



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

**TÍTULO: “RED DE ACCESO INALÁMBRICO PARA LA ZONA
CENTRO DE LA CIUDAD DE IBARRA”**

**TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
ELECTRÓNICA Y REDES DE COMUNICACIÓN**

Autor: JAVIER ANÍBAL ESPINOSA MARTÍNEZ

Director: Ing. JAIME ROBERTO MICHILENA

Ibarra a, abril de 2014



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional con la finalidad de apoyar los procesos de investigación docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	100294235-5
Apellidos y Nombres	Espinosa Martínez Javier Aníbal
Dirección	Ibarra, Mosquera Narváez 1-104
E-mail	javiem06@gmail.com
Teléfono Fijo	062953263
Teléfono Móvil	0996877876

DATOS DE LA OBRA	
Título	RED DE ACCESO INALÁMBRICO PARA LA ZONA CENTRO DE LA CIUDAD DE IBARRA
Autor	Javier Aníbal Espinosa Martínez
Fecha	9 de Mayo de 2014
Programa	Pregrado
Título por el que se aspira	Ingeniero en Electrónica y Redes de Comunicación
Director	Ing. Jaime Michilena


2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Javier Aníbal Espinosa Martínez, con cédula de identidad Nro. 100294235-5, en calidad de autor titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

DECLARACIÓN

Manifiesto que la presente obra es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto es original y que soy el titular de los derechos patrimoniales; por lo que asumo la responsabilidad sobre el contenido de la misma y saldré en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, a los 23 días del mes de Julio de 2014



JAVIER ANIBAL ESPINOSA MARTÍNEZ

1002942355

CERTIFICACIÓN

Certifico que el presente trabajo de titulación "**RED DE ACCESO INALÁMBRICO PARA LA ZONA CENTRO DE LA CIUDAD DE IBARRA**" fue desarrollado por **JAVIER ANIBAL ESPINOSA MARTINEZ**, bajo mi supervisión



Jorge Machuca
DIRECTOR DE TESIS

**CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO
A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE**

Yo, **JAVIER ANIBAL ESPINOSA MARTINEZ**, con cédula de identidad Nro 1002942355, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador artículos 4, 5 y 6, en calidad de autor (es) de la obra o trabajo de grado denominado **“RED DE ACCESO INALÁMBRICO PARA LA ZONA CENTRO DE LA CIUDAD DE IBARRA”**, que ha sido desarrollado para optar por el título de **INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN**, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte

Ibarra, a los 23 días del mes de Julio de 2014


JAVIER ANIBAL ESPINOSA MARTINEZ

1002942355

DEDICATORIA

A mi esposa:

Karen Segovia

Quien ha sido un pilar importante en la realización de este trabajo ya que con su amor y perseverancia me ha apoyado absolutamente

A mi madre:

Cecilia Martínez Meza

Quien toda mi vida estudiantil me ha apoyado incondicionalmente con cariño, afecto y comprensión.

A mis hermanas y mi hijo:

Zoily Espinosa

Ángeles Espinosa

José Javier Espinosa

Javier

AGRADECIMIENTO

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,

Javier

INTRODUCCIÓN

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 está dividido en 5 capítulos q nos llevaran a tener el diseño deseado.

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

En el segundo capítulo 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.

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.

SUMMARY

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 first chapter will include all the necessary theoretical foundation on technologies and terms to be used in the design.

In the second chapter a survey of geographical information which is included all studies of the coverage area in order to have the necessary information to help you get started with our design will be performed.

Once we have the geographical information, Get started with the planning of the network where the nodes and the equipment necessary for the design to be properly made will detail the location of the same is also detailing.

With the data obtained in the previous chapters and we can design our network and will be detailed network topology, coverage areas and services necessary to give a proper use of our network.

Finally there will be a cost benefit analysis on our project and configuration manuals, users and all required attachments which could support this project be included.

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.

ÍNDICE GENERAL

PORTADA	i
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE	ii
DECLARACIÓN	iv
CERTIFICACIÓN	v
CECIÓN DE DERECHOS	vi
DEDICATORIA	vii
AGRADECIMIENTO	viii
INTRODUCCIÓN	ix
SUMMARY	x
INDICE GENERAL	xi
INDICE DE FIGURAS	xiv
INDICE DE TABLAS	xvi
INDICE DE ANEXOS	xvii
ANTECEDENTES	xviii
CAPITULO 1.: FUNDAMENTOS TEORICOS.....	22
1.1.: TECNOLOGÍA WI-FI.....	22
1.1.1.: INTRODUCCIÓN.....	22
1.1.2.: EL NOMBRE WIFI	22
1.1.3.: ESTÁNDARES QUE CERTIFICA WIFI	23
1.1.3.1.: Tipos de estándares:	23
1.1.4.: SEGURIDAD Y FIABILIDAD	24
1.1.5.: DISPOSITIVOS	25

1.2.: SISTEMA DE DISTRIBUCION WIRELESS (WDS)	25
1.2.1.: VENTAJAS Y PROBLEMAS WDS	26
1.2.2.: OPERACIÓN	26
1.2.2.1.: Modalidades	27
1.2.3.: HAND OFF	27
1.3.: SOFTWARE LIBRE	28
1.3.1.: INTRODUCCIÓN.....	28
1.3.2.: LIBERTADES DEL SOFTWARE LIBRE.....	29
1.3.3.: TIPOS DE LICENCIAS	29
1.3.3.1.: Licencias GPL	30
1.3.3.2.: Licencias AGPL	30
1.3.3.3.: Licencias estilo BSD	30
1.3.3.4.: Licencias estilo MPL y derivadas	30
1.3.4.: Regulación en Ecuador.....	31
1.4.: SERVICIOS	31
1.4.1.: FIREWALL.....	31
1.4.1.1.: Definición de Firewall.....	32
1.4.1.2.: Firewall Proxy	32
1.4.2.: SERVIDOR DHCP	34
1.4.2.1.: Definición	34
1.4.2.2.: Asignación de direcciones IP	35
1.4.2.3.: Parámetros configurables	35
1.4.3.: PORTAL CAUTIVO.....	36
1.4.3.1.: Usos	37
1.4.4.: FIBRA OPTICA.....	39

1.4.4.1.: Introducción.....	39
1.4.4.2.: Características.....	39
1.4.4.3.: Ventajas	39
1.4.4.4.: Desventajas.....	40
1.4.4.5.: Fibra multimodo	40
1.4.4.6.: Fibra monomodo	41
1.4.5.: TRANSCEIVERS	41
1.4.6.: ACCESS POINT	41
1.4.7.: SWITCH.....	42
CAPITULO 2.: LEVANTAMIENTO DE INFORMACION GEOGRAFICA.....	44
2.1.: ESTUDIO DE LA ZONA DE COBERTURA.....	44
2.1.1.: SITUACIÓN INICIAL.....	44
2.1.2.: ZONAS DE INTERFERENCIA	46
2.1.3.: PROBLEMAS	48
2.2.: USUARIOS	48
CAPITULO 3.: PLANEACION DE LA RED.....	52
3.1.: NODO	52
3.2.: EQUIPOS	54
3.2.1.: UBICACIÓN DE LOS EQUIPOS	56
3.2.2.: LISTADO DETALLADO DE EQUIPOS.....	57
3.2.3.: listado detallado de software	57
CAPITULO 4.: DISEÑO DE LA RED.....	58
4.1.: TOPOLOGIA	58
4.2.: DETALLE POR NODO.....	59
4.2.1.: ZONAS DE COBERTURA	61

4.3.: SERVIDOR	63
4.3.1.: SISTEMA OPERATIVO	63
4.3.2.: WEBMIN	64
4.3.3.: FIREWALL SHOREWALL	64
4.3.4.: FIREWALL PROXY	65
4.3.5.: PORTAL CAUTIVO.....	65
4.3.6.: SOFTWARE UNI FI.....	66
4.4.: ADMINISTRACIÓN	66
4.4.1.: POLITICAS DE ACCESO	67
4.4.2.: PRUEBAS	72
CAPITULO 5.: ANALISIS COSTO BENEFICIO.....	83
5.1.: DEFINICIÓN	83
5.2.: UTILIDAD	83
5.2.1.: PROCESO	83
CONCLUSIONES.....	87
RECOMENDACIONES	88
Bibliografía.....	89

ÍNDICE DE FIGURAS

Fig.1.1.: Logo de Wi-Fi.....	23
Fig.1.2.: Sistema de Distribución Wireless (WDS).....	266
Fig.1.3: Esquema de donde se localizaría un cortafuegos en una red de ordenadores.....	31
Fig.1.4: Gráfica de firewall proxy y servicios	33
Fig.1.5: Servidor DHCP	34
Fig.1.6: Conexión del Portal Cautivo	37

Fig.1.7: Access Point	42
Fig.1.8: Un conmutador en el centro de una red en estrella.	42
Fig.2.1.: Zona de Cobertura.....	45
Fig.2.2.: Fibra Principal.....	45
Fig.2.3.: Numero de Nodos en la Zona de Cobertura.....	46
Fig.2.4.: Interfaz de insSSIDer 3	47
Fig.3.1.: Detalle del Nodo	52
Fig.3.2.: Nodos	53
Fig.3.3.: UniFi AP Outdoor+.....	56
Fig.4.1.: Topología de Red	67
Fig.4.2.: Ubicación del Acces Point en Poste.....	60
Fig.4.3.: Conexión con el anillo de Fibra Óptica	60
Fig.4.4.: Zona de Cobertura.....	61
Fig.4.5.: Conexión tipo malla de los APs	62
Fig.4.6.: Conexión del Servidor Proxy	65
Fig.4.7.: Zonas de Red.....	67
Fig.4.8.: Interfaces de Red.....	68
Fig.4.9.: Enmascaramiento	68
Fig.4.10.: Políticas por Defecto.	69
Fig.4.11.: Reglas del Cortafuegos	69
Fig.4.12.: Puertos y Trabajo de Red	70
Fig.4.13.: Listas de Control de Acceso.....	71
Fig.4.14.: Restricciones Proxy.....	71
Fig.4.15.: Ping de Firewall Proxy a Google	72
Fig.4.16.: Google desde Firewall Proxy	73

Fig.4.17.: Ping Portal Cautivo a Google.....	73
Fig.4.18.: Google desde Portal Cautivo.....	74
Fig.4.19.: Visualización del comando ipconfig/all desde un usuario XP.....	75
Fig.4.20.: Parámetros de la cuenta.....	76
Fig.4.21.: Parámetros para generar usuario	76
Fig.4.22.: Usuario Creado	77
Fig.4.23.: Permitir acceso a www.ibarra.gob.ec.....	77
Fig.4.24.: Ingreso a www.ibarra.gob.ec	78
Fig.4.25.: Pantalla de Autenticación de usuarios.....	78
Fig.4.26.: Pantalla de Inicio de Sesión	79
Fig.4.27.: Acceso a Google desde Usuario XP.....	80
Fig.4.28.: Acceso a contenido sexual	80
Fig.4.29.: Acceso a Youtube	81
Fig.4.30.: Acceso a Facebook.....	81
Fig.4.31.: Acceso a Webmin desde Usuario XP	82
Fig.4.32.: Pantalla de Fin de Sesión	82

ÍNDICE DE TABLAS

Tabla 1.1.: Tabla comparativa entre los estándares 802.11.....	24
Tabla 1.2.: Libertades del Software libre	29
Tabla 2.1.: Datos de Usuarios Nomenclatura de Calles	49
Tabla 2.2.: Datos de Usuarios Día Lunes	49
Tabla 2.3.: Datos de Usuarios Día Martes.....	49
Tabla 2.4.: Datos de Usuarios Día Miércoles.....	50
Tabla 2.5.: Datos de Usuarios Día Jueves	50

Tabla 2.6.: Datos de Usuarios Día Viernes	50
Tabla 2.7.: Datos de Usuarios Resultados	51
Tabla 3.1.: Dirección de los nodos	53
Tabla 3.2.: Tabla comparativa de Equipos	55
Tabla 3.3.: Tabla de Direccionamiento.	59
Tabla.5.1.: Presupuesto Referencial.....	86

ÍNDICE DE ANEXOS

ANEXO A.....	91
ANEXO B	119
ANEXO C.....	139
ANEXO D	198
ANEXO E.....	200

ANTECEDENTES

1. PROBLEMA

Existe un Plan Nacional de Desarrollo de Comunicaciones al cual no se lo ha tomado en cuenta al realizar proyectos para la ciudad.

Actualmente, el Gobierno Nacional se ha enfocado mucho en promover tecnologías de información, esto obliga a los gobiernos seccionales a realizar proyectos enfocados en esta área, el Gobierno Autónomo Descentralizado de la San Miguel de Ibarra está realizando la implementación de fibra óptica en gran parte de la ciudad creando la necesidad de aprovechar este recurso.

El Gobierno Autónomo Descentralizado de San Miguel de Ibarra tiene una obligación con la ciudadanía de mejorar su calidad de vida, llevando de la mano el avance de la tecnología introduciendo nuevos servicios mediante tecnologías inalámbricas, cumpliendo con la iniciativa del Gobierno Nacional.

2. OBJETIVOS

OBJETIVO GENERAL

Diseñar una red de acceso inalámbrico utilizando la tecnología Wi-Fi IEEE 802.11 g y n; uniendo estos nodos a los anillos de fibra óptica tendidos por el gobierno Municipal permitiendo el acceso a internet a la ciudadanía.

OBJETIVOS ESPECÍFICOS

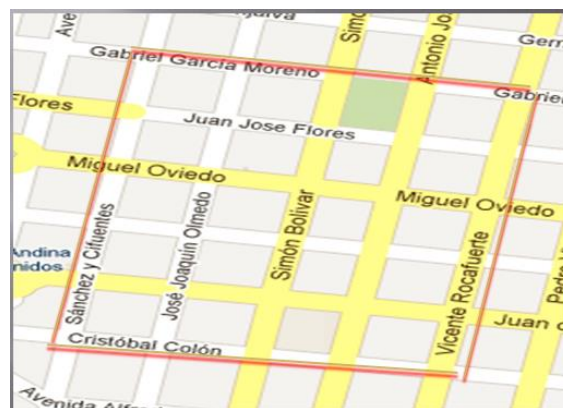
- Levantar información sobre la situación actual de la zona céntrica de la ciudad de Ibarra.

- Realizar un análisis de las tecnologías IEEE 802.11 g y n, fibra óptica, WDS y hand-off.
- Determinar cuántos nodos son necesarios para dar cobertura a esta zona.
- Diseñar una topología de red adecuada que garantice la conexión dentro de la zona planteada.
- Realizar una administración adecuada de los puntos de red.
- Crear políticas de acceso a esta red para poder administrar a los usuarios.
- Investigar los equipos inalámbricos existentes en el mercado que puedan satisfacer las necesidades de la red.
- Hacer un análisis costo beneficio de nuestro diseño.

3. ALCANCE

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 número 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 autenticación 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.

4. JUSTIFICACIÓN

Este proyecto será un aporte en el área de redes inalámbricas ya que se revisara temas como administración de Access Point y el tiempo de sesión de los usuarios.

El propósito de este proyecto además de lo antes mencionado es poder aprovechar el anillo de fibra óptica que el Municipio de Ibarra va a implementar en la ciudad y así poder brindar nuevos servicios para la ciudadanía.

Se utilizará una tecnología que está disponible en el mercado y al alcance de los usuarios como es Wi-Fi IEEE 802.11 g/n, hoy en día la mayoría de los dispositivos móviles que pueden navegar por internet utilizan esta tecnología.

Además este proyecto está acorde al plan nacional de desarrollo de las comunicaciones impulsado por el gobierno nacional cuyo principal objetivo es utilizar Tecnologías de Información y Comunicación para establecer el camino hacia la sociedad de la información y el conocimiento y al plan de Servicio Universal que nos dice que debe haber disponibilidad de los servicios de telecomunicaciones a una distancia aceptable con respecto a los hogares o lugares de trabajo.

CAPITULO 1.: FUNDAMENTOS TEÓRICOS

1.1.: TECNOLOGÍA WI-FI

Este capítulo empieza hablando de la tecnología Wi-Fi, ya que mediante esta basaremos nuestro diseño, a lo largo de este trabajo haremos muchas menciones a esta tecnología, por lo cual a continuación daremos algunos detalles de la misma.

1.1.1.: INTRODUCCIÓN

(Creative Commons., 2005) “Cuando hablamos de WIFI nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. WIFI, también llamada WLAN (wireless lan, red inalámbrica) o estándar IEEE 802.11. WIFI no es una abreviatura de Wireless Fidelity, simplemente es un nombre comercial.”

La tecnología WiFi es una de las tecnologías inalámbricas mediante ondas más utilizadas, convirtiéndose en una constante tecnológica en nuestras vidas. Hoy en día la mayoría de establecimientos tiene por lo menos una zona WiFi para permitir a sus clientes y usuarios tener un acceso a Internet, lo mismo pasa en los hogares, esto ha hecho a esta tecnología muy popular y conocida.

1.1.2.: EL NOMBRE WIFI

El nombre WiFi no proviene de Wireless Fidelity sino es un nombre comercial que se tomó del conocido término HiFi (High Fidelity) y así sonara común para las personas, y el fondo sobre el que descansan las letras no es otro que el símbolo oriental del yin-yang.



Fig.1.1.: Logo de Wi-Fi.

Fuente: <http://techtastico.com/post/estandares-wifi/>

1.1.3.: ESTÁNDARES QUE CERTIFICA WIFI

Todos los estándares fueron creados por una organización conocida como WiFi Alliance, la cual está compuesta por varias empresas que se interesan en promover la conexión a internet.

1.1.3.1.: Tipos de estándares:

- IEEE 802.11.- fue el primero y se creó en 1997 ahora ya está muerto, la velocidad máxima que soportaba era de 2 Mbps.
- IEEE 802.11a.- fue creado en 1999, trabaja a una frecuencia de 5 GHz y una velocidad máxima de 54 Mbps.
- IEEE 802.11b.- fue creado en 1999, trabaja a una frecuencia de 2.4 GHz y una velocidad máxima de 11 Mbps, este estándar fue el que le dio la popularidad a WiFi
- IEEE 802.11g.- fue creado en 2003, trabaja a una frecuencia de 2.4 GHz y a una velocidad de 54 Mbps este estándar trabaja hasta la fecha y es adoptado por la mayoría de las aplicaciones.
- IEEE 802.11n.- fue lanzado en 2009 es el estándar más reciente trabaja en las frecuencias de 2.4 y 5 GHz y alcanza velocidades de 600 Mbps

ESTÁNDAR	TASA DE TRANSFERENCIA	BANDA DE FRECUENCIA
802.11	2 Mbps	2.4 GHz
802.11 a	54 Mbps	5 GHz
802.11 b	11 Mbps	2.4 GHz
802.11 g	54 Mbps	2.4 GHz
808.11 n	600 Mbps	2.4 y 5 GHz

Tabla 1.1.: Tabla comparativa entre los estándares 802.11.

Fuente: Microsoft Word 2010

1.1.4.: SEGURIDAD Y FIABILIDAD

Uno de los principales problemas que enfrenta esta tecnología es la saturación del espectro radioeléctrico debido al incremento de usuarios, un elevado número de redes son instaladas sin tener en cuenta la seguridad creando redes abiertas y sin brindar protección a la información que cursa en ella.

Para mantener segura una red WiFi se puede tomar en cuenta estas recomendaciones:

- Cambiar frecuentemente la contraseña de acceso y utilizar caracteres especiales, así como mayúsculas y números.
- Cambiar el SSID que viene por defecto.
- Desactivar el Broadcasting de SSID y DHCP.
- Poner una IP fija a los dispositivos que están conectados
- Utilizar un cifrado WPA2.

Para que podamos garantizar la seguridad de las redes hay algunas alternativas, entre las más comunes podemos destacar la utilización de protocolos que realizan un cifrado de datos para estándares WiFi como WEP, WPA o WPA2, para codificar la información, a continuación un detalle de las alternativas que podemos utilizar para dar seguridad.

- WEP.- cifra los datos mediante una clave antes de ser enviados al aire, los cifrados pueden ser de 64 y 128 bits, esta seguridad no es muy aconsejable debido a que es fácil de vulnerar.
- WPA.- esta presenta mejoras en la generación de la clave ya que esta se insertan como dígitos alfanuméricos.
- La utilización de túneles IP (IPSEC) en los casos de utilización de VPNs (Redes Privadas Virtuales) y todo el conjunto de los estándares 801.1x que autoriza y autentifica a los usuarios.
- Realizar un filtrado MAC de manera que solo los dispositivos que estén autorizados puedan tener acceso a la red
- Ocultar el punto de acceso.
- Utilizar el protocolo WPA2 (estándar 802.11i) que es una mejora del WPA aunque necesita equipos compatibles.

1.1.5.: DISPOSITIVOS

Existen muchos dispositivos que utilizan la tecnología WiFi, los cuales podemos dividir en dos grupos, dispositivos de distribución de red y dispositivos terminales.

Entre los dispositivos de distribución de red encontramos los puntos de acceso, enrutadores y repetidores.

Entre los dispositivos terminales se encuentran mayoritariamente las tarjetas PCI para WiFi, las PCMCIA que son un modelo que utilizaron por primera vez los computadores portátiles y las tarjetas USB para WiFi.

1.2.: SISTEMA DE DISTRIBUCIÓN WIRELESS (WDS)

(López, 2011)” Los sistemas WDS (Wireless Distribution System) permiten conectar varios puntos de acceso de una red inalámbrica y ampliar así su cobertura. No obstante, conviene señalar que no todos los routers soportan esta tecnología, que hace que un ordenador cambie de un punto de acceso a otro sin notarlo, conservando la dirección MAC en la información enviada.”

En síntesis los sistemas de distribución Wireless permiten conectar varios puntos de acceso de una red y así se logra ampliar su cobertura, y podemos señalar que no todos los enrutadores soportan esta tecnología.

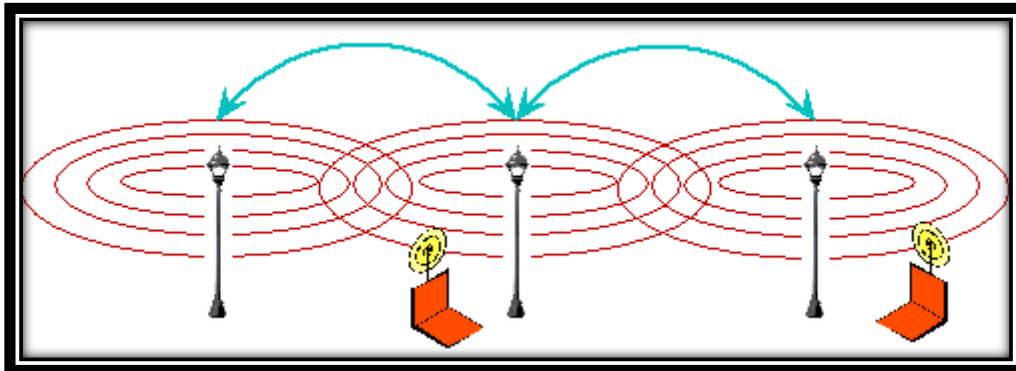


Fig.1.2.: Sistema de Distribución Wireless (WDS)

Fuente: <http://tecnovortex.com/como-mejorar-la-conexion-inalambrica-parte-4/>

1.2.1.: VENTAJAS Y PROBLEMAS WDS

Como ventajas podemos encontrar las siguientes:

- Conserva las direcciones MAC de los paquetes de los clientes a través de los distintos puntos de acceso.
- Es más fácil de configurar en relación a otros protocolos.

Pero también existen algunas desventajas como por ejemplo:

- Se reduce la velocidad de transferencia a la mitad de su magnitud en cada salto.
- No inter opera bien entre marcas de equipos, ya que no es un estándar IEEE, solamente está normado en parte.

1.2.2.: OPERACIÓN

Un sistema de distribución Wireless nos permite interconectar inalámbricamente enrutadores o puntos de acceso entre sí.

Para que se pueda establecer una comunicación entre 2 puntos de acceso o enrutadores, tenemos que verificar lo siguiente:

- Verificar si ambos aparatos soportan la función WDS (Sistema de Distribución Wireless).
- Debemos verificar que están configurados en el mismo canal, aunque es posible hacerlo con canales diferentes.
- Se debe verificar los nombres de red inalámbricos (SSID) que sean distintos, esto es para diferenciar a cuál de ellos está conectado nuestro terminal.
- Se deberá introducir en cada uno de ellos la dirección MAC del otro, con el objetivo de establecer la seguridad inalámbrica.

1.2.2.1.: Modalidades

En un Sistema de Distribución Wireless un punto de acceso puede funcionar solo como punto de acceso, como puente con otro punto de acceso o puede tener ambas funciones. Así es posible crear una gran red inalámbrica permitiendo que un punto de acceso pueda conectarse a otro disponible que use WDS y a cada punto de acceso se pueden conectar de forma cableada o inalámbrica.

Dos tipos de servicios se Pensaron cuando se diseñó el estándar 802.11

- **BSS** (Basic Service Set): solo existe un punto de acceso y una sola red inalámbrica definida por las estaciones que estén conectadas a ese único AP (Access Point).
- **ESS** (Extended Service Set): hay varios puntos de acceso y lo que interesa es que las estaciones conectadas a cualquier punto de acceso puedan interconectarse de forma transparente. El sistema que permite realizar esta interconexión es el DS (Distribution System, sistema de distribución).

1.2.3.: HAND OFF

Es necesario saber que es un hand off para poder entender como los usuarios se trasladan a través de la zona de cobertura sin perder conexión

Como definición podemos decir que (Fundación Wikimedia, Inc., 2006) Se denomina **handoff** o **traspaso** (también *handover* o transferencia) al sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente en una de las estaciones. Este mecanismo garantiza la realización del servicio cuando un móvil se traslada a lo largo de su zona de cobertura.

Si bien es una definición aplicada para la telefonía celular nos ayuda a entender muy de lo que necesita nuestra red para que el usuario no pierda conexión al trasladarse y se conecte automáticamente de un AP a otro.

1.3.: SOFTWARE LIBRE

Es muy necesario hablar de Software Libre debido a que este es el que utilizaremos en el software de nuestro servidor.

1.3.1.: INTRODUCCIÓN

(Free Software Foundation)” La definición de software libre estipula los criterios que se tienen que cumplir para que un programa sea considerado libre. De vez en cuando modificamos esta definición para clarificarla o para resolver problemas sobre cuestiones delicadas. Más abajo en esta página, en la sección Historial, se puede consultar la lista de modificaciones que afectan la definición de software libre.”

Software libre no significa gratis sino se denomina como el software que respeta la libertad de todos los usuarios que adquirieron el producto, por lo tanto, una vez obtenido el mismo el usuario puede usarlo, copiarlo, estudiarlo, modificarlo, y redistribuirlo libremente de varias formas.

1.3.2.: LIBERTADES DEL SOFTWARE LIBRE

Software libre garantiza las siguientes libertades:

LIBERTAD	DESCRIPCIÓN
0	Usar el programa con cualquier propósito
1	Estudiar el funcionamiento del programa y modificarlo con el fin de adaptarlo a sus necesidades
2	Distribuir copias del programa y así ayudar a los demás usuarios
3	Mejorar los programas y hacerlos públicos estos con sus mejoras con el fin de beneficiar a toda la comunidad.

Tabla 1.2.: Libertades del Software libre

Fuente: (Free Software Foundation)

En los numerales 1 y 3 es necesario conocer el código fuente, el software libre por definición no contempla el precio del producto, no tenemos que confundir entre libre de libertad y libre de gratis, es por eso que será común encontrar programas bajo software libre que pidan licencia y tenga un costo.

1.3.3.: TIPOS DE LICENCIAS

Se define por licencia a una autorización de forma formal con un carácter contractual que el autor otorga a un interesado para ejercer actos de explotación legales.

Existen distintos grupos de licencias.

1.3.3.1.: Licencias GPL

(GNU GPL) significa licencia publica general de GNU es una de las licencias más utilizadas. En esta licencia el autor conserva sus derechos como autor (copyright), y a su vez permite que se redistribuya y se modifique bajo términos diseñados por el autor que le permite asegurarse que las versiones modificadas de su software van a permanecer bajo los términos más restrictivos de la propia Licencia Pública General de GNU.

1.3.3.2.: Licencias AGPL

(AGPL) significa Licencia Pública General de Affero es una licencia copyleft es decir que exige que todas las versiones modificadas y extendidas de un programa sean también libres, esta se deriva de la GPL GNU.

1.3.3.3.: Licencias estilo BSD

Este tipo de Licencias son llamadas así porque utiliza una cantidad grande de software que se distribuye junto con los sistemas operativos BSD que es como se llamó a la forma de distribución del código fuente en la Universidad de Berkeley en California. El autor en este tipo de licencias mantiene una protección de derechos de autor únicamente para la renuncia de garantía y también para requerir una adecuada atribución de autoría en los trabajos derivados del suyo, pero también permite que se redistribuya y modifique libremente, incluyendo a los trabajos que tienen propietario.

1.3.3.4.: Licencias estilo MPL y derivadas

Esta licencia tiene un valor alto porque debido a que fue el instrumento que utilizo Netscape Communications Corp. para poder liberar su Netscape Communicator 4.0 y dio inicio al proyecto Mozilla. La licencia estilo MPL promueve de una forma eficaz la colaboración evitando un efecto viral como lo hace la GPL.

1.3.4.: REGULACIÓN EN ECUADOR

En el Ecuador existe un Decreto presidencial 1014 que fue expedido el 10 de abril de 2008, este nos dice que se establece una política pública para todas las entidades que realizan administración pública central a utilizar sistemas de Software Libre.

1.4.: SERVICIOS

En esta sección definiremos los servicios que serán necesarios implementar para poder cumplir con el propósito de este trabajo.

1.4.1.: FIREWALL

Firewall es un dispositivo acceso a Internet, esto para que funcione como un dispositivo de seguridad cuya función es permitir o denegar las transmisiones desde una red a otra. Típicamente se usa un Firewall al situarlo entre una red local y una red externa que es la que proporciona el que evite el acceso a intrusos hacia la información confidencial de nuestra red local.

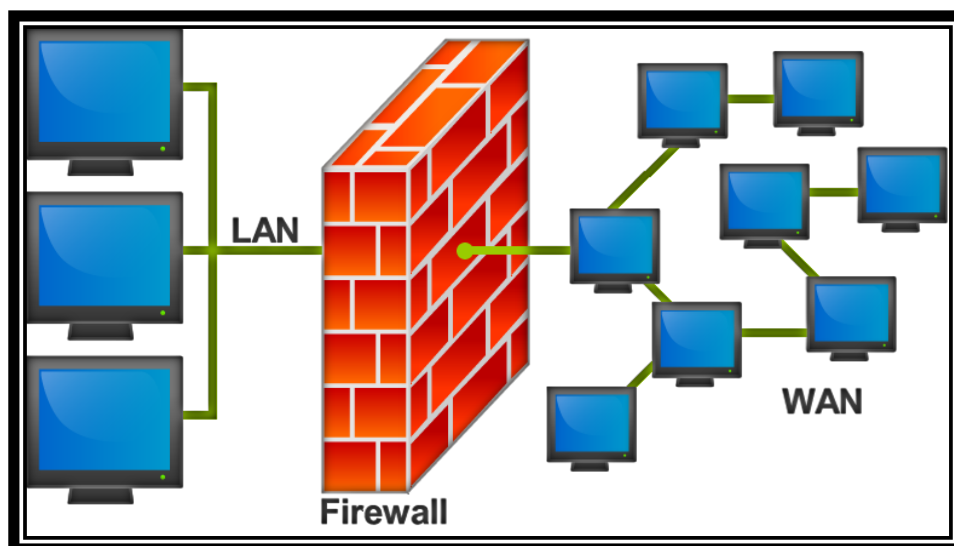


Fig.1.3.: Esquema de donde se localizaría un cortafuegos en una red de ordenadores.

Fuente: http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

1.4.1.1.: Definición de Firewall

(Álvarez, 2001)” Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.”

En resumen un firewall es un filtro que controla las comunicaciones que pasan de una red a la otra, dependiendo de los requerimientos y reglas que se le aplique permite o deniega la información que pasa por a través de este, también un firewall analiza la comunicación si es de entrada o de salida.

Un firewall puede ser de software, como un programa que se instale o un dispositivo de hardware, es decir un equipo físico que se conecte a nuestra red.

1.4.1.2.: Firewall Proxy

Es servidor Firewall Proxy se distingue de un firewall normal porque el Proxy realiza un filtrado de servicios y no solo de paquetes.

Un servidor firewall proxy es una aplicación que actúa como intermediario entre dos sistemas finales. Los servidores firewall proxy operan en la capa de aplicación del servidor de seguridad, en donde ambos extremos de una conexión se ven obligados a llevar a cabo la sesión a través del proxy. Esto lo hacen mediante la creación y ejecución de un proceso en el servidor de seguridad que refleja un servicio como si se estuviera ejecutando en el host final.

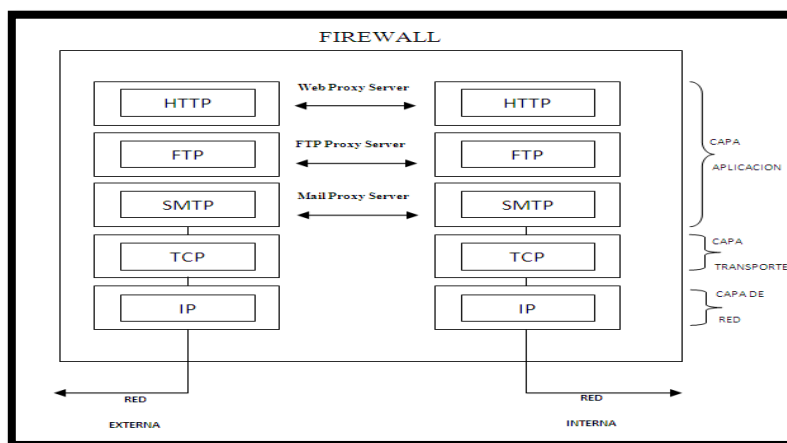


Fig.1.4.: Gráfica de firewall proxy y servicios

Fuente: http://www.akadia.com/services/firewall_proxy_server.html

Un servidor firewall proxy básicamente convierte una sesión de dos partes en una sesión de cuatro partes, con el proceso central emulando los dos host reales. Debido a que operan en la capa de aplicación, los servidores proxy también se conocen como corta fuegos de capa de aplicación. Un servicio del proxy se debe ejecutar para cada tipo de aplicación de Internet, el firewall soportará un servicio SMTP proxy para correo electrónico, un proxy HTTP para los servicios web, etc. Los servidores proxy casi siempre se los configura de un solo sentido de funcionamiento, desde la red interna a la red externa. En otras palabras, si un usuario interno quiere acceder a un sitio Web en Internet, los paquetes que componen dicha solicitud se procesan a través del servidor HTTP antes de ser enviados al sitio Web. Los paquetes devueltos desde el sitio Web a su vez son procesados a través del servidor HTTP antes de ser enviados de vuelta al servidor del usuario interno.

Dado que los servidores firewall proxy centralizan toda la actividad de una aplicación en un solo servidor, presentan una oportunidad ideal para realizar una variedad de funciones útiles. Tener la aplicación que corre en el firewall presenta la oportunidad de inspeccionar los paquetes mucho más que solo fuente direcciones y números de puerto de destino. Por eso casi todos los firewalls modernos incorporan algún tipo de arquitectura de servidor proxy. Por ejemplo, los paquetes entrantes se dirigieron a un servidor creado estrictamente para desembolsar la información (por ejemplo, un servidor FTP) pueden ser inspeccionados para ver si

contienen comandos de escritura (como el comando PUT). De esta manera, el servidor proxy podría permitir sólo las conexiones que contienen leer comandos.

1.4.2.: SERVIDOR DHCP

El protocolo DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Host) es un estándar diseñado de TCP/IP cuya función es poder simplificar la configuración del direccionamiento IP en los equipos que se encuentran en nuestra red.

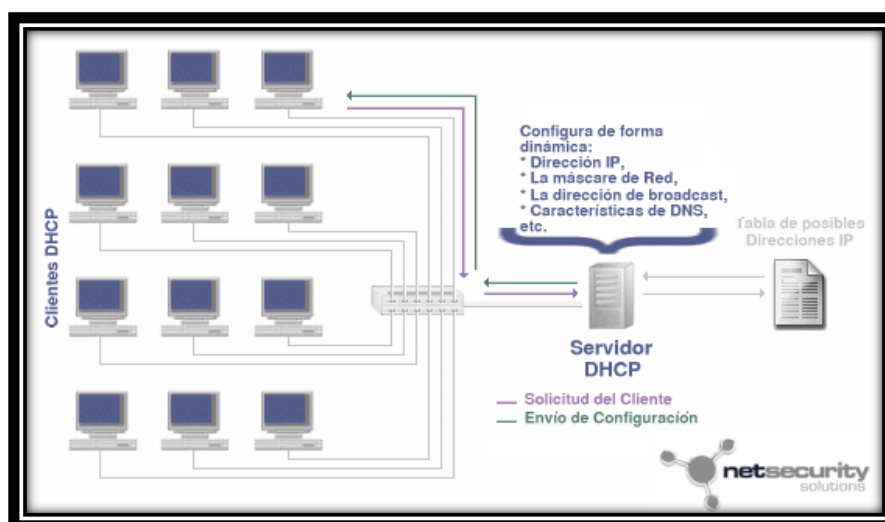


Fig.1.5.: Servidor DHCP

Fuente:http://www.netsecuritysolutionsltda.com/spanish//index.php?option=com_content&task=view&id=43&Itemid=58

1.4.2.1.: Definición

(2014 Microsoft, 2014) ” El protocolo de configuración dinámica de host (DHCP, <i>Dynamic Host Configuration Protocol</i>) es un estándar IP diseñado para simplificar la administración de la configuración IP del host.”

El estándar DHCP nos permite usar servidores DHCP con la finalidad de administrar la asignación dinámica de direcciones IP a los clientes DHCP de nuestra red, para utilizar este servicio los clientes deben estar configurados para utilizar DHCP.

Todo equipo que pertenece a una red TCP/IP debe tener una dirección IP única así como también un nombre único. DHCP nos permite asignar de forma dinámica una dirección IP a un cliente, las direcciones se encuentran en una base de datos la cual contiene las direcciones IP del servidor.

1.4.2.2.: Asignación de direcciones IP

Existen tres métodos de asignación de direcciones que están incluidas en el protocolo DHCP:

- **Método de asignación anual o asignación estática:** este método asigna una dirección IP a un cliente determinado. Este método se utiliza cuando se necesita controlar la asignación de dirección IP a cada uno de los clientes, y también evitar que se conecten clientes no están identificados.
- **Método de asignación automática:** este método asigna una dirección de manera permanente a un cliente cuando este realiza por primera vez una solicitud al servidor DHCP y la mantiene asignada hasta que el cliente libere esta dirección. Este método se utiliza cuando el número de clientes no varía demasiado.
- **Asignación dinámica:** este método permite reutilizar dinámicamente las direcciones. En este método existe un administrador de red es que determina los rangos de direcciones IP que se utilizara así como los dispositivo conectados.

1.4.2.3.: Parámetros configurables

El servidor DHCP puede proveer al cliente algunas configuraciones opcionales, entre las opciones más destacadas están las siguientes:

- La dirección IP del servidor DNS
- El nombre del dominio DNS

- La puerta de enlace.
- La dirección de Broadcast de la red
- Máscara de subred
- El tiempo máximo de espera de solicitudes ARP
- MTU para la interfaz
- Servidores NIS
- Dominios NIS
- Servidores NTP
- Servidor SMTP
- Servidor TFTP
- Nombre del servidor WINS

1.4.3.: PORTAL CAUTIVO

Un portal cautivo puede ser un programa o una máquina cuya función en la red es vigilar el tráfico HTTP en la red y obliga los usuarios de la red a ir por una página específica si estos desean navegar por Internet.

Un Portal Cautivo intercepta todo el tráfico HTTP y solicita una autenticación este se encargara de permitir establecer una sesión y que esta caduque al transcurrir un tiempo, además también puede controlar el uso del ancho de bando que cada cliente puede usar brindando Calidad de Servicio.

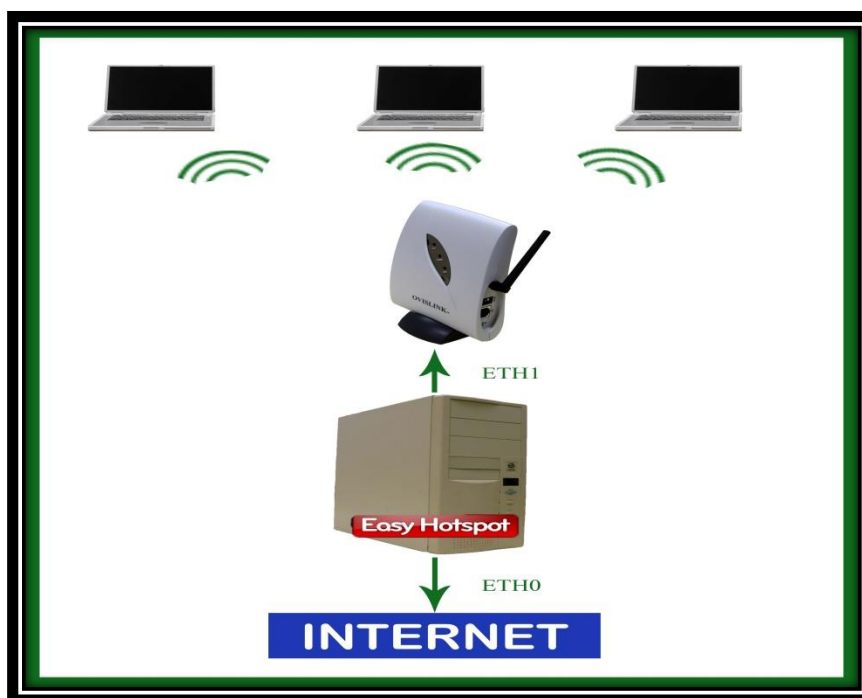


Fig.1.6.: Conexión del Portal Cautivo

Fuente: <http://recursostic.educacion.es/observatorio/web/fr/equipamiento-tecnologico/redes/1005-como-crear-tu-portal-cautivo-con-easy-hotspot>

1.4.3.1.: Usos

Un Portal Cautivo es usado en redes inalámbricas abiertas, donde nos interese mostrar un mensaje, sea este de bienvenida a los usuarios o para informar las condiciones del acceso, además se usa en redes donde se permite un tiempo de sesión determinado o controlar el tiempo que los usuarios están conectados, así como el ancho de banda que usan.

1.4.3.1.1.: Portales Cautivos por software

Un Portal Cautivo por software es un programa instalado en un equipo, estos pueden ser bajo software libre o no, aquí algunos:

- PepperSpot (Linux)
- NoCatAuth (Linux)

- Chillispot (Linux)
- CoovaChilli (Linux)
- WifiDog (embedded Linux - OpenWRT, Linux, Windows)
- Ewrt (embedded Linux - WRT54G, Linux)
- HotSpotSystem.com (embedded Linux, WRT54GL, Mikrotik, etc)
- FirstSpot (Windows)
- m0n0wall (embeddedFreeBSD)
- OpenSplash (FreeBSD)
- wicap (OpenBSD)
- Public IP (Linux)
- PfSense (FreeBSD)
- AirMarshal (Linux)
- AntamediaHotSpot Billing Software (Windows)
- ZeroShell (Linux)
- Easy Captive (Linux)
- Microsolut Professional HotSpot Software (Windows)

1.4.3.1.2.: Portales Cautivos por Hardware

Un Portal Cautivo por Hardware es en sí un equipo que cumple con estas funciones, a continuación algunos de ellos:

- Cisco BBSM-Hotspot
- Cisco Site Selection Gateway (SSG) / Subscriber Edge Services (SESM)
- NomadixGateway
- AntamediaHotspot Gateway
- AtiloAccess Gateway
- AnticaPayBridge: SolucionCarrier-class para redirección de usuarios 3/4G, Wimax, xDSL, Wifi.
- 4ipnet Hotspot Gateway

1.4.4.: FIBRA ÓPTICA

Es necesario hablar sobre la fibra óptica como medio de transmisión de datos, ya que, la red de nuestro proyecto esta implementada sobre este medio de transmisión.

1.4.4.1.: Introducción

Este es un medio de transmisión de datos, está compuesto de por un hilo de material transparente y de espesor muy fino, este puede ser vidrio o materiales plásticos, a través el cual se transmiten los datos en forma de pulsos de luz. El haz de luz se propaga por el interior de la fibra, el haz de luz puede ser emitido por medio de un láser o un LED.

1.4.4.2.: Características

El funcionamiento de la fibra óptica se basa en transmitir un haz de luz por el núcleo de la misma, impidiendo que atraviese el revestimiento, esto permite que se refleje y se propague a lo largo de la fibra, algunas de las características destacables de la fibra óptica son:

- Posee una cobertura más resistente a la de otros medios de transmisión.
- Tiene una gran resistencia contra el agua y las emisiones ultravioletas.
- Posee una mayor protección para lugares húmedos.
- Su empaquetado es de alta densidad.

1.4.4.3.: Ventajas

- Mayor Ancho de Banda, lo que permite velocidades en el orden del GHz (Giga Hertz).
- Pequeño tamaño.
- Gran flexibilidad.
- Gran ligereza.
- Total inmunidad a perturbaciones de origen electromagnético.
- Gran seguridad.

