un usuario cualquiera en este caso usaremos un usuario en Windows XP y verificaremos con desde la consola con el comando ipconfig/all nuestra IP y nuestro servidor DNS.


Visualización dl comando ipconfig/all desde un usuario XP

Con esta prueba podemos ver que nos asigno la ip 192.168.182.2/24 y una puerta de enlace 192.168.182.1 esto nos indica que el servidor DHCP de nuestro Portal Cautivo funciona además podemos ver como sufijo DNS chillispot.info.key que es el sufijo DNS del Portal Cautivo, también nos indica que estamos conectados con nuestro Portal Cautivo.

- Generación de Usuario.- crearemos una cuenta por tiempo que dure una hora y generaremos un usuario desde el Portal Cautivo.




Parámetros de la cuenta

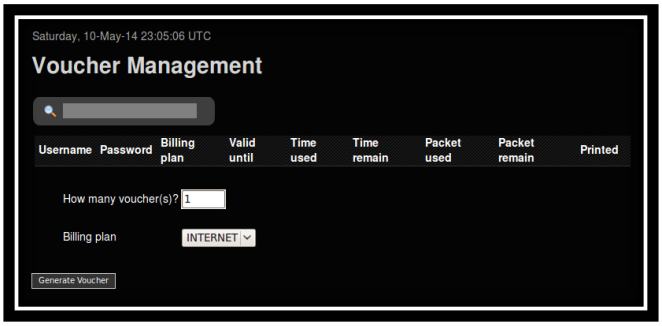
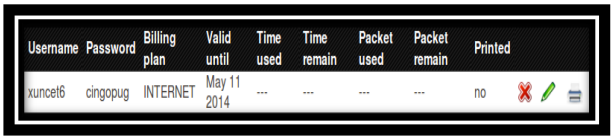


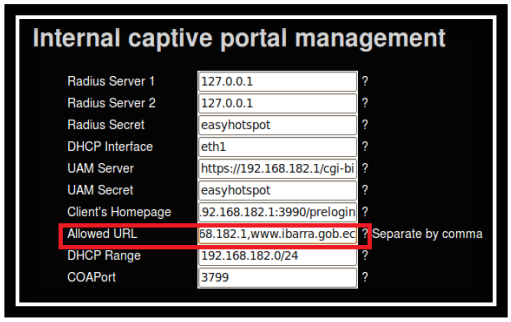

Fig.4.21.: Parámetros para generar usuario

Fuente: Portal Cautivo.

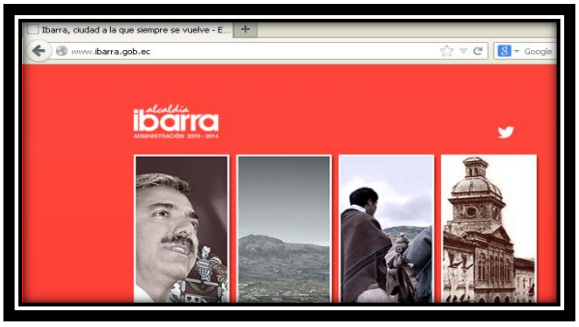



Usuario Creado

- Ingreso a Contenido sin Autenticación.- tenemos que permitir acceso a páginas gubernamentales como es la del GAD de San Miguel de Ibarra, para esto permitiremos en la configuración del Portal Cautivo el acceso a www.ibarra.gob.ec que es la página oficial y probaremos ingresando desde el usuario XP.



