

ANEXOS A

MODELO DE ENCUESTA REALIZADA A LOS REPRESENTANTES DE BARRIOS Y COMUNIDADES DE LA PARROQUIA DE CARANQUI

ENCUESTA PREVIO AL DISEÑO DE LA RED DE TELECOMUNICACIONES A BENEFICIO DE LA PARROQUIA DE CARANQUI

Red de telecomunicaciones:

Es una infraestructura tecnológica que brinda servicios de datos (internet), voz y video (videoconferencias) para la comunicación rápida y eficiente entre sectores que desean compartir recursos y diálogos a pesar de la distancia.

Video conferencias:

Comunicación visual y auditiva entre dos sectores que cuentan con la misma infraestructura y sirve para reuniones, capacitaciones e intercambio de ideas mediante una conversación virtual.

DATOS INFORMATIVOS:

Nombre del Barrio Comunidad San Francisco de Chelaviso

Representante legal (Presidente) Sr. Carlos Mesias Venegas Rivera

1.- Un estimado del número de familias que existe en su barrio

85

2.- Un estimado de número de estudiantes que existe en su barrio

50

3.- Que servicio de telecomunicaciones existe en su barrio? (Marque con una X)

- Telefonía celular
- Telefonía fija
- Servicio de Internet
- Cabinas telefónicas
- Cyber cafes

4.- Cuenta con un centro de reuniones (casa comuna!) su barrio? (Marque con una X)

SI

NO

5.- Cuenta con unidad educativa su barrio? (Marque con una X)

SI _____

Nombre de la unidad educativa _____

NO X

A que unidad educativa cercana acuden los estudiantes de su barrio

Esc. Oscar Freire Reyes -

6.- Piensa que es necesario la comunicación con entidades públicas y recibir capacitación mediante video conferencias.

Es muy necesario por la distancia, movilización para el desarrollo intelectual de la colectividad

7.- Como representante de su barrio piensa que es necesario tener una red de telecomunicaciones en su sector.

Es algo muy indispensable debido que ayudara al fortalecimiento de la comunidad, y así mejorar la calidad de vida de las personas

ANEXOS B

MODELO DE ENCUESTA REALIZADA A LOS REPRESENTANTES DE LAS UNIDADES EDUCATIVAS DE LA PARROQUIA DE CARANQUI

Encuesta dirigida a las Instituciones educativas de la parroquia de Caranqui previo al diseño de la Red de Telecomunicaciones

Red de telecomunicaciones:

Es una infraestructura tecnológica que brinda servicios de datos (internet), voz y video (videoconferencias) para la comunicación rápida y eficiente entre sectores que desean compartir recursos y diálogos a pesar de la distancia.

Video conferencias:

Comunicación visual y auditiva entre dos sectores que cuentan con la misma infraestructura y sirve para reuniones, capacitaciones e intercambio de ideas mediante una conversación virtual.

1.-Nombre de la institución educativa:

Agustin Cueva Dávila

2.-Nombre del representante (Director/Rector):

Dr. Fernando Escobar

3.-Nivel académico que brinda la institución (Marque con una X):

Pre-Primario

Primario

Secundario

4.- Numero de estudiantes que cuenta la institución actualmente

Pre-Primario _____

Primario 182 niños(as)

Secundario _____

5.- De que barrios o comunidades de la parroquia de Caranqui son sus estudiantes

Hernán González de Saá - B. 10 de Agosto - El Ejido

6.-Que materias impartidas en su institución son relacionadas con la computación o el internet

Informática 6 horas semanalmente

7.- Cuenta con laboratorio de computación su institución educativa (Marque con una X)

SI NO Prestadas

Su respuesta es SI

Cuántas computadoras posee su laboratorio

8

Cuenta con acceso a internet su laboratorio

SI NO

Su respuesta es SI

Que entidad le provee el servicio: CNT

8.- Ha escuchado sobre la videoconferencia, educación virtual y sus beneficios:

Si es muy importante en educación por el Adelanto Tecnológico y la Globalización.

9.- Que contenidos o páginas web ocupan en su institución educativa como apoyo en su trabajo tanto estudiantes como profesores:

MEC - AME - SI PROFE - otros Investigaciones: Cultural - Social - etc.

10.- Piensa usted que todo el contenido del internet ayuda al beneficio para mejorar el nivel académico de estudiantes y profesores

SI NO

Porque:

El profesor tiene la oportunidad de actualizarse en sus áreas de estudio y otros.

GRACIAS POR SU COLABORACION

Todas las encuestas se encuentran en los ANEXOS Digitales.