- No produce interferencias.
- Insensibilidad a señales parásitos
- La atenuación es muy pequeña.
- Gran resistencia mecánica.
- Gran resistencia a la corrosión, el frío y el calor.
- Una gran facilidad para localizar los cortes en la fibra.
- Tiene un coste menor con respecto al coste del cobre.
- Factores ambientales.

1.4.4.4.: Desventajas

Si bien hemos visto que tiene una gran cantidad de ventajas, también existen algunas desventajas en relación con otros medios de transmisión:

- Es muy frágil.
- Necesita el uso de transmisores y receptores con un alto costo económico.
- Existen mayor complejidad al momento de realizar los empalmes entre fibras.
- No transmite electricidad y no puede alimentar repetidores intermedios.
- La necesidad de realizar procesos en los cuales se realice una conversión eléctrica-óptica.
- La fibra óptica convencional no puede transmitir potencias elevadas.
- No existen memorias ópticas.
- La fibra óptica no transmite energía eléctrica.

1.4.4.5.: Fibra multimodo

Es aquella por la cual los haces de luz circula por varios caminos. Las aplicaciones para fibras multimodo son para corta distancia, esto quiere decir menores a 2 km, es mucho más sencillo y económico de diseñar.

Dependiendo cual sea el tipo de índice de refracción del núcleo de la fibra óptica, tenemos estos tipos:

- Índice escalonado: la refracción es constante a lo largo de la fibra.
- Índice gradual: la refracción no es constante a lo largo de la fibra.

1.4.4.6.: Fibra monomodo

Es una fibra óptica que sólo propaga un modo de luz. Permite alcanzar mayores distancias a las de la multimodo, hasta 400 km máximo.

1.4.5.: TRANSCEIVERS

(WIKIPEDIA, 2014) Un transceiver es un dispositivo que comprende tanto un transmisor y un receptor que se combinan y comparten circuitos comunes o una única carcasa. Cuando no hay circuitos es común entre las funciones de transmisión y recepción, el dispositivo es un receptor-transmisor.

Tenemos que tener en cuenta la utilización de transceiver siempre que utilicemos diferentes medios de transmisión, estos nos ayudarán a poder acoplar las distintas tecnologías y que la comunicación sea transparente.

1.4.6.: ACCESS POINT

(INFORMATICA MODERNA) Se trata de un dispositivo utilizado en redes inalámbricas de área local una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

En resumen un Access Point es un dispositivo utilizado en redes inalámbricas que permite el acceso a la red local en un lugar específico de la red.

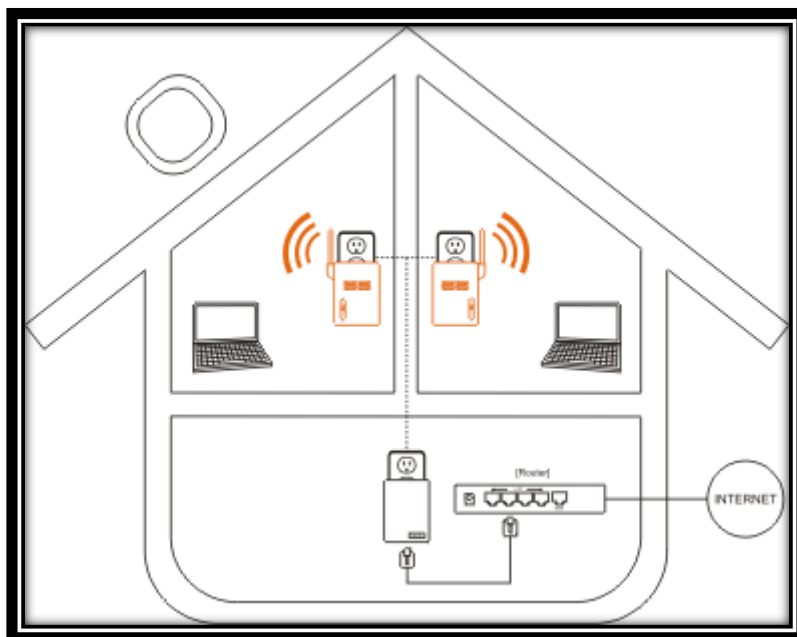


Fig.1.7.: Access Point

Fuente: http://www.gigafast.com/products/wireless_access_point.html

1.4.7.: SWITCH

(WIKIPEDIA, 2014) Un conmutador o switch es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

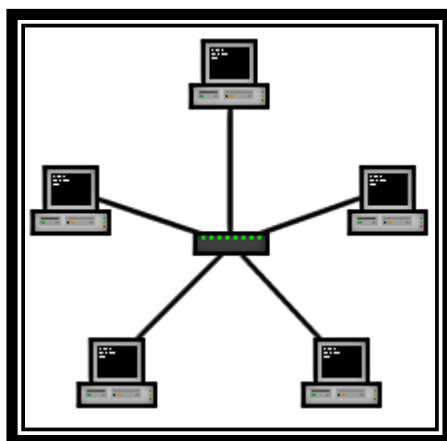


Fig.1.8.: Un conmutador en el centro de una red en estrella.

Fuente: http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

CAPÍTULO 2.: LEVANTAMIENTO DE INFORMACIÓN GEOGRÁFICA

En este capítulo se realizara un estudio de nuestra zona de cobertura para determinar la cobertura de nuestra red y además identificar posibles problemas que pudieran interferir con el correcto funcionamiento de nuestra red.

2.1.: ESTUDIO DE LA ZONA DE COBERTURA

Es importante realizar un estudio de nuestra zona de cobertura para así poder conocer la situación inicial y definir correctamente el diseño de nuestra red de acceso, esto permitirá que se tome decisiones correctas en nuestra red.

Zona de cobertura podemos decir que es la porción del territorio donde se despliegan las fuerzas de la cobertura para proporcionar seguridad a las operaciones estratégicas previas a la realización de la maniobra (movilización, concentración y despliegue estratégico).

2.1.1.: SITUACIÓN INICIAL

La ciudad de Ibarra se encuentra en un proceso de conectividad, para lo cual se han puesto en marcha algunos proyectos cuyo fin en crear una ciudad que permita el acceso a sus habitantes a la información de manera gratuita y rápida.

En la ciudad de Ibarra existe un tendido de fibra óptica que interconecta algunos nodos que se encuentran en nuestra zona de cobertura, la cual está delimitada por las calles:

- Sánchez y Cifuentes
- Gabriel García Moreno
- Vicente Rocafuerte
- Cristóbal Colón

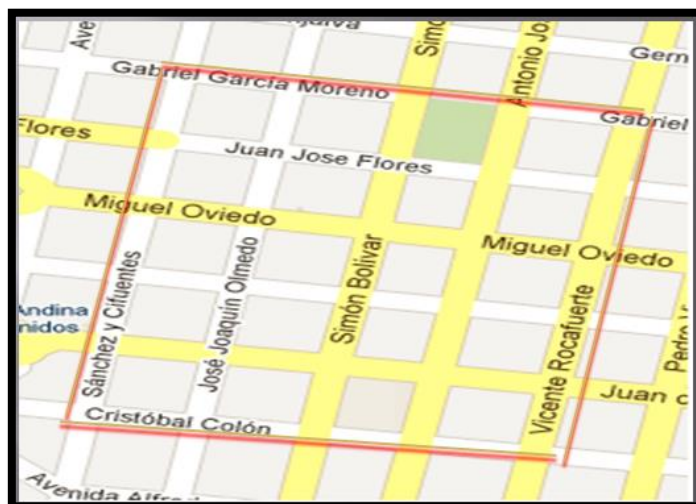


Fig.2.1.: Zona de Cobertura

Fuente: www.google.com.ec

En esta zona existen 3 nodos por los cuales atraviesa esta fibra óptica como a continuación se ve en la figura.

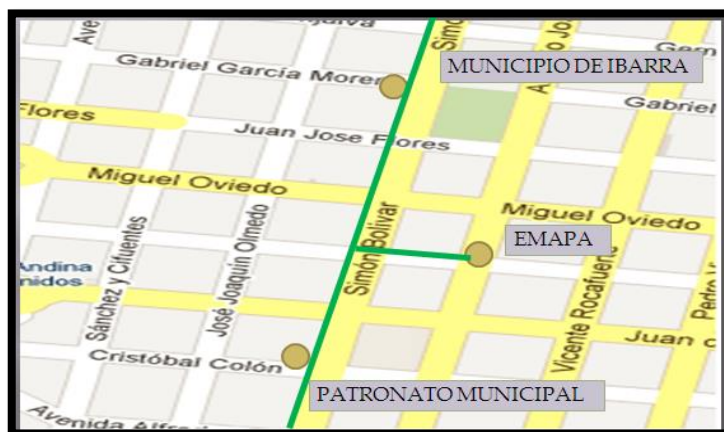


Fig.2.2.: Fibra Principal

Fuente: www.google.com.ec

A partir de estos nodos se tienden 3 anillos más los cuales darán cobertura a toda la zona.

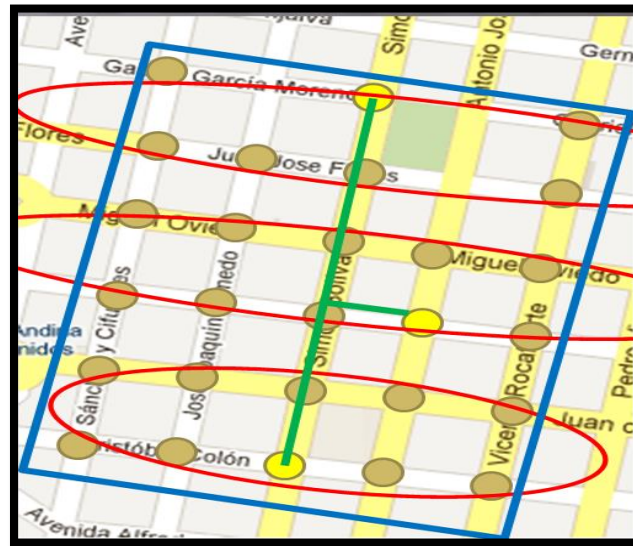


Fig.2.3.: Numero de Nodos en la Zona de Cobertura

Fuente: www.google.com.ec

Como podemos ver en la figura tenemos 27 nodos en nuestra zona de cobertura sobre el cual trabajaremos para realizar nuestro diseño.

Existe un Switch en cada nodo al cual llega la fibra óptica y se interconecta en forma de anillo con el siguiente, este Switch está instalado para el proyecto de semaforización del GAD de San Miguel de Ibarra por lo que para nuestro diseño solo necesitaremos el Access Point y conectarlo al Switch en un puerto designado.

2.1.2.: ZONAS DE INTERFERENCIA

Una zona de interferencia es una zona donde se emiten señales de las mismas características a las señales que emite nuestra red y estas pueden interferirse entre ellas provocando fallos en nuestra red.

Para detectar posibles zonas de interferencias utilizaremos un software llamado insSSIDer 3 de METAGEEK el cual utiliza la tarjeta wireless para determinar el espectro de las redes inalámbricas, el canal en el cual están trabajando, el SSID, el max rate, el fabricante del modem, la señal, el tipo de seguridad que posee, la dirección MAC y el estándar 802.11, con este software nos situaremos en cada nodo y

determinaremos las frecuencias y los canales en los que se encuentran trabajando las redes privadas instaladas en nuestra zona de cobertura y con esta información determinaremos como configurar nuestros equipos para que no sufran ningún tipo de interferencia.

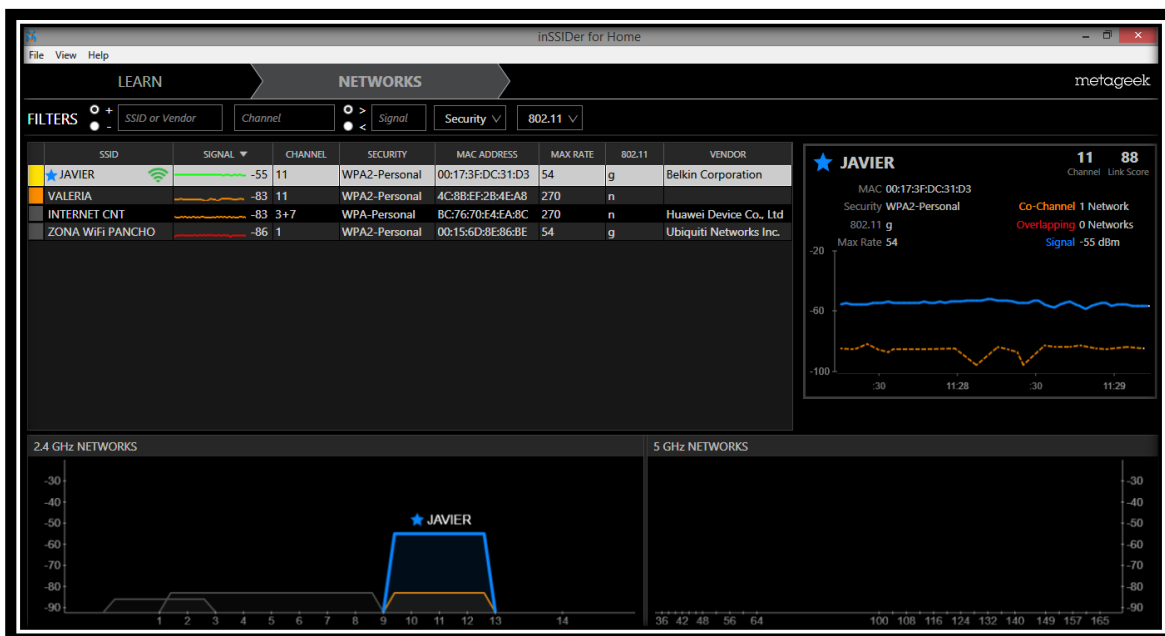


Fig.2.4.: Interfaz de insSSIDer 3

Fuente: insSSIDer 3

Podemos observar los resultados en el ANEXO A, a continuación se mostrara un análisis de los resultados.

Se hizo un barrido de las redes inalámbricas en cada nodo de nuestra zona y podemos observar que existen una gran cantidad de redes inalámbricas por cada zona, en el ANEXO A se muestran las 14 redes con más potencia y que podrían interferir en nuestra red.

El estudio que se ha hecho nos ha arrojado algunos datos importantes los cuales enumeraremos a continuación:

- Los canales que las redes inalámbricas en nuestra zona más trabajan son el 11 y el 6, debido a que la mayor parte de personas tienen contratado su servicio de internet con Claro o con CNT y ellos trabajan en estos canales como predeterminados.

- La red del municipio (ibarradigital) a la q también se acoplara nuestra red trabaja en el canal 4.
- Los estándares IEEE 802.11 más utilizados en nuestra zona son el IEEE 802.11 g y IEEE 802.11 n.
- No existe ninguna red que trabaje a 5 GHz, todas trabajan a 2.4 GHz.

2.1.3.: PROBLEMAS

Podemos observar que según los datos obtenidos podemos tener problemas de solapamiento de canal ya que en especial el canal 11 está muy saturado y necesitamos trabajar en un canal diferente para poder prevenir este problema.

Utilizaremos el mismo SSID en todos los AP para evitar problemas de conexión cuando el usuario se mueva de un nodo a otro y esto será solucionado con la configuración de los APs en modo WDS.

Se trabajara en el mismo canal que trabajan los APs de (ibarradigital) y para que no se tenga ningún problema con la conexión de los usuarios se trabajara a 2.4 GHz.

2.2.: USUARIOS

Para determinar el número de usuarios hemos planteado una observación de campo, donde nos situaremos en los nodos más concurridos, como son:

- Simón Bolívar y Miguel Oviedo.
- Sánchez y Cifuentes y Cristóbal Colón.
- José Joaquín de Olmedo y Pedro Moncayo.
- Simón Bolívar y Cristóbal Colón.
- Sánchez y Cifuentes y Miguel Oviedo.

Esta información ha sido dada por el departamento de TIC's del GAD de San Miguel de Ibarra, el levantamiento de información lo realizaremos en 3 horarios, de 8H00 a 10H00, de 14H00 a 15H00 y de 17H00 a 18H00, estos horarios también nos han proporcionado ya que son los horarios de más afluencia de gente en la zona de cobertura es decir son las horas donde más personas circulan en el centro de Ibarra según

información proporcionada por el departamento de TIC's del GAD de San Miguel de Ibarra, y mediante un conteo visual determinaremos un promedio de usuarios que se encuentran constantes en cada nodo.

A continuación podemos ver las tablas con los datos levantados en el ANEXO E.

#	NOMBRE DE LA CALLE
1	Simón Bolívar y Miguel Oviedo
2	Sánchez y Cifuentes y Cristóbal Colón
3	José Joaquín de Olmedo y Pedro Moncayo
4	Simón Bolívar y Cristóbal Colón
5	Sánchez y Cifuentes y Miguel Oviedo

Tabla 2.1.: Datos de Usuarios Nomenclatura de Calles

Fuente: Microsoft Excel 2010.

LUNES			
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00
1	27	29	31
2	34	33	36
3	22	21	18
4	26	24	33
5	28	26	30

Tabla 2.2.: Datos de Usuarios Día Lunes

Fuente: Microsoft Excel 2010.

MARTES			
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00
1	26	28	33
2	33	33	35
3	26	27	19
4	25	26	28
5	24	25	31

Tabla 2.3.: Datos de Usuarios Día Martes

Fuente: Microsoft Excel 2010.

MIÉRCOLES			
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00
1	25	28	31
2	31	30	32
3	29	30	30
4	28	25	20
5	21	20	18

Tabla 2.4.: Datos de Usuarios Día Miércoles

Fuente: Microsoft Excel 2010.

JUEVES			
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00
1	26	28	30
2	33	34	35
3	21	22	19
4	25	28	36
5	28	26	28

Tabla 2.5.: Datos de Usuarios Día Jueves

Fuente: Microsoft Excel 2010.

VIERNES			
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00
1	27	30	34
2	34	32	36
3	20	19	20
4	25	24	27
5	26	29	28

Tabla 2.6.: Datos de Usuarios Día Viernes

Fuente: Microsoft Excel 2010.

En la siguiente tabla podemos observar los resultados de la observación, en donde se ha determinado un promedio de 28 usuarios por nodo dándonos un total de 756 usuarios promedio en nuestra red.

RESULTADOS			
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00
1	26,2	28,6	31,8
2	33	32,4	34,8
3	23,6	23,8	21,2
4	25,8	25,4	28,8
5	25,4	25,2	27
PROMEDIO 5 NODOS	26,8	27,08	28,72
PROMEDIO 3 HORARIOS	27,53333333		
PROMEDIO POR NODO	28		
TOTAL USUARIOS	756		

Tabla 2.7.: Datos de Usuarios Resultados

Fuente: Microsoft Excel 2010.

CAPITULO 3.: PLANEACIÓN DE LA RED

3.1.: NODO

Cada nodo está constituido del Access Point y un Switch que como explicamos en la situación inicial interconecta con el anillo fibra óptica como se muestra en la Fig. 3.1

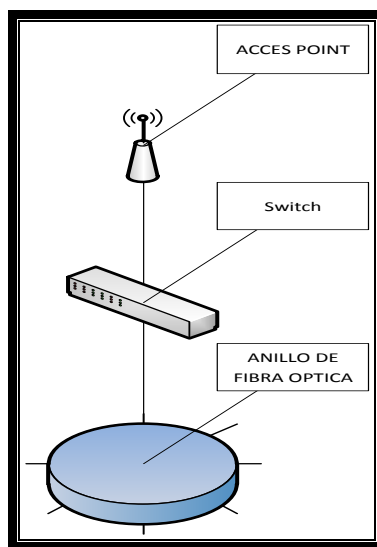


Fig.3.1.: Detalle del Nodo

Fuente: Microsoft Visio 2010

Para determinar los nodos hemos tomado en cuenta el alcance que tienen los APs que es de 180 metros y la ubicación de los semáforos inteligentes ya que estos están conectados a la red de fibra óptica que se conectara nuestros APs, como resultado hemos definido los siguientes nodos como necesarios para poder dar cobertura a toda nuestra zona de cobertura.

A continuación vamos a detallar el lugar donde se encontrara cada nodo, será en plena intersección de las calles para no tener edificaciones que bloqueen la señal de los APs, en la siguiente gráfica podemos observar nuestros nodos y en la tabla el nombres de las calles.



Fig.3.2.: Nodos

Fuente: www.google.com.ec

# NODO	DIRECCIÓN
1	Sánchez y Cifuentes y García Moreno
2	Sánchez y Cifuentes y Juan José Flores
3	Sánchez y Cifuentes y Miguel Oviedo
4	Sánchez y Cifuentes y Pedro Moncayo
5	Sánchez y Cifuentes y Juan de Velasco
6	Sánchez y Cifuentes y Cristóbal Colón
7	José Joaquín Olmedo y Juan José Flores
8	José Joaquín Olmedo y Miguel Oviedo
9	José Joaquín Olmedo y Pedro Moncayo
10	José Joaquín Olmedo y Juan de Velasco
11	José Joaquín Olmedo y Cristóbal Colón
12	Simón Bolívar y García Moreno
13	Simón Bolívar y Juan José Flores
14	Simón Bolívar y Miguel Oviedo

15	Simón Bolívar y Pedro Moncayo
16	Simón Bolívar y Juan de Velasco
17	Simón Bolívar y Cristóbal Colón
18	Antonio José de Sucre y Miguel Oviedo
19	Antonio José de Sucre y Pedro Moncayo
20	Antonio José de Sucre y Juan de Velasco
21	Antonio José de Sucre y Cristóbal Colón
22	Vicente Rocafuerte y García Moreno
23	Vicente Rocafuerte y Juan José Flores
24	Vicente Rocafuerte y Miguel Oviedo
25	Vicente Rocafuerte y Pedro Moncayo
26	Vicente Rocafuerte y Juan de Velasco
27	Vicente Rocafuerte y Cristóbal Colón

Tabla 3.1.: Dirección de los nodos.

Fuente: Microsoft Word 2010.

3.2.: EQUIPOS

Se han tomado en cuenta para este proyecto se han determinado 3 marcas de fabricantes que se encuentran en nuestro mercado y tienen soporte, las marcas a las cuales haremos el estudio para determinar cuál de ellas es la más indicada para utilizar en nuestro diseño son : Cisco Systems, Ubiquiti Networks y MikroTik.

Utilizaremos la norma IEEE Std 830-1998 que se basa en especificaciones de software para hacer un análisis de los fabricantes y los equipos que estos disponen en el mercado.

El documento se hizo según las necesidades y especificaciones del diseño (vea

ANEXO B).

A continuación se muestra una tabla comparativa entre equipos de las 3 marcas antes mencionadas donde comparamos algunos parámetros importantes para para este proyecto,

PARÁMETROS\MARCAS	CISCO (AIRONET)	MICROTIK(BA SE BOX 2)	UBIQUITI(UNIFI AP OUTDOOR++)
FRECUENCIA WDS	2,4 Y 5 GHz UTILIZANDO LAN CONTROLLER	2,4 GHZ NO	2.4 GHZ SI
POE SOFTWARE DE ADMINISTRACIÓN	SI UTILIZANDO LAN CONTROLLER	SI NO	SI SI
ESTÁNDARES WIRELESS LICENCIA	802.11 B/G/N ADQUIRIR	802.11 B/G/N ADQUIRIR	802.11 B/G/N NO NECESITA

Tabla 3.2.: Tabla comparativa de Equipos.

Fuente: Microsoft Excel 2010.

Según las necesidades se ha decidido utilizar el siguiente equipo, tomando en cuenta que la red sobre la que se va a implementar nuestro diseño ya consta con algunos equipos y tomando en cuenta el un parámetro muy importante que es el de administración y licencias.

- **Acces Point Outdoor**

Es compatible con 802.11n a 2,4 GHz, con velocidades de hasta 300 Mbps y un alcance de hasta 183 metros.

Aísla las señales en el canal de funcionamiento y elimina la interferencia de anal adyacente. La capacidad inalámbrica y el rendimiento se incrementan en áreas de alta densidad y múltiples puntos de acceso pueden operar en las proximidades.

El sistema Wi-Fi de empresa UniFi es una solución de punto de acceso empresarial escalable diseñado para ser desplegado y gestionado fácilmente, incluye el software del controlador de UniFi que se puede acceder fácilmente a

través de cualquier navegador web estándar. El software se instala en cualquier Windows, Mac, o Linux.

El software del controlador de UniFi se incluye con cada punto de acceso, es decir no hay licencia o suscripción costos adicionales de software necesarios para utilizar el controlador de UniFi.



Fig.3.3.: UniFi AP Outdoor+

Fuente: <https://store.ubnt.com/unifi/unifi-ap-outdoor-plus.html>

3.2.1.: UBICACIÓN DE LOS EQUIPOS

Cada nodo de nuestra red contara con el mismo hardware, por lo que se detallarán los equipos necesarios en los nodos, y en el Data Center.

En cada nodo:

- Access Point
- Switch

En el Data Center:

- Switch
- Servidor

3.2.2.: LISTADO DETALLADO DE EQUIPOS

A continuación vamos a realizar un listado detallado de los equipos que conformarían nuestro diseño tomando en cuenta los que a están instalados y posee el GAD de San Miguel de Ibarra, empezaremos desde el AP hasta el servidor que se encuentra en el Data Center del GAD de San Miguel de Ibarra.

- 27 Access Point Outdoor con POE.
- 27 Switch de 24 puertos con 2 SPF (estos equipos ya están en la red).
- 54 transivers de Fibra Óptica para los Switch (estos equipos ya están en la red).
- Un servidor tipo Blade (estos equipos ya están en la red).

3.2.3.: LISTADO DETALLADO DE SOFTWARE

En esta sección veremos todo el software necesario para este diseño, en su totalidad el software usado es con licencias libres por lo que podremos instalar todo el software sin condiciones.

- Ubuntu Server 12.04
- Interfaz Gráfica Webmin
- Firewall Shorewall
- Squid Proxy
- EasyHotSpot
- Software UniFi de Ubiquiti

CAPITULO 4.: DISEÑO DE LA RED

En este capítulo detallaremos nuestro diseño indicando la topología y la forma de conexión de los equipos.

4.1.: TOPOLOGÍA

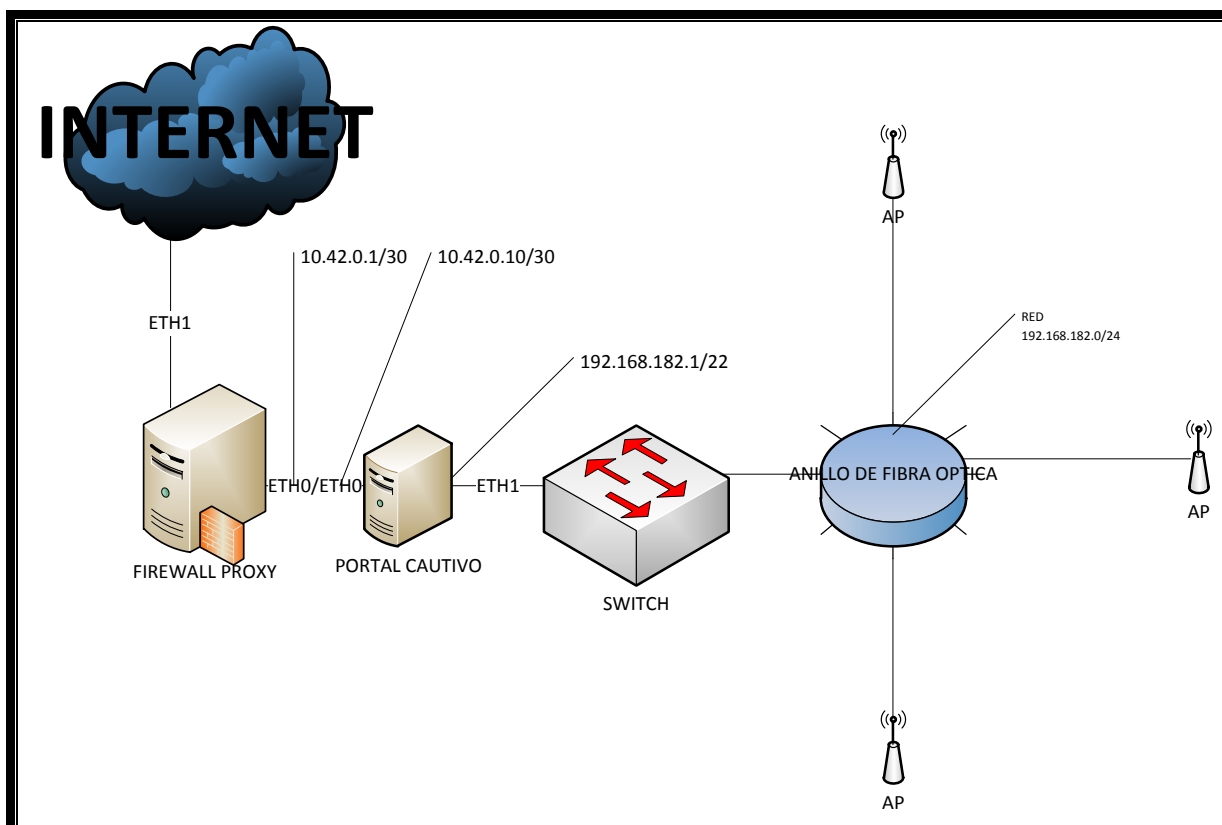


Fig.4.1.: Topología de Red

Fuente: Microsoft Visio 2010

En la topología mostramos los equipos que utilizará nuestro diseño tomando en cuenta que el anillo de fibra óptica ya está instalado.

Los Access Point (AP) son para exteriores y soportan la tecnología 802.11 a/b/g y n los cuales estarán configurados con el mismo SSID, la configuración se muestra en el ANEXO C.

Todos los AP son interconectados a través del anillo de fibra óptica que se concentra en el Data Center del GAD se San Miguel de Ibarra este anillo llega a un Switch el cual ya se encuentra en el Data Center este se conectara a nuestro servidor el cual contendrá el Firewall Proxy y Virtualizado el Portal Cautivo de tal forma que se conecten como indica la topología, es decir la red a la cual pertenecen los APs llegue por la interfaz del portal cautivo externa, el Firewall Proxy y el Portal estarán conectados en una red interna entre si y el Firewall Proxy se conectara a la red del municipio de donde obtendrá el acceso a internet.

A continuación mostraremos la tabla de direccionamiento.

TABLA DE DIRECCIONAMIENTO			
Nombre del Equipo	Interfaz	Dirección IP/CIDR	Mascara de Red
Firewall Proxy	ETH 0	Asignada por DHCP	Asignada por DHCP
Firewall Proxy	ETH 1	10.42.0.1	255.255.255.252
Portal Cautivo	ETH 0	10.42.0.2	255.255.255.252
Portal Cautivo	ETH 1	192.168.182.1	255.255.252.0

Tabla 3.3.: Tabla de Direccionamiento.

Fuente: Microsoft Word 2010.

Podemos Observar en la tabla de direccionamiento que la interfaz ETH 0 del Firewall Proxy está asignada por DHCP esto es porque todavía no está asignada por el administrador del departamento de TIC's del GAD de San Miguel de Ibarra, es por eso que tenemos asignado por DHCP para poder tener acceso a Internet.

La interfaz ETH 1 del Firewall Proxy y la ETH 0 del Portal Cautivo están directamente conectadas y utilizan la red 10.42.0.0/30 y por último la ETH 1 del Portal Cautivo está asignada la 192.168.182.1/22.

4.2.: DETALLE POR NODO

Los 27 nodos son iguales así que detallaremos un nodo para que se entienda cada uno.

Ubicación: se ubicará en el soporte del semáforo para que se encuentre en una zona central del nodo

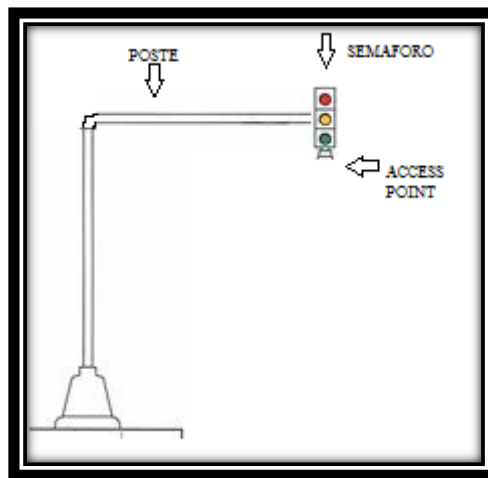


Fig.4.2.: Ubicación del Acces Point en Poste

Fuente: Paint

Conexión: el cable UTP cat 6A será enviado por el interior del poste hacia el Switch que se encuentra en cada nodo. Tenemos que tener en cuenta que cada AP se energiza con POE (Power over Ethernet).

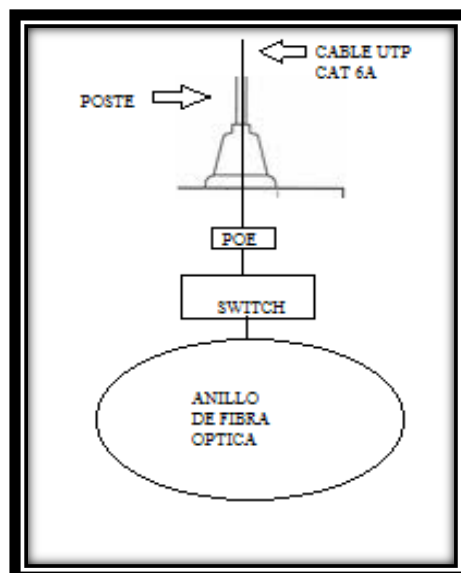


Fig.4.3.: Conexión con el anillo de Fibra Óptica

Fuente: Paint

4.2.1.: ZONAS DE COBERTURA

Cada Access Point tiene un rango de 183 metros siendo suficiente uno central en cada nodo para cubrir con toda nuestra zona de cobertura como se muestra en el diagrama.

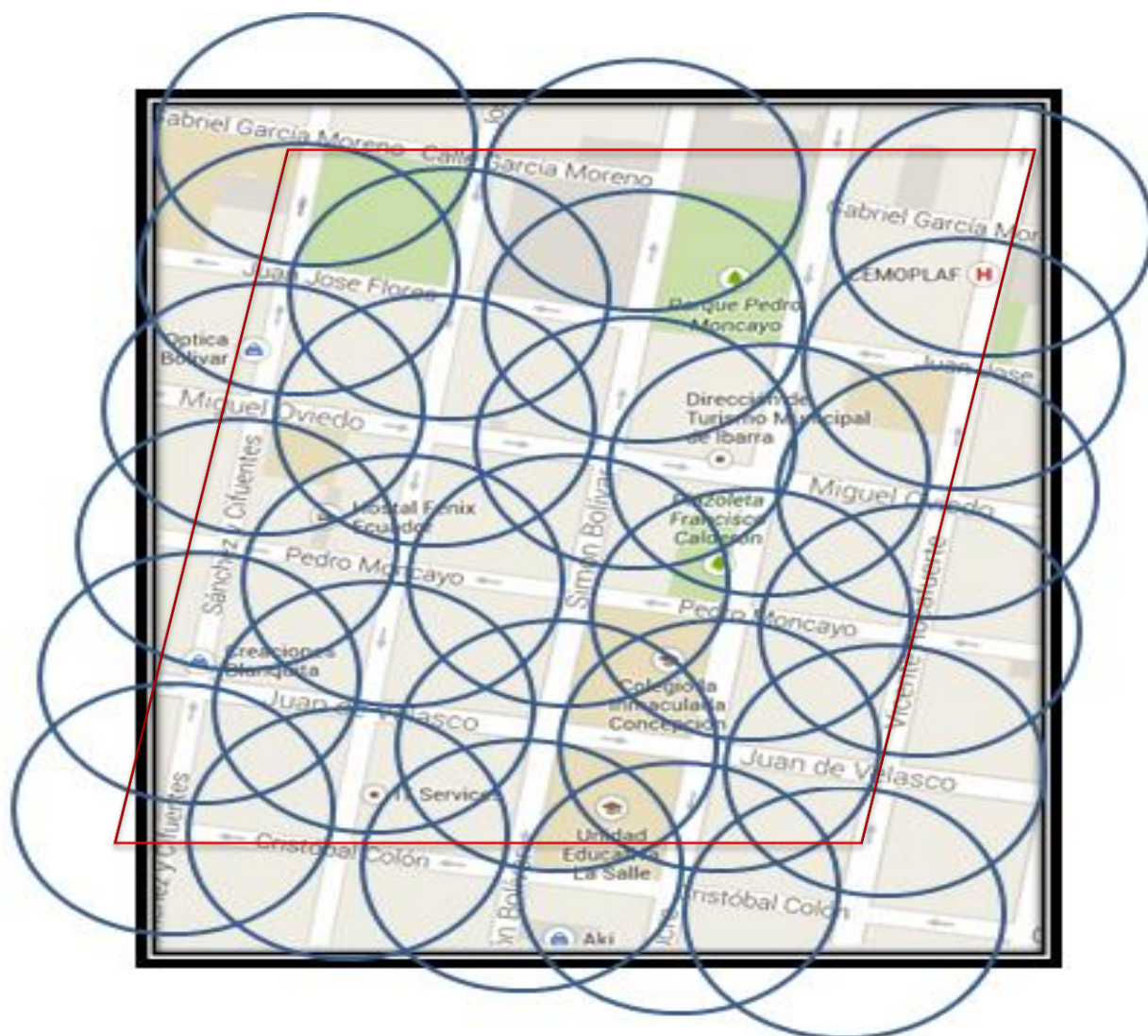


Fig. 4.4.: Zona de Cobertura

Fuente: Google Maps

Es importante que cada Access Point este asociado a mínimo dos Access Point para que nuestra red de APs pueda utilizar WDS y que formen una malla tipo full mesh como podemos ver a continuación en la figura 4.5.



Fig. 4.5.: Conexión tipo malla de los APs

Fuente: Microsoft Visio 2010

4.3.: SERVIDOR

En esta sección vamos a describir el software que se instalará en nuestro servidor, incluyendo un detalle de cada uno. Para las pruebas se ha montado los servidores en Máquina Virtual para poder simular el funcionamiento de nuestra red.

4.3.1.: SISTEMA OPERATIVO

Para este diseño se ha seleccionado Ubuntu Server 12.04 como el sistema operativo que vamos a usar tal y como se solicita en el Anexo C, a continuación sus características más importantes:

- Entorno de escritorio GNOME 3.2, con algunos paquetes de GNOME 3.4. Interfaz Unity personalizable.
- 100% accesible.
- Centro de control más limpio.
- Mejoras a Mozilla Thunderbird.
- Reproductor de música Rhythmbox.
- Proceso de arranque sin parpadeos.
- Mejorada la velocidad del arranque.
- Mejorado el soporte para múltiples monitores.
- Python 3.2 y 2.7.
- Mejorado el soporte para plataformas ARM.
- Mejoras a las imágenes nube de cloud-init, cloud-utils.
- Mejorado Orchestra.
- Implementación de la producción en Juju.
- Gestión de la energía en la nube y proyecto Cloud-Live.

Para ver la instalación del sistema operativo de una manera detallada y gráfica vea el Manual de Administrador.

4.3.2.: WEBMIN

Hemos seleccionado este software para este proyecto para poder cumplir con los requerimientos solicitados en el Anexo C que nos pide que el software tenga una interfaz gráfica y sencilla

Webmin es una herramienta que nos permite administrar sistemas Linux de una manera gráfica a través de una interfaz web. Podemos utilizar cualquier navegador web para tener acceso a la administración como son cuentas de usuarios y algunos servicios instalados en nuestro equipo sin tener la necesidad de ir a los archivos de configuración y editarlos manualmente, además nos permite un manejo remoto del equipo

La instalación de Webmin ha sido hecha en nuestro sistema operativo Ubuntu server con la finalidad de administrar nuestro servidor, es decir nuestro Firewall Shorewall y Squid Proxy.

La instalación de Webmin podemos ver en el Manual de Administrador.

4.3.3.: FIREWALL SHOREWALL

Shorewall es una herramienta robusta de alto nivel para configurar firewalls. Shorewall a diferencia de iptables necesita solo de datos y éste se encargara de crear las reglas de nuestro firewall mediante iptables creará las reglas de cortafuegos correspondientes a través de iptables, también nos permite utilizarlo como un firewall dedicado, como un Gateway, como un enrutador o como servidor.

La finalidad de instalar un firewall Shorewall es que permita bloquear cierto tráfico desde internet hacia nuestra red y viceversa, además que nos permitirá la salida a internet.

Para ver la instalación del Firewall Shorewall de una manera detallada y gráfica vea el Manual de Administrador.

4.3.4.: FIREWALL PROXY

Un proxy es un servidor que nos sirve como intermediario entre nuestra red local y la conexión de internet, de tal forma que el usuario realiza una petición al Proxy y en realidad es el proxy quien tiene el acceso al internet, luego el proxy será quien se encarga de enviar los datos al usuario, de esta forma el usuario no tiene una conexión directa a internet obligando que el proxy sea el que realice las solicitudes de esta formase puede restringir ciertas peticiones de los usuarios a contenido en el internet.

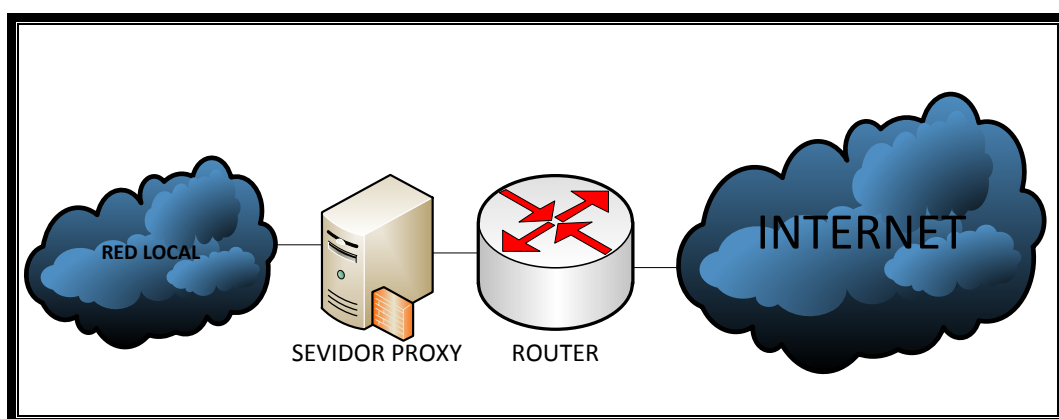


Fig.4.6.: Conexión del Servidor Proxy

Fuente: Microsoft Visio 2010

Utilizaremos un Proxy para que nos permita bloquear acceso a contenido web como son paginas para adultos y páginas que utilicen una gran cantidad de ancho de banda, con el fin de impedir que nuestra red se sature y tengamos problemas.

Para ver la instalación del Servidor Squid Proxy de una manera detallada y gráfica vea el Manual de Administrador.

4.3.5.: PORTAL CAUTIVO

Como definición podemos decir que un portal cautivo puede ser un programa o una maquina conectada en la red que observa el tráfico HTTP, este hace que los usuarios se dirijan obligadamente a una página específica si quieren tener acceso a navegar por

internet. El Portal Cautivo lo que hace es interceptar el tráfico HTTP y no permite a los usuarios navegar hasta que estos se autentifiquen. Este portal también es el encargado de caducar las conexiones en un periodo de tiempo, además que también puede controlar el ancho de banda de cada usuario.

Los usos de un Portal Cautivo son en redes inalámbricas abiertas donde tenemos que dar una bienvenida al usuario e indicar que condiciones tiene el uso de nuestra red.

Tenemos también que definir el concepto de HotSpot, que es una zona donde existe un alto tráfico.

Se decidió utilizar EasyHotSpot debido a que posee una interfaz amigable y nos permite ingresar usuarios fácilmente como nos pide en el Anexo C y además se puede utilizar como software de facturación y posee un servidor DHCP que nos ayudara para la asignación de IP en nuestros AP's.

Para ver la instalación del Portal Cautivo de una manera detallada y gráfica vea el Manual de Administrador.

4.3.6.: SOFTWARE UNI FI

Se utilizó este software debido a la marca de APs que usaremos, que es Ubiquiti, este software nos permitirá controlar mejor nuestros APs y una de la ventajas de este es que nos soporta sobre Windows, Mac, o Linux. En nuestro caso es ideal ya que utilizaremos Ubuntu Server.

Una de las ventajas más importantes es que no usa licencias por lo que podemos utilizar un gran número de APs sin la necesidad de también adquirir el mismo número de licencias.

Este software nos permitirá que los usuarios en nuestra red no se sufran desconexión a lo largo de nuestra zona de cobertura.

4.4.: ADMINISTRACIÓN

Para la administración se establece 4 niveles cada uno con una función específica, se detallará estos niveles que son los siguientes:

- Firewall.- Este será encargado de dar una protección e impedir el acceso a nuestros servicios, realizar un enmascaramiento y nateo en las interfaces del servidor y permitir que nuestro Proxy trabaje de forma transparente.
- Proxy.- Este tendrá la función específica de bloquear el contenido web y generar un nivel de acceso a este contenido.
- Portal Cautivo.- Este será el encargado de permitir la autenticación de los usuarios, controlar el ancho de banda y controlar las condiciones de uso del servicio y su sesión.
- UniFi.- Esta es una herramienta muy importante para poder administrar nuestros Access Point ya que nos indicara el número de usuarios conectados a cada a AP y permitirá el trabajo de nuestra WDS como tal.