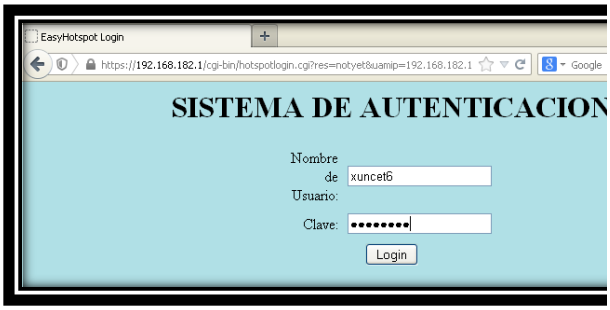

Permitir acceso a www.ibarra.gob.ec



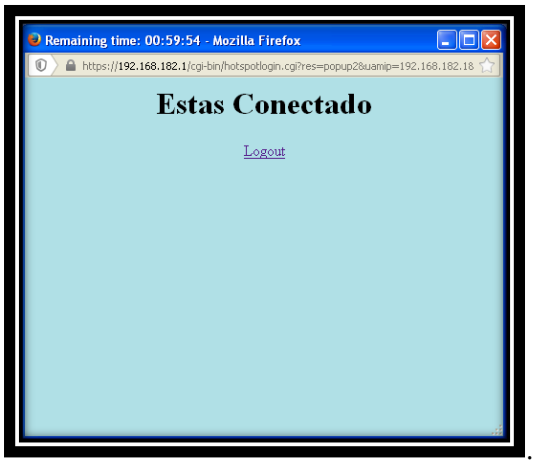

Ingreso a www.ibarra.gob.ec

Como podemos ver en esta prueba ingresa a www.ibarra.gob.ec sin necesidad de autentificarse.

- Autenticación de Usuario.- trataremos de ingresar a google y nos deberá pedir un usuario y contraseña, ingresaremos el generado anteriormente.




Pantalla de Autenticación de Usuarios




Pantalla de Inicio de Sesión

Con esta prueba podemos ver que es sistema de autenticación de nuestro Portal Cautivo funciona y como vemos en la figura 4.26 tenemos un contador que nos indica que tenemos una hora de conexión con lo que también verificamos que el portal cautivo nos esta controlando la sesión de la manera que establecimos anteriormente.

- Ingreso a Internet del Usuario.- en esta prueba ingresaremos a www.google.com para comprobar que una ves que hemos iniciado sesión tenemos acceso a internet.


Acceso a Google desde Usuario XP

Nos da acceso a Internet y con esto también se comprueba la regla de Shorewall que permite a la red local acceso a internet.

- Prueba de reglas del Proxy.- en esta prueba se verificara las siguientes reglas del Proxy:
- Prohibir todas las páginas con contenido sexual.
- Prohibir páginas de gran tráfico de datos como son YouTube y Facebook.


Acceso ha contenido sexual


Fig.4.29.: Acceso a Youtube

Fuente: Usuario Windows XP


Acceso a Facebook

Como se puede ver en las imágenes las reglas del Firewall Proxy funcionan y nos niega el acceso y también podemos ver que nuestro proxy trabaja de forma transparente, como conclusión las reglas del proxy y la configuración de Shorewall para que este trabaje de modo transparente funciona.

- Denegar el tráfico de la red local hacia el firewall proxy en el puerto de Webmin para evitar las conexiones que permitan el ingreso a la configuración de nuestro firewall.


Acceso a Webmin desde usuario XP

No permite el acceso al servidor Firewall Proxy a través de Webmin.

- Fin de Sesión.- una vez terminado el tiempo la sesión caducara.


Pantalla de Cierre de Sesión

**Una vez finalizada la sesión nos muestra una venta con el mensaje**

# Conclusiones

- Es muy importante realizar un levantamiento correcto de información para que nuestro diseño este echo de una manera adecuada.

- La utilización de Software Libre nos abre un sin número de puertas para poder solucionar problemas, como en este trabajo el software libre nos da una variedad de recursos que pueden trabajar entre sí para brindarnos un servicio óptimo.

- Proyectos de este tipo ayudan a mejorar la calidad de vida de los habitantes de una ciudad y estar encaminados hacia un mundo tecnológico.

- La difusión de Tecnologías de Información y Comunicación es muy positivo en los habitantes, porque nos lleva a estar comunicados e informados cada día más.

- Al utilizar Fibra Óptica como medio de transmisión tenemos una ventaja enorme a la hora de montar servicios sobre nuestra red, ya que el ancho de banda y las velocidades con las que trabajamos son muy altas.