ANEXO C

**SIMULACIÓN DE RADIOENLACES DE LAS 21 ESTACIONES CLIENTE HACIA LA EB
MEDIANTE EL SIMULADOR RADIO MOBILE Y SU HERRAMIENTA RADIO LINK.**

Simulación entre la Estación Base y la estación cliente Juan de dios Navas –Naranjito

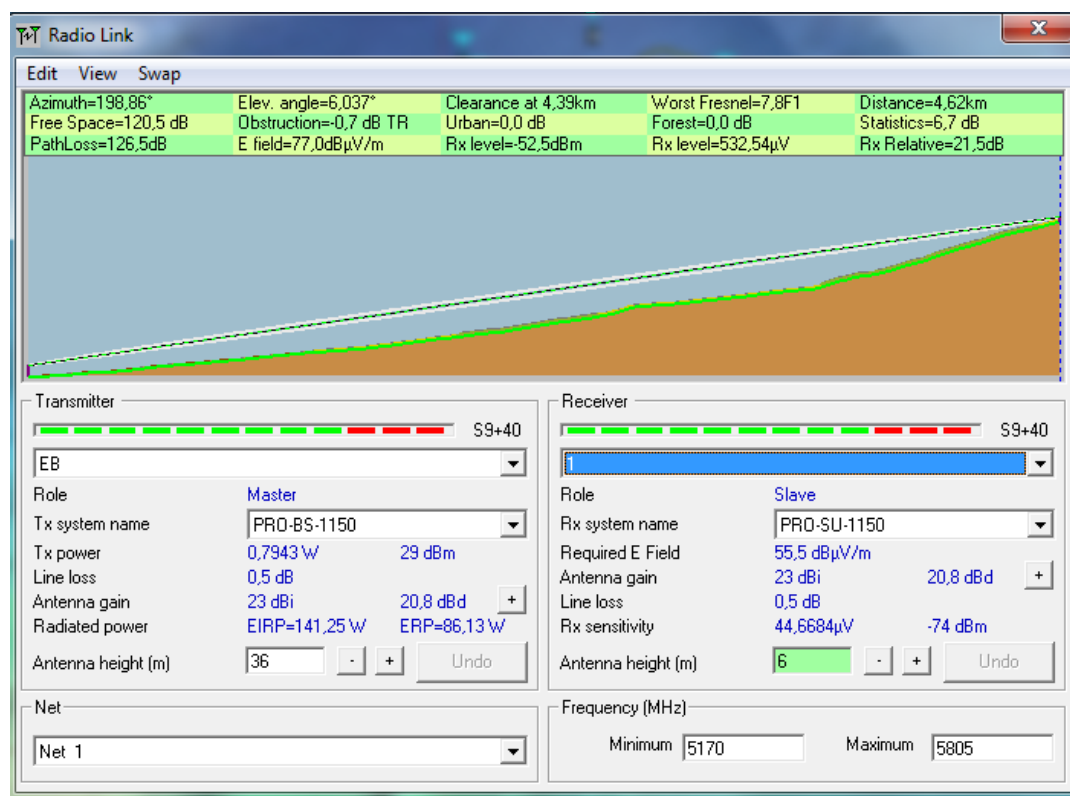


Figura C.1. Simulación del enlace Estación Base y la estación cliente Juan de dios Navas – Naranjito

Simulación entre la Estación Base y la estación cliente Leopoldo N Chávez - San Cristóbal Alto - San Cristóbal de Caranqui.

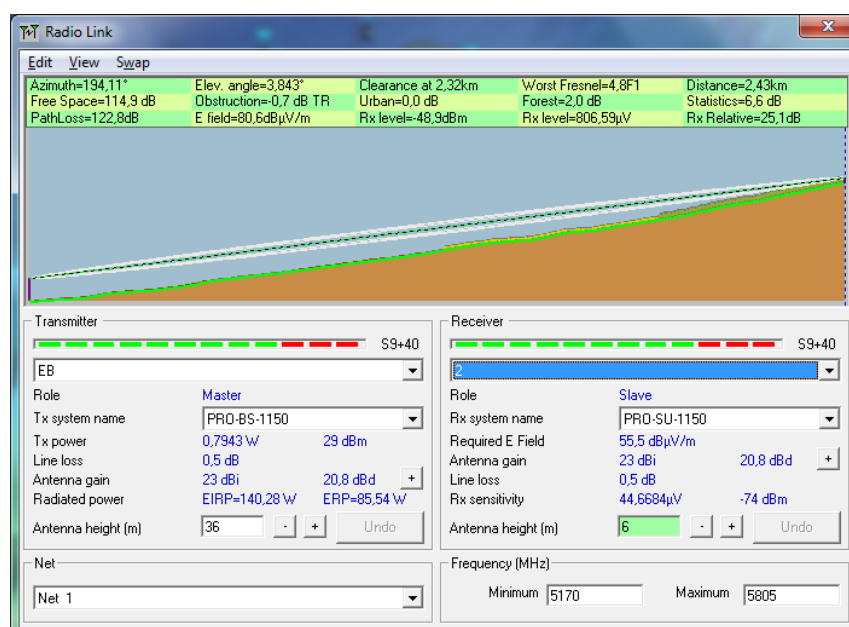


Figura C.2. Simulación del enlace Estación Base y la estación cliente Leopoldo N Chávez - San Cristóbal Alto - San Cristóbal de Caranqui.