4.4.1.: POLÍTICAS DE ACCESO

Se detallara las políticas que vamos a utilizar para dar seguridad, se puede ver la configuración detallada en el Manual de Administrador.

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.

Indice de Módulo

Zonas de Red

Las zonas listadas en esta página representan diferentes redes accesibles desde tu sistema. No obstante, éstas entradas no tienen ningún efecto sobre el cortafuegos - simplemente definen nombres y descripciones de zona.

Seleccionar todo. | Invertir selección. | Agregar una nueva zona de red.

ID de zona	Parent zone	Zone type	Comment	Desplazar	Añadir
<input type="checkbox"/> fw		Firewall system		↓	↑ ↓
<input type="checkbox"/> local		IPv4		↑ ↓	↑ ↓
<input type="checkbox"/> net		IPv4		↑	↑ ↓

Seleccionar todo. | Invertir selección. | Agregar una nueva zona de red.

Delete Selected

Editar el Fichero Manualmente Presione este botón para editar manualmente el fichero /etc/shorewall/zones de Shorewall, donde están guardadas las entradas de arriba.

Regresar a lista de tablas

Fig.4.7.: Zonas de Red

Fuente: Webmin

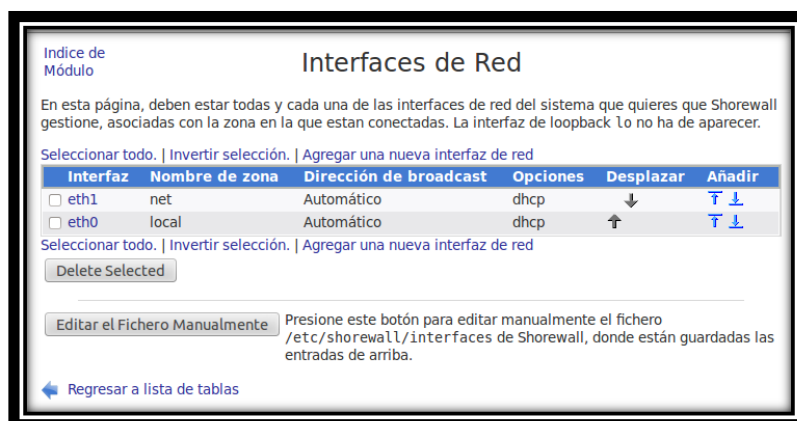


Fig.4.8.: Interfaces de Red

Fuente: Webmin

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

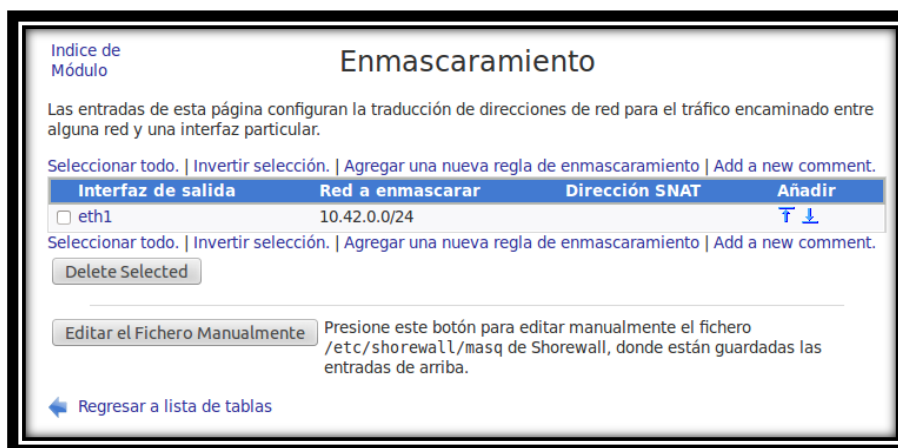


Fig.4.9.: Enmascaramiento

Fuente: Webmin

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.

Indice de Módulo

Políticas por Defecto

Esta página permite configurar las acciones por defecto para el tráfico entre zonas diferentes del cortafuegos. Pueden ser particularizadas para ciertos hosts o tipo de tráfico en la página de reglas del Cortafuegos.

Seleccionar todo. | Invertir selección. | Agregar una nueva política por defecto

Zona origen	Zona destino	Política	Nivel de syslog	Límite de tráfico	Desplazar	Añadir
<input type="checkbox"/> local	net	DROP	Ninguno	Ninguno	↓	↑ ↓
<input type="checkbox"/> Cortafuegos	net	DROP	Ninguno	Ninguno	↑ ↓	↑ ↓
<input type="checkbox"/> net	Cualquiera	DROP	info	Ninguno	↑ ↓	↑ ↓
<input type="checkbox"/> Cualquiera	Cualquiera	REJECT	info	Ninguno	↑	↑ ↓

Seleccionar todo. | Invertir selección. | Agregar una nueva política por defecto

Delete Selected

Editar el Fichero Manualmente Presione este botón para editar manualmente el fichero /etc/shorewall/policy de Shorewall, donde están guardadas las entradas de arriba.

Regresar a lista de tablas

Fig.4.10.: Políticas por Defecto.

Fuente: Webmin.

Indice de Módulo

Reglas del Cortafuegos

Esta tabla lista las excepciones de las políticas por defecto para cierto tipo de tráfico, origen, o destino. La acción seleccionada se aplicará a los paquetes que coincidan con los criterios seleccionados en contra de la política por defecto.

Seleccionar todo. | Invertir selección. | Agregar una nueva regla del cortafuegos | Add a new comment.

Acción	Origen	Destino	Protocolo	Puertos de origen	Puertos destino	Desplazar	Añadir
<input type="checkbox"/> DROP	Zona local	Cortafuegos	TCP	Cualquiera	10000	↓	↑ ↓
<input type="checkbox"/> REDIRECT	Zona local	Puerto 3128	TCP	Cualquiera	80	↑ ↓	↑ ↓
<input type="checkbox"/> ACCEPT	Zona local	Cualquiera	Cualquiera			↑ ↓	↑ ↓
<input type="checkbox"/> ACCEPT	Cortafuegos	Cualquiera	Cualquiera			↑ ↓	↑ ↓
<input type="checkbox"/> DROP	Cualquiera	Cualquiera	Cualquiera			↑	↑ ↓

Seleccionar todo. | Invertir selección. | Agregar una nueva regla del cortafuegos | Add a new comment.

Delete Selected

Editar el Fichero Manualmente Presione este botón para editar manualmente el fichero /etc/shorewall/rules de Shorewall, donde están guardadas las entradas de arriba.

Regresar a lista de tablas

Fig.4.11.: Reglas del Cortafuegos

Fuente: Webmin.

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 rechazarán 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.

Opciones de Puertos y Trabajo en Red		
Direcciones y puertos de Proxy		
<input type="radio"/> Por defecto (normalmente 3128) <input checked="" type="radio"/> Listados abajo..		
Puerto	Nombre de máquina/Dirección IP	Opciones de puerto
3128	<input checked="" type="radio"/> All <input type="radio"/>	transparent
	<input checked="" type="radio"/> All <input type="radio"/>	

Fig.4.12.: Puertos y Trabajo de Red

Fuente: Webmin

Indice de M3dulo Ayuda.. Aplicar Cambios Parar Squid

Control de Acceso

Listas de control de Acceso Restricciones Proxy Restricciones ICP Programas externos ACL Rej

Nombre	Tipo	Coincidiendo con...
manager	Protocolo URL	cache_object
localhost	Dirección de Cliente	127.0.0.1/32 ::1
to_localhost	Dirección de Servidor Web	127.0.0.0/8 0.0.0.0/32 ::1
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	591
Safe_ports	Puerto URL	777
CONNECT	M3todo de Petición	CONNECT
youtube	Expresi3n Regular URL	-i youtube
red_local	Direcci3n de Cliente	10.42.0.0/24
facebook	Expresi3n Regular URL	-i facebook
LAN	Direcci3n de Cliente	192.168.182.0/24
PORNO	Expresi3n Regular URL	-i sexo xxx rubias follar mamada orgia anal pornotube petardas calientes pornografia cachondas adultos xtube
DESCARGAS	Expresi3n Regular URL	-i .exe .wmv .wav .mp3 .mp4 .mpge .3gp .avi

Crear nueva ACL Autenticaci3n Externa

[Regresar a 3ndice squid](#)

Fig.4.13.: Listas de Control de Acceso

Fuente: Webmin.

Indice de M3dulo Ayuda.. Aplicar Cambios Parar Squid

Control de Acceso

Listas de control de Acceso **Restricciones Proxy** Restricciones ICP Programas externos ACL Rej

A3adir restricci3n proxy

Acci3n	ACLs	Mover
<input type="checkbox"/> Denegar	red_local PORNO	↓
<input type="checkbox"/> Denegar	youtube red_local	↓↑
<input type="checkbox"/> Denegar	red_local facebook	↓↑
<input type="checkbox"/> Permitir	red_local	↓↑
<input type="checkbox"/> Permitir	localhost	↓↑
<input type="checkbox"/> Permitir	manager localhost	↓↑
<input type="checkbox"/> Denegar	manager	↓↑
<input type="checkbox"/> Denegar	!Safe_ports	↓↑
<input type="checkbox"/> Denegar	CONNECT !SSL_ports	↑

A3adir restricci3n proxy

Delete Selected Restrictions

[Regresar a 3ndice squid](#)

Fig.4.14.: Restricciones Proxy

Fuente: Webmin.

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

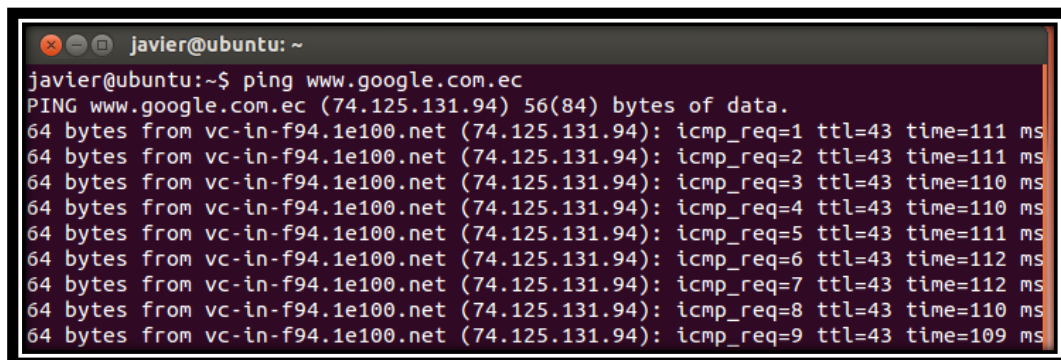
Hemos utilizado EasyHotSpot para poder cumplir con estos requerimientos, ya que en este sistema ya se encuentran configurados y corriendo tanto Free Radius como Chillispot.

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

4.4.2.: 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 página a través del navegador web.



```
javier@ubuntu: ~
javier@ubuntu:~$ ping www.google.com.ec
PING www.google.com.ec (74.125.131.94) 56(84) bytes of data.
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=1 ttl=43 time=111 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=2 ttl=43 time=111 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=3 ttl=43 time=110 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=4 ttl=43 time=110 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=5 ttl=43 time=111 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=6 ttl=43 time=112 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=7 ttl=43 time=112 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=8 ttl=43 time=110 ms
64 bytes from vc-in-f94.1e100.net (74.125.131.94): icmp_req=9 ttl=43 time=109 ms
```

Fig.4.15.: Ping de Firewall Proxy a Google

Fuente: Firewall Proxy.



Fig.4.16.: Google desde Firewall Proxy

Fuente: 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.

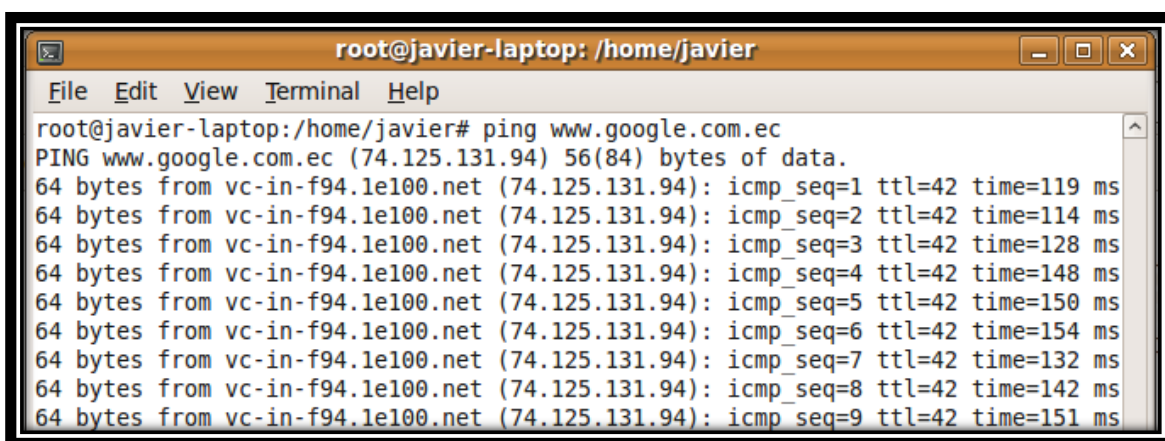


Fig.4.17.: Ping de Portal Cautivo a Google

Fuente: Portal Cautivo.



Fig.4.18.: Google desde el Portal Cautivo

Fuente: Portal Cautivo.

Con esta prueba comprobamos que nuestro Portal Cautivo tiene salida a Internet y también nos dice que el Firewall está 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.

```

C:\Documents and Settings\javier>ipconfig/all

Configuração de IP do Windows

Nome do host . . . . . : javier-a4226a42
Sufixo DNS primário . . . . . :
Tipo de nó . . . . . : desconhecido
Roteamento de IP ativado . . . . . : não
Proxy WINS ativado . . . . . : não
Lista de pesquisa de sufixo DNS . . : chillisport.info.key

Adaptador Ethernet Conexão local:

Sufixo DNS específico de conexão . : chillisport.info.key
Descrição . . . . . : AMD PCNET Family PCI Ethernet Adap
ter
Endereço físico . . . . . : 08-00-27-83-49-7E
DHCP ativado . . . . . : Sim
Configuração automática ativada . . : Sim
Endereço IP . . . . . : 192.168.182.2
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão . . . . . : 192.168.182.1
Servidor DHCP . . . . . : 192.168.182.1
Servidores DNS . . . . . : 10.42.0.1
                               10.42.0.1
Concessão obtida . . . . . : Lunes, 28 de Abril de 2014 23:44:0
9
Concessão expira . . . . . : Lunes, 28 de Abril de 2014 23:54:0
9

```

Fig.4.19.: Visualización dl comando ipconfig/all desde un usuario XP

Fuente: Usuario Windows XP.

Con esta prueba podemos ver que nos asignó 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 chillisport.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.

[Cashier Menu] - [Admin Menu]

Saturday, 10-May-14 23:05:02 UTC

Billing Plan

id	Name	Type	Amount	Valid for	Price	DL rate	Up rate	Created by
	INTERNET	Time Based	60	1	0	default	default	
			15					

Name: ?
 Type: ?
 Amount: ?
 Valid for: ?
 Price: ?
 Download Rate: ?
 Upload Rate: ?
 Idle Timeout: ?

Fig.4.20.: Parámetros de la cuenta

Fuente: Portal Cautivo.

Saturday, 10-May-14 23:05:06 UTC

Voucher Management

Username	Password	Billing plan	Valid until	Time used	Time remain	Packet used	Packet remain	Printed
		INTERNET						

How many voucher(s)?

Billing plan:

Fig.4.21.: Parámetros para generar usuario

Fuente: Portal Cautivo.

Username	Password	Billing plan	Valid until	Time used	Time remain	Packet used	Packet remain	Printed
xuncet6	cingopug	INTERNET	May 11 2014	---	---	---	---	no   

Fig.4.22.: Usuario Creado

Fuente: Portal Cautivo.

- 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.

Internal captive portal management

Radius Server 1	<input type="text" value="127.0.0.1"/>	?
Radius Server 2	<input type="text" value="127.0.0.1"/>	?
Radius Secret	<input type="text" value="easyhotspot"/>	?
DHCP Interface	<input type="text" value="eth1"/>	?
UAM Server	<input type="text" value="https://192.168.182.1/cgi-bi"/>	?
UAM Secret	<input type="text" value="easyhotspot"/>	?
Client's Homepage	<input type="text" value="192.168.182.1:3990/prelogin"/>	?
Allowed URL	<input type="text" value="68.182.1,www.ibarra.gob.ec"/>	? Separate by comma
DHCP Range	<input type="text" value="192.168.182.0/24"/>	?
COAPort	<input type="text" value="3799"/>	?

Fig.4.23.: Permitir acceso a www.ibarra.gob.ec

Fuente: Portal Cautivo.

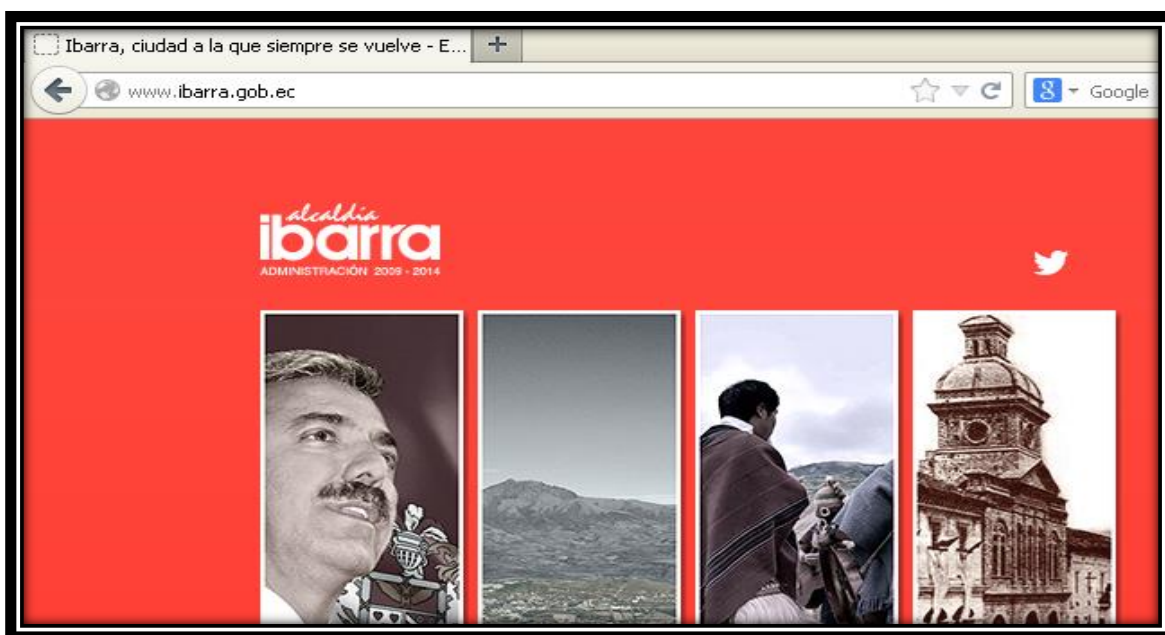


Fig.4.24.: Ingreso a www.ibarra.gob.ec

Fuente: Portal Cautivo.

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

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

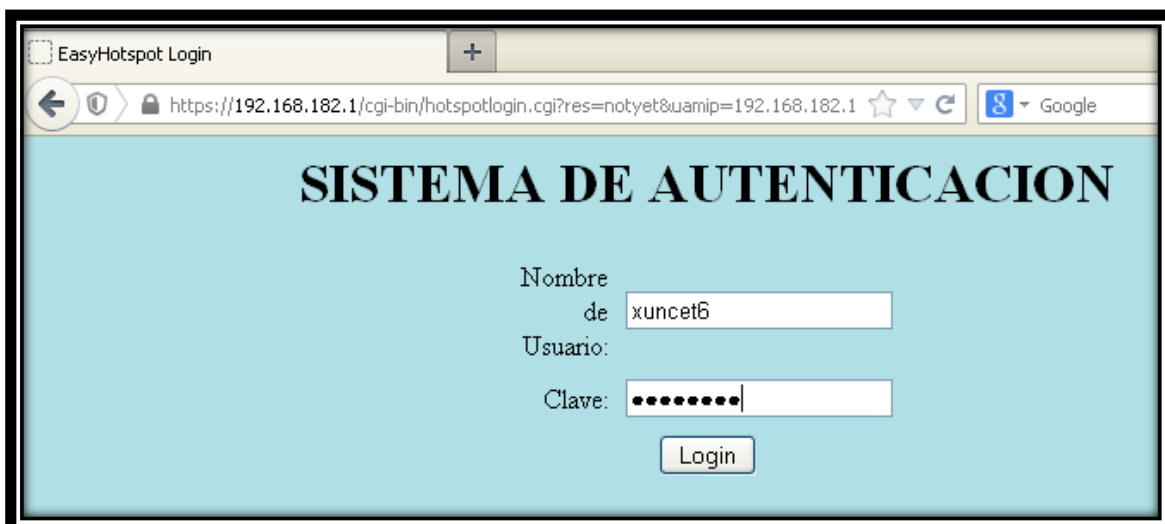


Fig.4.25.: Pantalla de Autenticación de Usuarios

Fuente: Usuario Windows XP



Fig.4.26.: Pantalla de Inicio de Sesión

Fuente: Usuario Windows XP

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 está 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 vez que hemos iniciado sesión tenemos acceso a internet.

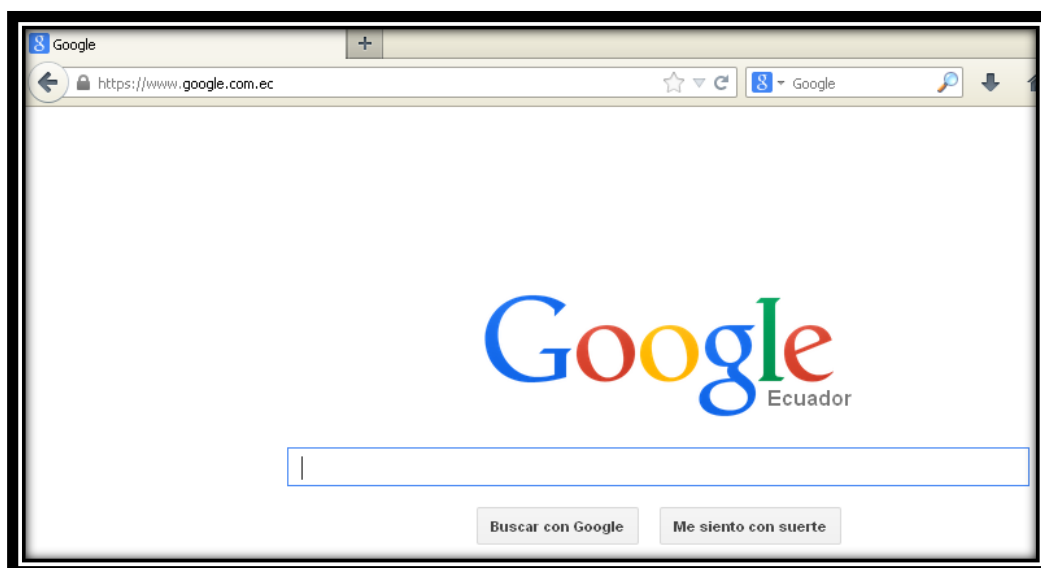


Fig.4.27.: Acceso a Google desde Usuario XP

Fuente: Usuario Windows 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.



Fig.4.28.: Acceso ha contenido sexual

Fuente: Usuario Windows XP

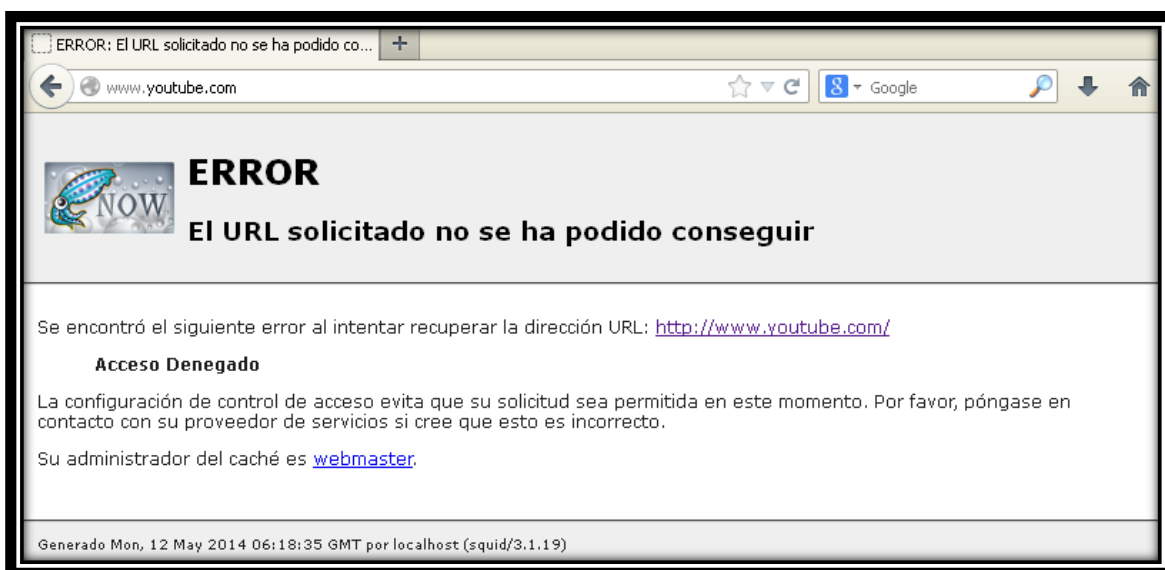


Fig.4.29.: Acceso a Youtube

Fuente: Usuario Windows XP



Fig.4.30.: Acceso a Facebook

Fuente: Usuario Windows XP

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.



Fig.4.31.: Acceso a Webmin desde usuario XP

Fuente: Usuario Windows XP

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

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



Fig.4.32.: Pantalla de Cierre de Sesión

Fuente: Usuario Windows XP

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

CAPITULO 5: ANÁLISIS COSTO BENEFICIO

5.1.: DEFINICIÓN

(Sociedad Latinoamericana para la Calidad, 2000) "El Análisis Costo / Beneficio es el proceso de colocar cifras en dólares en los diferentes costos y beneficios de una actividad. Al utilizarlo, podemos estimar el impacto financiero acumulado de lo que queremos lograr."

5.2.: UTILIDAD

(Sociedad Latinoamericana para la Calidad, 2000) "Se debe utilizar el Análisis Costo / Beneficio al comparar los costos y beneficios de las diferentes decisiones. Un Análisis de Costo / Beneficio por si solo puede no ser una guía clara para tomar una buena decisión. Existen otros puntos que deben ser tomados en cuenta, ej. La moral de los empleados, la seguridad, las obligaciones legales y la satisfacción del cliente."

5.2.1.: PROCESO

El Análisis de Costo / Beneficio involucra los siguientes 6 pasos:

Llevar a cabo una Lluvia de Ideas o reunir datos provenientes de factores importantes relacionados con cada una de sus decisiones.

- a) ¿Es factible cobrar por un servicio de internet?
- b) ¿Cuánto estarían dispuestas las personas a pagar por un servicio de internet?
- c) ¿Cuál es el mayor gasto que se debería hacer para implementar este proyecto?
- d) ¿El servicio gratuito ayuda a la ciudadanía?

- e) ¿Es necesario realizar la implementación a través del portal de compras públicas simplemente utilizar la mano de obra del GAD de San Miguel de Ibarra?
- f) ¿Hay que hacer un gasto en capacitación de personal?
- g) ¿Hay que gastar en herramientas?

Determinar los costos relacionados con cada factor. Algunos costos, como la mano de obra, serán exactos mientras que otros deberán ser estimados.

a) Al momento de cobrar un servicio de internet tenemos que tener en cuenta que se tendrá gastos de personal que este dedicado a atender a las personas que quieren adquirir el servicio, para esto se debe contratar unas 3 personas a un sueldo básico de 340 dólares.

b) Para brindar este servicio el costo del mismo debe estar acorde a con los del mercado actual, por ejemplo la hora de servicio 60 centavos de dólar.

c) El mayor gasto del proyecto serían la adquisición de los Access Point que está a un precio referencial de 158.95 dólares cada uno.

d) El servicio de internet gratuito podría ayudar a la ciudadanía permitiendo realizar sus trámites como el SRI.

e) Es posible utilizar al mismo personal del municipio para poder instalar los Access Point así que el costo de mano de obra se reduciría.

f) Se tiene que aumentar un rubro de capacitación para el personal que va a instalar y configurar el precio estaría en los 150 dólares por persona que se va a capacitar y sería necesario por los menos unas 10 personas.

g) No habría que hacer gasto en herramientas porque con las que el GAD de San Miguel de Ibarra posee es suficiente para este tipo de instalación.

Sumar los costos totales para cada decisión propuesta.

Tomando en cuenta los rubros antes expuestos tendríamos:

- Personal para atención al público 1020 dólares.
- Para adquisición de Access Point 4291,65 dólares.
- Para capacitación 1500 dólares.

Esto nos da un valor de 6811.65 dólares aproximados que se necesitaría para poder implementar el proyecto teniendo en cuenta que los demás elementos de la red ya posee la institución.

Determinar los beneficios en dólares para cada decisión.

Es muy difícil determinar los beneficios en dólares para cada decisión que se tomó porque en si es un proyecto con fin social y la decisión de cobrar por un servicio no está tomada solo está estimada.

Poner las cifras de los costos y beneficios totales en la forma de una relación donde los beneficios son el numerador y los costos son el denominador:

En esta parte del análisis ya que no tenemos un valor en dólares de los beneficios tampoco podríamos sacar una relación entre los dos pero tenemos que tomar en cuenta que el beneficio social podría ser muy alto.

Comparar las relaciones Beneficios a Costos para las diferentes decisiones propuestas. La mejor solución, en términos financieros es aquella con la relación más alta beneficios a costos.

En este proyecto no se espera tener ingresos económicos aunque se podría ver una forma de rédito económico utilizando el servidor pero en si este es un proyecto social, lo cual el beneficio de este proyecto no es económico.

Si bien es necesaria una inversión inicial para la implementación de este proyecto el fin del mismo es dar un servicio social, al permitir a los ciudadanos ingresar a páginas web permitidas gratuitamente.

A continuación se detallará los costos de equipos de este proyecto tomando en cuenta solo los equipos que harían falta de adquirir sería los APs adicional sería también tomado en cuenta el cable.

Los datos mostrados son datos consultados hasta abril de 2014.

DESCRIPCIÓN	UNIDADES	VALOR UNITARIO	VALOR TOTAL
UniFi AP Outdoor+	27	158.95 \$	4291.65 \$
Cable UTP cat 6 A	1 rollo	149.99 \$	149.99 \$
TOTAL			4441.64 \$

Tabla.5.1.: Presupuesto Referencial

Fuente: <http://www.amazon.com>

Podemos concluir este análisis diciendo que el beneficio de este proyecto es muy alto ya que aporta con el Plan Nacional de Desarrollo, El Plan del Buen Vivir y el Plan Nacional de Telecomunicaciones, no es necesario que este proyecto no genere ingresos para poder concluir que la inversión que se realizará en este proyecto es baja comparada con el aporte social que este tiene.

CONCLUSIONES Y RECOMENDACIONES

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.

RECOMENDACIONES

- Para obtener un correcto levantamiento de información debemos pedir q se nos autorice el acceso a la información en la institución donde realizaremos el trabajo.
- Es importante descargarse de la página oficial el sistema operativo para tenerlo completo y que no se nos presente ningún contratiempo.
- Tenemos que tratar de hacer entender a las autoridades que van a dar su autorización o permiso para la realización de este trabajo lo importante que son estos proyectos.
- Una recomendación muy importante a la hora de configurar los servidores es que se lo haga en un terminal y no en Webmin para no tener inconvenientes a la hora que corra el servicio, Webmin se lo utiliza para una fácil administración y monitoreo.
- Sigamos el orden del manual de usuario para configurar nuestro servidor, debido a que es importante probar en orden los servicios, es decir primero el firewall, después el proxy y por último el portal cautivo.

BIBLIOGRAFÍA

- 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](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. (SEPTIEMBRE 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*.

ANEXO A

INTERFERENCIAS

Los datos mostrados a continuación han sido obtenidos mediante el programa InSSiDer 3 instalado en una PC portátil que posee una tarjeta de red Qualcomm Atheros AR9485WB-EG Wireless Network Adapter que nos permite analizar las redes Wi-fi de 5 y 2.4 GHz.

El programa nos muestra el SSID, la Señal, el Canal, el tipo de seguridad, la dirección MAC, el MAX RATE, que tipo de estándar 802.11 y la marca del AP, además de una gráfica que nos indica el canal y la potencia que tienen cada red inalámbrica.

Se hizo un barrido de las redes con este programa ubicándose en cada nodo de nuestra zona de cobertura, a continuación mostraremos las pantallas con los resultados que nos da el programa, la primera pantalla nos muestra las redes con más potencia y sus características y la segunda nos muestra las gráficas de las redes.

Nodo 1: Sánchez y Cifuentes y García Moreno

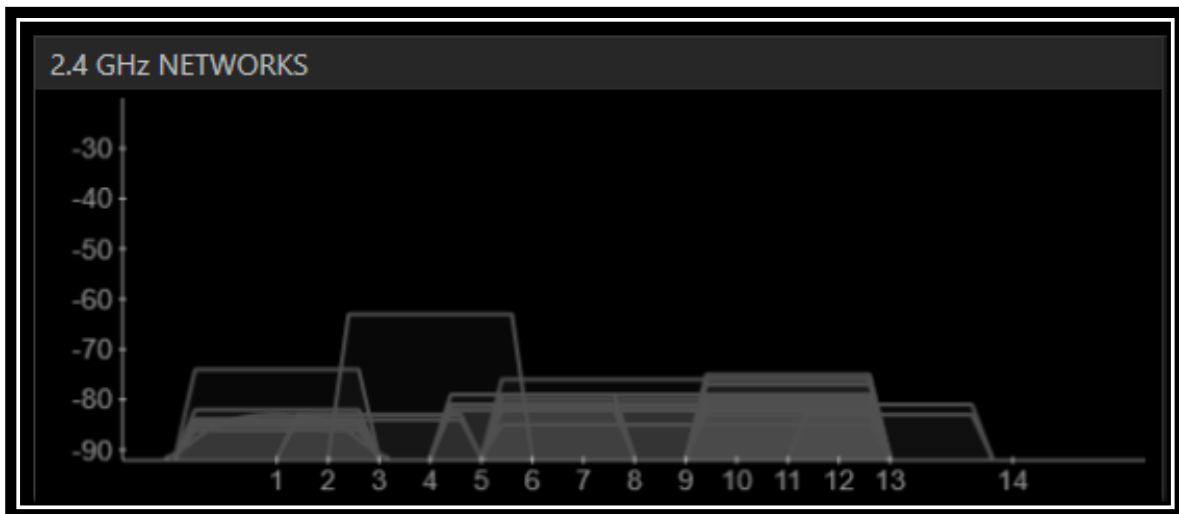
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ibarradigital	-63	4	Open	00:15:6D:69:3B:A1	54	g	Ubiquiti Networks Inc.
PATRICIO EDUARDO P...	-74	1	WPA2-Personal	D8:5D:4C:A0:DD:08	54	g	TP-LINK Technologies
ALMACEN ASTRA.	-75	11	WPA2-Personal	88:53:D4:91:FA:B4	270	n	Huawei Technologies C
ROCIO PIEDAD RUBIO	-76	11+7	WPA2-Personal	F8:3D:FF:20:26:FC	270	n	Huawei Technologies C
VICTOR SALAZAR	-76	11	WPA-Personal	00:E0:4D:BF:78:D0	54	g	INTERNET INITIATIVE J
ING ROSIO ERAZO	-77	11	WPA2-Personal	88:53:D4:91:FC:08	270	n	Huawei Technologies C
INTERNET CNT	-79	11	WPA-Personal	F8:3D:FF:1E:EC:B0	270	n	Huawei Technologies C
INCYTECH	-79	11	WPA-Personal	00:26:B6:81:8E:9A	54	g	Askey Computer
dlinklocal	-79	6	WPA2-Personal	14:D6:4D:B4:5C:14	72	n	D-Link International
FLIA.MONTERO	-79	11+7	WPA-Personal	00:E0:4D:D7:64:F8	135	n	INTERNET INITIATIVE J
FLIA. CIFUENTES	-79	11+7	WPA-Personal	00:E0:4D:9E:6E:10	135	n	INTERNET INITIATIVE J
CHILDFOUND1	-80	11	WPA2-Personal	88:53:D4:FB:72:A8	270	n	Huawei Technologies C
FABRICIOCH	-80	11	WPA-Personal	00:E0:4D:9B:0F:78	54	g	INTERNET INITIATIVE J
ParaTI	-80	11+7	WPA2-Personal	A4:99:47:96:42:8C	270	n	Huawei Technologies C



Nodo 2: Sánchez y Cifuentes y Juan José Flores

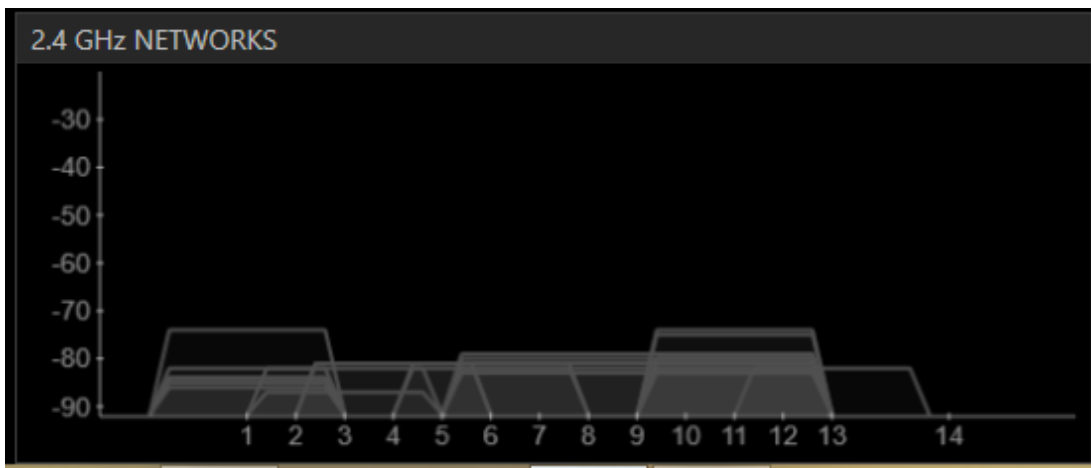
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
PATRICIO EDUARDO P...	-74	1	WPA2-Personal	D8:5D:4C:A0:DD:08	54	g	TP-LINK Technologies
INTERNET CNT	-74	11	WPA2-Personal	F8:3D:FF:1E:EC:B0	270	n	Huawei Technologies C
ALMACEN ASTRA.	-75	11	WPA2-Personal	88:53:D4:91:FA:B4	270	n	Huawei Technologies C
FLJA. CIFUENTES	-79	11+7	WPA2-Personal	00:E0:4D:9E:6E:10	135	n	INTERNET INITIATIVE J
ParaTI	-80	11+7	WPA2-Personal	A4:99:47:96:42:8C	270	n	Huawei Technologies C
CHILDFUND1	-80	11	WPA2-Personal	88:53:D4:FB:72:A8	270	n	Huawei Technologies C
FABRICIOCH	-80	11	WPA2-Personal	00:E0:4D:9B:0F:78	54	g	INTERNET INITIATIVE J
ibarradigital	-81	4	Open	00:15:6D:6B:11:CA	54	g	Ubiquiti Networks Inc.
Claro_LOZANO000086	-81	11	WPA2-Personal	1C:3E:84:54:BD:06	72	n	
ibarradigital	-81	4	Open	00:15:6D:69:3B:A1	54	g	Ubiquiti Networks Inc.
REFUJIO DE BELEN	-81	11+7	WPA2-Personal	BC:76:70:E5:22:48	270	n	Huawei Device Co., Ltd
Claro_THE HOUSE CLAI	-81	6	WEP	C0:F8:DA:AC:D4:24	54	g	Hon Hai Precision Ind.
Claro_RIVERA00008829	-82	11	WEP	F4:B7:E2:5F:5A:AF	72	n	
OPTICA BOLIVAR	-82	11+7	WPA2-Personal	BC:76:70:E4:A1:B4	270	n	Huawei Device Co., Ltd



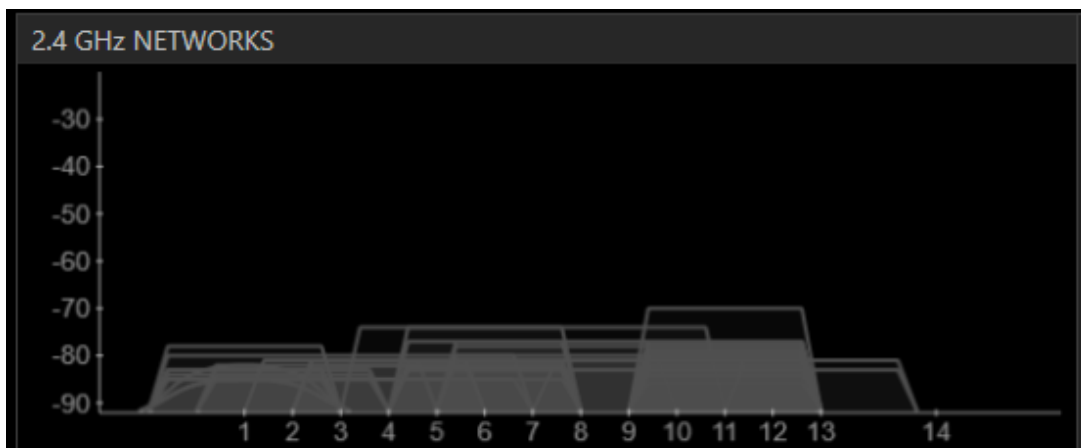
Nodo 3. Sánchez y Cifuentes y Miguel Oviedo

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ALMACEN ASTRA.	-70	11	WPA2-Personal	88:53:D4:91:FA:B4	270	n	Huawei Technologies C
PEREZ GUEVARA	-74	9+5	WPA-Personal	00:E0:4D:BE:14:68	135	n	INTERNET INITIATIVE J.
Claro_THE HOUSE CLAI	-74	6	WEP	C0:F8:DA:AC:D4:24	54	g	Hon Hai Precision Ind.
ANTONIO POTOSI	-77	11	WPA2-Personal	A4:99:47:84:03:68	270	n	Huawei Technologies C
Konica	-77	11	WPA2-Personal	C8:D7:19:E7:99:F4	144	n	Cisco Consumer Produ
FLIA. RODRIGUEZ	-77	11+7	WPA2-Personal	BC:76:70:DF:5E:24	270	n	Huawei Device Co., Ltd
ALBAJOCOSTO1	-77	6	WPA2-Personal	B8:A3:86:54:71:32	300	n	D-Link International
FRIGOCENTRO	-78	11+7	WPA2-Personal	A4:99:47:83:FF:24	270	n	Huawei Technologies C
Claro_ALMEIDA000076	-78	1	WEP	5C:AC:4C:B6:1E:3A	54	g	Hon Hai Precision Ind.
Claro_CHAMORRO0000	-78	11	WEP	4C:0F:6E:3C:75:09	54	g	Hon Hai Precision Ind.
Claro_SANCHEZ000056	-78	11	WEP	CC:AF:78:5F:66:89	144	n	Hon Hai Precision Ind.
Claro_MAYON0000503	-79	11	WEP	EC:55:F9:96:E6:D0	144	n	Hon Hai Precision Ind.
WSENECYT	-80	11	WPA2-Personal	B8:A3:86:27:97:F8	116	n	D-Link International
Claro_NOGUERA00006	-80	11	WEP	64:27:37:43:41:1F	144	n	Hon Hai Precision Ind.