- La utilización de un Firewall Shorewall es muy importante en el diseño de una red, este nos proporciona una seguridad muy alta a la vez que no es tan complejo como lo son otros Firewalls, además que se puede montar sobre cualquier servidor con base Linux.

- Squid Proxy es una herramienta efectiva a la hora de restringir contenido web, siempre es importante restringir este tipo de contenido es redes abiertas.

- Utilizar EasyHotSpot como nuestro Portal Cautivo es una manera rápida y eficiente de dar un servicio de autenticación y un control de ancho de banda a nuestros usuarios.

• Es muy importante una correcta configuración de los APs porque estos son los que nos permiten el acceso a nuestra red.

## Agradecimientos

Agradezco principalmente a Dios por la vida, la salud y las oportunidades que tengo de realizar todo lo que me propongo, honrando y poniendo al todopoderoso por encima de todas las cosas.

Mi más sincero agradecimiento a la Universidad Técnica del Norte y a todos mis docentes en general por brindarme sus conocimientos y apoyo, al Ing. Jaime Michilena por el esfuerzo, paciencia y dedicación demostrados a lo largo del proceso y por forjar en mí conocimientos teóricos y valores humanos que me ayudarán a lo largo de la vida,

## Referencias Bibliográficas

2014 Microsoft. (2014). technet microsoft. Obtenido de http://technet.microsoft.com/es-es/library/cc780906%28v=ws.10%29.aspx

WIKIPEDIA. (21 de ABRIL de 2014). Recuperado el 23 de MARZO de 2014, de http://en.wikipedia.org/wiki/Transceiver

Álvarez, M. Á. (22 de Agosto de 2001). desarrolloweb. Obtenido de http://www.desarrolloweb.com/articulos/513.php

Colobran M. Arqués. & Galindo, E. (s.f.). Administración de Sistemas operativos de red. Barcelona.

Creative Commons. (junio de 2005). Aula Clic. Recuperado el 2013, de aulaclic.es: http://www.aulaclic.es/articulos/wifi.html

D, J. (2007). TEORIA DE LA COMUNICACION. BARCELONA: HERDER.

Free Software Foundation. (s.f.). gnu. Obtenido de https://www.gnu.org/philosophy/free-sw.es.html

Fundación Wikimedia, Inc. (SEPTIEMPBRE de 2006). Recuperado el FEBRERO de 2014, de WIKIPEDIA: http://es.wikipedia.org/wiki/Handover

INFORMATICA MODERNA. (s.f.). INFORMATICA MODERNA. Obtenido de http://www.informaticamoderna.com/Acces_point.htm

López, R. G. (06 de abril de 2011). itespresso. Obtenido de http://www.itespresso.es/sistema-de-distribucion-inalambrica-wds-50183.html

LUIS, R. Y. (2011). BASE DE DATOS DOCUMENTALES . MALDONADO: MALDONADO.

Sociedad Latinoamericana para la Calidad. (2000). Análisis Costo/Beneficio.

W, T. (2010). Sistemas de Comunicaciones Electrónicas. Madrid: Prentice-Hall.

W., S. (2007). Fundamentos de Seguridad en edes. Aplicaciones y Estándares.

WIKIPEDIA. (7 de MAYO de 2014). WIKIPEDIA. Recuperado el 4 de ENERO de 2014, de http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29

Zimmermann, A. (2007). La Gestion de redes. En A. Zimmermann, La Gestion de redes.

## Sobre los Autores...

**Javier ESPINOSA**, Bachiller Físico Matemático en el Colegio San Francisco de la ciudad de Ibarra,

Estudiante de Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.

**Jaime MICHILENA** Bachiller en Físico Matemático en el Colegio San Francisco de la ciudad de Ibarra.

Graduado en Ingeniería Electrónica y Telecomunicaciones de la Universidad Politécnica Nacional de la ciudad de Quito