Simulación entre la Estación Base y la estación cliente Manzanal

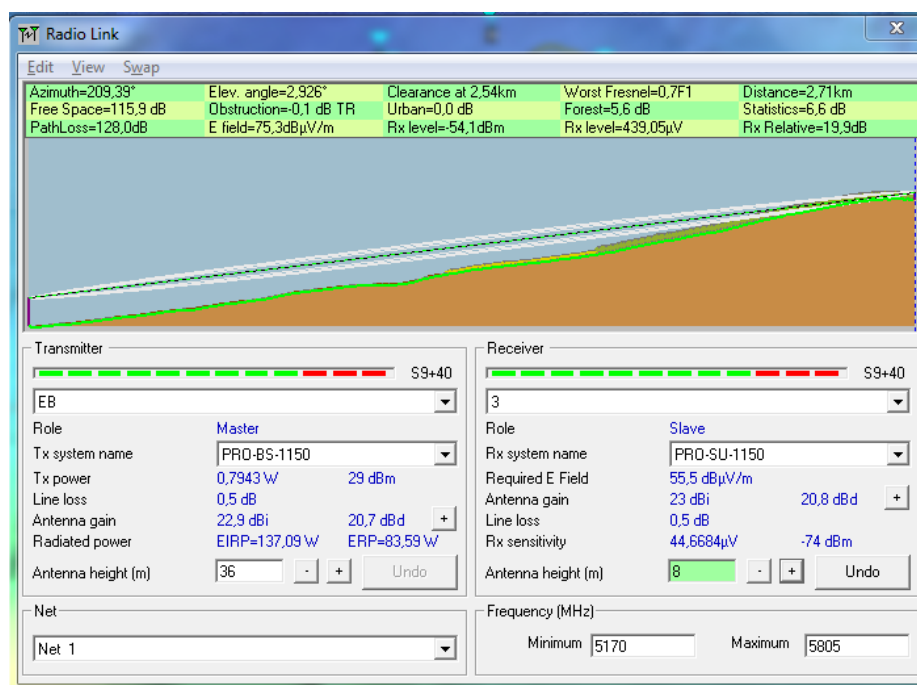


Figura C.3. Simulación del enlace Estación Base y la estación cliente Manzanal.

Simulación entre la Estación Base y la estación cliente Turupamba – San Francisco de Chorlavi.

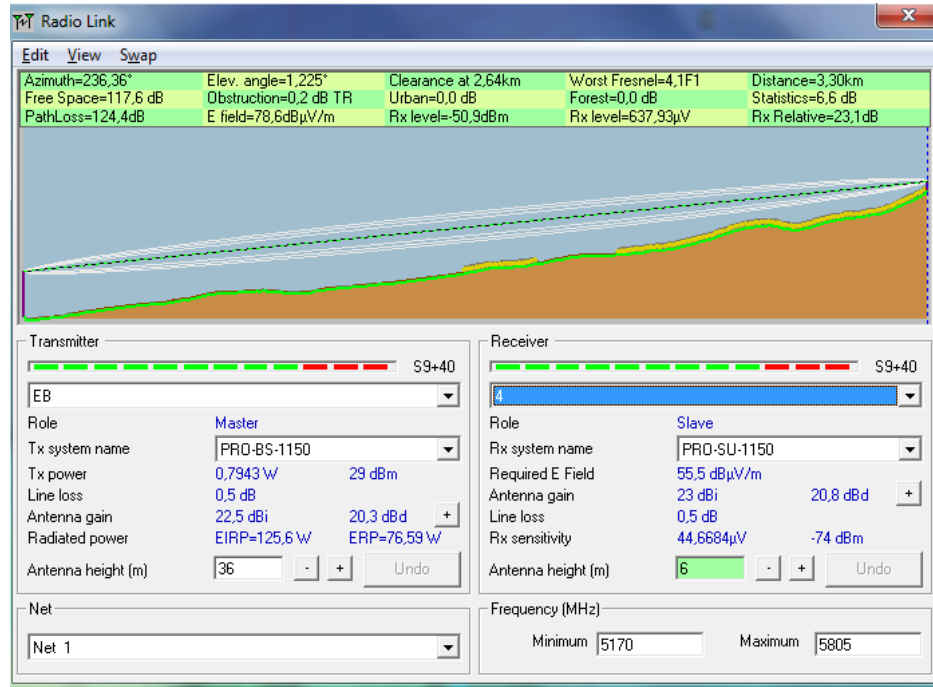


Figura C.4. Simulación del enlace Estación Base y la estación cliente Turupamba – San Francisco de Chorlavi.