Nodo 4: Sánchez y Cifuentes y Pedro Moncayo

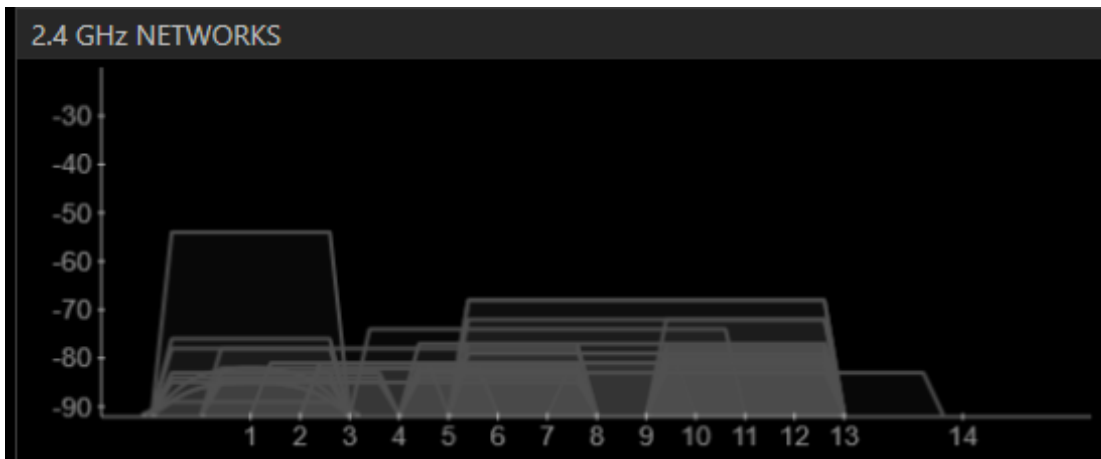
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS + SSID or Vendor Channel > Signal < Security 802.11

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
wireless	-64	1	WEP	14:D6:4D:BA:9E:2C	54	g	D-Link International
MACRO IBARRA	-68	11+7	WPA-Personal	00:E0:4D:9A:72:48	135	n	INTERNET INITIATIVE J.
RT3390_2	-68	11+7	Open	00:E0:4D:9A:72:49	135	n	INTERNET INITIATIVE J.
"AnnyCell"	-72	11+7	WPA-Personal	BC:76:70:DF:9D:A8	270	n	Huawei Device Co., Ltd
Claro_SALAS00008828z	-72	11	WEP	F4:B7:E2:5F:69:BF	72	n	
PEREZ GUEVARA	-74	9+5	WPA-Personal	00:E0:4D:BE:14:68	135	n	INTERNET INITIATIVE J.
Claro_MUNOZ0000710	-56	1	WEP	C0:F8:DA:AC:D6:25	54	g	Hon Hai Precision Ind.
FLIA. RODRIGUEZ	-77	11+7	WPA2-Personal	BC:76:70:DF:5E:24	270	n	Huawei Device Co., Ltd
ALBAJOCOSTO1	-77	6	WPA2-Personal	B8:A3:86:54:71:32	300	n	D-Link International
Konica	-77	11	WPA2-Personal	C8:D7:19:E7:99:F4	144	n	Cisco Consumer Produ
Claro_SANCHEZ000056	-78	11	WEP	CC:AF:78:5F:66:89	144	n	Hon Hai Precision Ind.
Claro_CHAMORRO0000	-78	11	WEP	4C:0F:6E:3C:75:09	54	g	Hon Hai Precision Ind.
COMPRAVENTA-IBARA	-78	6+2	WPA-Personal	00:E0:4D:9E:6C:78	135	n	INTERNET INITIATIVE J.
Claro_ALMEIDA000076	-78	1	WEP	5C:AC:4C:B6:1E:3A	54	g	Hon Hai Precision Ind.



Nodo 5: Sánchez y Cifuentes y Juan de Velasco

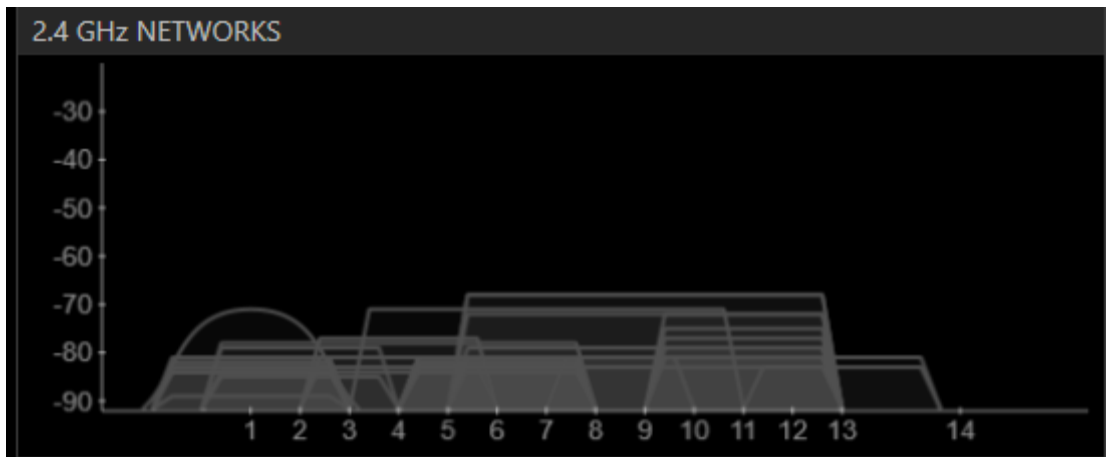
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
RT3390_2	-68	11+7	Open	00:E0:4D:9A:72:49	135	n	INTERNET INITIATIVE J.
MACRO IBARRA	-68	11+7	WPA-Personal	00:E0:4D:9A:72:48	135	n	INTERNET INITIATIVE J.
PEREZ GUEVARA	-71	9+5	WPA-Personal	00:E0:4D:BE:14:68	135	n	INTERNET INITIATIVE J.
meraki-scanning	-75	1	Open	00:18:0A:01:5C:33	11	b	Meraki, Inc.
Claro_SALAS000088284	-72	11	WEP	F4:B7:E2:5F:69:BF	72	n	
"AnnyCell"	-72	11+7	WPA-Personal	BC:76:70:DF:9D:A8	270	n	Huawei Device Co., Ltd
MAXIMS	-75	11	WPA2-Personal	F8:3D:FF:1E:EF:70	270	n	Huawei Technologies C
apc1	-77	4	WEP	00:26:99:10:85:C0	54	g	Cisco Systems
TONKA	-77	11	WPA-Personal	00:26:B6:7B:7F:6C	54	g	Askey Computer
COMPRAVENTA-IBARA	-78	6+2	WPA-Personal	00:E0:4D:9E:6C:78	135	n	INTERNET INITIATIVE J.
Claro	-79	2	WPA2-Personal	78:54:2E:5A:A1:BE	150	n	
Claro_VARGAS0000787	-79	11	WPA2-Personal	CC:AF:78:43:FA:5C	144	n	Hon Hai Precision Ind.
INTERNET GRATIS 1PA	-79	11+7	WPA-Personal	BC:76:70:E3:F9:51	270	n	Huawei Device Co., Ltd
silvia chalacan	-79	11	WPA-Personal	00:E0:4D:D7:47:90	54	g	INTERNET INITIATIVE J.



Nodo 6: Sánchez y Cifuentes y Cristóbal Colón

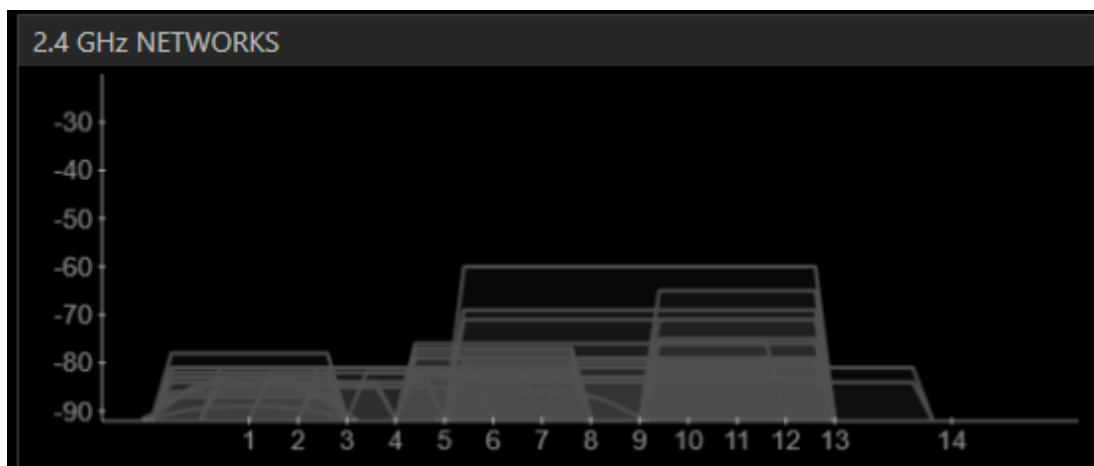
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
TATIANA	✓ -60	11+7	WPA-Personal	BC:76:70:E7:5B:E0	270	n	Huawei Device Co., Ltd
silvia chalacan	✓ -65	11	WPA-Personal	00:E0:4D:D7:47:90	54	g	INTERNET INITIATIVE J.
MIS PRECIOSAS	✓ -69	11+7	WPA-Personal	BC:76:70:E4:A1:60	270	n	Huawei Device Co., Ltd
ESPINOSA	✓ -71	11+7	WPA-Personal	BC:76:70:DD:53:84	270	n	Huawei Device Co., Ltd
TONKA	✓ -71	11	WPA-Personal	00:26:B6:7B:7F:6C	54	g	Askey Computer
Claro_ROJAS00007988:	✓ -75	11	WEP	CC:AF:78:5F:34:5E	144	n	Hon Hai Precision Ind.
PASOS	✓ -76	11	WPA2-Personal	4C:8B:EF:50:E7:F4	270	n	
CNT PINCHAO	✓ -76	6+10	WPA-Personal	BC:76:70:E4:08:20	270	n	Huawei Device Co., Ltd
Claro_BANALCAZAR000	✓ -77	6	WEP	C0:F8:DA:A5:3B:95	54	g	Hon Hai Precision Ind.
dlink	✓ -77	6	Open	14:D6:4D:BA:20:10	72	n	D-Link International
CAMARA_COMERCIO	✓ -78	6	WPA-Personal	00:21:63:DE:14:6A	54	g	ASKEY COMPUTER COI
LONDON1	✓ -78	1	WPA2-Personal	00:E0:4D:D7:1F:70	65	n	INTERNET INITIATIVE J.
PLATINO4LIFE	✓ -79	11+7	WPA-Personal	00:E0:4D:BF:6A:48	135	n	INTERNET INITIATIVE J.
Claro_CEVALLOS00008:	✓ -79	11	WEP	F4:B7:E2:5F:8A:2B	72	n	



Nodo 7: José Joaquín Olmedo y Juan José Flores

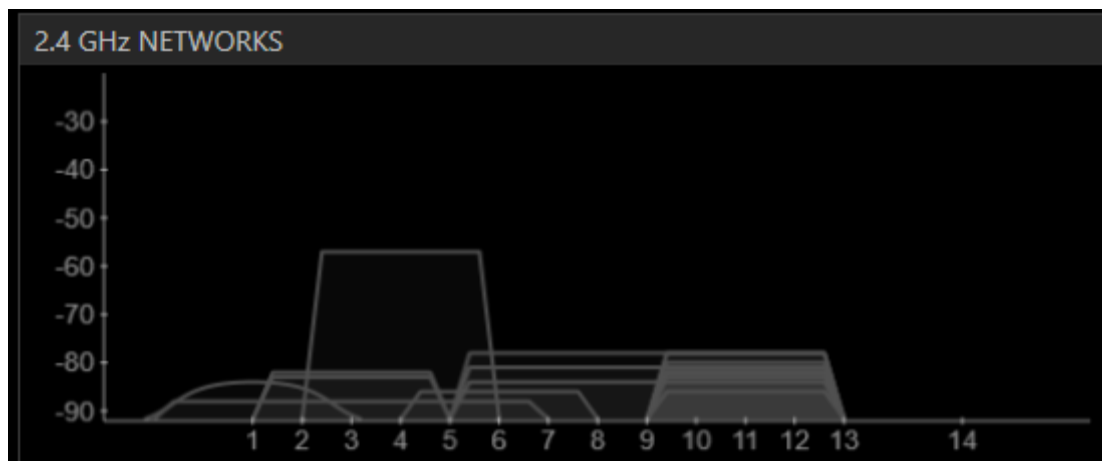
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ibarradigital	-61	4	Open	00:15:6D:6B:11:CA	54	g	Ubiquiti Networks Inc.
Organo Gold	-76	11	WPA2-Personal	88:53:D4:80:B1:88	270	n	Huawei Technologies C
IAMDIPRO	-80	11+7	WPA-Personal	BC:76:70:F0:80:08	270	n	Huawei Device Co., Ltd
Claro_YEPEZ000087253	-74	11	WEP	68:94:23:D2:B4:23	72	n	
Claro_AGUILAR000084	-80	11	WEP	F4:B7:E2:5F:4D:8C	72	n	
MIRIAN	-81	11+7	WPA-Personal	BC:76:70:DD:98:78	270	n	Huawei Device Co., Ltd
ING ROSIO ERAZO	-82	11	WPA2-Personal	88:53:D4:91:FC:08	270	n	Huawei Technologies C
CNT FOCI	-82	11	WPA-Personal	F8:3D:FF:20:11:98	270	n	Huawei Technologies C
Claro_JARAMILLOARQL	-82	11	WEP	88:9F:FA:4A:9D:57	54	g	Hon Hai Precision Ind.
ibarr@digital	-82	3	Open	00:15:6D:69:3B:A0	54	g	Ubiquiti Networks Inc.
Claro_SILVA000049411	-82	11	WEP	EC:55:F9:62:B9:A5	144	n	Hon Hai Precision Ind.
ibarr@digital	-83	3	Open	00:15:6D:6B:0E:50	54	g	Ubiquiti Networks Inc.
FLIA: PARRAGA	-83	11	WPA2-Personal	4C:8B:EF:2B:0F:E4	270	n	
HNE01	-84	1	WPA-Personal	00:15:6D:72:A2:A0	11	b	Ubiquiti Networks Inc.



Nodo 8: José Joaquín Olmedo y Miguel Oviedo

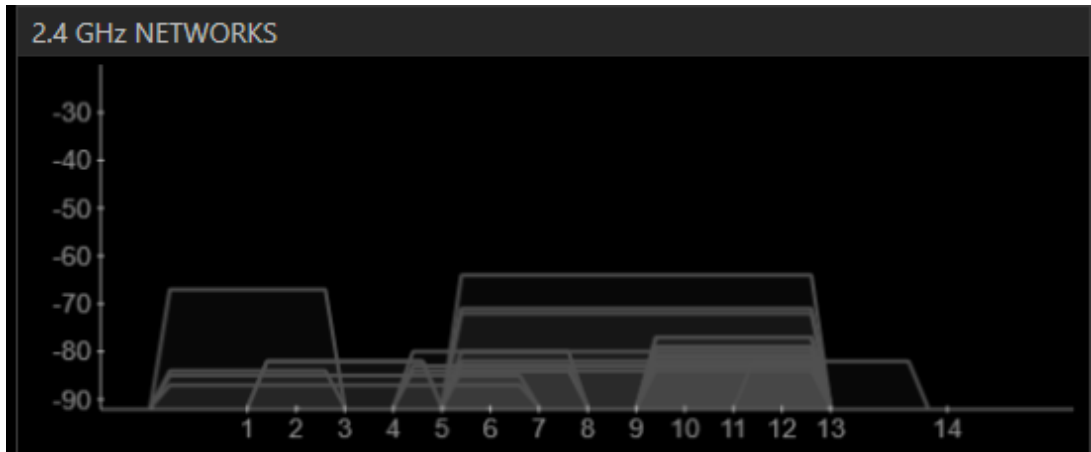
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
MM Asesores Contable	-64	11+7	WPA-Personal	BC:76:70:E5:08:E0	270	n	Huawei Device Co., Ltd
Claro_POZO000078184	-67	1	WEP	C0:F8:DA:4B:11:54	54	g	Hon Hai Precision Ind.
MIRIAN	-71	11+7	WPA2-Personal	A4:99:47:7F:3C:94	270	n	Huawei Technologies C
INTERNET GRATIS 1 PA	-72	11+7	WPA-Personal	BC:76:70:E5:1C:F1	270	n	Huawei Device Co., Ltd
Claro_PEREZ000052437	-77	11	WEP	C0:F8:DA:44:20:34	54	g	Hon Hai Precision Ind.
Claro_BENALCAZAR000	-77	11	WEP	CC:AF:78:44:0E:D7	144	n	Hon Hai Precision Ind.
ARQ YEPEZ	-79	11	WPA2-Personal	88:53:D4:B0:88:24	270	n	Huawei Technologies C
FAMILIA LASTRA	-79	11	WPA-Personal	00:26:B6:82:3C:2E	54	g	Askey Computer
Claro_ALULEMA000077	-80	11	WEP	EC:55:F9:49:2F:58	144	n	Hon Hai Precision Ind.
luis1	-80	6	WEP	00:19:5B:D2:B7:BB	54	g	D-Link Corporation
IAMDIPRO	-80	11+7	WPA-Personal	BC:76:70:F0:80:08	270	n	Huawei Device Co., Ltd
Organo Gold	-81	11	WPA2-Personal	88:53:D4:B0:B1:88	270	n	Huawei Technologies C
Dr Sandoval	-82	11+7	WPA-Personal	BC:76:70:E3:76:70	270	n	Huawei Device Co., Ltd
ibarr@digital	-82	3	Open	00:15:6D:69:3B:A0	54	g	Ubiquiti Networks Inc.



Nodo 9: José Joaquín Olmedo y Pedro Moncayo

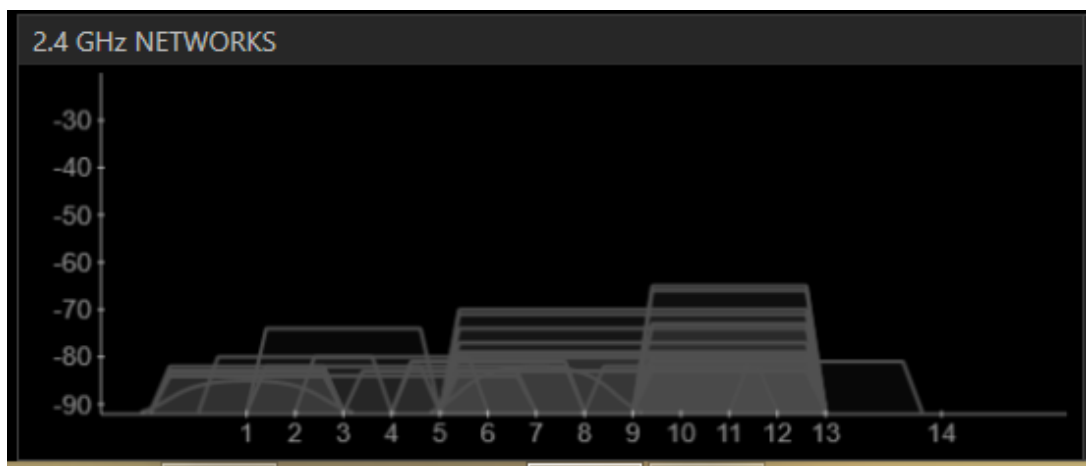
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS + SSID or Vendor Channel > Signal < Security 802.11

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
Claro_PINEDA00007874	-65	11	WEP	60:D8:19:58:36:06	144	n	Hon Hai Precision Ind.
ESHOTEG	-66	11	WPA2-Personal	88:53:D4:C4:8B:6C	270	n	Huawei Technologies C
--RUIZ DAVILA--	-70	11+7	Open	BC:76:70:E5:1C:F0	270	n	Huawei Device Co., Ltd
MIRIAN	-71	11+7	WPA2-Personal	A4:99:47:7F:3C:94	270	n	Huawei Technologies C
Claro_BENALCAZAR000	-73	11	WEP	CC:AF:78:44:0E:D7	144	n	Hon Hai Precision Ind.
FAMILIA LASTRA	-73	11	WPA-Personal	00:26:B6:82:3C:2E	54	g	Askey Computer
Mundy_Express	-74	3	WPA-Personal	F4:EC:38:FB:37:F8	54	g	TP-LINK TECHNOLOGII
MM Asesores Contable	-74	11+7	WPA-Personal	BC:76:70:E5:08:E0	270	n	Huawei Device Co., Ltd
FLIA ACOSTA	-77	11+7	WPA2-Personal	88:53:D4:91:FA:C4	270	n	Huawei Technologies C
Claro_DAVILA00008174	-79	11	WEP	EC:55:F9:38:3F:77	144	n	Hon Hai Precision Ind.
INTERNET GRATIS 1 PA	-79	11+7	WPA-Personal	BC:76:70:E5:1C:F1	270	n	Huawei Device Co., Ltd
GESTOR1	-80	2	WPA-Personal	00:21:63:E0:60:FD	54	g	ASKEY COMPUTER COI
Claro_TORRES00008274	-80	11	WPA2-Personal	F4:B7:E2:5F:4A:E9	72	n	
JANETH SANTILLAN	-80	11+7	WPA2-Personal	08:7A:4C:AE:B1:10	270	n	



Nodo 10: José Joaquín Olmedo y Juan de Velasco

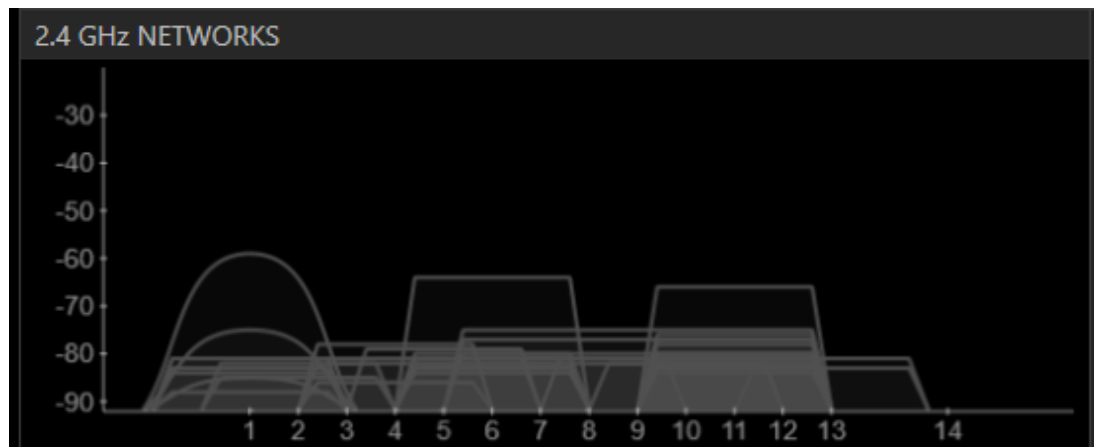
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
CERELECTRIC	-59	1	WEP	F4:EC:38:F8:1B:D4	11	b	TP-LINK TECHNOLOGII
ALBAJOCOSTOAP	-64	6	WEP	00:25:86:CD:37:F6	54	g	TP-LINK Technologies t
Claro_ROJAS00007988:	-66	11	WEP	CC:AF:78:5F:34:5E	144	n	Hon Hai Precision Ind.
MAGAP_ZONA1	-75	11+7	WPA2-Personal	F8:3D:FF:1D:47:10	270	n	Huawei Technologies C
meraki-scanning	-75	1	Open	00:18:0A:01:59:96	11	b	Meraki, Inc.
MONO	-76	11	WPA-Personal	00:21:63:DD:EB:A7	54	g	ASKEY COMPUTER COI
ESHOTEG	-77	11	WPA2-Personal	88:53:D4:C4:8B:6C	270	n	Huawei Technologies C
intenrte gratis 1pago 0	-77	11+7	WPA-Personal	BC:76:70:E4:07:FD	270	n	Huawei Device Co., Ltd
ibarradigital	-78	4	Open	00:15:6D:6B:11:CA	54	g	Ubiquiti Networks Inc.
CIMAN	-78	11	WPA2-Personal	84:C9:B2:67:9A:92	130	g, n	D-Link International
Hotel ROYAL RUIZ	-79	5	WPA-Personal	00:14:D1:C6:6F:E8	144	n	TRENDnet
LINUMOBI	-80	11+7	WPA-Personal	BC:76:70:ES:0B:80	270	n	Huawei Device Co., Ltd
JAEL ANDRES.	-80	11	WPA2-Personal	4C:8B:EF:2A:82:44	270	n	
Claro_PINEDA0000787:	-80	11	WEP	60:D8:19:58:36:06	144	n	Hon Hai Precision Ind.



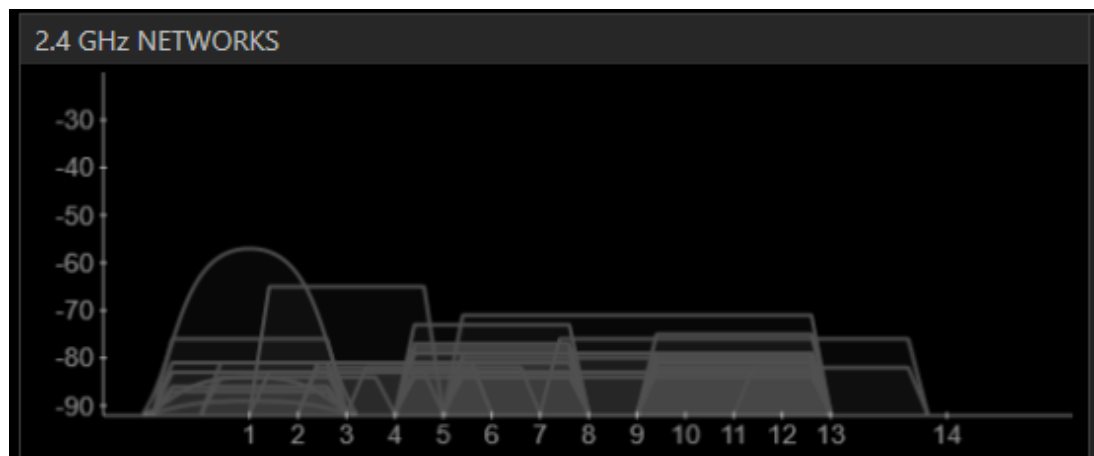
Nodo 11: José Joaquín Olmedo y Cristóbal Colón

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
meraki-scanning	-57	1	Open	00:18:0A:01:59:96	11	b	Meraki, Inc.
ositadlink	-65	3	WPA2-Personal	90:94:E4:AA:8A:5E	150	n	D-Link International
ESPINOSA	-71	11+7	WPA-Personal	BC:76:70:DD:53:84	270	n	Huawei Device Co., Ltd
INTY	-73	6	WPA2-Personal	30:E4:DB:8C:91:CC	144	n	Cisco Systems
Claro_ROJAS00007988	-75	11	WEP	CC:AF:78:5F:34:5E	144	n	Hon Hai Precision Ind.
Claro_CAMUEZ000061	-76	1	WEP	C0:F8:DA:AC:CD:A5	54	g	Hon Hai Precision Ind.
CASA_COMERCIAL	-76	13+9	WPA2-Personal	DC:9F:DB:36:A4:60	300	n	Ubiquiti Networks, Inc.
dlink	-77	6	Open	14:D6:4D:BA:20:10	72	n	D-Link International
CAMARA_COMERCIO	-78	6	WPA-Personal	00:21:63:DE:14:6A	54	g	ASKEY COMPUTER COI
Claro_CADENA000056	-79	11	WEP	C0:F8:DA:AC:B6:47	54	g	Hon Hai Precision Ind.
PLATINO4LIFE	-79	11+7	WPA-Personal	00:E0:4D:BF:6A:48	135	n	INTERNET INITIATIVE J.
83572914	-79	6	WEP	00:1E:58:C5:0E:65	54	g	D-Link Corporation
Claro_GUAMANI00004	-79	11	WEP	88:9F:FA:4A:94:D5	54	g	Hon Hai Precision Ind.
TORRES	-79	6	WPA-Personal	00:21:63:DF:D3:B3	54	g	ASKEY COMPUTER COI



Nodo 12: Simón Bolívar y García Moreno

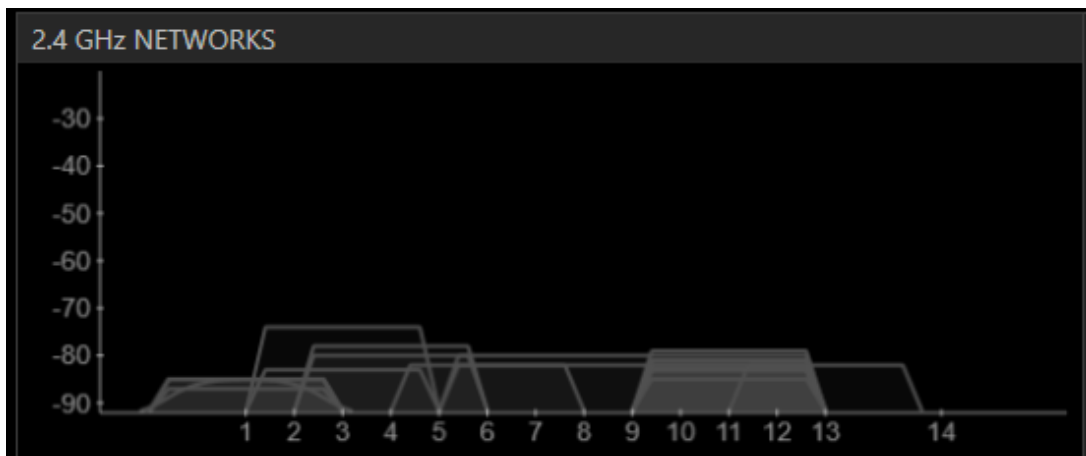
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ibarr@digital	-74	3	Open	00:15:6D:69:3B:A0	54	g	Ubiquiti Networks Inc.
ibarradigital	-78	4	Open	00:15:6D:69:3B:A1	54	g	Ubiquiti Networks Inc.
IMITI	-79	11	WPA-Personal	00:0D:54:A0:BA:13	54	g	3Com Ltd
MIRIAN	-80	11+7	WPA-Personal	BC:76:70:DD:98:78	270	n	Huawei Device Co., Ltd
ibarradigital	-80	4	Open	00:15:6D:6B:11:CA	54	g	Ubiquiti Networks Inc.
FLIA: PARRAGA	-81	11	WPA2-Personal	4C:8B:EF:2B:0F:E4	270	n	
Claro_JARAMILLOARQL	-81	11	WEP	88:9F:FA:4A:9D:57	54	g	Hon Hai Precision Ind.
gato	-81	11	WPA-Personal	00:26:B6:81:AE:32	54	g	Askey Computer
Consuelo	-82	11	WPA-Personal	00:26:B6:4A:8C:E6	54	g	Askey Computer
Cartagena	-82	11+7	WPA-Personal	00:E0:4D:9B:63:48	135	n	INTERNET INITIATIVE J.
dlinklocal	-82	6	WPA2-Personal	14:D6:4D:B4:5C:14	72	n	D-Link International
Organo Gold	-82	11	WPA2-Personal	88:53:D4:B0:B1:88	270	n	Huawei Technologies C
Enmita	-82	13	WPA-Personal	00:27:22:EC:77:21	130	n	Ubiquiti Networks
Claro_SILVA000049411	-83	11	WEP	EC:55:F9:62:B9:A5	144	n	Hon Hai Precision Ind.



Nodo 13: Simón Bolívar y Juan José Flores

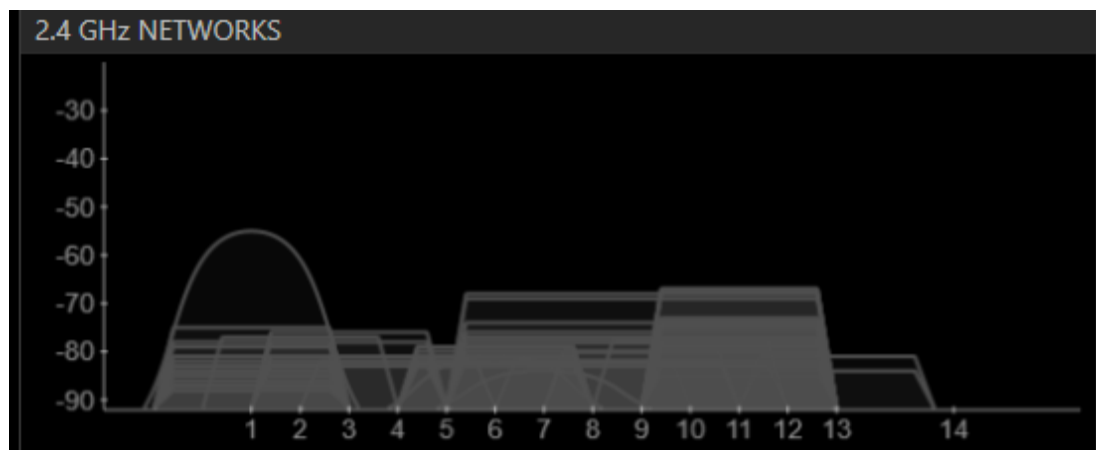
File View Help

LEARN NETWORKS

✕ Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
Online Private Network	-55	1	WPA2-Personal	00:27:22:98:82:3D	11	b	Ubiquiti Networks
COPYCENTER	-67	11	WPA2-Personal	88:53:D4:B0:81:54	270	n	Huawei Technologies C
WORKS&FUN	-67	11	WPA2-Personal	F8:3D:FF:1E:E8:88	270	n	Huawei Technologies C
SIN COSTURAS	-67	11	WPA2-Personal	4C:8B:EF:50:F6:60	270	n	
MICHELOB.	-68	11	WPA2-Personal	F8:3D:FF:1D:5B:EC	270	n	Huawei Technologies C
CONTAXCOM	-68	11+7	WPA-Personal	00:E0:4D:D7:62:30	135	n	INTERNET INITIATIVE J.
Don Lucho	-69	11+7	WPA-Personal	BC:76:70:E4:11:F8	270	n	Huawei Device Co., Ltd
HUGO ACOSTA	-73	11	WPA2-Personal	88:53:D4:C5:D5:C0	270	n	Huawei Technologies C
CHRISTIAN	-74	11	WPA2-Personal	4C:8B:EF:2B:29:D8	270	n	
freeNet-WiFi-MCO	-74	11	WPA2-Personal	CC:B2:55:1D:DE:98	150	n	D-Link International
INTERNET CNT	-74	11	WPA-Personal	00:26:B6:83:19:D2	54	g	Askey Computer
ORTEGA SHOES	-74	11	WPA2-Personal	88:53:D4:FB:14:E8	270	n	Huawei Technologies C
MAGAP_ZONA1	-74	11+7	WPA2-Personal	F8:3D:FF:1D:47:10	270	n	Huawei Technologies C
GPI_wifi	-75	1	WPA2-Personal	C2:9F:DB:97:27:B3	130	n	



Nodo 14: Simón Bolívar y Miguel Oviedo

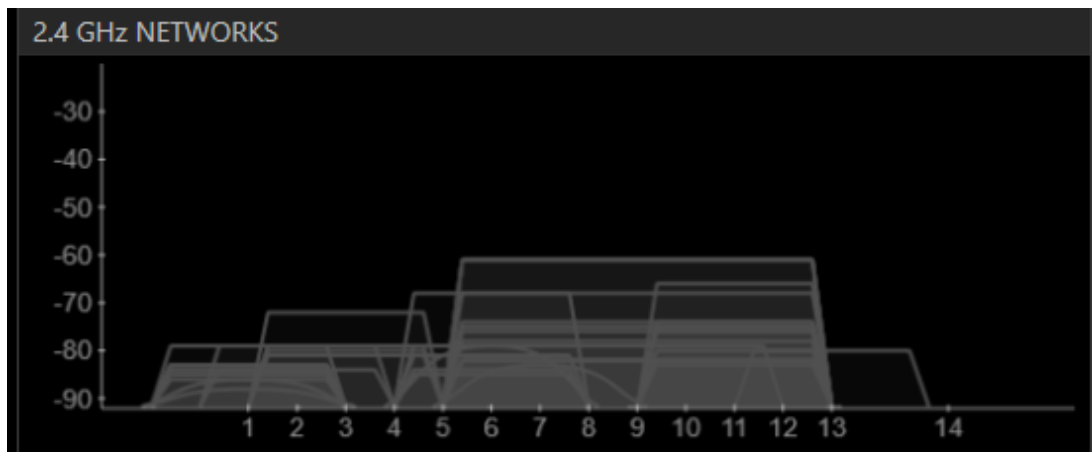
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
CONTAXCOM	-61	11+7	WPA-Personal	00:E0:4D:D7:62:30	135	n	INTERNET INITIATIVE J
MIRIAN	-61	11+7	WPA2-Personal	A4:99:47:7F:3C:94	270	n	Huawei Technologies C
CARLOS IBARRA	-61	11+7	WPA-Personal	BC:76:70:E1:E8:2C	270	n	Huawei Device Co., Ltd
d-pilate	-66	11	WPA2-Personal	4C:8B:EF:2B:3E:EC	270	n	
MAURICIO MALES	-68	6	WPA2-Personal	88:53:D4:B0:BB:BC	270	n	Huawei Technologies C
JUAN FCO VACA	-68	11+7	WPA-Personal	BC:76:70:E2:1E:BC	270	n	Huawei Device Co., Ltd
Mundy_Express	-72	3	WPA-Personal	F4:EC:38:FB:37:F8	54	g	TP-LINK TECHNOLOGII
FREAKY MONKEY	-74	11	WPA2-Personal	4C:8B:EF:4F:78:D0	270	n	
MATIAS	-74	11+7	WPA-Personal	00:E0:4D:9E:95:08	135	n	INTERNET INITIATIVE J
FAMILIA LASTRA	-75	11	WPA-Personal	00:26:B6:82:3C:2E	54	g	Askey Computer
MM Asesores Contable	-75	11+7	WPA-Personal	BC:76:70:E5:08:E0	270	n	Huawei Device Co., Ltd
FLIA ACOSTA	-76	11+7	WPA2-Personal	88:53:D4:91:FA:C4	270	n	Huawei Technologies C
CHRISTIAN	-76	11	WPA2-Personal	4C:8B:EF:2B:29:D8	270	n	
JANETH SANTILLAN	-78	11+7	WPA2-Personal	08:7A:4C:AE:B1:10	270	n	



Nodo 15: Simón Bolívar y Pedro Moncayo

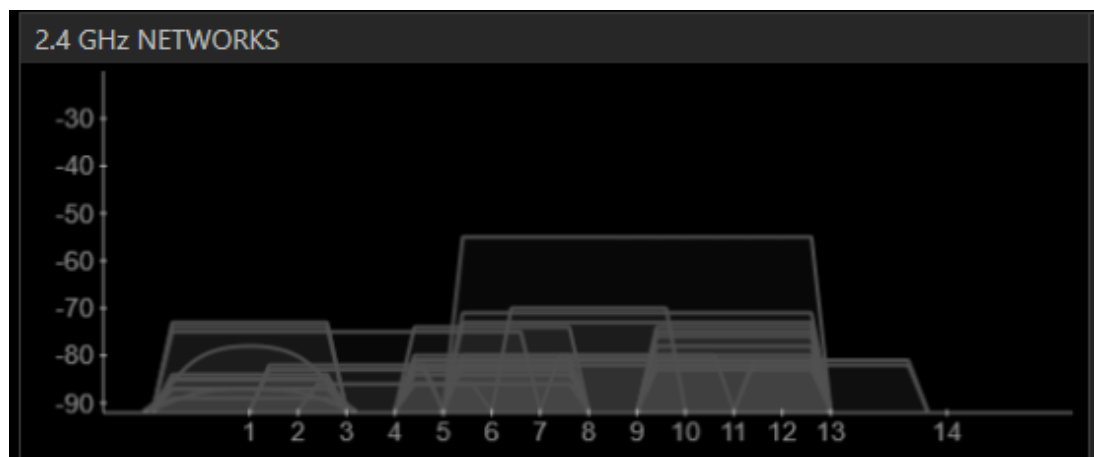
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
EL DESCUENTO	-55	11+7	WPA-Personal	00:E0:4D:A0:17:90	135	n	INTERNET INITIATIVE J.
ORAL-DENTAL	-70	8	WEP	00:27:19:19:42:F0	54	g	TP-LINK TECHNOLOGII
MAURICIO	-71	11+7	WPA-Personal	BC:76:70:E1:E7:CC	270	n	Huawei Device Co., Ltd
FON_freeNet-WiFi	-76	1	Open	00:18:84:A5:D3:B5	54	g	Fon Technology S.L.
CELULAR CENTER	-73	11+7	WPA2-Personal	08:63:61:B3:50:64	270	n	
Claro_GUEVARA00005E	-82	6	WEP	CC:AF:78:35:D5:42	54	g	Hon Hai Precision Ind.
freeNet-WiFi-Oficina	-78	1	WPA2-Personal	00:18:84:A5:D3:B6	54	g	Fon Technology S.L.
freeNet-WiFi-MCO	-74	11	WPA2-Personal	CC:B2:55:1D:DE:98	150	n	D-Link International
IMSA	-75	1+5	WPA2-Personal	00:E0:4D:D7:8F:10	135	g, n	INTERNET INITIATIVE J.
	-75	11	WPA2-Personal	20:3A:07:96:1F:48	144	n	
Claro_MACIAS0000788	-76	11	WEP	CC:AF:78:5F:4B:35	144	n	Hon Hai Precision Ind.
apantenainternetUELIC	-78	11	WPA-Personal	00:26:5A:6F:EC:8E	54	g	D-Link Corporation
meraki-scanning	-78	1	Open	00:18:0A:01:50:15	11	b	Meraki, Inc.
prueba	-80	9	Open	DC:9F:DB:9C:12:86	130	n	Ubiquiti Networks, Inc.



Nodo 16: Simón Bolívar y Juan de Velasco

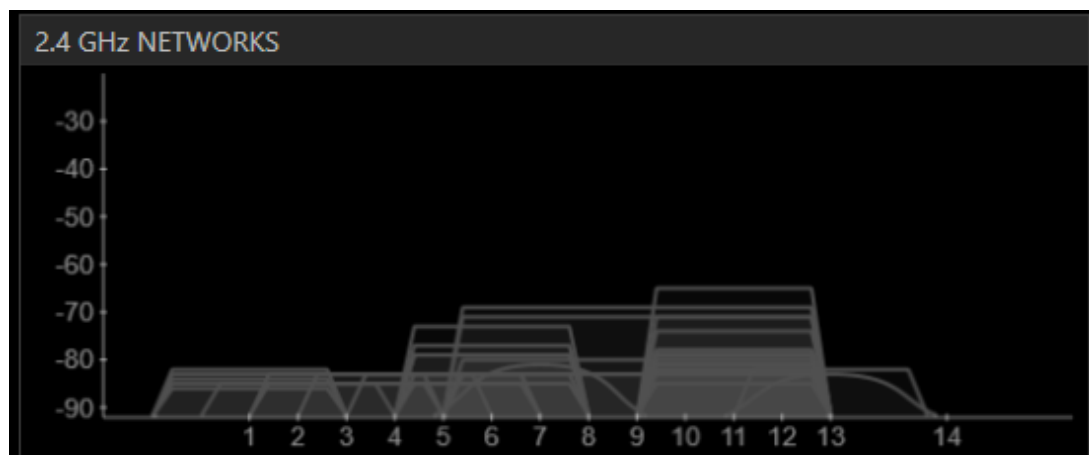
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS + - SSID or Vendor Channel > < Signal Security 802.11

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ODONTOIMAGENES	-65	11	WPA2-Personal	F8:3D:FF:1D:4E:94	270	n	Huawei Technologies C
CELULAR CENTER	-69	11+7	WPA2-Personal	08:63:61:83:50:64	270	n	
Claro_MACIAS0000788	-71	11	WEP	CC:AF:78:5F:4B:35	144	n	Hon Hai Precision Ind.
MAURICIO	-71	11+7	WPA2-Personal	BC:76:70:E1:E7:CC	270	n	Huawei Device Co., Ltd
COMUNITY1	-73	6	WPA2-Personal	FC:75:16:45:AF:94	72	n	D-Link International
Claro_JURADO0000885	-74	11	WEP	F4:B7:E2:5F:87:2D	72	n	
Central	-77	6	WEP	00:1E:58:96:21:DE	54	g	D-Link Corporation
Tania Fuentes	-78	11	WPA2-Personal	4C:8B:EF:16:63:10	270	n	
Claro_PATRONATOMIIN	-78	11	WEP	C0:F8:DA:78:14:86	54	g	Hon Hai Precision Ind.
link_la_salle2	-79	6	Open	00:18:39:0C:AB:9E	54	g	Cisco-Linksys LLC
ARTE MAGICO	-79	11	WPA2-Personal	88:53:D4:FB:0F:14	270	n	Huawei Technologies C
PATRONATOI	-79	6	WPA2-Personal	1C:7E:E5:8A:EC:96	72	n	D-Link International
NEGRITA	-80	11	WPA2-Personal	F8:3D:FF:1E:E2:F0	270	n	Huawei Technologies C
Medicos del Mundo_Cl	-80	11+7	WPA2-Personal	00:E0:4D:D7:20:70	135	n	INTERNET INITIATIVE J



Nodo 17: Simón Bolívar y Cristóbal Colón

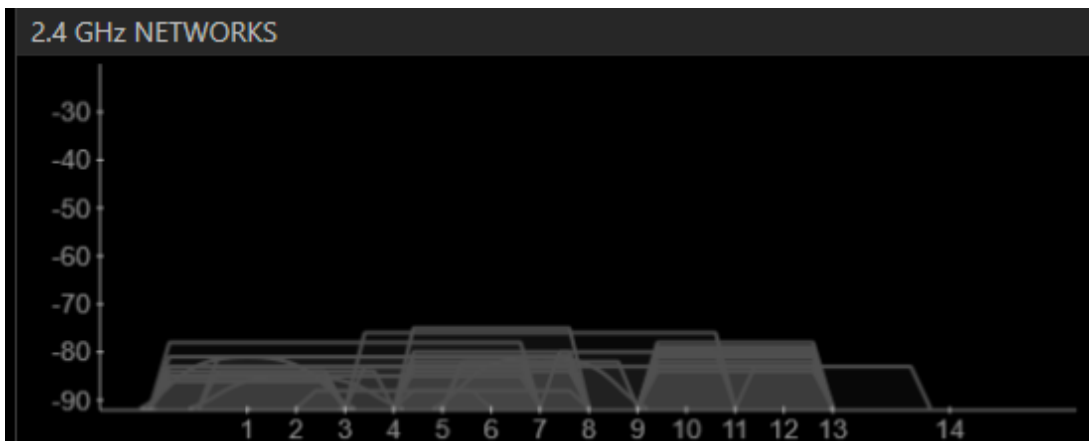
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security 802.11

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
Central	-75	6	WEP	00:1E:58:96:21:DE	54	g	D-Link Corporation
ibarradigit@l	-76	9+5	Open	90:F6:52:A4:89:90	300	n	TP-LINK TECHNOLOGII
Tania Fuentes	-78	11	WPA2-Personal	4C:8B:EF:16:63:10	270	n	
Control Comisariato	-68	5+1	WPA2-Personal	1C:7E:E5:34:AA:94	300	n	D-Link International
ARTE MAGICO	-79	11	WPA2-Personal	88:53:D4:FB:0F:14	270	n	Huawei Technologies C
juliana	-80	11	WPA-Personal	00:21:63:E0:4A:0F	54	g	ASKEY COMPUTER COI
Familia Moran	-80	11	WEP	BC:76:70:E1:E6:40	130	n	Huawei Device Co., Ltd
NEGRITA	-80	11	WPA2-Personal	F8:3D:FF:1E:E2:F0	270	n	Huawei Technologies C
JIREH CYBERCAFE 1	-80	9	WPA2-Personal	BC:F6:85:3E:FC:F0	144	n	D-Link International
DP_IBARRA	-80	6	WPA2-Personal	20:3A:07:CB:0F:C0	144	n	
FLIA PEREZ	-80	11	WPA-Personal	00:26:B6:4A:13:8A	54	g	Askey Computer
dpe-imbabura	-81	11	WPA2-Personal	C8:CB:B8:9C:7A:D0	300	n	
ibarra111	-81	7	Open	00:02:2D:61:60:E1	11	b	Agere Systems
DIEGO_Network	-81	6+2	WPA2-Personal	94:44:52:42:CF:1C	300	n	Belkin International, Inc



Nodo 18: Antonio José de Sucre y Miguel Oviedo

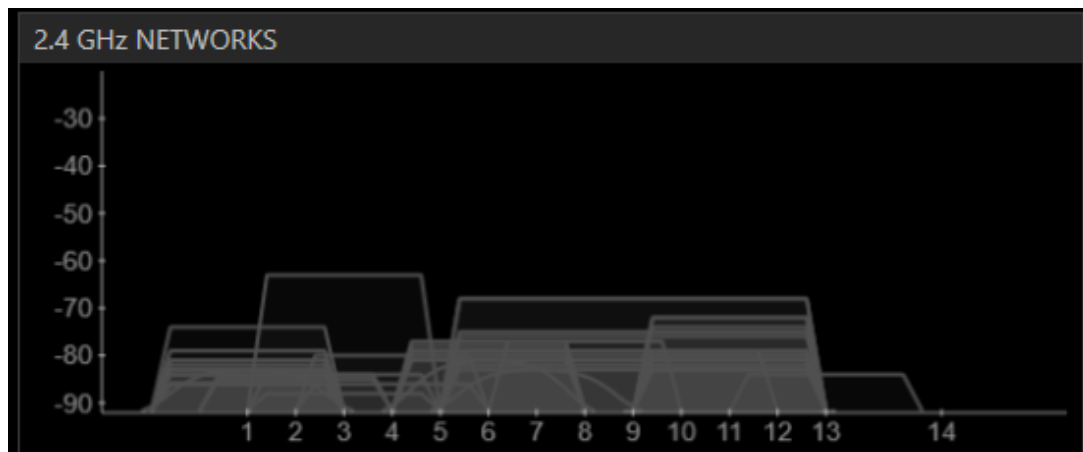
File View Help

LEARN NETWORKS

Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ibarradit@l	-63	3	Open	00:0C:42:69:9D:D0	54	g	Routerboard.com
JUAN FCO VACA	-68	11+7	WPA2-Personal	BC:76:70:E2:1E:BC	270	n	Huawei Device Co., Ltd
YURIBARRA	-68	11+7	WPA2-Personal	A4:99:47:84:42:78	270	n	Huawei Technologies C
CHRISTIAN	-72	11	WPA2-Personal	4C:8B:EF:2B:29:D8	270	n	
yuribarra	-72	11	WEP	00:22:80:B5:21:9A	54	g	D-Link Corporation
FREAKY MONKEY	-74	11	WPA2-Personal	4C:8B:EF:4F:78:D0	270	n	
Claro_MORALES000077	-74	1	WEP	C0:F8:DA:78:19:8F	54	g	Hon Hai Precision Ind.
systemPC	-75	11+7	WPA2-Personal	F8:3D:FF:1E:E2:48	270	n	Huawei Technologies C
CONTAXCOM	-76	11+7	WPA2-Personal	00:E0:4D:D7:62:30	135	n	INTERNET INITIATIVE J
YEPEZ	-77	8	WPA2-Personal	00:21:63:DF:E2:95	54	g	ASKEY COMPUTER COI
Picos	-77	6	WPA2-Personal	44:2B:03:7E:69:BC	144	n	Cisco Systems
INTERNETU	-78	6	WPA2-Personal	C2:9F:DB:F7:85:F6	130	n	
FERNANDO	-79	10+6	WPA2-Personal	BC:76:70:E7:54:78	270	n	Huawei Device Co., Ltd
LEONARDO CASTRO	-79	11	WPA2-Personal	4C:8B:EF:50:E5:E0	270	n	



Nodo 19: Antonio José de Sucre y Pedro Moncayo

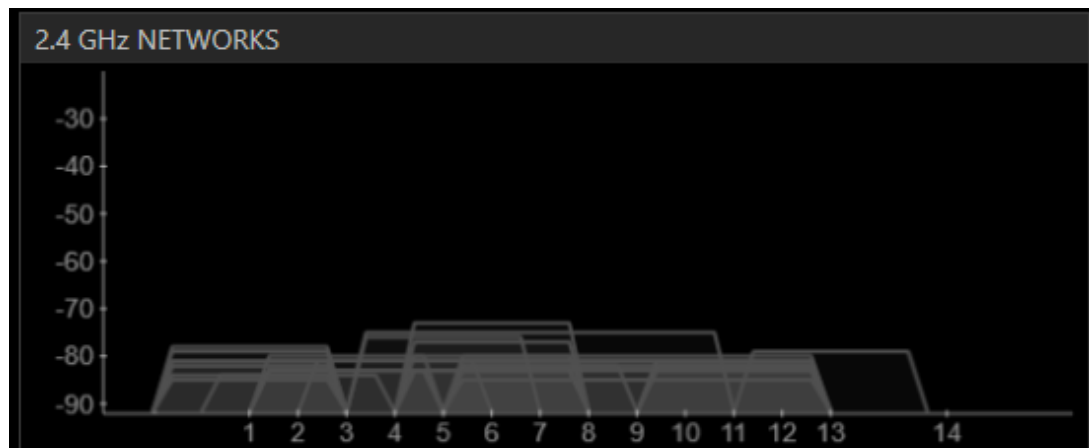
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
INTERNETU	-73	6	WPA2-Personal	C2:9F:DB:F7:85:F6	130	n	
ibarradigit@l	-75	9+5	Open	90:F6:52:A4:89:90	300	n	TP-LINK TECHNOLOGII
WSENECYT	-76	5	WPA2-Personal	54:78:1A:21:0C:C0	144	n	
Cevallos s4	-77	6	WPA2-Personal	CC:3A:61:7F:72:E8	72	n	
DSPI PBAJA	-78	1	WEP	00:1E:58:B4:55:46	54	g	D-Link Corporation
Enmita	-79	13	WPA-Personal	00:27:22:EC:77:21	130	n	Ubiquiti Networks
INFORCONT	-79	1	WPA-Personal	00:21:63:E0:4E:1A	54	g	ASKEY COMPUTER COI
IMLEX Abogados	-80	11+7	WPA2-Personal	4C:8B:EF:2B:3B:EC	270	n	
Central	-80	6	WEP	00:1E:58:96:21:DE	54	g	D-Link Corporation
ibarr@digital	-80	3	Open	00:15:6D:69:3B:A0	54	g	Ubiquiti Networks Inc.
FLIA_GARCIA	-81	11	WPA2-Personal	4C:8B:EF:4F:53:98	270	n	
JANETH SANTILLAN	-81	11+7	WPA2-Personal	08:7A:4C:AE:81:10	270	n	
Claro_MORAN000466	-81	11	WEP	EC:55:F9:5D:1A:9C	144	n	Hon Hai Precision Ind.
ibarradigital	-81	4	Open	00:15:6D:69:3B:A1	54	g	Ubiquiti Networks Inc.



Nodo 20: Antonio José de Sucre y Juan de Velasco

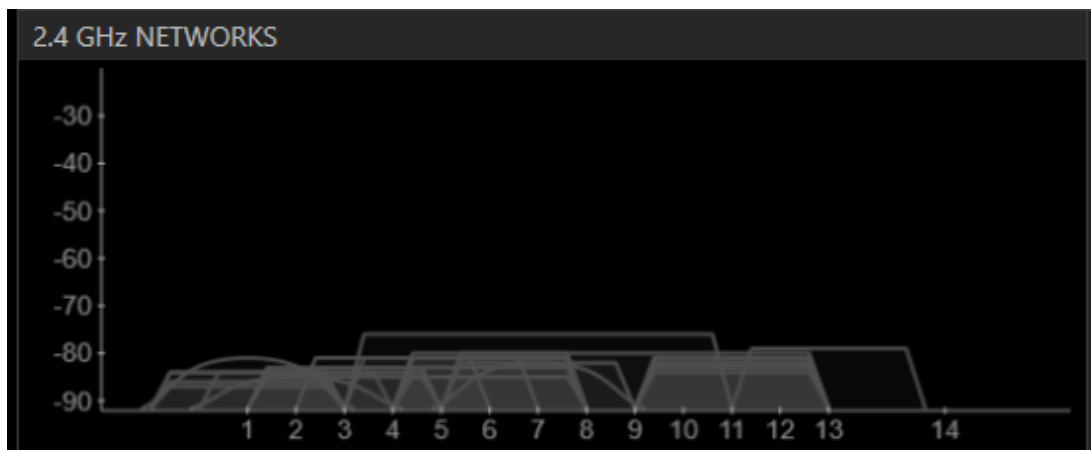
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ibarradigit@l	-76	9+5	Open	90:F6:52:A4:89:90	300	n	TP-LINK TECHNOLOGII
Enmita	-79	13	WPA-Personal	00:27:22:EC:77:21	130	n	Ubiquiti Networks
DP_IBARRA	-80	6	WPA2-Personal	20:3A:07:CB:0F:C0	144	n	
IMLEX Abogados	-80	11+7	WPA2-Personal	4C:8B:EF:2B:3B:EC	270	n	
Claro_MORAN0000466	-81	11	WEP	EC:55:F9:5D:1A:9C	144	n	Hon Hai Precision Ind.
GPI-TICs	-81	6	Open	D8:5D:4C:C3:CB:04	54	g	TP-LINK Technologies I
Central	-81	6	WEP	00:1E:58:96:21:DE	54	g	D-Link Corporation
WSENECYT	-81	5	WPA2-Personal	54:78:1A:21:0C:C0	144	n	
WORLDCOMPUTERS	-81	1	WEP	00:15:6D:1A:4F:AF	11	b	Ubiquiti Networks Inc.
FLIA_GARCIA	-81	11	WPA2-Personal	4C:8B:EF:4F:53:98	270	n	
Tania_Fuentes	-81	11	WPA2-Personal	4C:8B:EF:16:63:10	270	n	
dpe-imbabura	-81	11	WPA2-Personal	C8:CB:B8:9C:7A:D0	300	n	
FLIA PEREZ	-81	11	WPA-Personal	00:26:B6:4A:13:8A	54	g	Askey Computer
ibarradigital	-81	4	Open	00:15:6D:69:3B:A1	54	g	Ubiquiti Networks Inc.



Nodo 21: Antonio José de Sucre y Cristóbal Colón

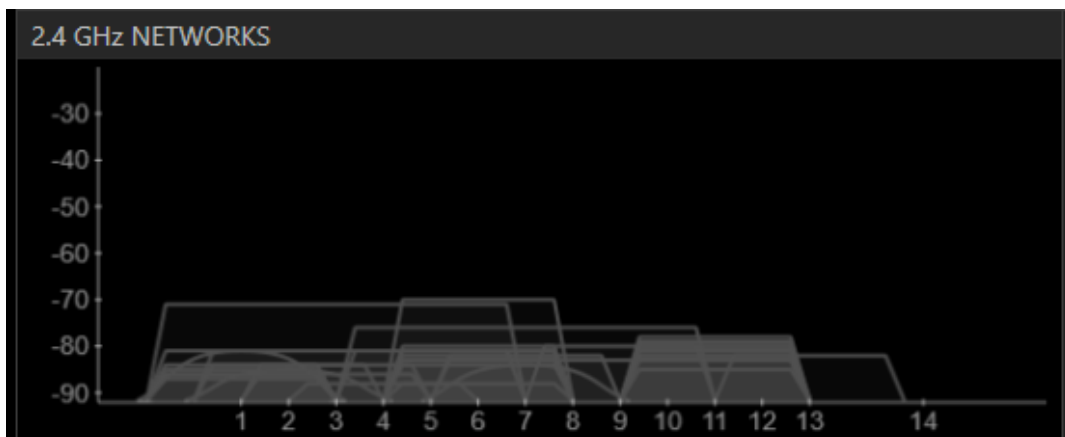
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
Central	-70	6	WEP	00:1E:58:96:21:DE	54	g	D-Link Corporation
UCACNORFIREWALL	-71	1+5	WPA2-Personal	90:F6:52:3D:3A:24	300	n	TP-LINK TECHNOLOGII
ibarradigit@l	-76	9+5	Open	90:F6:52:A4:89:90	300	n	TP-LINK TECHNOLOGII
NEGRITA	-78	11	WPA2-Personal	F8:3D:FF:1E:E2:F0	270	n	Huawei Technologies C
ARTE MAGICO	-79	11	WPA2-Personal	88:53:D4:FB:0F:14	270	n	Huawei Technologies C
Familia Moran	-80	11	WEP	BC:76:70:E1:E6:40	130	n	Huawei Device Co., Ltd
juliana	-80	11	WPA-Personal	00:21:63:E0:4A:0F	54	g	ASKEY COMPUTER COI
DP_IBARRA	-80	6	WPA2-Personal	20:3A:07:CB:0F:CO	144	n	
FLIA PEREZ	-80	11	WPA-Personal	00:26:B6:4A:13:8A	54	g	Askey Computer
JIREH CYBERCAFE 1	-80	9	WPA2-Personal	BC:F6:85:3E:FC:F0	144	n	D-Link International
SANTAAGUA	-81	6	WPA2-Personal	F4:EC:38:FB:37:F6	54	g	TP-LINK TECHNOLOGII
WORLDCOMPUTERS	-81	1	WEP	00:15:6D:1A:4F:AF	11	b	Ubiquiti Networks Inc.
JIREH CYBERCAFE2	-81	1+5	WPA2-Personal	00:1C:F0:70:DD:DA	300	n	D-Link Corporation
DIEGO_Network	-81	6+2	WPA2-Personal	94:44:52:42:CF:1C	300	n	Belkin International, Inc



Nodo 22: Vicente Rocafuerte y García Moreno

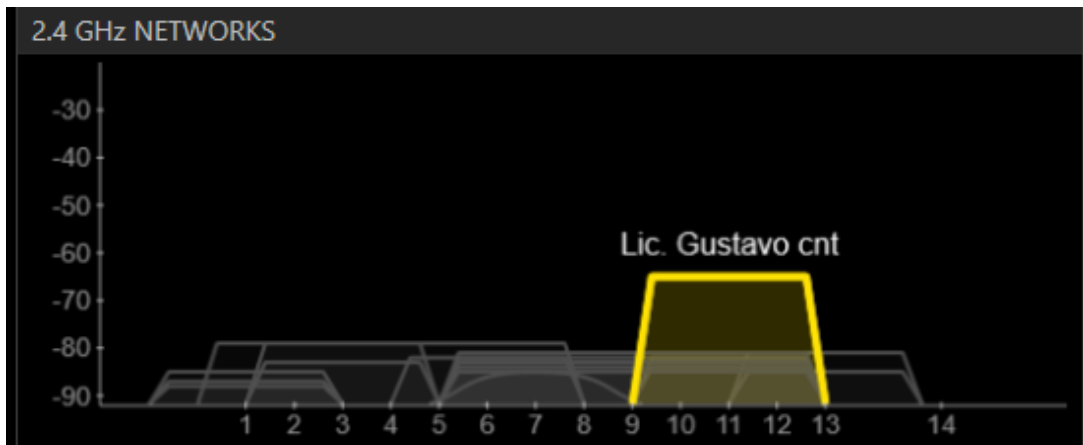
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
Lic. Gustavo cnt	-65	11	WPA2-Personal	4C:8B:EF:5E:C5:C4	270	n	
ibarradigit@l	-79	6+2	Open	90:F6:52:A4:9E:6A	300	n	TP-LINK TECHNOLOGII
ibarr@digital	-79	3	Open	00:15:6D:69:3B:A0	54	g	Ubiquiti Networks Inc.
WLANPUCESI	-81	13	WPA-Personal	00:80:48:53:31:DF	54	g	COMPEX INCORPORAT
Flia. Guamani	-81	11+7	WPA-Personal	00:E0:4D:BF:E8:A8	135	n	INTERNET INITIATIVE J.
AARON	-82	11+7	WPA-Personal	BC:76:70:EE:BB:7C	270	n	Huawei Device Co., Ltd
Android Ana Catalina	-82	6	WPA2-Personal	A4:EB:D3:7B:47:C5	65	n	
FLIA. CORAL	-82	11	WPA-Personal	00:26:B6:7B:D3:00	54	g	Askey Computer
ibarr@digital	-83	3	Open	00:15:6D:6B:0E:50	54	g	Ubiquiti Networks Inc.
FILIA RECALDE	-83	11+7	WPA-Personal	00:E0:4D:9E:E2:B0	135	n	INTERNET INITIATIVE J.
Dr. Aguilar	-83	11+7	WPA2-Personal	4C:8B:EF:50:F1:0C	270	n	
Yolanda	-84	11	WPA2-Personal	4C:8B:EF:50:EA:F4	270	n	
RT3390_2	-84	11+7	Open	00:E0:4D:9E:E2:B1	135	n	INTERNET INITIATIVE J.
Flia. Martinez	-85	11+7	WPA2-Personal	4C:8B:EF:4F:85:0C	270	n	



Nodo 23: Vicente Rocafuerte y Juan José Flores

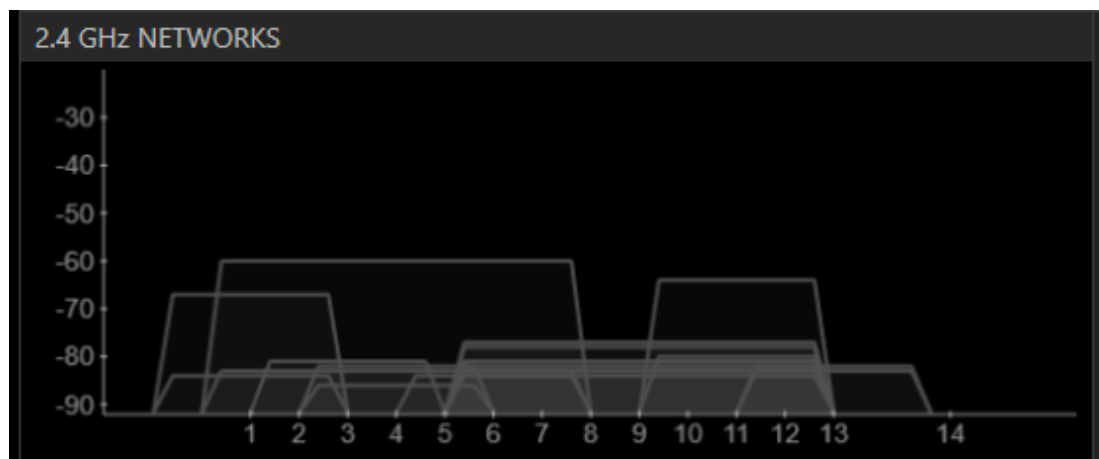
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS + - SSID or Vendor Channel > < Signal Security 802.11

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
ibarradigit@l	-60	6+2	Open	90:F6:52:A4:9E:6A	300	n	TP-LINK TECHNOLOGII
Yolanda	-64	11	WPA2-Personal	4C:8B:EF:50:EA:F4	270	n	
inticisco	-67	1	WPA2-Personal	48:F8:B3:21:46:7B	144	n	
FLIA OROZCO.	-77	11+7	WPA2-Personal	E8:CD:2D:33:04:5C	270	n	
BOLIVAR NELSON	-78	11+7	WPA2-Personal	4C:8B:EF:4F:53:20	270	n	
FLIAJAUREGUI	-80	11	WPA2-Personal	F8:3D:FF:1E:E3:00	270	n	Huawei Technologies C
PRIMERA IMPRESION	-81	11+7	WPA-Personal	BC:76:70:E5:22:0C	270	n	Huawei Device Co., Ltd
ibarr@digital	-81	3	Open	00:15:6D:6B:0E:50	54	g	Ubiquiti Networks Inc.
FLIA CHILUISA	-81	11+7	WPA-Personal	BC:76:70:E4:31:9C	270	n	Huawei Device Co., Ltd
ibarradigital	-82	4	Open	00:15:6D:69:3B:A1	54	g	Ubiquiti Networks Inc.
Enmita	-82	13	WPA-Personal	00:27:22:EC:77:21	130	n	Ubiquiti Networks
JORGE ALMEIDA	-82	11+7	WPA2-Personal	A4:99:47:7F:43:04	270	n	Huawei Technologies C
Diego	-83	6+2	WPA2-Personal	CC:B2:55:1D:DE:3A	150	n	D-Link International
IMLEX	-83	11+7	Open	00:E0:4D:D6:3A:38	135	n	INTERNET INITIATIVE J.



Nodo 24: Vicente Rocafuerte y Miguel Oviedo

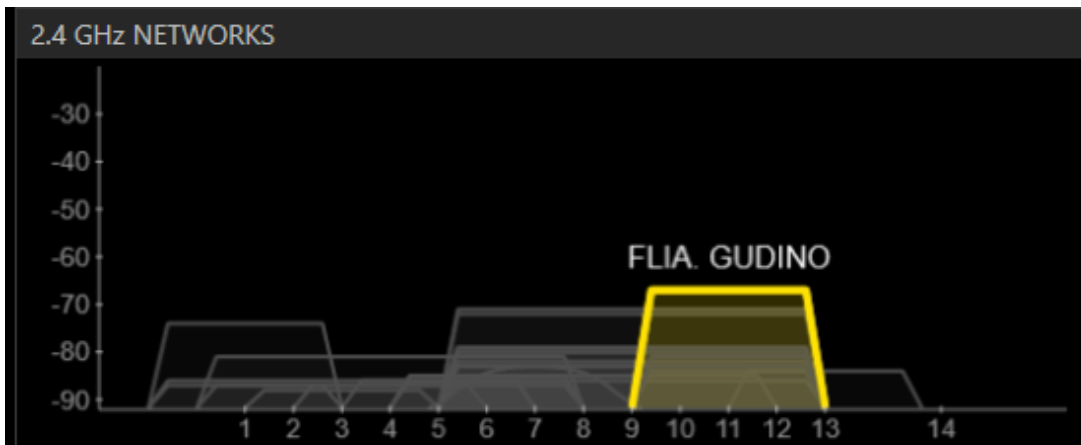
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
FLIA. GUDINO	-70	11	WPA-Personal	00:26:B6:4B:15:96	54	g	Askey Computer
FLIA.PAREDES	-71	11+7	WPA-Personal	BC:76:70:E5:1D:2C	270	n	Huawei Device Co., Ltd
Flia.Dolores	-72	11+7	WPA-Personal	00:E0:4D:C0:2D:50	135	n	INTERNET INITIATIVE J.
BOHEMIA	-71	1	WEP	88:A5:BD:00:2E:B7	54	g	QPCOM INC.
MARCO	-81	11+7	WPA-Personal	00:E0:4D:D7:B9:D0	135	n	INTERNET INITIATIVE J.
MAGO	-79	11+7	WPA2-Personal	88:53:D4:B1:BA:40	270	n	Huawei Technologies C
FLIA.ARROYO	-80	11+7	WPA-Personal	00:E0:4D:D7:BB:C8	135	n	INTERNET INITIATIVE J.
MANUEL	-80	11+7	WPA2-Personal	A4:99:47:96:44:A0	270	n	Huawei Technologies C
ALEJANDRO ALBUJA	-81	11	WPA2-Personal	A4:99:47:84:9C:50	270	n	Huawei Technologies C
DIEGO_Network	-81	6+2	WPA2-Personal	94:44:52:42:CF:1C	300	n	Belkin International, Inc
LARA	-82	11+7	WPA-Personal	00:E0:4D:BF:78:38	135	n	INTERNET INITIATIVE J.
PEDRO QUINTANA	-83	11	WPA2-Personal	A4:99:47:8D:A3:9C	270	n	Huawei Technologies C
ibarra111	-83	7	Open	00:02:2D:61:60:E1	11	b	Agere Systems
KAREN CNT	-83	11+7	WPA-Personal	00:E0:4D:D7:48:F8	135	n	INTERNET INITIATIVE J.



Nodo 25: Vicente Rocafuerte y Pedro Moncayo

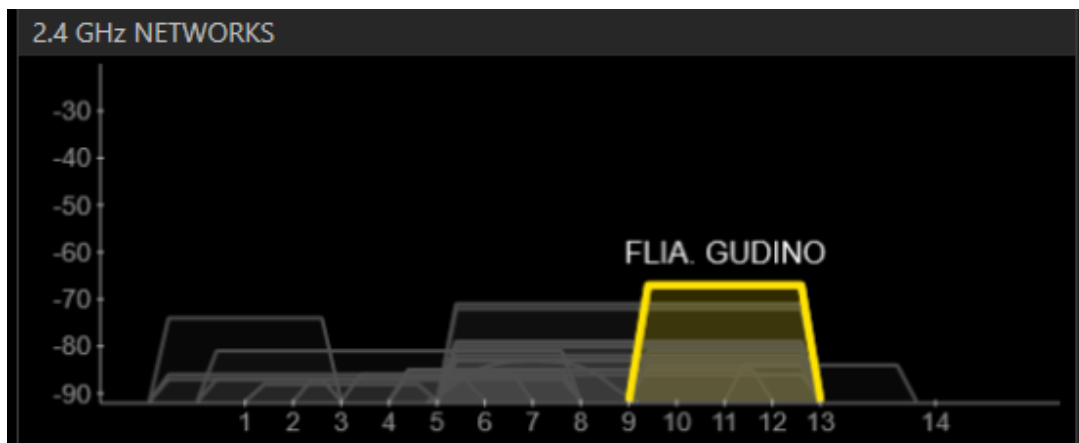
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
FLIA. GUDINO	-70	11	WPA-Personal	00:26:B6:4B:15:96	54	g	Askey Computer
FLIA.PAREDES	-71	11+7	WPA-Personal	8C:76:70:E5:1D:2C	270	n	Huawei Device Co., Ltd
Flia.Dolores	-72	11+7	WPA-Personal	00:E0:4D:C0:2D:50	135	n	INTERNET INITIATIVE J.
BOHEMIA	-71	1	WEP	88:A5:BD:00:2E:B7	54	g	QPCOM INC.
MARCO	-81	11+7	WPA-Personal	00:E0:4D:D7:B9:D0	135	n	INTERNET INITIATIVE J.
MAGO	-79	11+7	WPA2-Personal	88:53:D4:B1:BA:40	270	n	Huawei Technologies C
FLIA.ARROYO	-80	11+7	WPA-Personal	00:E0:4D:D7:BB:C8	135	n	INTERNET INITIATIVE J.
MANUEL	-80	11+7	WPA2-Personal	A4:99:47:96:44:A0	270	n	Huawei Technologies C
ALEJANDRO ALBUJA	-81	11	WPA2-Personal	A4:99:47:84:9C:50	270	n	Huawei Technologies C
DIEGO_Network	-81	6+2	WPA2-Personal	94:44:52:42:CF:1C	300	n	Belkin International, Inc
LARA	-82	11+7	WPA-Personal	00:E0:4D:BF:78:38	135	n	INTERNET INITIATIVE J.
PEDRO QUINTANA	-83	11	WPA2-Personal	A4:99:47:8D:A3:9C	270	n	Huawei Technologies C
ibarra111	-83	7	Open	00:02:2D:61:60:E1	11	b	Agere Systems
KAREN CNT	-83	11+7	WPA-Personal	00:E0:4D:D7:48:F8	135	n	INTERNET INITIATIVE J.



Nodo 26: Vicente Rocafuerte y Juan de Velasco

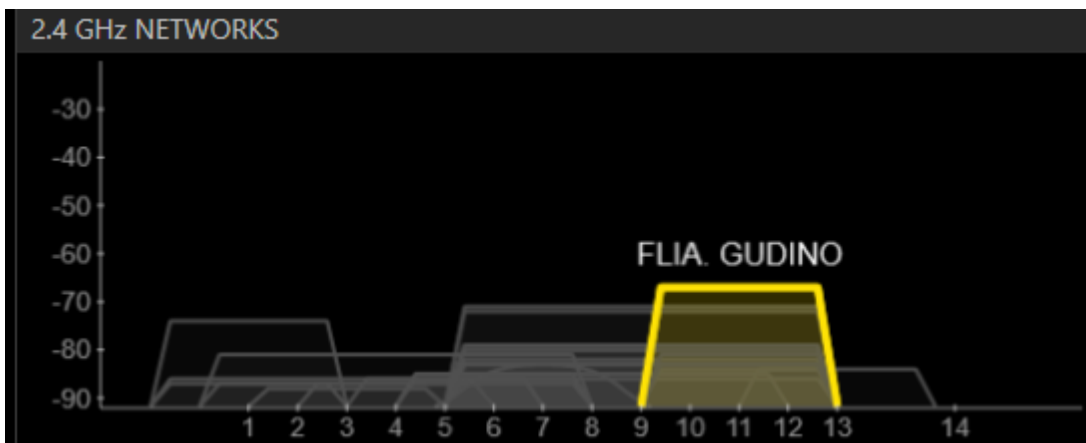
File View Help

LEARN NETWORKS

Star the network you are optimizing in the Networks list below

FILTERS

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
FLIA. GUDINO	-70	11	WPA-Personal	00:26:86:4B:15:96	54	g	Askey Computer
FLIA.PAREDES	-71	11+7	WPA-Personal	BC:76:70:E5:1D:2C	270	n	Huawei Device Co., Ltd
Flia.Dolores	-72	11+7	WPA-Personal	00:E0:4D:C0:2D:50	135	n	INTERNET INITIATIVE J
BOHEMIA	-71	1	WEP	88:A5:BD:00:2E:B7	54	g	QPCOM INC.
MARCO	-81	11+7	WPA-Personal	00:E0:4D:D7:B9:D0	135	n	INTERNET INITIATIVE J
MAGO	-79	11+7	WPA2-Personal	88:53:D4:B1:BA:40	270	n	Huawei Technologies C
FLIA.ARROYO	-80	11+7	WPA-Personal	00:E0:4D:D7:BB:C8	135	n	INTERNET INITIATIVE J
MANUEL	-80	11+7	WPA2-Personal	A4:99:47:96:44:A0	270	n	Huawei Technologies C
ALEJANDRO ALBUJA	-81	11	WPA2-Personal	A4:99:47:84:9C:50	270	n	Huawei Technologies C
DIEGO_Network	-81	6+2	WPA2-Personal	94:44:52:42:CF:1C	300	n	Belkin International, Inc
LARA	-82	11+7	WPA-Personal	00:E0:4D:BF:78:38	135	n	INTERNET INITIATIVE J
PEDRO QUINTANA	-83	11	WPA2-Personal	A4:99:47:8D:A3:9C	270	n	Huawei Technologies C
ibarra111	-83	7	Open	00:02:2D:61:60:E1	11	b	Agere Systems
KAREN CNT	-83	11+7	WPA-Personal	00:E0:4D:D7:48:F8	135	n	INTERNET INITIATIVE J



Nodo 27: Vicente Rocafuerte y Cristóbal Colón

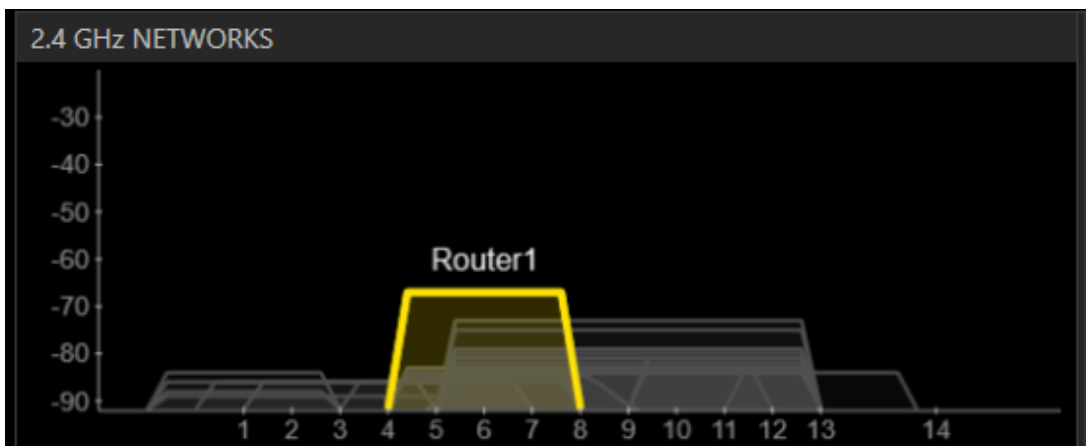
File View Help

LEARN NETWORKS

X Star the network you are optimizing in the Networks list below

FILTERS Security

SSID	SIGNAL	CHANNEL	SECURITY	MAC ADDRESS	MAX RATE	802.11	VENDOR
Router1	-67	6	WEP	00:21:91:E5:EA:E7	54	g	D-Link Corporation
FUNDACION 4 DE JULI	-73	11+7	WPA-Personal	BC:76:70:E5:07:0C	270	n	Huawei Device Co., Ltd
FLIA JARRIN	-75	11+7	WPA2-Personal	88:53:D4:C5:0F:80	270	n	Huawei Technologies C
MAGO	-79	11+7	WPA2-Personal	88:53:D4:B1:BA:40	270	n	Huawei Technologies C
GEOVANNYJC	-80	11+7	WPA-Personal	00:E0:4D:C1:71:30	135	n	INTERNET INITIATIVE J.
flia.Calvache	-81	11	WPA-Personal	00:26:B6:49:B7:86	54	g	Askey Computer
Andinatel	-81	11	WPA-Personal	00:21:63:DE:50:6F	54	g	ASKEY COMPUTER COI
LARA	-81	11+7	WPA-Personal	00:E0:4D:BF:78:38	135	n	INTERNET INITIATIVE J.
INTERNET un PAGO 09	-82	11+7	WPA-Personal	BC:76:70:D7:68:B1	270	n	Huawei Device Co., Ltd
ibarra111	-83	7	Open	00:02:2D:61:60:E1	11	b	Agere Systems
KAREN CNT	-83	11+7	WPA-Personal	00:E0:4D:D7:48:F8	135	n	INTERNET INITIATIVE J.
Gabyta	-83	11+7	WPA2-Personal	88:53:D4:9B:F2:3C	270	n	Huawei Technologies C
CSFI	-83	7	WEP	00:15:6D:60:A1:1E	11	b	Ubiquiti Networks Inc.
dlink	-83	6	Open	CC:82:55:D4:29:BA	300	n	D-Link International



ANEXO B

Especificación de requisitos de software

**Proyecto: Red de acceso inalámbrico para la zona
centro de la ciudad de San Miguel de Ibarra**

Noviembre del 2013

Instrucciones para el uso de este formato

Este formato es una plantilla tipo para documentos de requisitos del software.

Está basado y es conforme con el estándar IEEE Std 830-1998.

Las secciones que no se consideren aplicables al sistema descrito podrán de forma justificada indicarse como no aplicables (NA).

Notas:

Los textos en color azul son indicaciones que deben eliminarse y, en su caso, sustituirse por los contenidos descritos en cada apartado.

Los textos entre corchetes del tipo “[Inserte aquí el texto]” permiten la inclusión directa de texto con el color y estilo adecuado a la sección, al pulsar sobre ellos con el puntero del ratón.

Los títulos y subtítulos de cada apartado están definidos como estilos de MS Word, de forma que su numeración consecutiva se genera automáticamente según se trate de estilos “Titulo1, Titulo2 y Titulo3”.

La sangría de los textos dentro de cada apartado se genera automáticamente al pulsar Intro al final de la línea de título. (Estilos Normal indentado1, Normal indentado 2 y Normal indentado 3).

El índice del documento es una tabla de contenido que MS Word actualiza tomando como criterio los títulos del documento.

Una vez terminada su redacción debe indicarse a Word que actualice todo su contenido para reflejar el contenido definitivo.

Ficha del documento

Fecha	Revisión	Autor	Verificado dep. Calidad.
05/11/2013		Javier Aníbal Espinosa Martínez	

1 INTRODUCCIÓN

Este documento es una Especificación de Requisitos Software (ERS) para el Diseño de la red de acceso inalámbrico. Esta especificación se ha estructurado basándose en las directrices dadas por el estándar IEEE Práctica Recomendada para Especificaciones de Requisitos Software ANSI/IEEE 830, 1998.

1.1 PROPÓSITO

El presente documento tiene como propósito definir las especificaciones funcionales, no funcionales para el desarrollo de un diseño de red acceso que permitirá el acceso a internet y la red del GAD de San Miguel de Ibarra. Éste será utilizado por la ciudadanía.

1.2 ALCANCE

Esta especificación de requisitos está dirigida al usuario del sistema, para continuar con el plan del GAD de San Miguel de Ibarra de incluir TIC's (Tecnologías de Información y Comunicación), la cual tiene por objetivo principal mejorar la calidad de vida de los habitantes de la ciudad de Ibarra.

1.3 PERSONAL INVOLUCRADO

Nombre	Javier Aníbal Espinosa Martínez
Rol	Autor
Categoría Profesional	Tecnologías Inalámbricas y Redes de Comunicación

Responsabilidad	Realizar el Diseño de la Red
Información de contacto	jaem6@hotmail.com

1.4 DEFINICIONES, ACRÓNIMOS Y ABREVIATURAS

<i>Nombre</i>	<i>Descripción</i>
usuario	Persona que tendrá acceso a la red
ERS	Especificación de Requisitos Software
RF	Requerimiento Funcional
RNF	Requerimiento No Funcional
FTP	Protocolo de Transferencia de Archivos

1.5 REFERENCIAS

Título del Documento	Referencia
Standard IEEE 830 - 1998	IEEE

1.6 RESUMEN

Este documento consta de tres secciones. En la primera sección se realiza una introducción al mismo y se proporciona una visión general de la especificación de recursos del diseño.

En la segunda sección del documento se realiza una descripción general del diseño, con el fin de conocer las principales funciones que éste debe realizar, los datos asociados y los factores, restricciones, supuestos y dependencias que afectan al desarrollo, sin entrar en excesivos detalles.

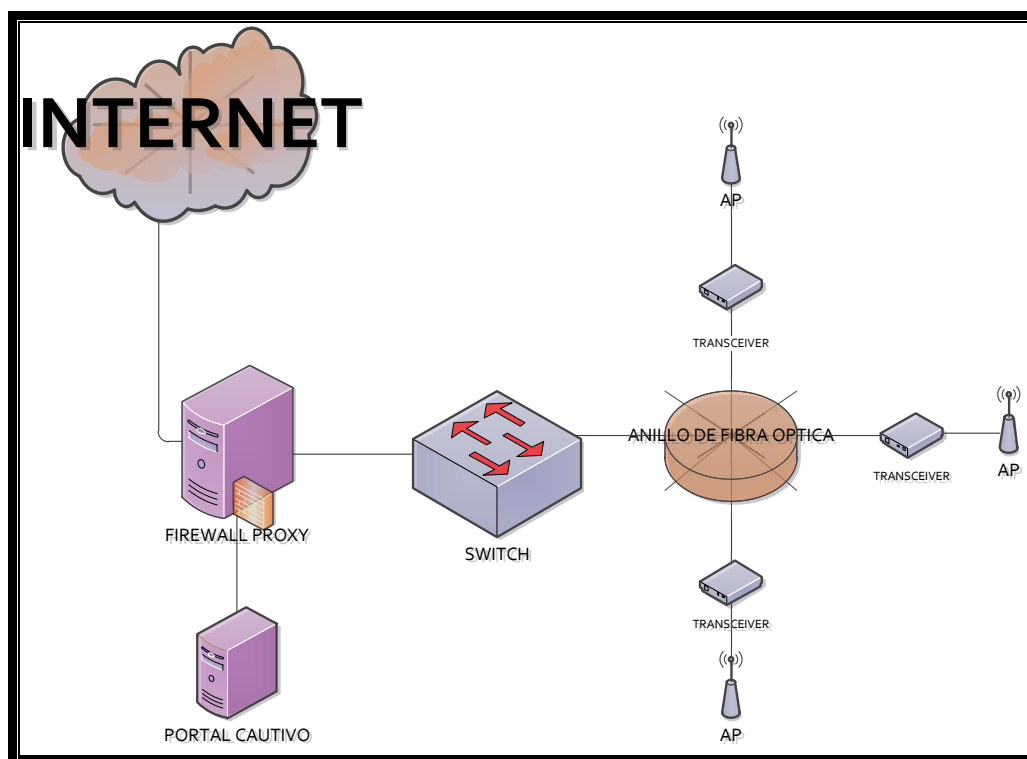
Por último, la tercera sección del documento es aquella en la que se definen detalladamente los requisitos que debe satisfacer el diseño.

2 DESCRIPCIÓN GENERAL

2.1 PERSPECTIVA DEL PRODUCTO

El diseño será un producto diseñado para acceso a Internet, lo que permitirá su utilización de forma rápida y eficaz, además se integrara conjuntamente con un servidor para lograr una mejor respuesta.

2.2 FUNCIONALIDAD DEL PRODUCTO



2.3 CARACTERÍSTICAS DE LOS USUARIOS

Tipo de usuario	Administrador
Formación	Conocimientos de Informática
Actividades	Control y manejo del sistema en general

Tipo de usuario	Visitante
Formación	NA
Actividades	Acceso a la red de acceso

2.4 RESTRICCIONES

- Interfaz para ser usada con internet.
- Uso de Dominio (X)
- Lenguajes y tecnologías en uso: HTML, JAVA.
- Los servidores deben ser capaces de atender consultas concurrentemente.
- El sistema se diseñará según un modelo cliente/servidor.
- El sistema deberá tener un diseño e implementación sencilla, independiente de la plataforma o del lenguaje de programación.

2.5 SUPOSICIONES Y DEPENDENCIAS

- Se asume que los requisitos aquí descritos son estables
- Los equipos en los que se vaya a ejecutar el sistema deben cumplir los requisitos antes indicados para garantizar una ejecución correcta de la misma

3 REQUISITOS ESPECÍFICOS

REQUERIMIENTOS DEL ACCESS POINT

Requerimientos Funcionales

IDENTIFICACIÓN DEL REQUERIMIENTO:	RF01
NOMBRE DEL REQUERIMIENTO:	AUTENTIFICACIÓN DE USUARIO.
CARACTERÍSTICAS:	PERMITA UNA AUTENTIFICACIÓN ABIERTA.
DESCRIPCIÓN DEL REQUERIMIENTO:	LOS USUARIOS DEBERÁN PODER INGRESAR SIN NECESIDAD DE UNA CLAVE.
REQUERIMIENTO NO FUNCIONAL:	<ul style="list-style-type: none"> • RNF01 • RNF02
<p>PRIORIDAD DEL REQUERIMIENTO:</p> <p>Alta</p>	

REQUERIMIENTOS DEL PORTAL CAUTIVO

IDENTIFICACIÓN DEL REQUERIMIENTO:	RF02
NOMBRE DEL	REGISTRAR USUARIOS.

REQUERIMIENTO:	
CARACTERÍSTICAS:	LOS USUARIOS DEBEN PODER SER REGISTRADOS DE UNA MANERA SENCILLA
DESCRIPCIÓN DEL REQUERIMIENTO:	EL USUARIO SERÁ REGISTRADO EN EL SERVIDOR.
REQUERIMIENTO NO FUNCIONAL:	<ul style="list-style-type: none"> • RNF01 • RNF02 • RNF05 • RNF08
<p style="text-align: center;">PRIORIDAD DEL REQUERIMIENTO:</p> <p>Alta</p>	

REQUERIMIENTOS DEL SOFTWARE DE LOS ACCESS POINT

IDENTIFICACIÓN DEL REQUERIMIENTO:	RF03
NOMBRE DEL REQUERIMIENTO:	ADMINISTRAR NODOS
CARACTERÍSTICAS:	Los equipos de la red podrán ser administrados y su licencia deberá ser gratuita.
DESCRIPCIÓN DEL REQUERIMIENTO:	SE TENDRÁ LA CAPACIDAD DE VER EL ESTADO DE LOS NODOS

REQUERIMIENTO NO FUNCIONAL:	<ul style="list-style-type: none"> • RNF01 • RNF02
PRIORIDAD DEL REQUERIMIENTO:	
Alta	

REQUERIMIENTO PARA TODO EL SOFTWARE

Requerimientos No Funcionales.