Simulación entre la Estación Base y la estación cliente Catzoloma.

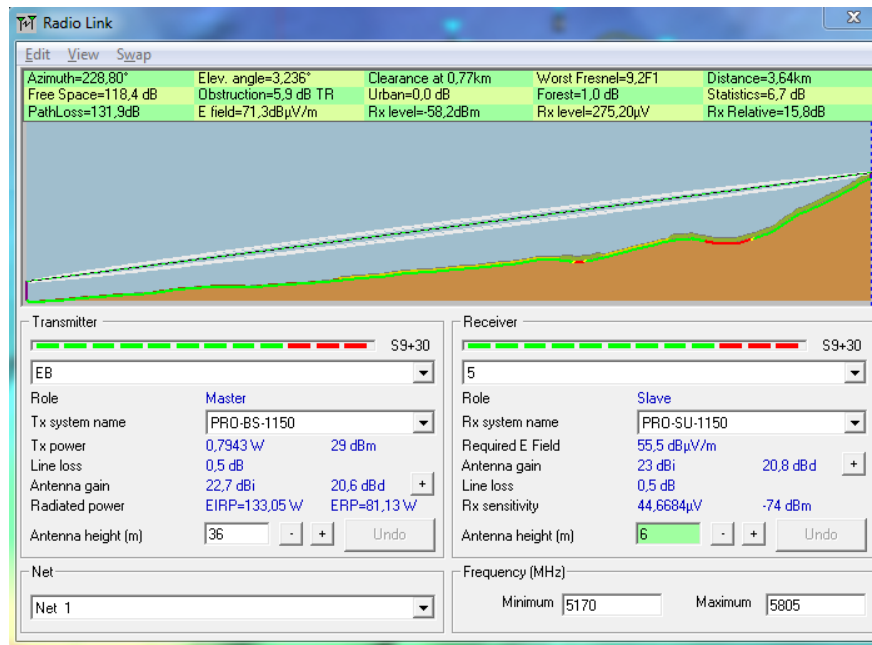


Figura C.5. Simulación del enlace Estación Base y la estación cliente Catzoloma.

Simulación entre la Estación Base y la estación cliente San Francisco de Chorlavisito.

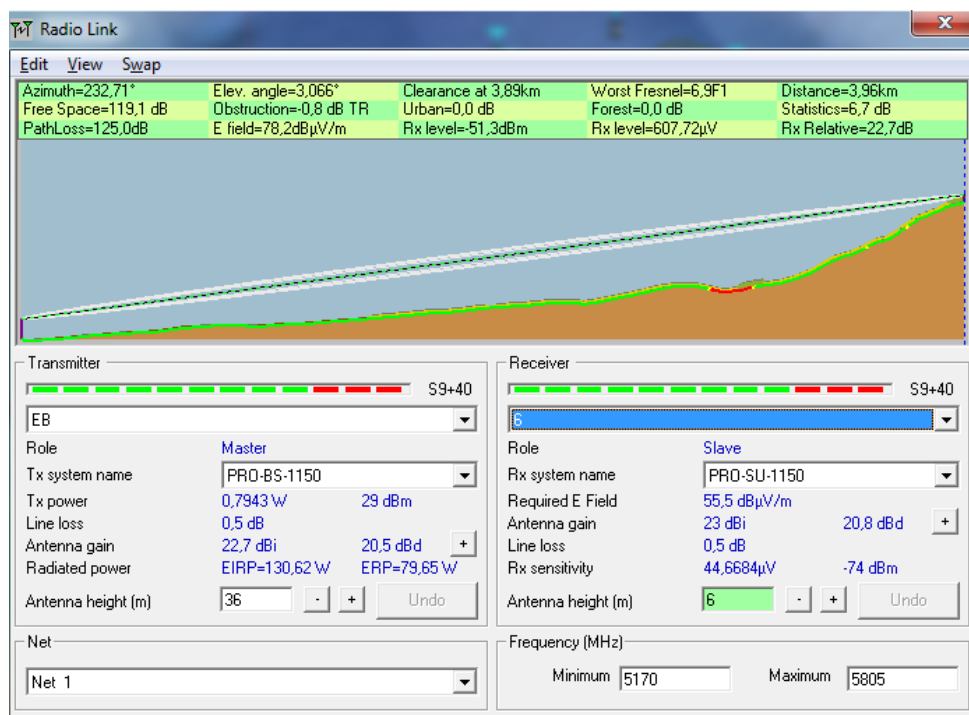


Figura C.6. Simulación del enlace Estación Base y la estación cliente San Francisco de Chorlavisito.