IDENTIFICACIÓN DEL REQUERIMIENTO:	RNF01
NOMBRE DEL REQUERIMIENTO:	INTERFAZ DEL SISTEMA.
CARACTERÍSTICAS:	EL SISTEMA PRESENTARA UNA INTERFAZ DE USUARIO SENCILLA PARA QUE SEA DE FÁCIL MANEJO A LOS USUARIOS DEL SISTEMA.
DESCRIPCIÓN DEL REQUERIMIENTO:	El sistema debe tener una interfaz de uso intuitiva y sencilla.
PRIORIDAD DEL REQUERIMIENTO:	
Alta	

IDENTIFICACIÓN DEL REQUERIMIENTO:	RNF02
NOMBRE DEL REQUERIMIENTO:	MANTENIMIENTO.
CARACTERÍSTICAS:	El sistema deberá de tener un manual de instalación y manual de usuario para facilitar los mantenimientos que serán realizados por el administrador.
DESCRIPCIÓN DEL REQUERIMIENTO:	El sistema debe disponer de una documentación fácilmente actualizable que permita realizar operaciones de mantenimiento con el menor esfuerzo posible.
PRIORIDAD DEL REQUERIMIENTO:	
Alta	

IDENTIFICACIÓN DEL REQUERIMIENTO:	RNF03
NOMBRE DEL REQUERIMIENTO:	DISEÑO DE LA INTERFAZ A LA CARACTERÍSTICA DE LA WEB.
CARACTERÍSTICAS:	El sistema deberá de tener una interfaz de usuario, teniendo en

	cuenta las características de la web de la institución.
DESCRIPCIÓN DEL REQUERIMIENTO:	La interfaz de usuario debe ajustarse a las características de la web de la institución.
PRIORIDAD DEL REQUERIMIENTO:	
Alta	

3.1 REQUISITOS COMUNES DE LAS INTERFACES

3.1.1 Interfaces de usuario

La interfaz con el usuario consistirá en un conjunto de ventanas con botones, listas y campos de textos. Ésta deberá ser construida específicamente para el sistema propuesto y, será visualizada desde un navegador de internet.

3.1.2 Interfaces de hardware

Será necesario disponer de equipos de cómputos en perfecto estado con las siguientes características:

- Adaptadores de red.
- Procesador de 1.66GHz o superior.
- Memoria mínima de 256Mb.
- Mouse.
- Teclado.

3.1.3 Interfaces de software

- Sistema Operativo: Ubuntu.
- Explorador: Mozilla o Chrome.

3.1.4 Interfaces de comunicación

Los servidores, clientes y aplicaciones se comunicarán entre sí, mediante protocolos estándares en internet, siempre que sea posible. Por ejemplo, para transferir archivos o documentos deberán utilizarse protocolos existentes (FTP u otros convenientes).

3.2 REQUISITOS FUNCIONALES

3.2.1 Requisito funcional 1

- **Autenticación de Usuarios:** los usuarios no deberán identificarse para acceder a la red.
 - ✓ El sistema deberá permitir el acceso a los usuarios automáticamente.

3.2.2 Requisito funcional 2

- **Registrar Usuarios:** se deberá poder registrar los usuarios de una manera sencilla.
 - ✓ El registro permitirá la administración de la red.

3.2.3 Requisito funcional 3

- **Administrar Nodos:** Los equipos de la red deberán poder ser administrados.
 - ✓ Se debe poder saber si los equipos están funcionando y si lo hacen correctamente.

3.3 REQUISITOS NO FUNCIONALES

3.3.1 Requisitos de rendimiento

- Garantizar que el diseño no afecte el desempeño de la red.

3.3.2 Seguridad

- Garantizar la confiabilidad, la seguridad y el desempeño del diseño a los diferentes usuarios. En este sentido la información almacenada o registros realizados podrán ser consultados y actualizados permanente y simultáneamente, sin que se afecte el tiempo de respuesta.
- Garantizar la seguridad del sistema con respecto a la información y datos que se manejan tales sean documentos, archivos y contraseñas.
- Facilidades y controles para permitir el acceso a la información al personal autorizado a través de Internet, con la intención de consultar y subir información pertinente para cada una de ellas.

3.3.3 Fiabilidad

- El sistema debe tener una interfaz de uso intuitiva y sencilla

- La interfaz de usuario debe ajustarse a las características de la web de la institución, dentro de la cual estará incorporado el sistema de gestión de procesos y el inventario

3.3.4 Disponibilidad

- La disponibilidad debe ser continua con un nivel de servicio para los usuarios de 7 días por 24 horas, garantizando un esquema adecuado que permita la posible falla en cualquiera de sus componentes, contar con una contingencia, generación de alarmas.

3.3.5 Mantenibilidad

- El diseño debe disponer de una documentación fácilmente actualizable que permita realizar operaciones de mantenimiento con el menor esfuerzo posible
- La interfaz debe estar complementada con un buen sistema de ayuda (la administración puede recaer en personal con poca experiencia en el uso de aplicaciones informáticas).

3.3.6 Portabilidad

- El diseño será implantado bajo la plataforma de Ubuntu.

ACCESS POINT			
	Ubiquiti	Cisco	Mikrotik
Permite Autenticación Abierta	SI	SI	SI
Interfaz Gráfica de Autenticación	SI	SI	SI
Licencia Gratuita	SI	NO	NO
Convive con Ubuntu	SI	SI	SI
Documentación	SI	SI	SI
Poseen Software de Administración	SI	NO	NO

Tomando en cuenta los parámetros mostrados en la tabla anterior se toma la decisión de utilizar Ubiquiti debido a la licencia gratuita y que posee un software de administración.

ANEXO C

MANUAL DE ADMINISTRADOR

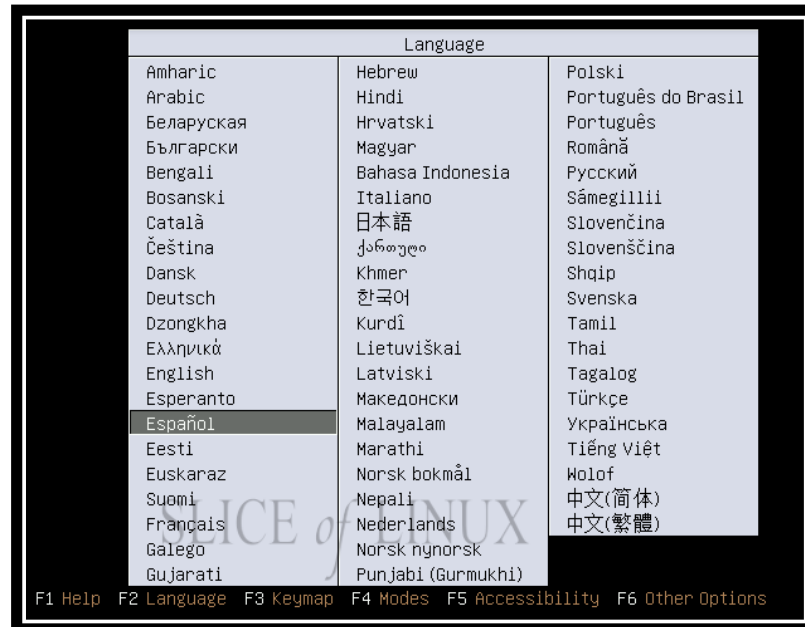
ÍNDICE

- 1. INSTALACIÓN Y CONFIGURACIÓN DE UBUNTU SERVER**
- 2. INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN**
- 3. INSTALACIÓN Y CONFIGURACIÓN DE FIREWALL SHOREWALL**
- 4. INSTALACIÓN Y CONFIGURACIÓN DE FIREWALL PROXY**
- 5. INSTALACIÓN Y CONFIGURACIÓN DE EASYHOTSPOT**

1. INSTALACIÓN DE UBUNTU SERVER

(<http://www.taringa.net/posts/info/3206877/Como-instalar-Ubuntu-Server-grafico-y-montate-un-servidor.html>)

Paso 1: Arranca el PC desde el CD de Ubuntu

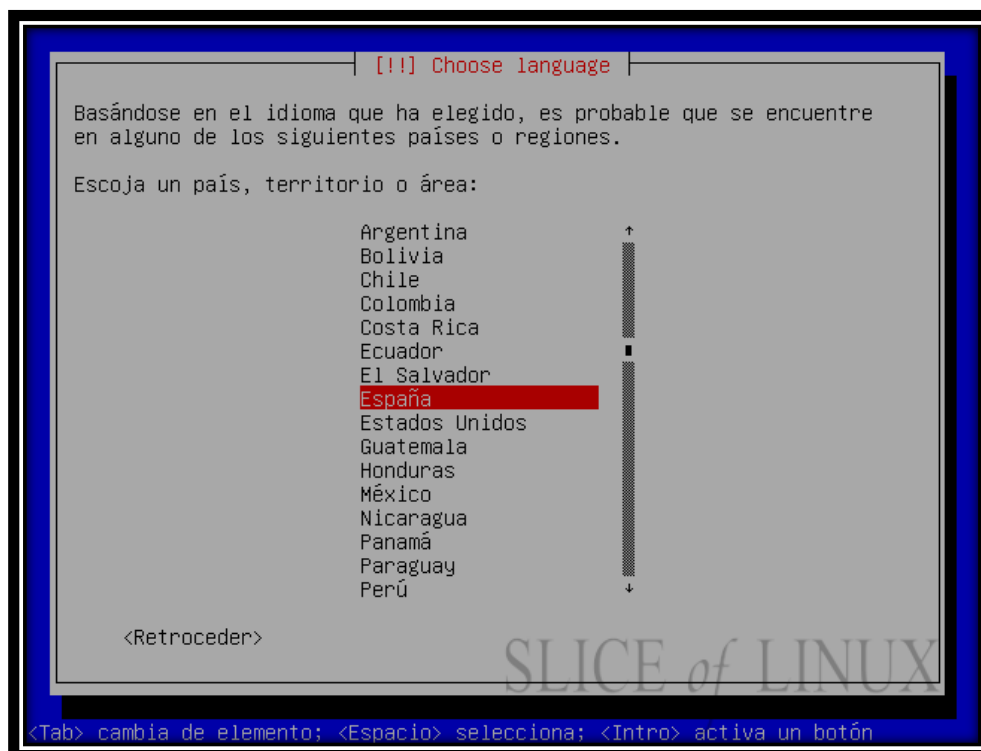


Arranquen desde el CD y llegarán a la pantalla de elección de idioma. Elijan su idioma y pulsen Intro. A continuación les saldrá esta pantalla:



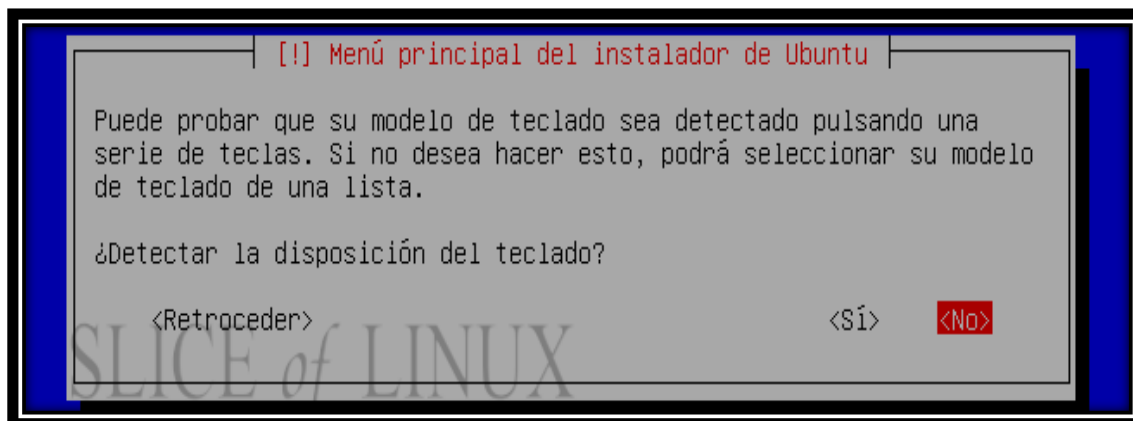
Seleccionen "Instalar Ubuntu Server" (sin las comillas) y pulsen Intro.

Paso 2: Elijan el país donde residen

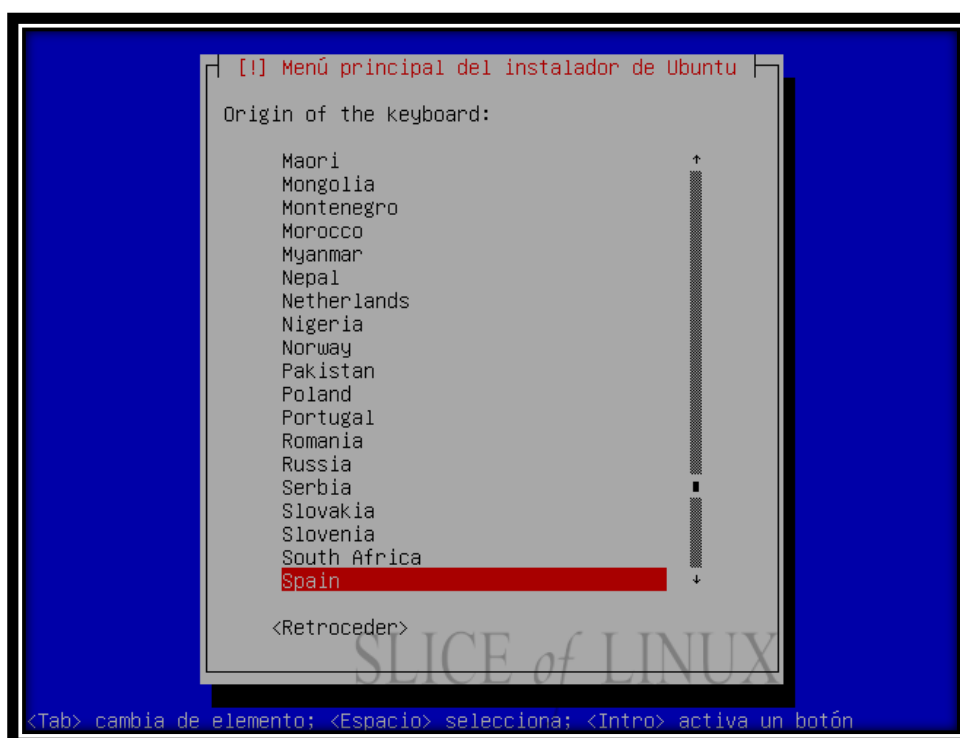


Seleccionen el país donde viven y pulsen Intro.

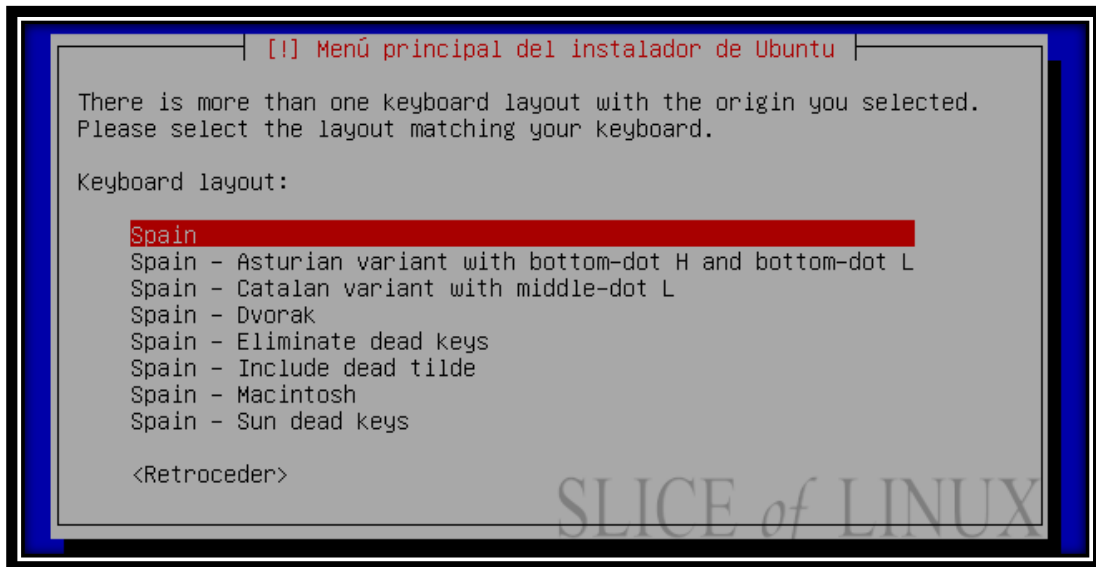
Paso 3: Elija la distribución de teclado



Les saltará una pantalla que les pregunta si desean que la instalación les detecte automáticamente la distribución de teclado. Pulsen No y llegarán a esta pantalla:

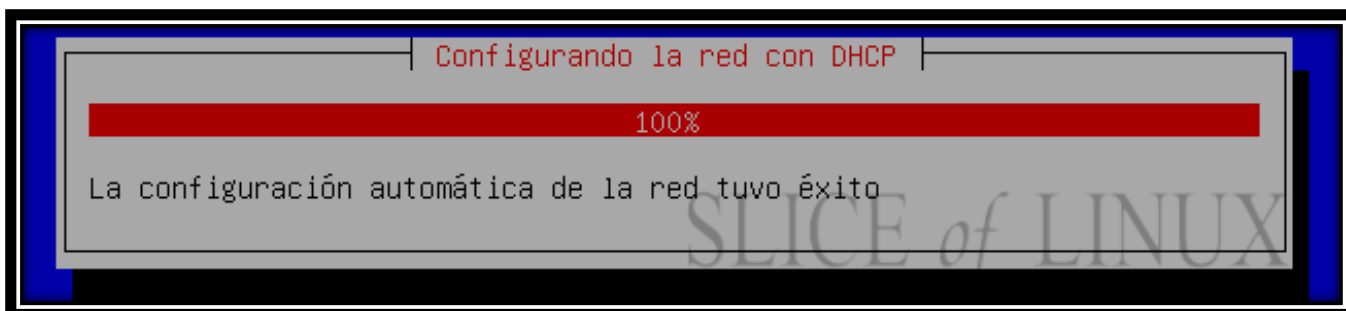


En esa pantalla elijan el país de origen de vuestro teclado y pulsen Intro. Llegarán a esta otra pantalla:



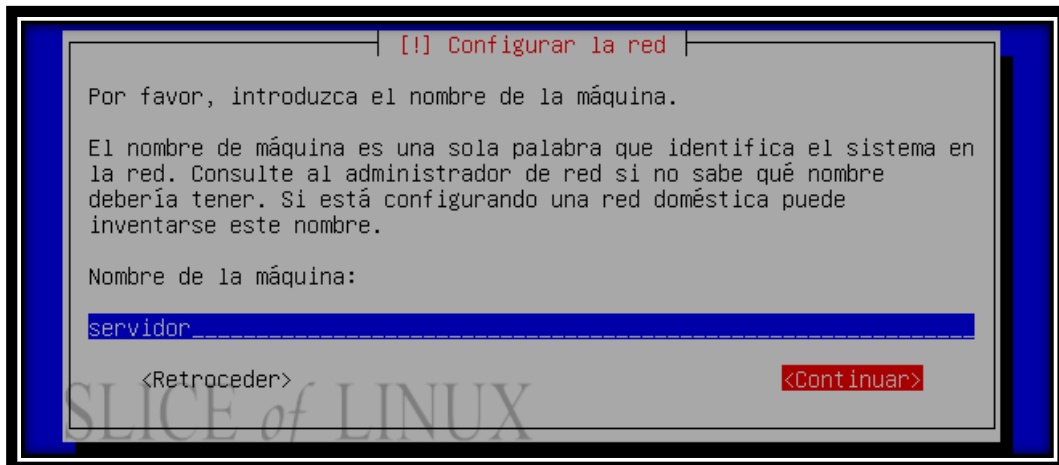
Y ahí eligen la distribución de teclado más apropiada para vuestra zona y pulsen Intro.

Paso 4: Configurar la red



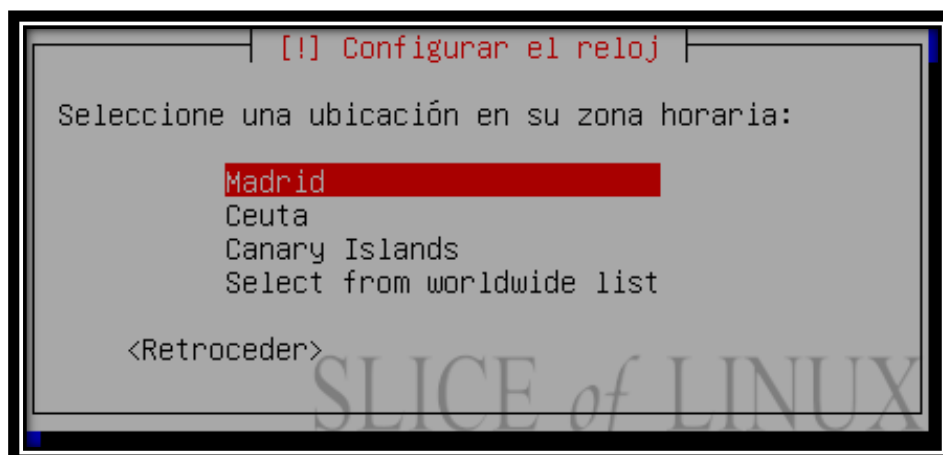
Por defecto, la red será configurada por DHCP. Si quieren pueden modificarla después.

Después de que la configure, llegarán a esta pantalla:



Elijan el nombre del servidor. Si el servidor es para una red local (por ejemplo, para guardar los datos importantes de vuestro PC principal que está conectado a la red local del servidor) elijan el nombre que quieran. Cuando hayan escrito el nombre del servidor, desplácese hasta "Continuar" (sin comillas) y pulsen Intro.

Paso 5: Configurar el reloj



Elijan su zona horaria y pulsen Intro.

Paso 6: Particionado (empieza lo bueno .)

El particionado de discos es el proceso más complicado (si es que hay algo complicado) de toda la instalación y, además, en este caso vamos a usar LVM (Logical Volume Manager). Sin embargo, y para que nos podamos sentir todo lo cómodo que queramos vamos primero a ver las opciones para particionar el disco con las que contamos:

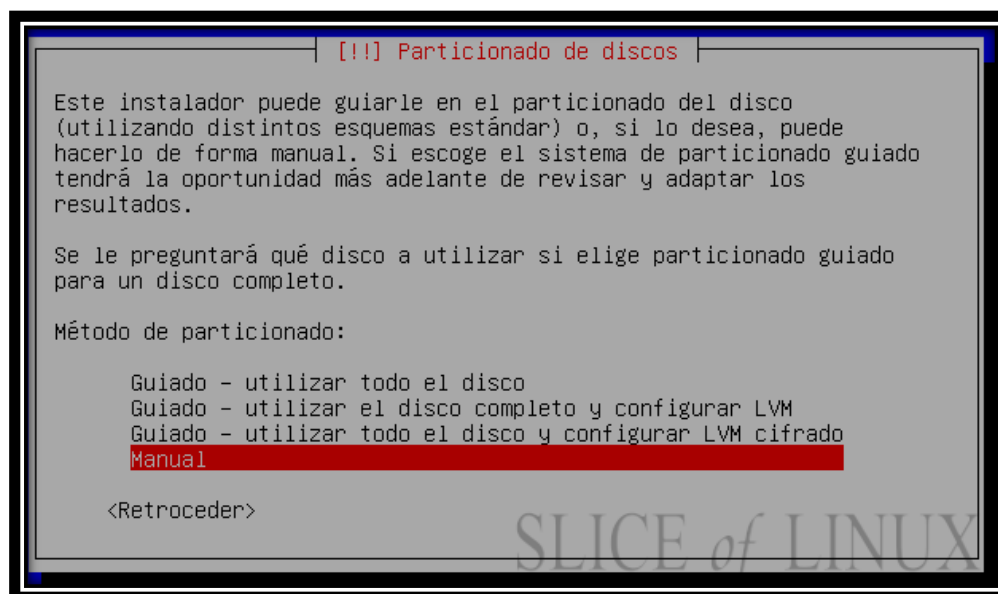
- * Guiado – utilizar todo el disco: el asistente creará dos particiones (raíz y swap).
- * Guiado – utilizar el disco completo y configurar LVM: se crea una partición de arranque (boot) y un volumen físico que contendrá dos volúmenes lógicos (raíz y swap).
- * Guiado – utilizar todo el disco y configurar LVM cifrado: igual que el anterior pero en este caso se cifra el volumen lógico que contiene la raíz.
- * Manual: nos permite particionar como queramos. Con o sin LVM, cifrando o sin cifrar y creando el número de particiones que necesitemos.

Si tienes prisa, utiliza cualquiera de los particionados guiados y vayas al siguiente paso (mucho más abajo). Te recomiendo especialmente que elijas uno de los que use LVM. Pero si por casualidad no tienes prisa, vamos a ver como particionar el disco manualmente y usando LVM paso a paso.

Al igual que en un equipo doméstico es recomendable tener tres particiones (raíz, home y swap), en un servidor también se suelen usar tres (como mínimo) que se corresponden con las siguientes:

- * / (raíz): contiene el sistema y las aplicaciones que se instalen.
- * var: alberga las páginas web, directorios de ftp, caché de un proxy-caché, buzones de correo electrónico...
- * swap: el área de intercambio.

Ahora bien, el particionado tradicional es muy rígido y una vez definidas las particiones no podemos modificar su tamaño. Por lo tanto, vamos a usar LVM. Crearemos un grupo de volúmenes físico en el que incluiremos tres volúmenes lógicos que almacenarán las tres particiones definidas anteriormente (raíz, var y swap). El tamaño inicial de cada una de estas particiones será el más pequeño que estimemos porque podremos ir aumentando su tamaño conforme lo necesitemos. Una de las grandes ventajas del LVM.



Una vez sentadas las bases elegimos particionar nuestro disco usando el particionado Manual y pulsamos Intro. Si quieren solamente Ubuntu Server en el servidor, elijan la primera opción y se quitan de líos. (Los que elijan la primera opción, pasen directamente al paso 7).

```

[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene
configurados actualmente. Seleccione una partición para modificar sus
valores (sistema de ficheros, puntos de montaje, etc.), el espacio
libre para añadir una partición nueva o un dispositivo para
inicializar la tabla de particiones.

Particionado guiado
Ayuda del particionado

SCSI1 (0,0,0) (sda) - 107.4 GB ATA VBOX HARDDISK

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>

```

Después se nos muestra un resumen con las particiones y puntos de montaje. Como nuestro disco duro está vacío, sólo vemos el disco duro completo, lo seleccionamos y pulsamos

Intro para seguir con el particionado.

```

[!!] Particionado de discos

Ha seleccionado particionar el dispositivo completo. Si continúa
creará una tabla de particiones en el dispositivo y se eliminarán
todas las particiones que existían previamente.

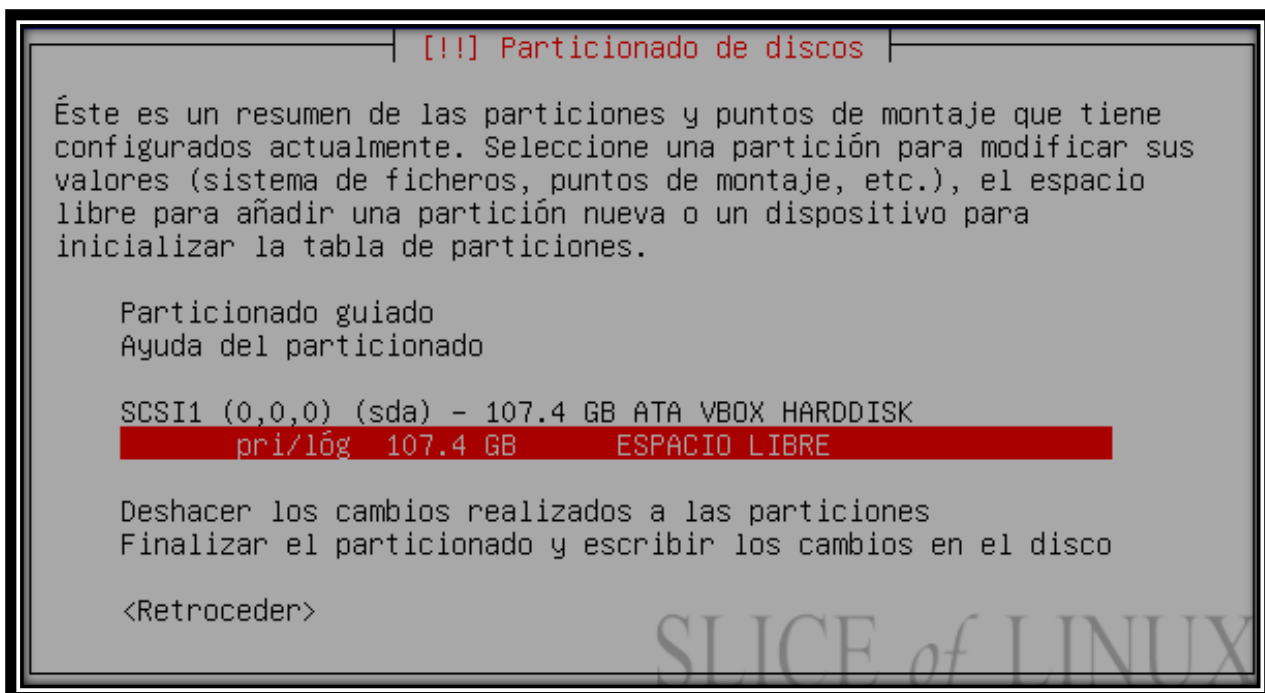
Observe que podrá deshacer esta operación más adelante si lo desea.

¿Crear una nueva tabla de particiones vacía en este dispositivo?

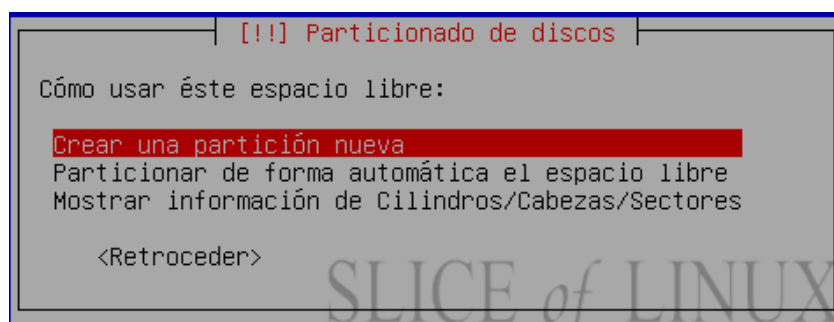
<Retroceder> <Sí> <No>

```

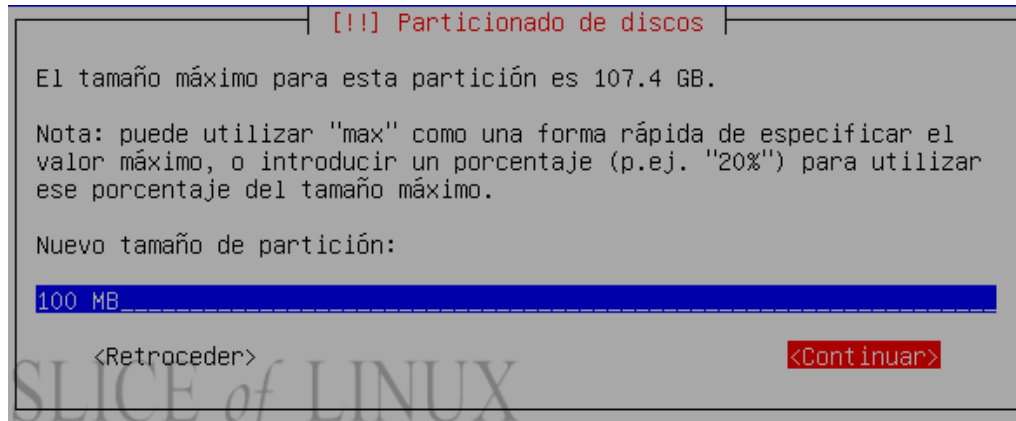
Al elegir el disco duro el programa de instalación nos avisa de que se va a crear una nueva tabla de particiones. Seleccionamos Sí y pulsamos Intro.



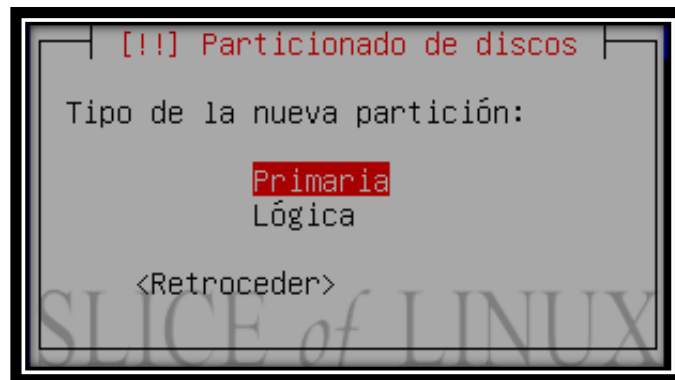
Volvemos a ver el resumen de las particiones pero en este caso, ya tenemos una partición libre, tan grande como nuestro disco duro. La seleccionamos porque en ella vamos a crear las particiones y pulsamos Intro.



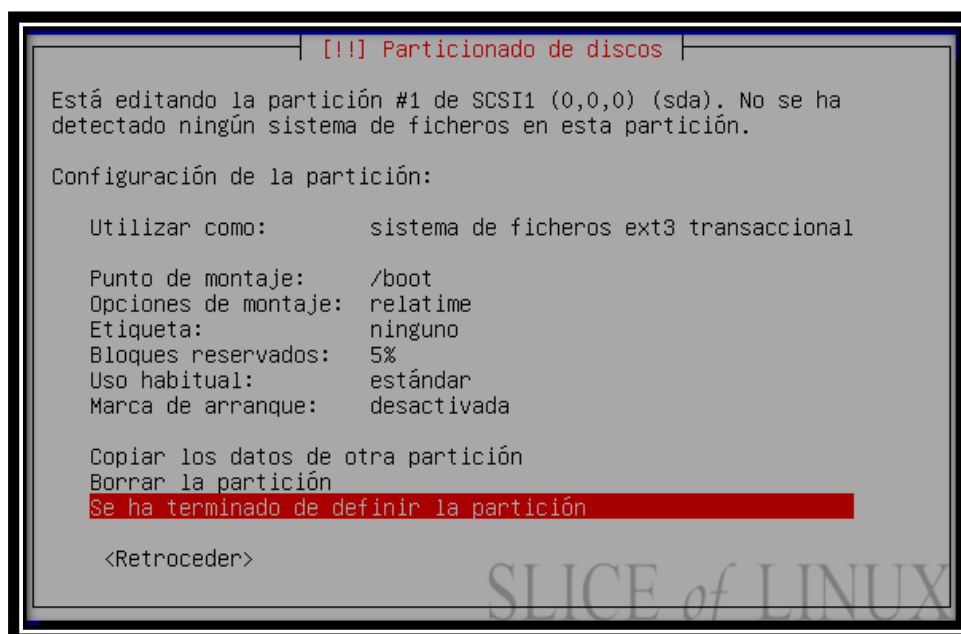
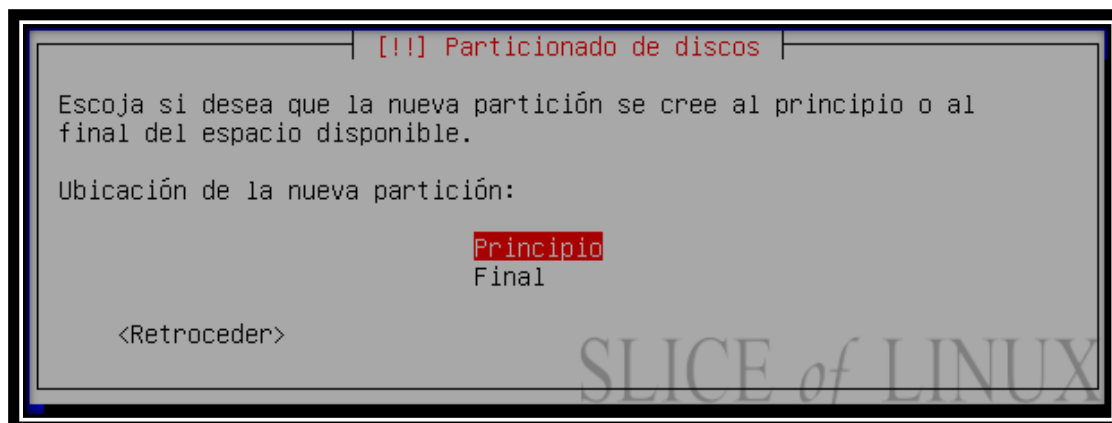
A continuación, elegimos Crear una partición nueva y pulsamos Intro.



La primera partición que vamos a crear es una partición de arranque (boot). Como vamos a particionar el resto del disco usando LVM y como los gestores de arranque no suelen soportar el arranque desde un volumen LVM, tenemos que crear la partición de boot. El tamaño de esta partición no tiene porqué exceder los 200 MB y, en principio, con 100 MB tenemos de sobra.



Seleccionamos que esa partición sea primaria y pulsa Intro.



En la siguiente pantalla tenemos que seleccionar el punto de montaje /boot. Y despu3s, bajamos hasta Se ha terminado de definir la partici3n y pulsamos Intro.

```

[!!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene
configurados actualmente. Seleccione una partición para modificar sus
valores (sistema de ficheros, puntos de montaje, etc.), el espacio
libre para añadir una partición nueva o un dispositivo para
inicializar la tabla de particiones.

Particionado guiado
Ayuda del particionado

SCSI1 (0,0,0) (sda) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 98.7 MB f ext3 /boot
pri/lóg 107.8 GB ESPACIO LIBRE

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>

```

Una vez que tenemos nuestra primera partición creada, que nos aparecerá en el resumen de particiones, seleccionamos el espacio libre y pulsamos Intro para definir la siguiente partición.

```

[!!!] Particionado de discos

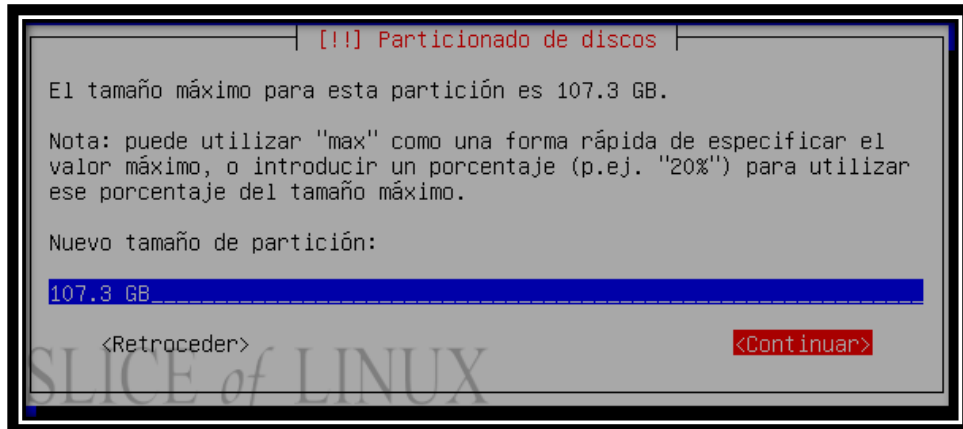
Cómo usar éste espacio libre:

Crear una partición nueva
Particionar de forma automática el espacio libre
Mostrar información de Cilindros/Cabezas/Sectores

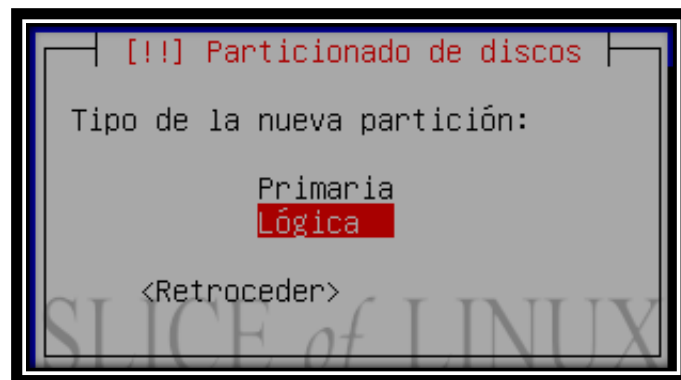
<Retroceder>

```

En el nuevo espacio libre elegimos crear una partición nueva y pulsamos Intro.



Esta nueva partición que vamos a crear la vamos a utilizar como volumen físico para LVM, que albergará el resto de particiones, por lo que le asignamos el tamaño máximo. En este caso 107,3 GB y continuamos.



El tipo de partición para esta partición puede ser tanto primaria como lógica. En este caso me decido ponerla como lógica.

```

[!!] Particionado de discos

Está editando la partición #5 de SCSI1 (0,0,0) (sda). No se ha
detectado ningún sistema de ficheros en esta partición.

Configuración de la partición:

    Utilizar como:      volumen físico para LVM

    Marca de arranque:  desactivada

    Copiar los datos de otra partición
    Borrar la partición
    Se ha terminado de definir la partición

<Retroceder>

```

Ahora debemos cambiar el valor del parámetro Utilizar como para que sea volumen físico para LVM, en lugar de sistema de ficheros ext3 transaccional que viene por defecto. Y después, bajamos hasta Se ha terminado de definir la partición y pulsamos Intro.

```

[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene
configurados actualmente. Seleccione una partición para modificar sus
valores (sistema de ficheros, puntos de montaje, etc.), el espacio
libre para añadir una partición nueva o un dispositivo para
inicializar la tabla de particiones.

Configurar el Gestor de Volúmenes Lógicos (LVM)
Particionado guiado
Ayuda del particionado

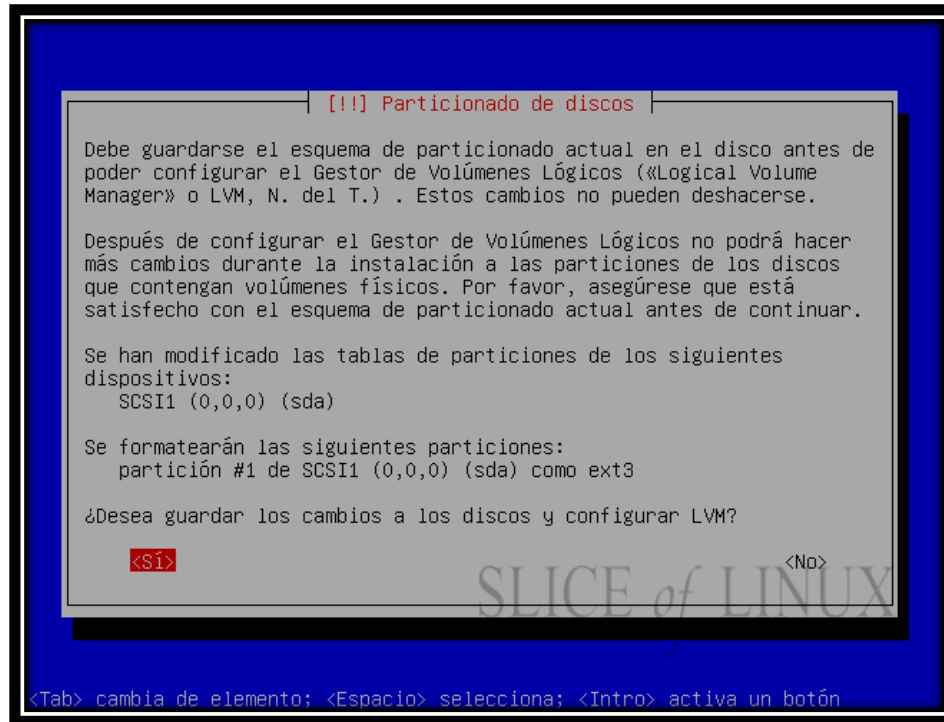
SCSI1 (0,0,0) (sda) - 107.4 GB ATA VBOX HARDDISK
#1 primaria  98.7 MB  f ext3  /boot
#5 lógica    107.3 GB  K lvm

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

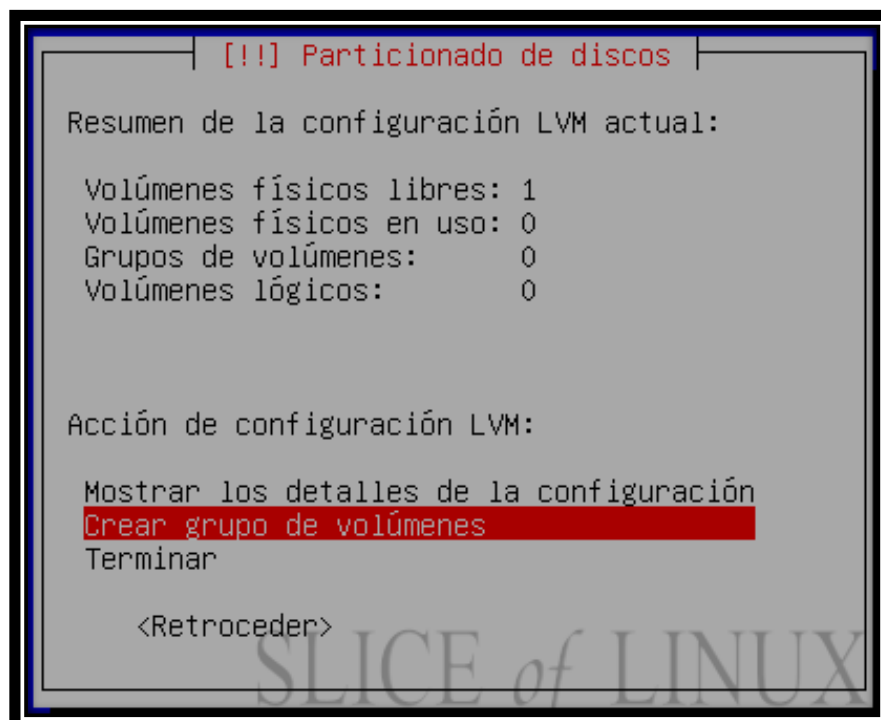
<Retroceder>

```

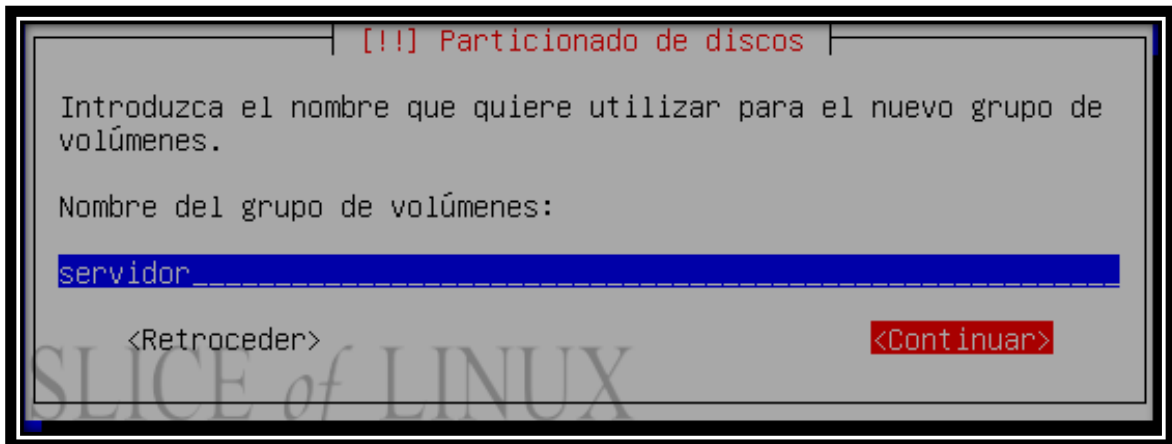
Una vez definidas las dos particiones que necesitábamos pasamos a Configurar el Gestor de Volúmenes Lógicos (LVM).



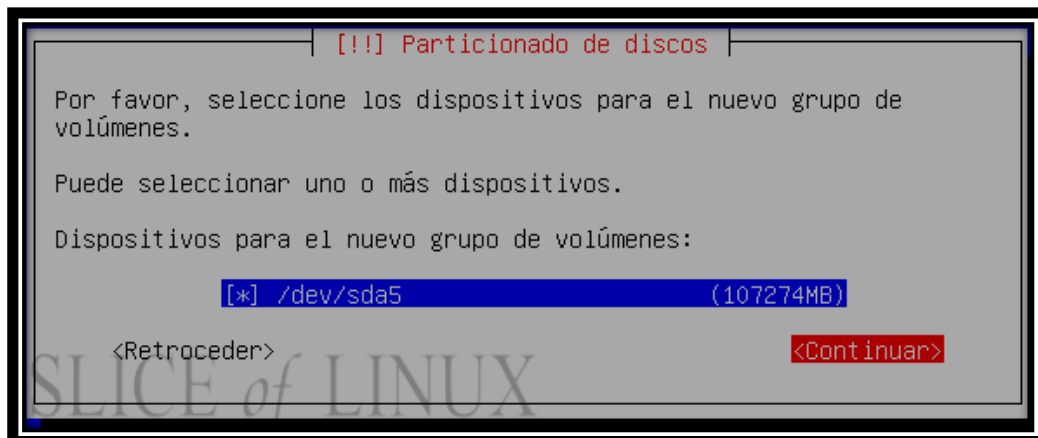
Antes de poder configurar el gestor de volúmenes lógicos debemos guardar las particiones que hemos creado. Por lo tanto, a la pregunta ¿desea guardar los cambios a los discos y configurar LVM? Respondemos que sí.



En esta pantalla obtenemos un resumen de la configuración LVM en el que nos indica que tenemos un volumen físico libre. Y de entre las acciones disponibles seleccionamos Crear grupo de volúmenes y pulsamos Intro.



Tras esto debemos escribir el nombre del grupo de volúmenes y pulsamos Intro.



El siguiente paso consiste en seleccionar los dispositivos para el grupo de volúmenes. Si tuviésemos más de un disco duro, sería más interesante y podríamos seleccionar uno o más. Sin embargo, en este caso sólo contamos con uno que aparece seleccionado directamente por lo que pulsamos Intro sobre Continuar.


```
[!!] Particionado de discos

Resumen de la configuración LVM actual:

Volúmenes físicos libres: 0
Volúmenes físicos en uso: 1
Grupos de volúmenes:      1
Volúmenes lógicos:       0

Acción de configuración LVM:

Mostrar los detalles de la configuración
Crear un volumen lógico
Borrar un grupo de volúmenes
Terminar

<Retroceder>
```

Volvemos de nuevo al resumen de la configuración LVM que nos muestra que no hay ningún volumen físico libre y sí uno en uso. Si nos fijamos, también veremos que la opción de crear un grupo de volúmenes ha sido sustituida por Crear un volumen lógico. Seleccionamos esta opción y continuamos con la configuración.

```
[!!] Particionado de discos

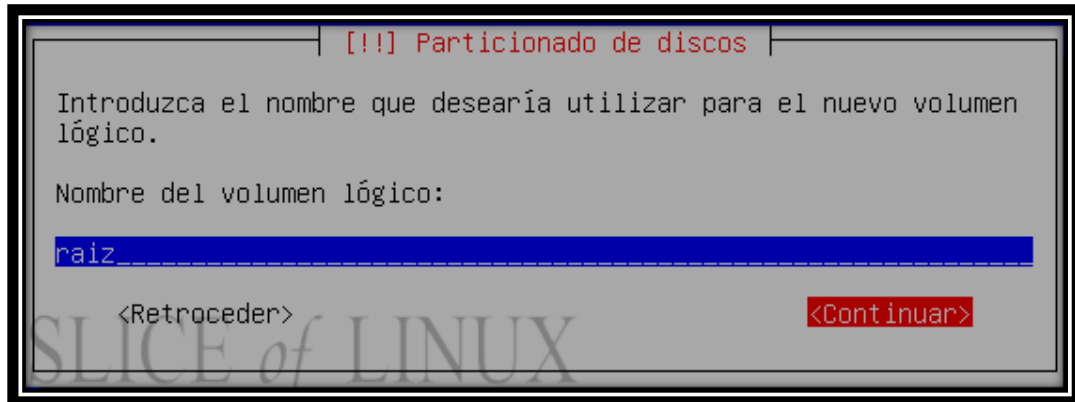
Seleccione uno de los siguientes grupos de volúmenes donde crear un
nuevo volumen lógico.

Grupo de Volúmenes:

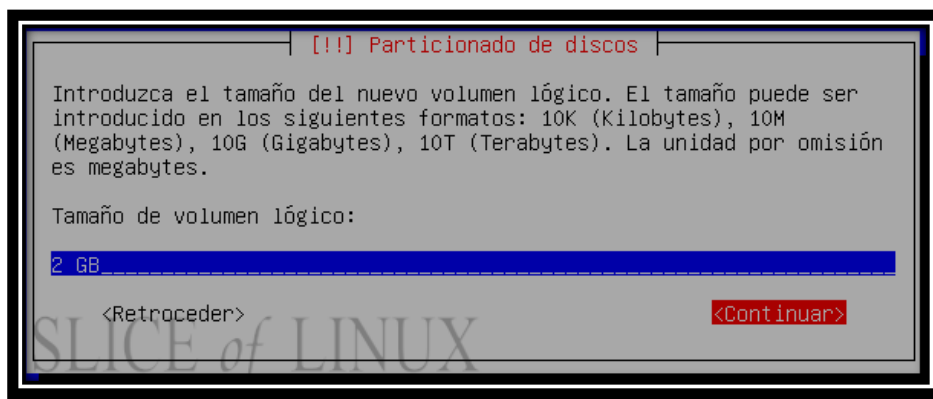
servidor (107273MB)

<Retroceder>
```

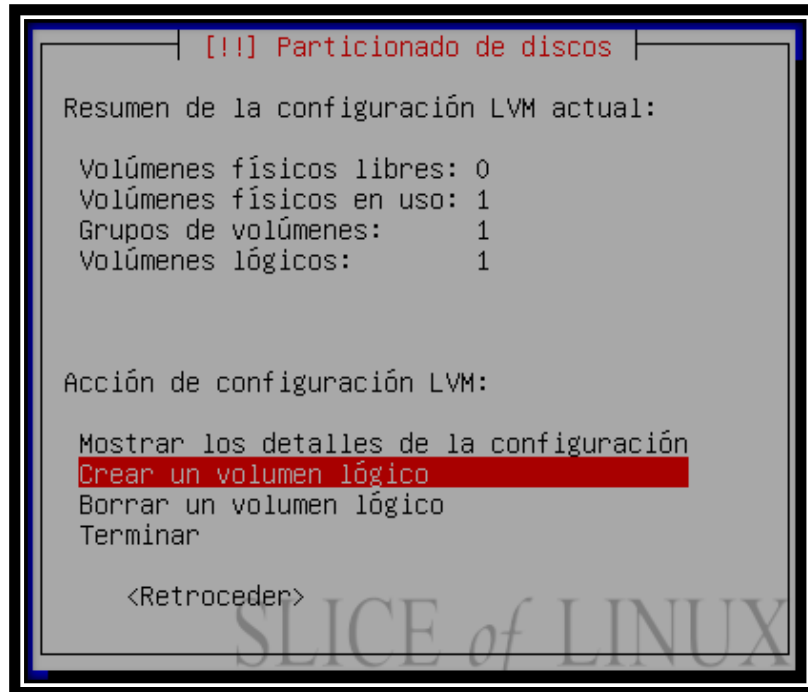
Lo primero que hacemos para crear un volumen lógico es indicar el grupo de volúmenes al que va a pertenecer. Como solamente tenemos uno, lo seleccionamos y pulsamos Intro.



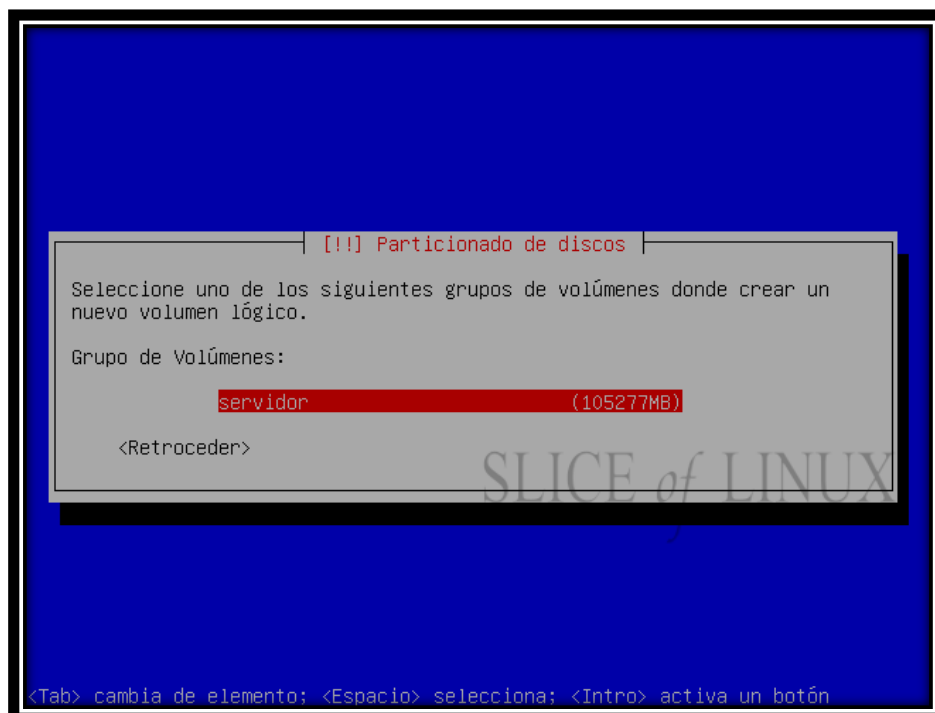
El volumen lógico necesita un nombre: raíz, en este caso. Lo escribimos y pulsamos Intro.



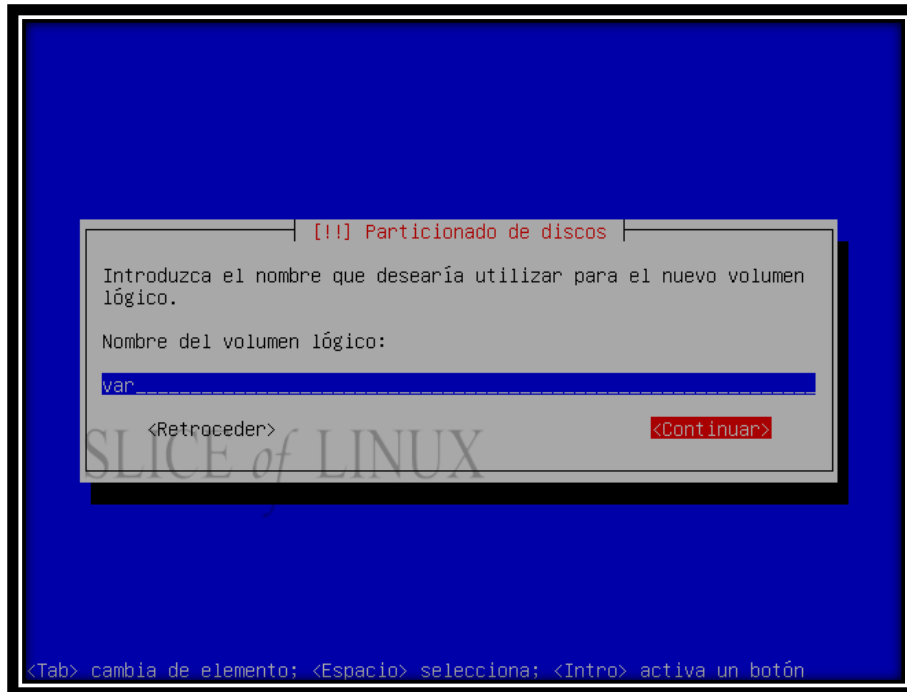
Ahora nos toca escribir el tamaño de la partición. Como podremos hacerla más grande, gracias al LVM, le ponemos un tamaño relativamente pequeño: 2 GB.



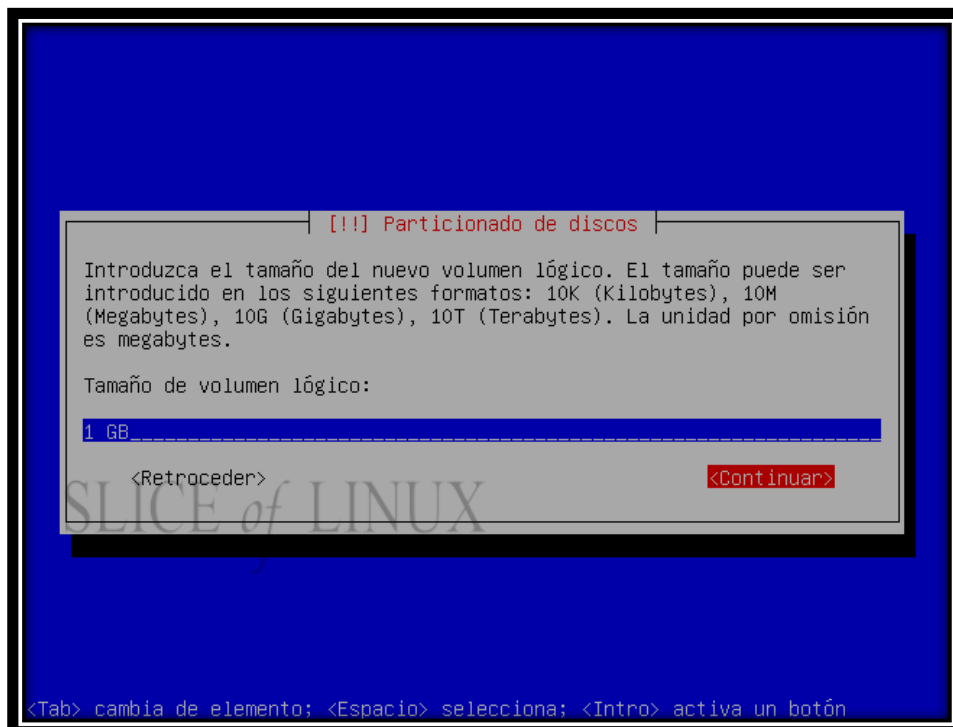
Una vez creado el primer volumen lógico, vamos a por el segundo. Así que seleccionamos crear un volumen lógico.



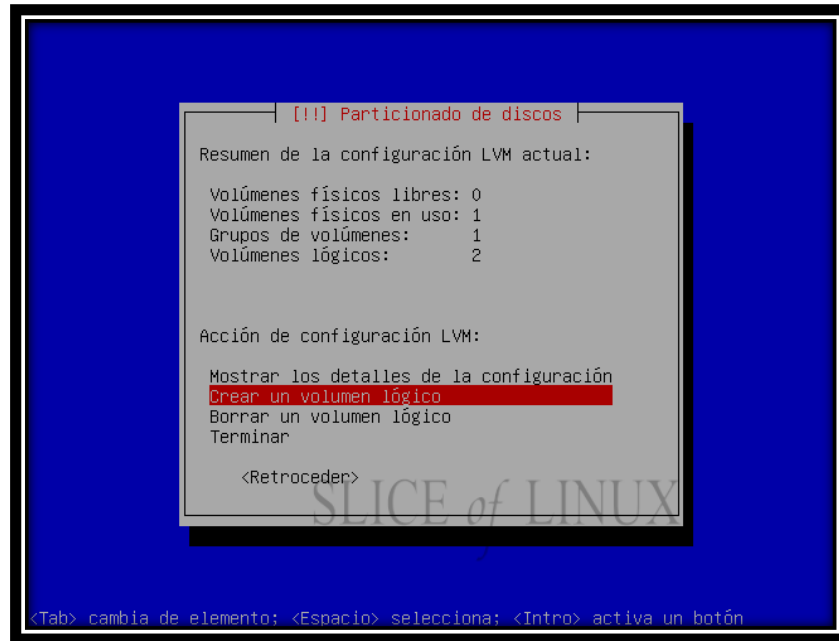
Seleccionamos de nuevo el único grupo de volúmenes que tenemos y pulsamos Intro.



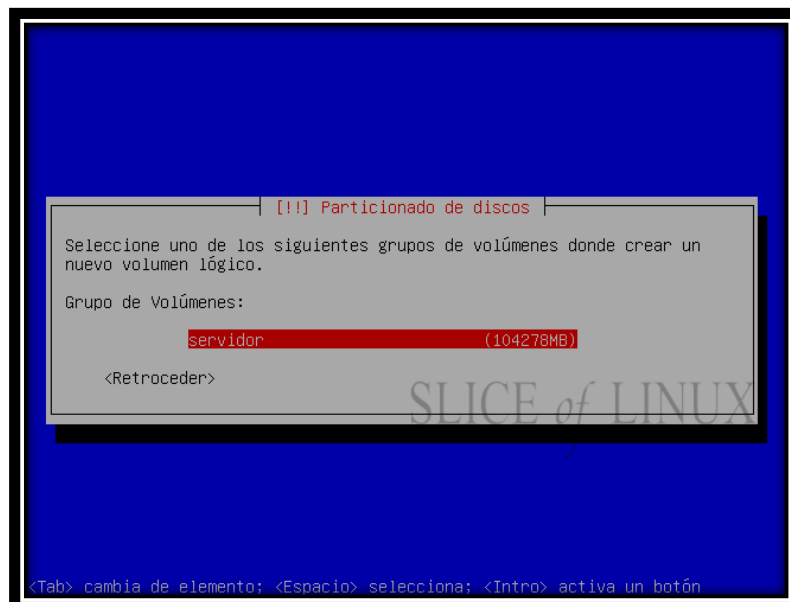
Escribimos el nombre del nuevo volumen lógico: var.



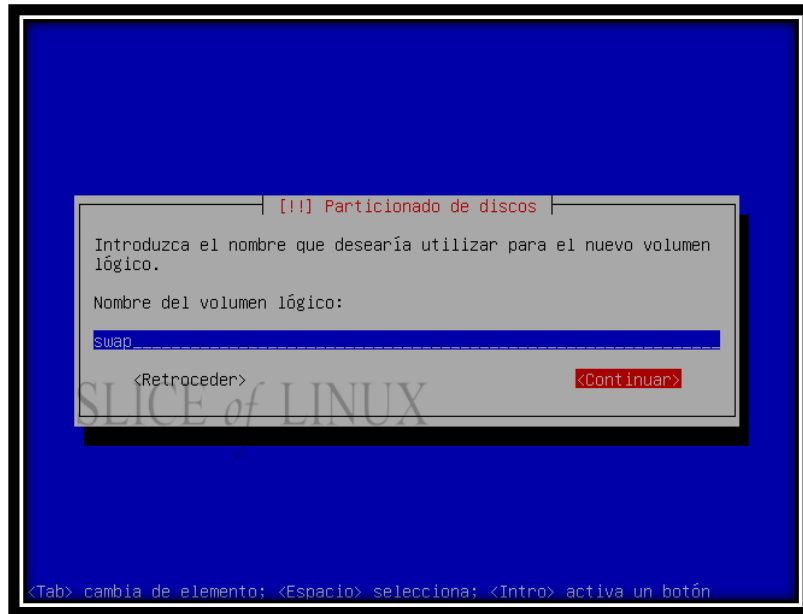
Y elegimos el tamaño del volumen lógico var. Podemos empezar con 1 GB y si necesitamos más lo iremos ampliando.



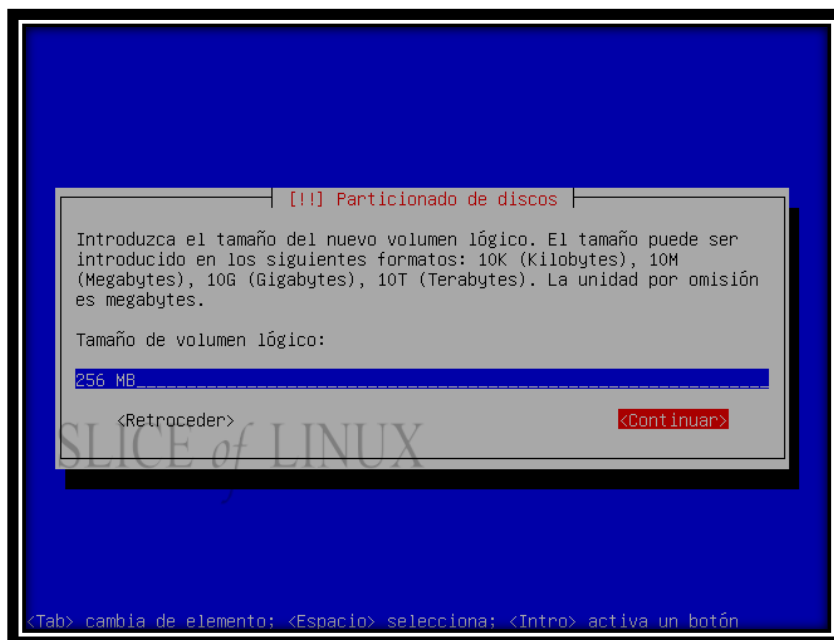
Vemos en el resumen que tenemos ya dos volúmenes lógicos creados y nos ponemos manos a la obra para definir el tercer y último volumen lógico seleccionando Crear un volumen lógico.



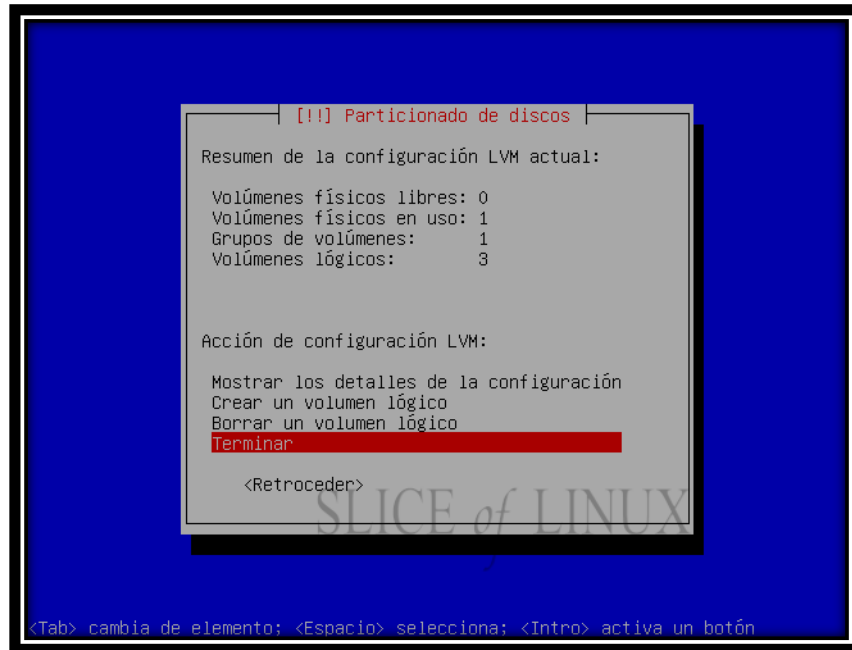
Otra vez marcamos el único grupo de volúmenes que tenemos y pulsamos Intro.



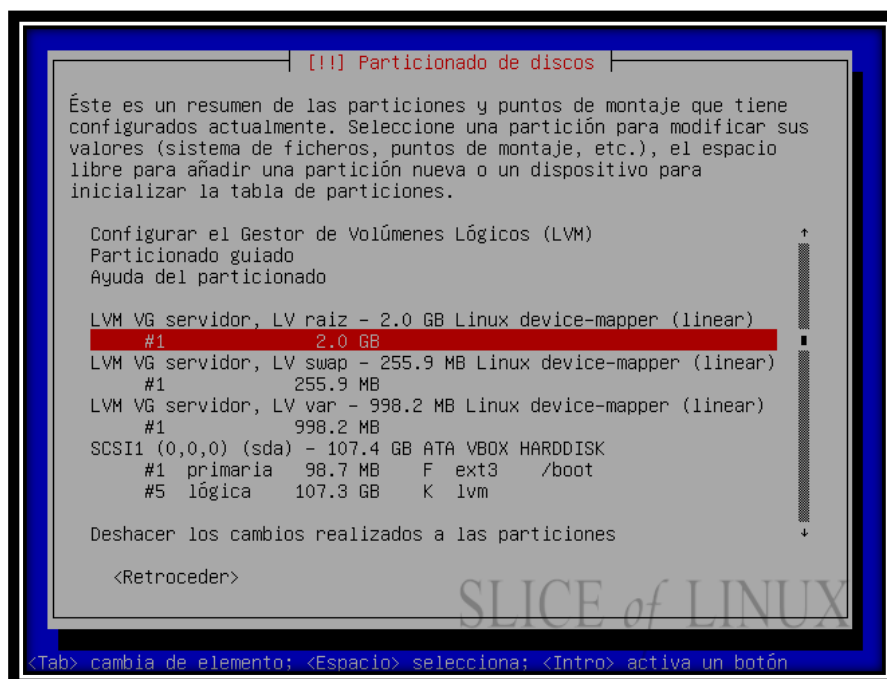
Nombramos con swap el nuevo volumen lógico y continuamos.



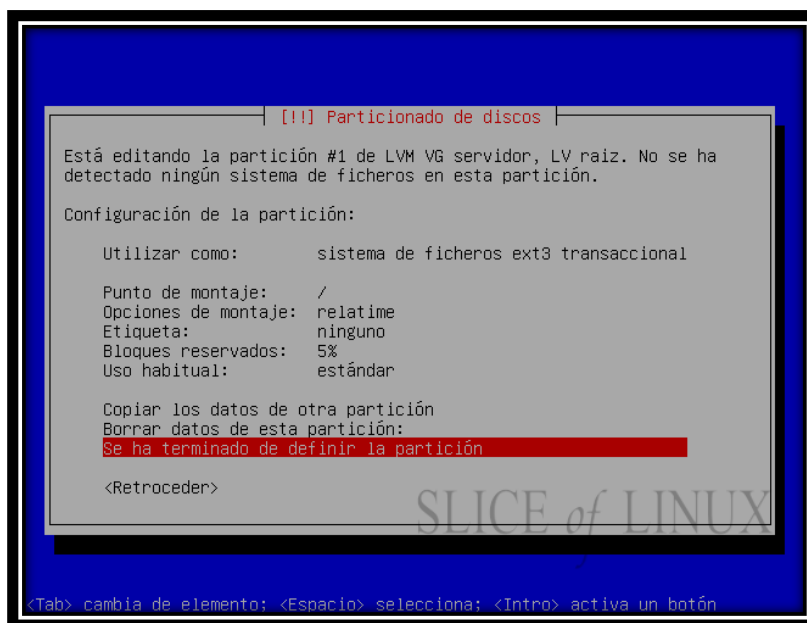
El tamaño de este volumen lógico lo ponemos en 256 MB. En principio será suficiente teniendo en cuenta que no queremos que nuestro servidor haga swapping.



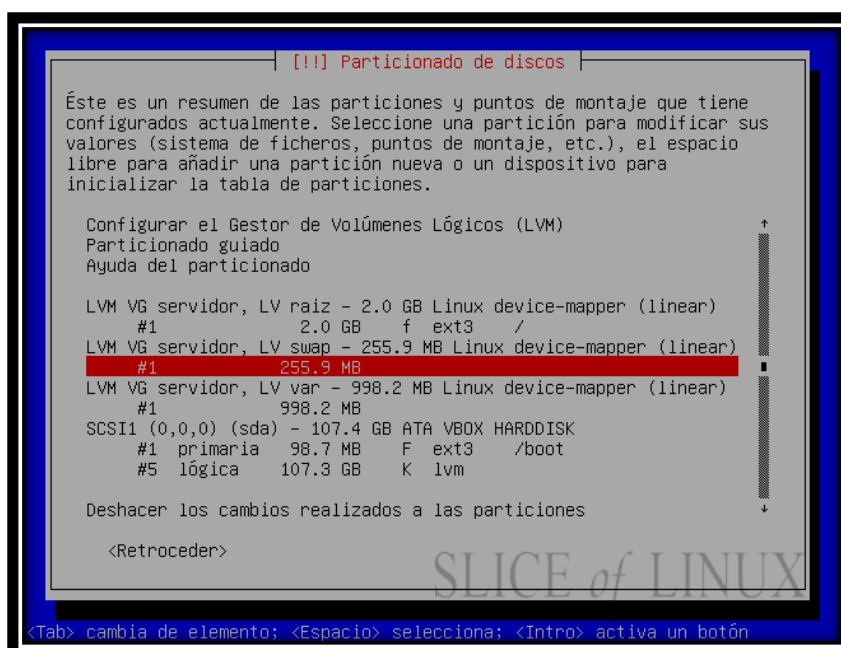
Una vez definidos los tres volúmenes lógicos, seleccionamos la opción Terminar para finalizar con la configuración LVM.



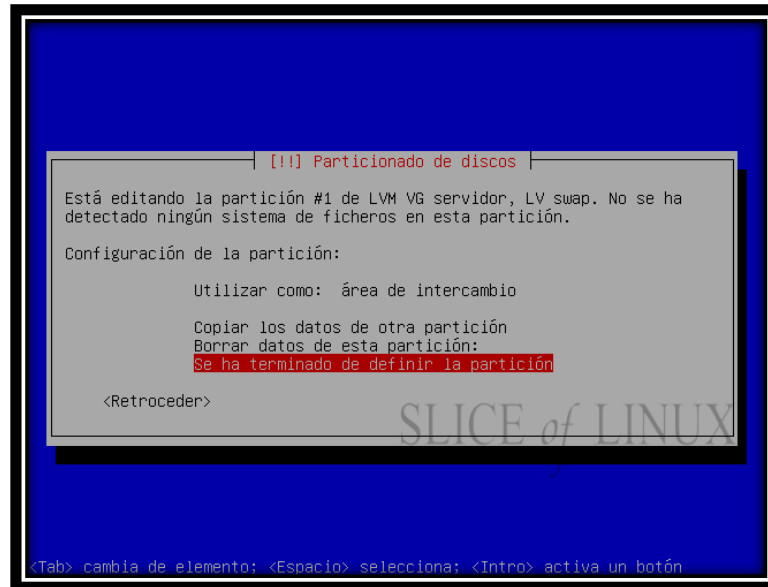
A continuación, vamos a ir creando en cada uno de los volúmenes lógicos las particiones correspondientes. Así que seleccionamos la partición libre del volumen lógico raíz y pulsamos Intro.



Cuando editemos la partición raíz, es fundamental indicar el punto de montaje que es /. Y hecho esto bajamos hasta Se ha terminado de definir la partición y pulsamos Intro.

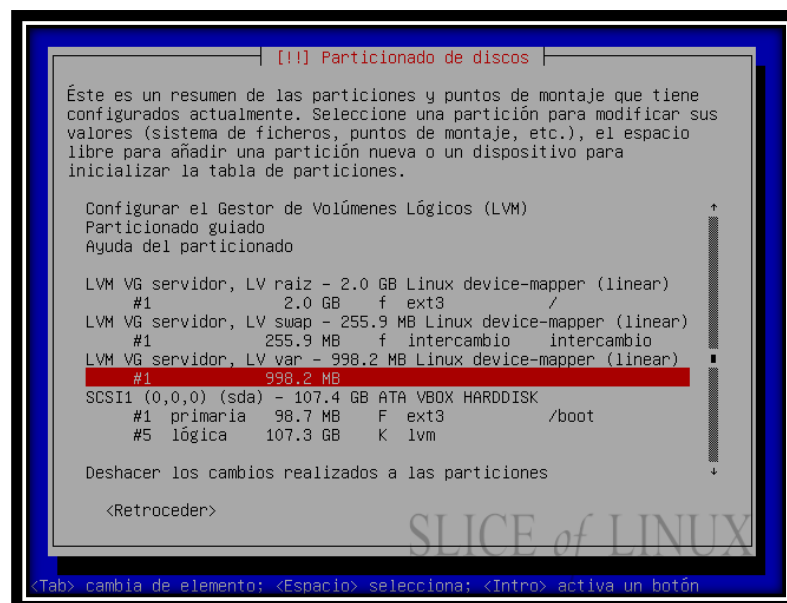


Después seleccionamos la partición libre del volumen lógico swap y pulsamos Intro.



En la definición de esta partición tenemos que indicarle que se utilice como área de intercambio. Y nos movemos hasta Se ha terminado de definir la partición para pulsar

Intro.



Para definir la última partición seleccionamos la partición libre del volumen var y

pulsamos Intro.

```
[!!] Particionado de discos

Está editando la partición #1 de LVM VG servidor, LV var. No se ha
detectado ningún sistema de ficheros en esta partición.

Configuración de la partición:

  Utilizar como:          sistema de ficheros ext3 transaccional

  Punto de montaje:      /var
  Opciones de montaje:   relatime
  Etiqueta:              ninguno
  Bloques reservados:    5%
  Uso habitual:          estándar

  Copiar los datos de otra partición
  Borrar datos de esta partición:
  Se ha terminado de definir la partición

  <Retroceder>
```

SLICE of LINUX

<Tab> cambia de elemento; <Espacio> selecciona; <Intro> activa un botón

Al editar esta partición debemos indicar que el punto de montaje será /var y, sin más, pulsamos Intro sobre Se ha terminado de definir la partición.

```

[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene
configurados actualmente. Seleccione una partición para modificar sus
valores (sistema de ficheros, puntos de montaje, etc.), el espacio
libre para añadir una partición nueva o un dispositivo para
inicializar la tabla de particiones.

Particionado guiado
Ayuda del particionado

LVM VG servidor, LV raíz - 2.0 GB Linux device-mapper (linear)
#1      2.0 GB      f ext3      /
LVM VG servidor, LV swap - 255.9 MB Linux device-mapper (linear)
#1      255.9 MB    f intercambio intercambio
LVM VG servidor, LV var - 998.2 MB Linux device-mapper (linear)
#1      998.2 MB    f ext3      /var
SCSI1 (0,0,0) (sda) - 107.4 GB ATA VBOX HARDDISK
#1 primaria 98.7 MB    F ext3      /boot
#5 lógica  107.3 GB    K lvm

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco
<Retroceder>

```

Por último, bajamos hasta Finalizar el particionado y escribir los cambios en el disco y pulsamos Intro.

```

[!!] Particionado de discos

Se escribirán en los discos todos los cambios indicados a
continuación si continúa. Si no lo hace podrá hacer cambios
manualmente.

AVISO: Esta operación destruirá todos los datos que existan en las
particiones que haya eliminado así como en aquellas particiones que
se vayan a formatear.

Se han modificado las tablas de particiones de los siguientes
dispositivos:
LVM VG servidor, LV raíz
LVM VG servidor, LV swap
LVM VG servidor, LV var

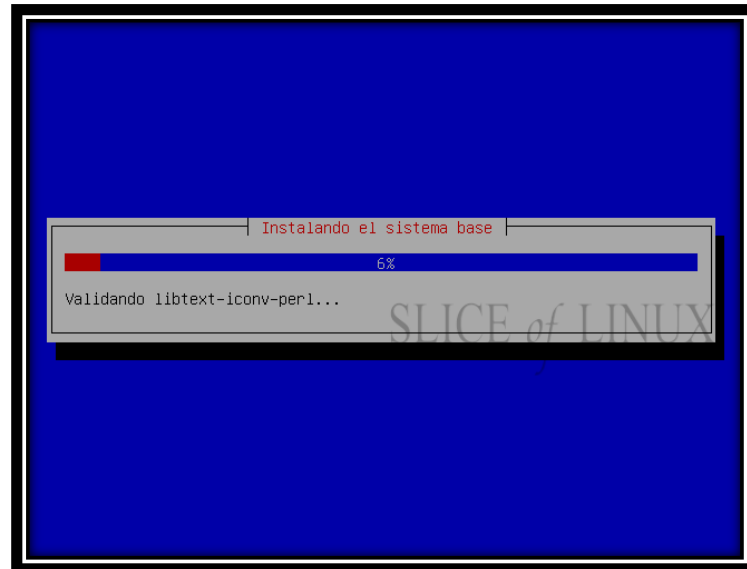
Se formatearán las siguientes particiones:
LVM VG servidor, LV raíz como ext3
LVM VG servidor, LV swap como intercambio
LVM VG servidor, LV var como ext3

¿Desea escribir los cambios en los discos?
<Si> <No>

```

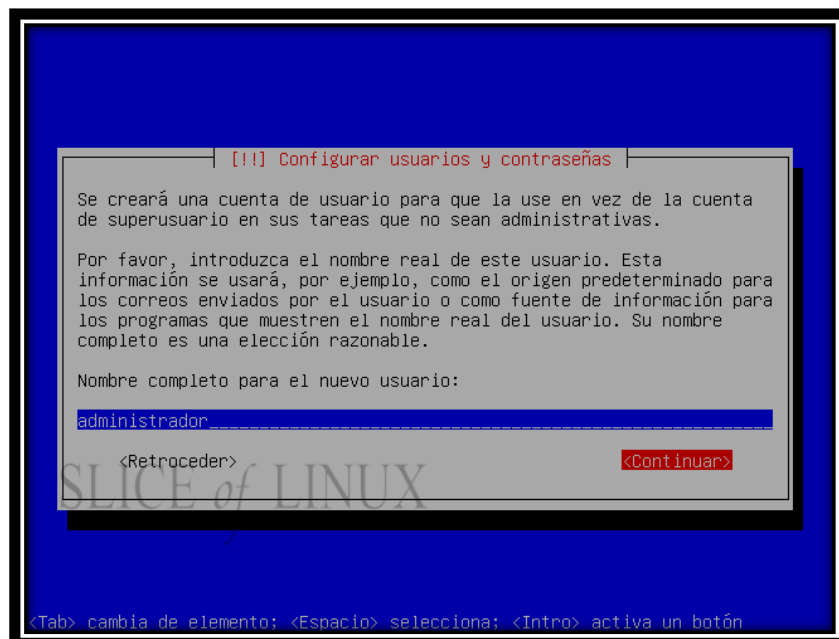
Entonces se nos preguntará si queremos escribir los cambios en los discos, a lo que contestaremos que Sí.

Paso 7: Instalando el sistema



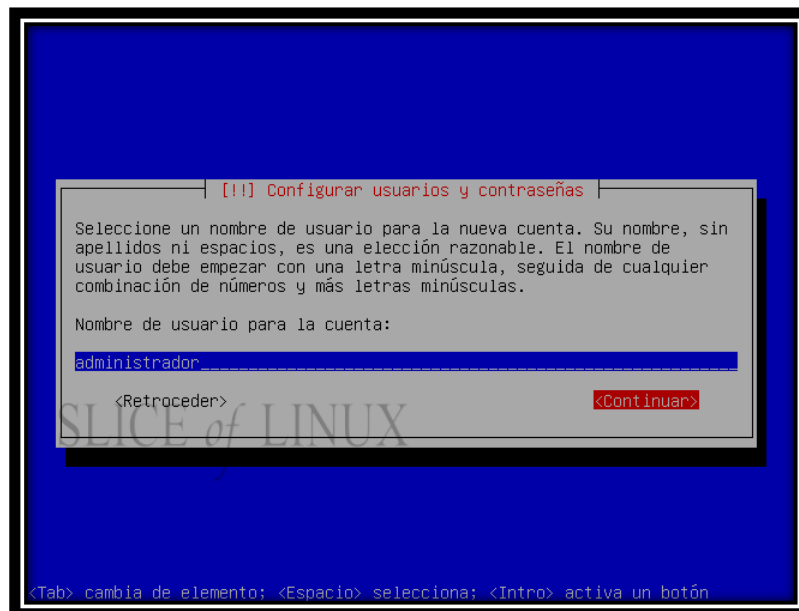
Seguidamente comenzará la instalación del sistema base. Y esperen.

Paso 8: Configurar usuarios y contraseñas

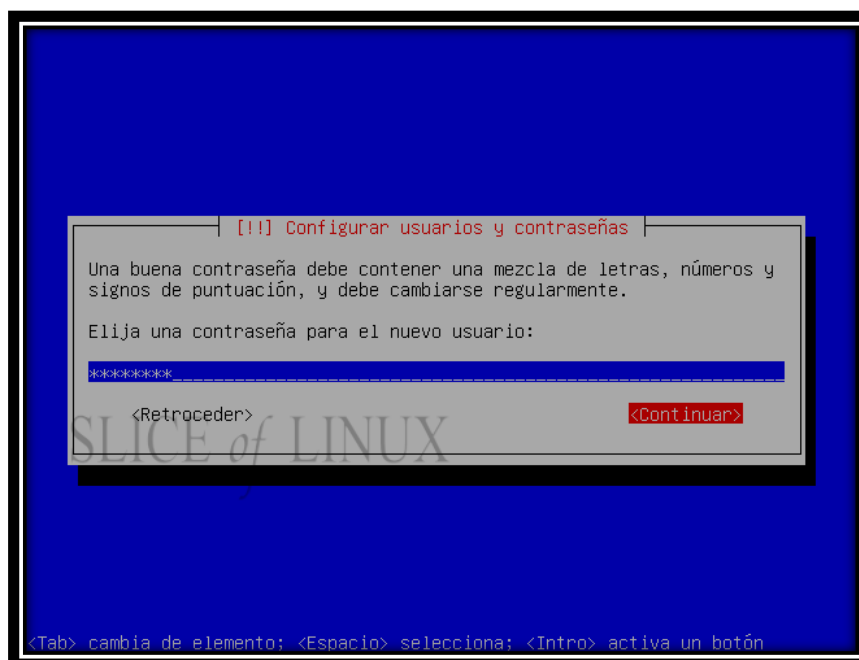


En este paso debemos configurar una cuenta de usuario que será el que usemos por defecto

en lugar del supe usuario para ejecutar tareas no administrativas. Lo primero que debemos introducir es el nombre completo del usuario. Yo he elegido administrador.



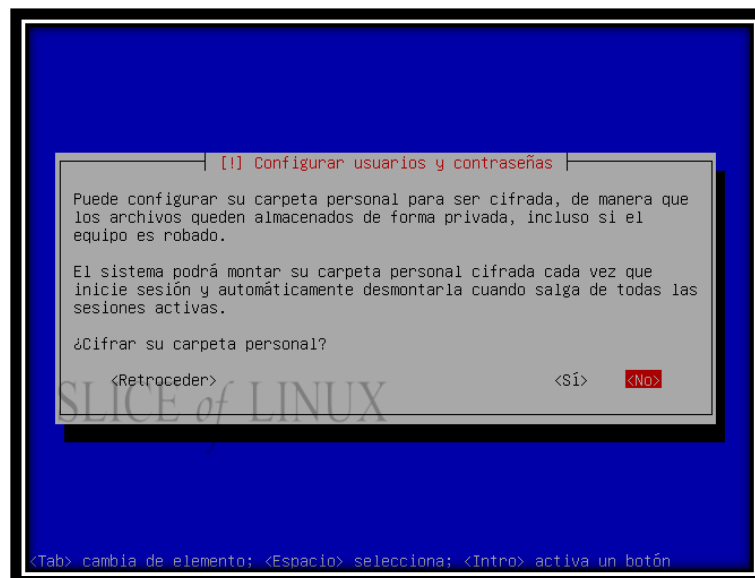
A continuación escribimos el nombre de usuario. El nombre de usuario debe empezar con una letra minúscula y no puede contener espacios en blanco ni caracteres especiales.