Simulación entre la Estación Base y la estación cliente 19 de Enero.

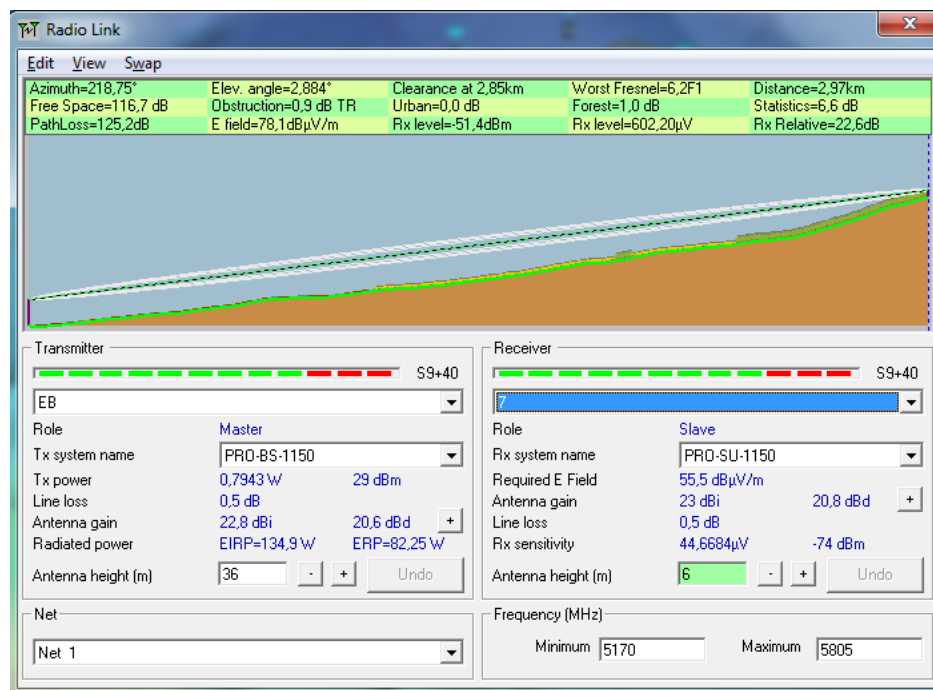


Figura C.7. Simulación del enlace Estación Base y la estación cliente 19 de Enero.

Simulación entre la Estación Base y la estación cliente Oscar Efren Reyes - Ejido de Caranqui – Unión y Progreso.

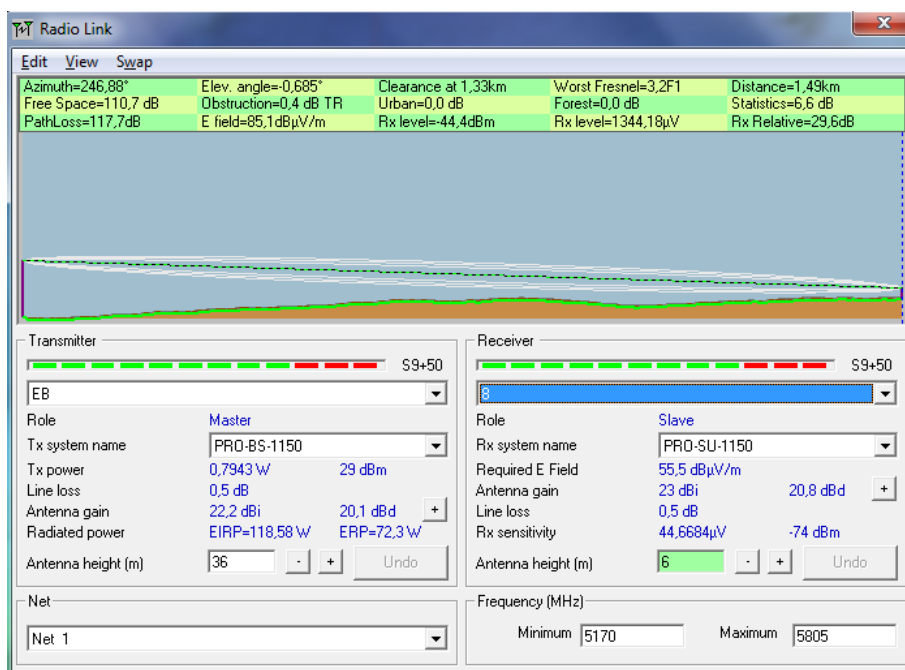


Figura C.8. Simulación del enlace Estación Base y la estación cliente Oscar Efren Reyes - Ejido de Caranqui – Unión y Progreso.

Simulación entre la Estación Base y la estación cliente Chamanal.

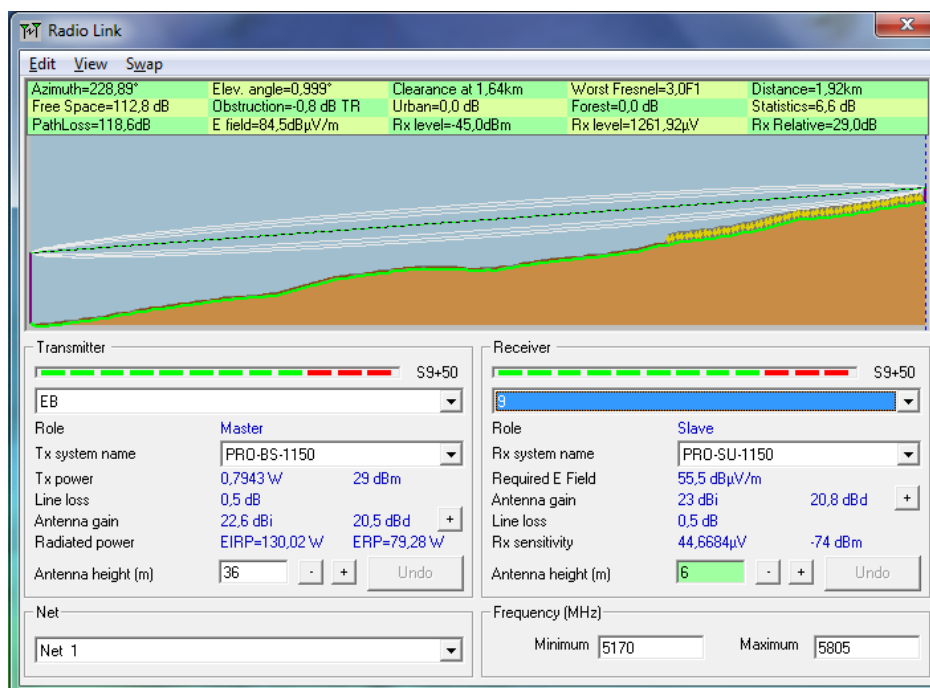


Figura C.9. Simulación del enlace Estación Base y la estación cliente Chamanal.

Simulación entre la Estación Base y la estación cliente 20 de Octubre.

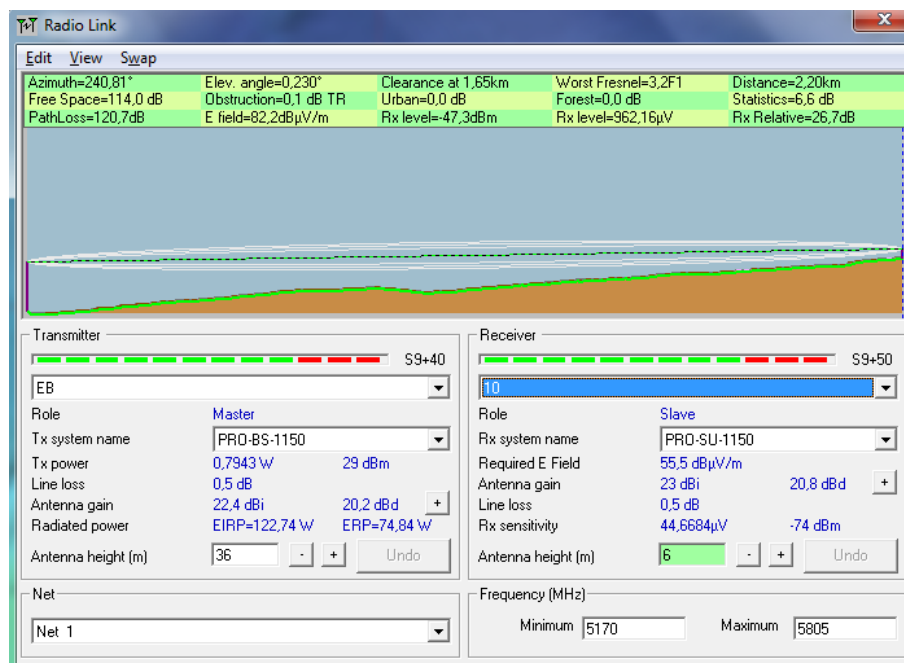


Figura C.10. Simulación del enlace Estación Base y la estación cliente 20 de Octubre.