Ahora es el turno de la contraseña para este usuario. Se recomienda que contenga letras, números, signos de puntuación, mayúsculos y minúsculos.



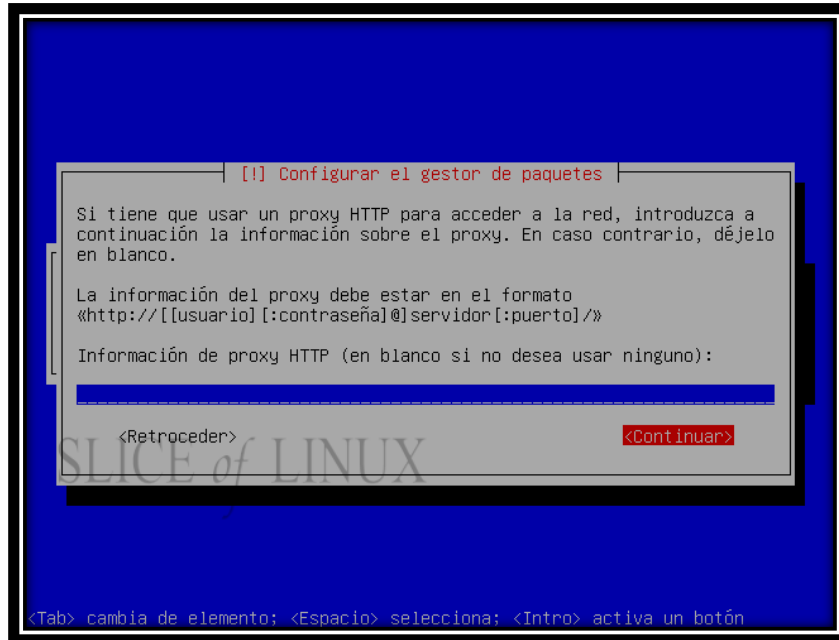
Y la tenemos que escribir de nuevo para comprobar que no nos hemos equivocado al escribirla (pulsando un par de teclas a la vez, por ejemplo).



También debemos elegir si queremos que nuestra carpeta personal (nuestro home) esté cifrada. Esto es interesante para mantener seguros nuestros datos incluso si nos roban el equipo. Sin embargo, en mi caso voy a seleccionar que no quiero cifrar la carpeta

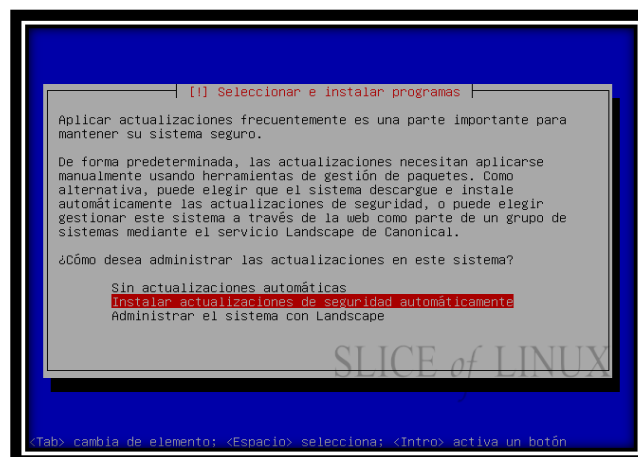
personal.

Paso 9: Configurar el gestor de paquetes



Solamente es necesario configurar el gestor de paquetes si tenemos que usar un proxy para acceder a la red. En mi caso, como no tengo que usarlo, dejo esta información en blanco.

Paso 10: Seleccionar e instalar programas



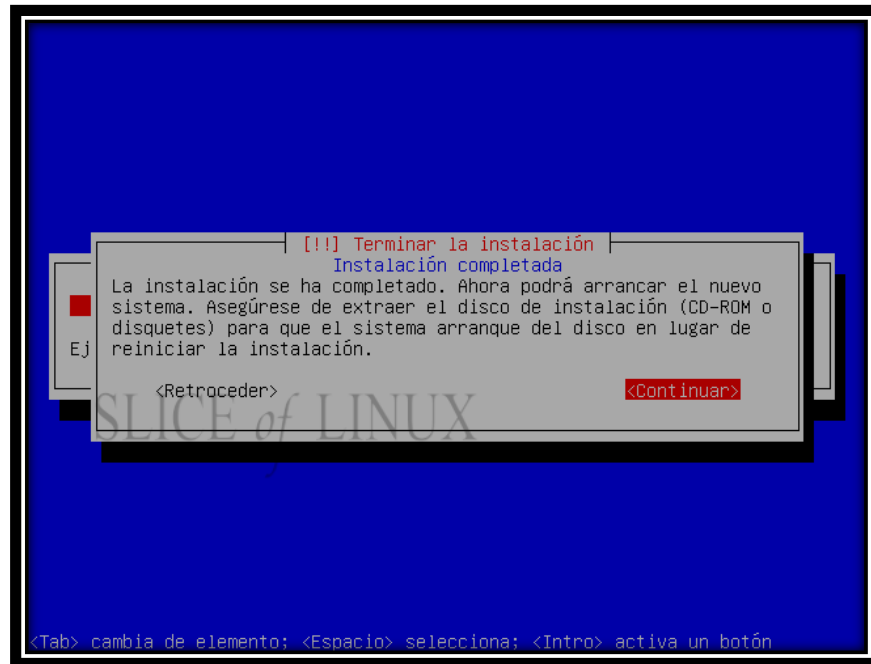
En este paso tenemos que seleccionar si queremos que se instalen las actualizaciones de seguridad de forma automática o no, o si queremos administrar el sistema con Landscape. Landscape es en una interfaz web para administrar y monitorizar equipos con Ubuntu, pero es de pago.

Yo prefiero que se instalen las actualizaciones de seguridad automáticamente.



Después podemos elegir qué programas queremos instalar como son un servidor DNS, un servidor LAMP, de correo, Samba... La verdad es que casi es mejor instalar cualquiera de estos servicios de forma manual cuando ya esté instalado el sistema para controlar todos los pasos. Sin embargo, sí que resulta muy cómodo instalar desde el principio el servidor SSH para poder administrarlo desde cualquier sitio.

Paso 11: Terminando la instalación



Una vez que haya terminado la instalación tenemos que reiniciar el sistema, asegurándonos de haber sacado el CD-ROM de la unidad.

Paso 12: Inicio de Ubuntu Server

```

/dev/sda1: clean, 31/24096 files, 22326/96356 blocks
/dev/mapper/servidor-var: clean, 2061/60928 files, 44606/243712 blocks
[ OK ]
* Mounting local filesystems... [ OK ]
* Activating swapfile swap... [ OK ]
* Starting AppArmor [ OK ]
* Mounting securityfs on /sys/kernel/security... [ OK ]
* Loading AppArmor profiles ... [ OK ]

* Skip starting firewall: ufw (not enabled)... [ OK ]
* Configuring network interfaces... [ OK ]
* Setting up console font and keymap... [ OK ]
* Loading ACPI modules... [ OK ]
* Starting ACPI services... [ OK ]
* Starting system log daemon... [ OK ]
* Starting kernel log daemon... [ OK ]
* Starting system message bus dbus [ OK ]
* Starting OpenBSD Secure Shell server sshd [ OK ]
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Restarting OpenBSD Secure Shell server sshd

Ubuntu 9.04 servidor tty1
servidor login: _

```

Una vez reiniciado el sistema nos encontraremos cara a cara con la mejor interfaz de usuario: el terminal.

EXTRA: Cómo instalar una interfaz gráfica en Ubuntu Server

Si quieren instalar un entorno gráfico en Ubuntu Server con todas las aplicaciones usen estas claves dependiendo del entorno gráfico que quieran instalar:

-Si quieren instalar GNOME, tecleen esto en Ubuntu Server: `sudo apt-get install ubuntu-desktop`

-Si quieren instalar KDE, tecleen esto en Ubuntu Server: `sudo apt-get install kubuntu-desktop`

-Si quieren instalar Xfce, tecleen esto en Ubuntu Server: `sudo apt-get install xubuntu-desktop`

-Si quieren instalar FluxBox, tecleen esto en Ubuntu Server: `sudo apt-get install xorg xdm fluxbox xterm leafpad`

-Si quieren instalar Wmaker, tecleen esto en Ubuntu Server: `sudo apt-get install xorg gdm gdm-themes wmaker wmakerconf`

Esas claves son si quieren instalar el entorno completo, pero el entorno completo lleva programas que nunca vais a utilizar en un servidor. Los que quieran un entorno gráfico mínimo, sigan estos pasos:

1. Tecleen en Ubuntu Server esto para instalar GNOME con los programas básicos:
`sudo apt-get install x-window-system-core gnome-core`
2. NOTA: Si usan Ubuntu Server 8.04 deben teclear esto: `sudo apt-get install xorg gnome-core`
3. Después de instalarlo, tecleen esto en Ubuntu Server: `startx`
4. Y ya tenéis el escritorio mínimo. Lo que os ha instalado ha sido los "Accesorios" (solamente el editor de textos y la terminal) y Firefox para navegar por Internet. Pero como es una instalación mínima, el idioma por defecto es el inglés. Para

pasarlo a español, abre la Terminal y teclea cada código individualmente:

```
sudo apt-get install language-pack-es
```

```
sudo apt-get install language-pack-es-base
```

```
sudo apt-get install language-pack-gnome-es
```

```
sudo apt-get install language-pack-gnome-es-base
```

```
sudo apt-get install language-selector
```

```
sudo apt-get install language-support-es
```

5. Después de haber ejecutado todo eso, deben instalar gksu para que funcionen correctamente los menús: `sudo apt-get install gksu`

Para instalar las Herramientas de red, teclea esto en la Terminal: `sudo apt-get install gnome-system-tools gnome-nettool`

Y ya tienes un entorno gráfico instalado en tu Ubuntu Server.

2. INSTALACIÓN Y CONFIGURACIÓN DE WEBMIN

(<http://sliceoflinux.wordpress.com/2009/09/07/instalar-webmin-en-ubuntu-paso-a-paso/>)

- Actualizamos la información de los repositorios (fundamental antes de instalar cualquier aplicación):

```
sudo aptitude update
```

- Instalamos una serie de paquetes que nos hacen falta para la instalación de Webmin y para que se configure con SSL:

```
sudo aptitude install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions
```

- Nos aseguramos de estar en nuestro *home*:

```
cd
```

- Descargamos [la última versión de Webmin](http://downloads.sourceforge.net/webadmin/webmin_1.520_all.deb) (la 1.520 en este caso).

```
wget http://downloads.sourceforge.net/webadmin/webmin\_1.520\_all.deb
```

- Instalamos Webmin:

```
sudo dpkg -i webmin_1.520_all.deb
```

- Una vez instalado podemos acceder a la interfaz web de Webmin usando un navegador y escribiendo la dirección IP del equipo donde está instalado seguida del puerto donde está escuchando, por defecto, el 10.000. Eso sí, debemos estar atentos porque en vez de usar el protocolo HTTP, usaremos el HTTPS. En mi caso la IP de mi Ubuntu Server es 192.168.1.3:

```
https://192.168.1.3:10000
```

- En teoría, esto ya está listo. Sin embargo, tenemos nos encontraremos con la siguiente advertencia si accedemos desde Firefox:



Advertencia de seguridad de Firefox

Para que no nos vuelva a aparecer hacemos clic sobre “**O puede añadir una excepción...**”

- A continuación hacemos clic sobre **Añadir excepción...**



Añadimos la excepción

- En el siguiente paso hacemos clic sobre **Obtener certificado** y después sobre **Confirmar excepción de seguridad**.



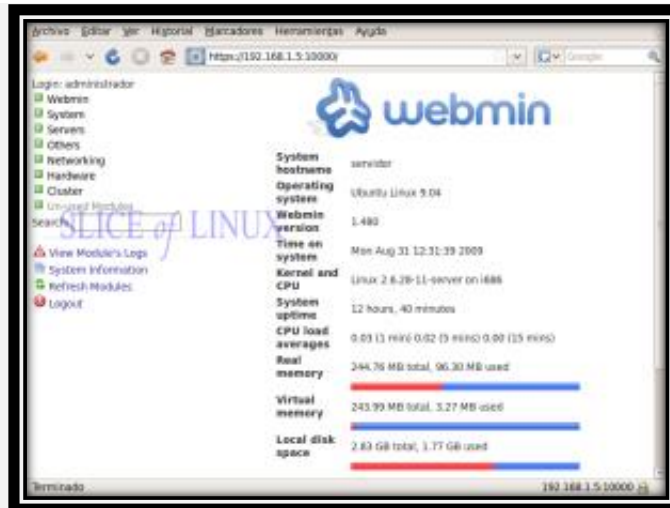
Obtenemos el certificado y confirmamos la excepción

- Ahora ya podemos iniciar sesión en Webmin. Como nombre de usuario podemos usar *root* (si lo tenemos habilitado) o cualquier usuario del sistema con privilegios de administrador.



Iniciamos la sesión en Webmin

- Y así accedemos a la interfaz de Webmin.



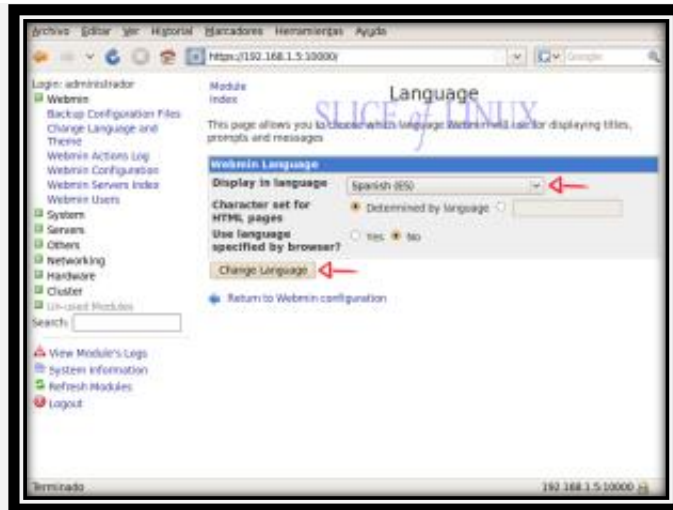
Página de inicio de Webmin

- Para cambiar el idioma hacemos clic sobre **Webmin** en el menú de la izquierda, después en **Webmin Configuration** y, por último, sobre **Language**.



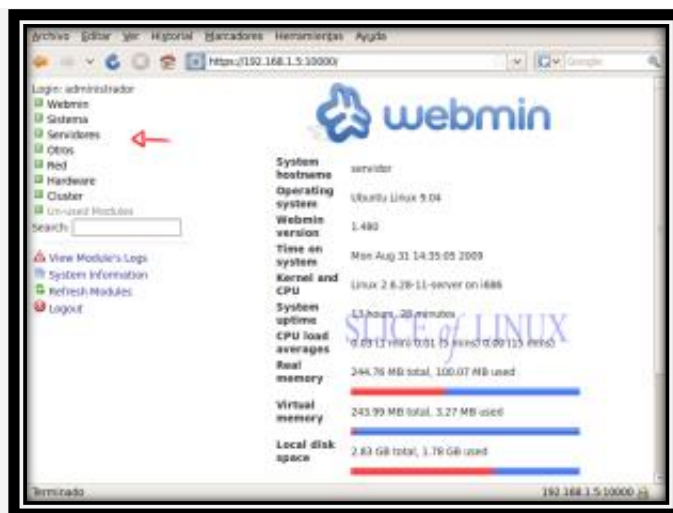
Accedemos a la configuración de Webmin

- Ahora en **Display in language** seleccionamos **Spanish (ES)** y hacemos clic en **Change Language**.



Cambiamos el idioma a Spanish (Español)

- Seguramente veremos parte de la interfaz en español pero no toda pero bastará con pulsar la tecla **F5** para actualizar la página.
- Ya tenemos la interfaz de Webmin en español como podemos comprobar en el menú de la izquierda.



Interfaz de Webmin en español

3. INSTALACIÓN Y CONFIGURACIÓN DE FIREWALL SHOREWALL

(<http://www.letrasdehercules.com/instalar-firewall-shorewall-en-ubuntu-server-10-04-lts-paso-a-paso/>)

Primero debemos instalar shorewall en nuestro servidor con el siguiente comando: **sudo apt-get update && sudo apt-get install shorewall**

Una vez instalado configuramos el fichero **/etc/default/shorewall** y cambiamos la línea **startup = 0** por **startup = 1** para que el cortafuegos se ejecute como servicio al iniciar el sistema.

Configuraremos ahora los siguientes ficheros en el directorio **/etc/shorewall**: zones, interfaces, policy, params, params.ips y rules

Zones: Como su nombre indica establece las zonas del cortafuegos (en mi caso fw para el firewall y net para internet) y quedaría algo así:

```
#####
#####

#ZONE  TYPE      OPTIONS   IN        OUT

fw     firewall

net    ipv4

#LAST LINE — ADD YOUR ENTRIES BEFORE THIS ONE — DO NOT REMOVE
```

interfaces: Se establecen las interfaces de red (en mi caso eth0) y quedaría:

```
#####
#####
```

```
#ZONE INTERFACE BROADCAST OPTIONS
```

```
net bond0 detect dhcp,tcpflags,logmartians,nosmurfs
```

```
#LAST LINE — ADD YOUR ENTRIES BEFORE THIS ONE — DO NOT REMOVE
```

policy: Establece que tipo de firewall será (restrictivo o permisivo). Yo uso un firewall restrictivo y abro aquellos puertos o servicios que me interesan. Quedaría algo así:

```
#####
```

```
#####
```

```
#SOURCE DEST POLICY LOG LIMIT: CONNLIMIT:
```

```
fw net ACCEPT
```

```
net fw DROP info
```

```
net all DROP info
```

```
# The FOLLOWING POLICY MUST BE LAST
```

```
all all DROP info
```

```
#LAST LINE — ADD YOUR ENTRIES ABOVE THIS LINE — DO NOT REMOVE
```

params: Permite definir parámetros (en mi caso incluyo un fichero con las IPs a las que permito acceder). Sería así:

```
#####
```

```
#####
```

```
INCLUDE params.ips
```

```
#LAST LINE — DO NOT REMOVE
```

params.ips: El fichero en el que defino la lista de IPs a las que permito acceder.

IPS_PERMITIDAS=XXX.XXX.XXX:XXX # (Sustituya las X por la dirección IP que quieras. Se pueden poner tantas como quieras separadas por coma.) rules: En este fichero es donde realmente se definen las reglas del cortafuegos. Como hemos establecido un firewall restrictivo, únicamente tendremos que especificar aquellos puertos o servicios a los que queramos dar acceso. Pongamos algunos ejemplos:

Abrir el puerto 80 o servicio HTTP para un servidor web

```
HTTP/ACCEPT net fw
```

Abrir el puerto 3452 para el protocolo TCP

```
ACCEPT net fw tcp 3452
```

#Abrir el puerto SSH únicamente a una IP de las que hemos definido como permitidas anteriormente

```
SSH/ACCEPT net:$IPS_PERMITIDAS fw
```

Y así sucesivamente con las reglas que queramos añadir.

Comprobamos que hemos configurado bien el cortafuegos con **sudo shorewall check**

Si todo ha ido bien, reiniciamos el cortafuegos **sudo shorewall start**

¡Listo! Ya tenemos nuestro shorewall configurado en Ubuntu.

4. INSTALACIÓN Y CONFIGURACIÓN DE SQUID PROXY

1. INSTALAR EL PROXY

PARA INSTALAR SQUID ESCRIBE EN UN TERMINAL:

```
SUDO APT-GET INSTALL SQUID
```

2. CONFIGURAR EL PROXY

LA CONFIGURACIÓN DE SQUID SE HACE EDITANDO EL ARCHIVO /ETC/SQUID/SQUID.CONF

PARA EDITAR ESTE ARCHIVO, PRESIONA ALT+F2 Y:

```
GKSU GEDIT /ETC/SQUID/SQUID.CONF
```

2.1 Nombrar el proxy

Squid necesita conocer el nombre de la máquina. Para ello, ubica la línea **visible_hostname**.

Por ejemplo, si la máquina se llama “ubuntu”, pon:

```
visible_hostname ubuntu
```

2.2 Elegir el puerto

Por defecto, el puerto de escucha del servidor proxy será 3128. Para elegir otro puerto, ubica la línea:

```
http_port 3128
```

Y cambia el número de puerto, por ejemplo:

```
http_port 3177
```

2.3 Elegir la interfaz

Por defecto el servidor proxy escucha por todas las interfaces. Por razones de seguridad, sólo debes hacer que escuche en tu red local

Por ejemplo si la tarjeta de red ligada a tu LAN tiene el IP 10.0.0.1, modifica la línea a:

http_port 10.0.0.1:3177

2.4 Definir los derechos de acceso

Por defecto, nadie está autorizado a conectarse al servidor proxy, excepto tu máquina. Entonces hay que crear una lista de autorización.

Por ejemplo vamos a definir un grupo que abarca toda la red local.

Ubica la línea del archivo que comienza por `acl localhost...`

Al final de la sección, agrega:

acl lanhome src 10.0.0.0/255.255.255.0

(lanhome es un nombre arbitrario que hemos elegido)

```
#
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443          # https
acl SSL_ports port 563          # snews
acl SSL_ports port 873          # rsync
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl Safe_ports port 631         # cups
acl Safe_ports port 873         # rsync
acl Safe_ports port 901         # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
acl lanhome src 10.0.0.0/255.255.0
```

2.5 Autorizar al grupo

Ahora que el grupo está definido, vamos a autorizar para que utilice el proxy.

Ubica la línea `http_access allow...`

Y agrega debajo (antes de la línea `http_access deny all`)

`http_access allow lanhome`

```
# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks
http_access allow localhost
http_access allow lanhome

# And finally deny all other access to this proxy
http_access deny all
```

2.6 Autorizar los puertos no estándar

Por defecto, Squid sólo autoriza el tráfico HTTP en algunos puertos (80, etc.)

Esto puede ocasionar problemas a algunas páginas web que utilizan otros puertos

Ejemplo: <http://toto.com/>: 81/images/titi.png sería bloqueado por Squid.

Para evitar que lo bloquee, encuentra la línea:

```
http_access deny !Safe_ports
```

Y agrega un comentario:

```
#http_access deny !Safe_ports
```

3. INICIAR EL PROXY

Reinicia el proxy para que tome en cuenta la nueva configuración que acabamos de realizar.

Escribe:

```
sudo /etc/init.d/squid restart
```

A partir de ahora el proxy debería funcionar. Sólo hay que configurar los diversos programas para que lo utilicen.

Información

LOS LOGS DEL PROXY SE ENCUENTRAN EN **/VAR/LOG/SQUID/ACCESS.LOG**

Modificar el tamaño del caché

Por defecto, el caché de Squid está activado, lo que permite que las páginas se carguen más rápido.

El tamaño por defecto es de 100 Mo (ubicado en /var/spool/squid).

Para cambiar su tamaño, modifica el archivo /etc/squid/squid.conf

Encuentra la línea:

```
# cache_dir ufs /var/spool/squid 100 16 256
```

Modifícala, puedes cambiar el valor de 100 por el valor que desees (por ejemplo 200 para 200 Mo):

```
cache_dir ufs /var/spool/squid 200 16 256
```


5. INSTALACIÓN Y CONFIGURACIÓN DE EASYHOTSPOT

(https://groups.google.com/forum/#!topic/teletriunfador/blkpRoU_Icw)



El objetivo de este artículo es implementar un portal cautivo en una red WiFi de pequeño tamaño, para de esta manera mantener un control de la navegación de los usuarios. Al ser un centro pequeño se utilizará autenticación local, no se utilizará autenticación mediante un Servidor Radius, que se utiliza para centros de mayor envergadura. Resumiendo, el objetivo final es controlar el acceso a internet vía WiFi mediante autenticación.

NOTA: Para el correcto entendimiento de este artículo es necesario tener ciertos conocimientos de administración de redes informáticas y de Linux.

En este artículo se va a implementar un servicio de Portal Cautivo de forma rápida y sencilla. Para aquel que desconozca qué es un portal cautivo, es un programa o máquina que, en una red informática, controla el tráfico HTTP y fuerza a los usuarios a pasar por una página pasarela para habilitar la navegación por Internet de forma normal. Un sistema de Portal Cautivo puede ser un ordenador haciendo de router, o un router hardware. En nuestro caso vamos a usar un ordenador por ser la opción más fácil y económica.

REQUISITOS PREVIOS

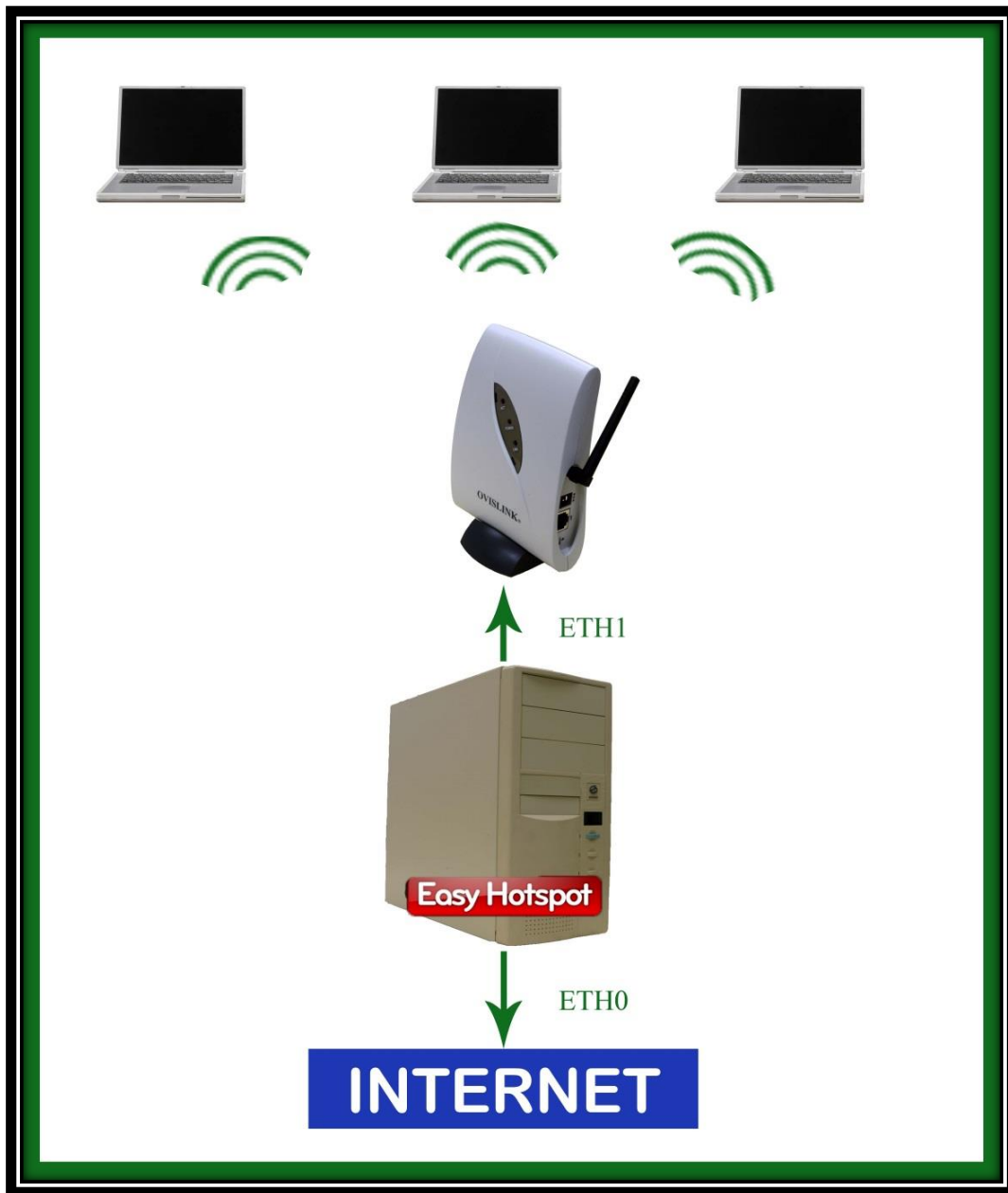
Para el montaje del Captive Portal (Portal Cautivo) necesitaremos:

- Un ordenador donde instalar el portal cautivo con 2 tarjetas de red
- Un Wireless Access Point (Punto de acceso WiFi)

- Cables de red
- Acceso a Internet
- Nociones medias de Linux
- CD de instalación de EasyHotSpot

Vamos a englobar en 4 apartados los pasos necesarios para la instalación y gestión del portal cautivo: Hardware, instalación, configuración y administración de EasyHotSpot. La autenticación se va a llevar a cabo en local (en el propio servidor donde está instalado Easy HotSpot) por lo que la instalación se simplifica.

HARDWARE



Tras comprobar que tenemos todo el Hardware necesario, comenzaremos por conectar el punto de acceso a una de las tarjetas de red de nuestro ordenador, concretamente en la ETH1, conectando la tarjeta ETH0 a la red de internet.

INSTALACIÓN

EasyHotSpot viene como live CD con distribución Ubuntu, la cual tras descargarla de la página web oficial deberás grabarla en un cd-rom o dvd en blanco con formato .iso. Una vez tienes el cd de EasyHotSpot, arrancas el PC desde el CD-ROM (configurar en la BIOS).

Tras cargar la interfaz gráfica de Ubuntu, verás un acceso directo en el escritorio sobre el cual harás clic para instalar el sistema operativo (Ubuntu) junto al portal cautivo, todo esto se hace como una instalación normal de Ubuntu, sólo tendrás que seguir las instrucciones mostradas en pantalla.

Una vez la instalación haya finalizado y veas que tu ordenador se ha reiniciado y el sistema operativo está iniciado, abre un navegador en Ubuntu y teclea “<http://localhost/easyhotspot>” para acceder al Panel de Control del portal cautivo. Por defecto tendrás estos datos de acceso:

Admin: admin
Password: admin123

Si has conseguido llegar hasta aquí y los cables de red e internet los tienes correctamente conectados, tu portal cautivo ya debería funcionar. Para comprobar su funcionamiento basta con acceder a la red por defecto que brinda el punto de acceso mediante un dispositivo con WiFi. Si al conectar y entrar en el navegador te re direcciona a la página de acceso, ¡enhorabuena! Has conseguido montar un portal cautivo.

CONFIGURACIÓN

Después de que el proceso de instalación haya finalizado con éxito, hay varios pasos más a tener en cuenta para asegurarse de que EasyHotSpot se está ejecutando sin problemas.

1. **Edición de información del Hotspot (portal cautivo).** EasyHotSpot te permite editar la información del punto de acceso de la página de la gestión administrativa. Para editar la información del portal cautivo tienes que editar el archivo `/opt/local/web/easyhotspot/system/application/config/easyhotspot.php` , y editar los campos como “empresa”, “dirección”, etc.
2. **Configuración del idioma.** Por suerte para muchos, EasyHotspot está en español. Sólo tienes que editar la configuración del idioma que se encuentra en `system/application/config/config.php` , y modificar el campo `$config['language']`. Por `$config['language'] = 'latin';`
3. **Editar Homepage.** De forma predeterminada, EasyHotspot sólo es accesible desde el propio servidor (localhost), si quieres entrar para configurar el HotSpot desde una máquina remota sólo tienes que editar `/opt/local/web/htdocs/easyhotspot/system/application/config/config.php` y escribir tu dirección IP, por ejemplo: `$config['base_url'] = "http://192.168.182.1/";`

ADMINISTRACIÓN

Tras acceder al panel de administración de EasyHotSpot mediante `http://localhost/easyhotspot` con nombre de usuario: admin y contraseña; admin123, navega un poco por la interfaz para familiarizarte con ella. Como veremos más adelante (apartado "cambiar contraseña"), es muy importante cambiar la contraseña para incrementar la seguridad de nuestra administración.

La función que nosotros le daremos al portal cautivo nos hace tener en cuenta sólo algunas partes de la administración olvidándonos de las otras por completo. Tenemos diferenciadas dos administraciones, la de administrador (refiriéndose al servidor radius, página de inicio, etc) y la de cashier, desde donde se crearían los tickets de los usuarios.

Desde la interfaz de administrador accedemos a:

Easy Hotspot 0.2

[Cashier Menu] - [Admin Menu]

Tuesday, 06-Oct-09 17:10:14 UTC

Welcome to the admin console

Hotspot Info

Company Name	EasyHotspot OpenSource
Company Address	Legian Street Kuta Bali - Indonesia
Phone	+62 231 999999
Tax Code	

System Info

Hostname	panduhotspot
Operating System	GNU/Linux
MySQL ?	1
Chillspot ?	1
Chillspot COAPORT ?	1
Radius 1812 ?	1
Radius 1813 ?	1
Radius 1814 ?	1

You are logged in as admin
Here You can manage system configuration.
Use the menu above to perform different management operations

EasyHotspot - OpenSource Hotspot Management System

- **Chillispot Configuration**

Radius Server 1: (Dirección primaria del servidor RADIUS, por defecto 127.0.0.1)

Esta opción no la vamos a configurar porque vamos a hacer la autenticación en local.

Radius Server 2 :(Dirección secundaria del servidor RADIUS, por defecto 127.0.0.1) Esta opción no la vamos a configurar porque vamos a hacer la autenticación en local.

Radius Secret: (Secret phrase entre el servidor RADIUS y Chillispot) Viene configurada por defecto

DHCP Interface: (Indica la interfaz que quieres que el Hotspot use como tal) Viene configurada por defecto

UAM Server: (Dirección donde está guardado el captive portal) Configurada por defecto

UAM Secret: (Secret phrase entre la página de login y Chillispot) Configurada por defecto.

Client's Homepage: (Donde quieres que se re direcciona el cliente una vez ha iniciado sesión)

Allowed URL: (URL que los clientes puede buscar sin estar logueados, NO PONGAS ESPACIOS, ej: www.google.com,www.twitter.com")

DHCP Range: (Rango DHCP), conviene dejarlo por defecto teniendo en cuenta que la red a configurar no va a superar los 50 equipos.

Redirect after login: Es la página que quieras que aparezca una vez estás logueado, en nuestro caso podemos poner la web del instituto desde el que estemos montando el portal cautivo.

Internal captive portal management		
Radius Server 1	127.0.0.1	?
Radius Server 2	127.0.0.1	?
Radius Secret	easyhotspot	?
DHCP Interface	eth1	?
UAM Server	http://192.168.182.1/hotspo	?
UAM Secret	easyhotspot	?
Client's Homepage	http://192.168.182.1:3990/p	?
Allowed URL	192.168.182.1	? Separate by comma
DHCP Range	192.168.182.0/19	?
Redirect after login	http://google.com	?

Save Configuration Restore Default

*Al final del documento encontrarás un glosario con la definición de los términos aquí expuestos.

Billing plan

La página de plan de facturación o billing plan se utiliza para crear una pauta de facturación que después será utilizada como plantilla en la creación de los cupones de conexión. Al decir facturación no quiere decir que tengamos que cobrar por el servicio sino que es la forma de administrar el tiempo de conexión desde EasyHotSpot.

Para crear un nuevo plan de facturación tienes que rellenar los campos bajo la lista de planes de facturación existentes. También podrás eliminar un plan de facturación existente

haciendo clic en la ‘X’ en la fila del plan de facturación que desees eliminar, o también puedes modificar el plan de facturación haciendo clic en el icono del lápiz.

Un campo importante a tener en cuenta para nosotros será el de “Amount” en el cual podrás definir los minutos que durará la validez de la cuenta.

Name: Nombre del plan de facturación

Type: Tipo de facturación en datos o tiempo.

Amount: minutos que durará la validez de la cuenta

Valid for: Válido durante el periodo de días definido

Price: Precio del plan

Download rate: Tarifa máxima de descarga de archivos

Upload Rate: Tarifa máxima de subida de archivos

Idle Timeout: Tiempo de desconexión tras inactividad del usuario

Friday, 26-Mar-10 04:03:10 UTC

[Cashier Menu] - [Admin Menu]

Billing Plan

id	Name	Type	Amount	Valid for	Price	DL rate	Up rate	Created by	
8	1 hour	time	60	30	\$ 1,000.00	1024000	1024000	admin	✖
10	prueba	time	10	10	\$ 10.00	96000	96000	admin	✖

Name

Type

Amount

Valid for

Price

Download Rate

Upload Rate

Idle Timeout

Recuerda cambiar la contraseña de administrador en Manage Admins, por seguridad.

Además, ten en cuenta la posibilidad de crear nuevos administradores  y nuevos

Cashier .

Desde la interfaz de Cashier accedemos a:

Postpaid Account Management

Postpaid account management es un sistema de facturación postpago. El primer paso para utilizar esta característica, es crear un usuario con su respectiva contraseña. Una vez creado se le dan los datos de acceso al usuario (tienes la opción de imprimirlos) para que pueda acceder a Internet con su portátil u ordenador. Desde este menú puedes ver el nombre de usuario, la contraseña, si ha usado la cuenta, el tipo de facturación que tiene, el total facturado, la fecha válida del usuario y puedes editar todos los campos, imprimir o generar

una factura, así como eliminarlo. Una vez que la cuenta ha sido cerrada, no podrá ser usada de nuevo.

Una cuenta de este tipo puede facturar de dos maneras diferentes: por tiempo o por volumen de datos.

Realname: Nombre real de la persona

Username: Nombre de usuario

Password: Contraseña

Used: La cantidad del paquete usado

Bill By: Facturación por paquetes o tiempo

Total: Total disponible

Valid until: Válido hasta 'X' días

Postpaid

Real Name	Username	Password	used	Bill by	Total	Valid until	Action
pandu	pandu	pandu	3.78	packet	1.89		✖ 🍃 🗑️ 📄
easy	easy	easy	0.00	time	0.00	September 12 2009	✖ 🍃 🗑️ 📄

Name

Username


Password

Bill by days

Valid until days

Voucher Management

Otra opción para dar acceso a internet a los usuarios es mediante el Voucher Management

voucher , quizás una forma más cómoda que la anterior. Este submenú es un sistema de facturación prepago. El Cashier (en este caso el que administre el servicio) puede generar a la vez tantos “cupones” como necesite. Simplemente introducirá el número de cupones a crear y el Billing Plan (estos han sido creados por el administrador definiendo si el cupón va por tiempo o por datos descargados). También tienes la opción de imprimir el cupón para facilitar la tarea de darle los datos de acceso al usuario.

Username: Nombre de usuario

Password: Contraseña

Billing Plan: Plan de facturación

Valid until: Válido hasta

Time used: Tiempo usado

Time remain: Tiempo restante

Packet used: Paquete usado

Packet remain: Paquete restante

Printed: Imprimir

Voucher Management

Username	Password	Billing plan	Valid until	Time used	Time remain	Packet used	Packet remain	Printed			
husxub14	demmetis	5 minutes	October 7 2009	---	---	---	---	no	✘	✎	☰
yugbow5	melrideb	5 minutes	October 7 2009	---	---	---	---	no	✘	✎	☰
posyoh12	nuspatob	5 Mega		---	---	---	---	no	✘	✎	☰
tibtaw8	tugmocas	5 Mega		---	---	---	---	no	✘	✎	☰
riryid10	kicdiluk	5 Mega		0	---	5	0	no	✘	✎	☰

Export to Excel

How many voucher(s)?

Billing plan

Cambiar contraseña

Para cambiar la contraseña solamente tienes que acceder a este submenú e introducir la vieja contraseña (para dar permiso de cambio) e introducir una nueva contraseña.

Easy Hotspot 0.2

[Cashier Menu] - [Admin Menu]

Friday, 26-Mar-10 08:03:32 UTC

Change Password

Change Password

User Name:

Old Password:

New Password:

Confirm:

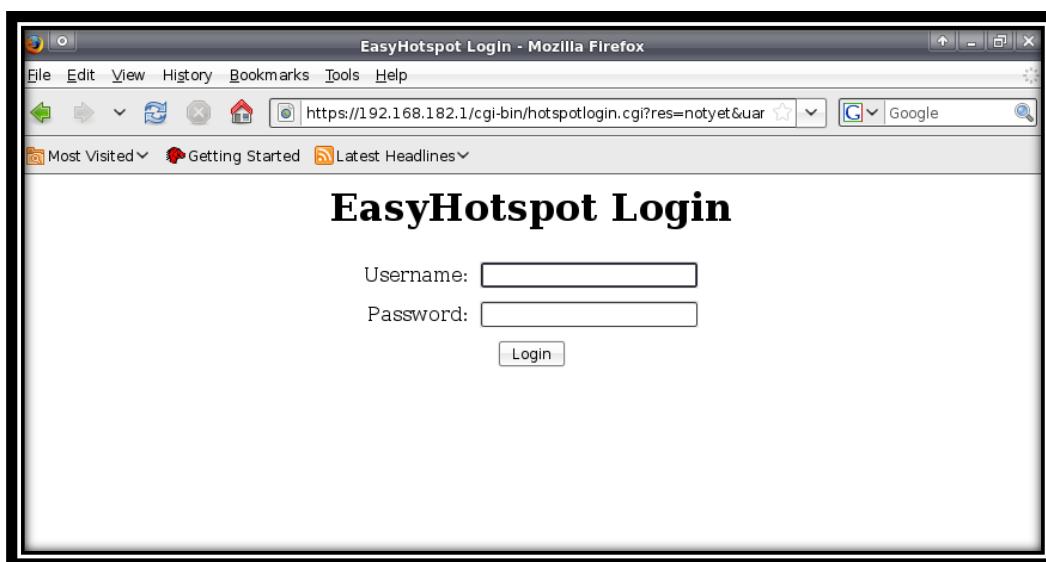
ANEXO D

MANUAL DE USUARIO

1. ACCEDER A INTERNET

PANTALLA DE LOGIN (ACCESO A INTERNET)

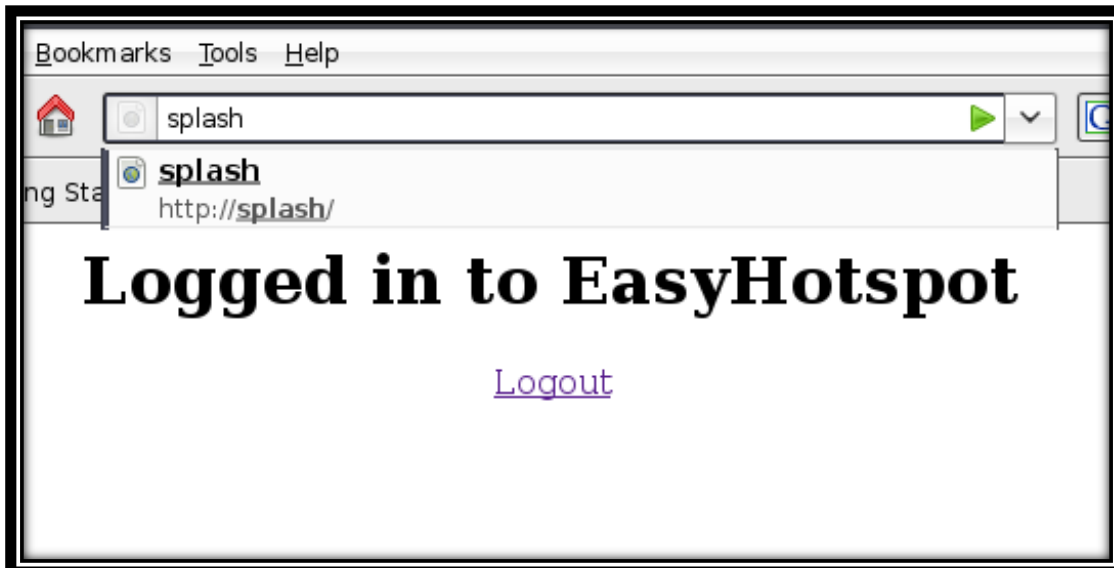
Para conectarse al Hotspot el usuario tendrá que acceder de forma habitual a la red WiFi donde se encuentra en Portal Cautivo, y una vez establecida la conexión verá que su navegador se redirecciona a una página de login.



Tienes que introducir el nombre de usuario y la contraseña proporcionada por el administrador y clickar en login. Una vez hecho esto verás la pantalla que confirma que estás logeado y podrás navegar por internet.

2. CERRAR SESIÓN

Para cerrar sesión solo bastara con escribir splash en la barra de direcciones.



ANEXO E

TABLAS DE LOS DATOS DE USUARIOS EN NUESTRA ZONA DE COBERTURA

LUNES				
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00	FECHA
1				
2				
3				
4				
5				

MARTES				
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00	FECHA
1				
2				
3				
4				
5				

MIÉRCOLES				
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00	FECHA
1				
2				
3				
4				
5				

JUEVES				
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00	FECHA
1				
2				
3				
4				
5				

VIERNES				
CALLE\HORA	8H00-10H00	12H00-14H00	17H00-18H00	FECHA
1				
2				
3				
4				
5				