Simulación entre la Estación Base y la estación cliente Guayaquil de Caranqui.

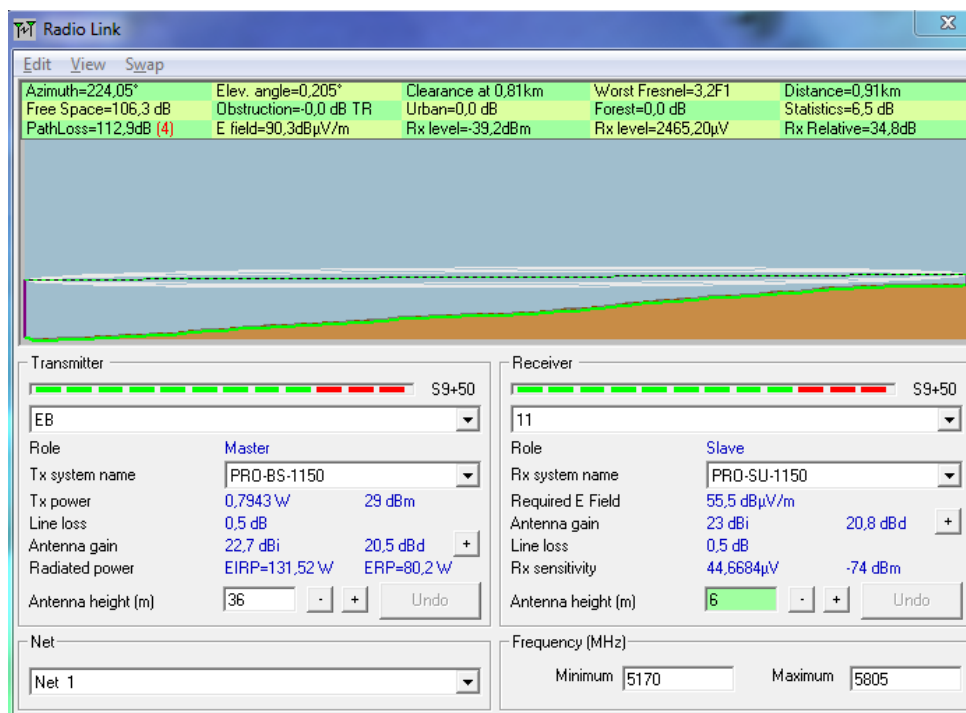


Figura C.11. Simulación del enlace Estación Base y la estación cliente Guayaquil de Caranqui.

Simulación entre la Estación Base y la estación cliente Agustín Cueva Dávila - Vista Hermosa – 10 de Agosto.

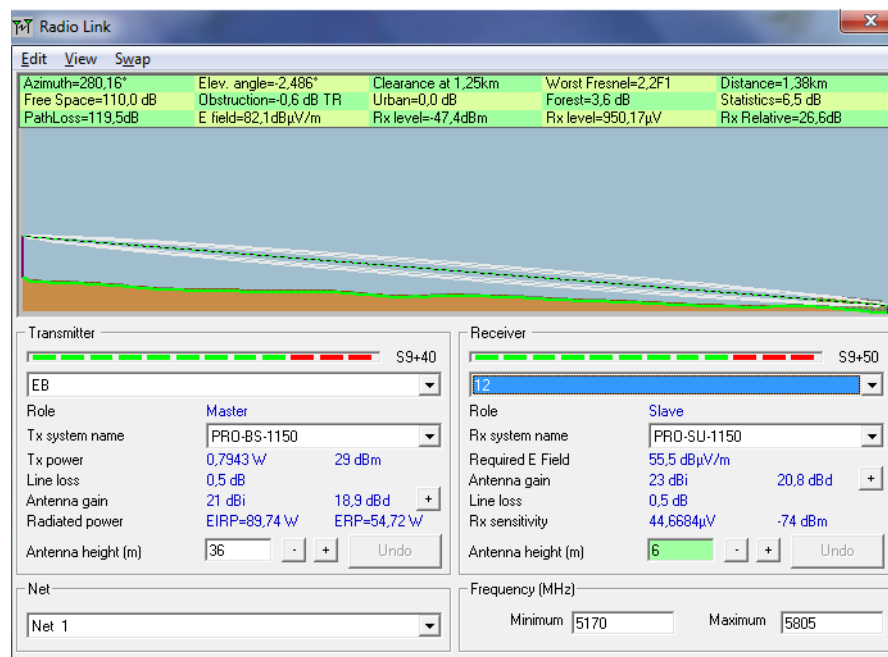


Figura C.12. Simulación del enlace Estación Base y la estación cliente Agustín Cueva Dávila - Vista Hermosa – 10 de Agosto.

Simulación entre la Estación Base y la estación cliente El Naranjal.

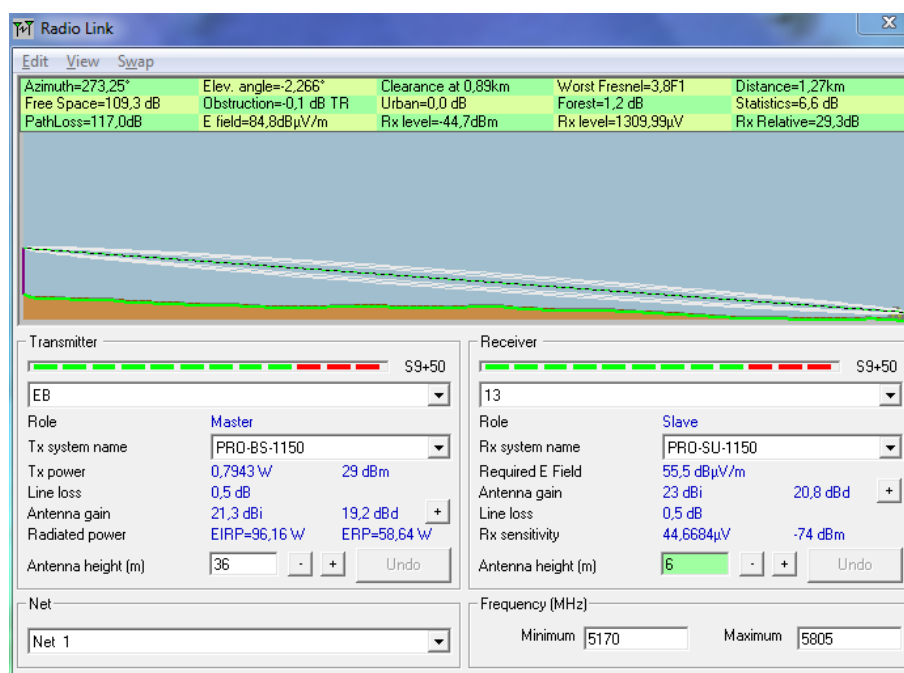


Figura C.13. Simulación del enlace Estación Base y la estación cliente El Naranjal.

Simulación entre la Estación Base y la estación cliente Yuyucocha.

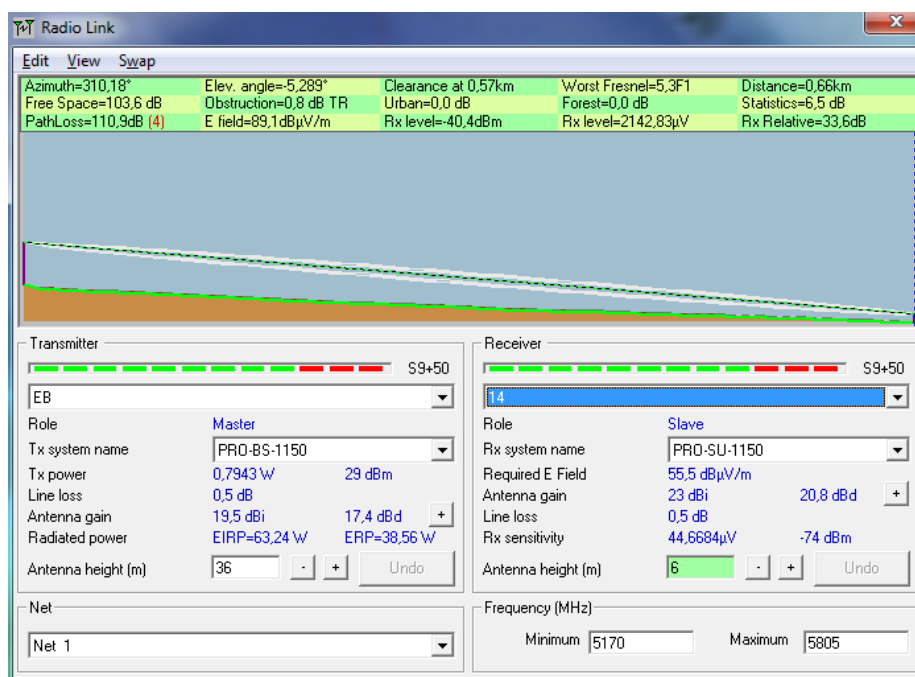


Figura C.14. Simulación del enlace Estación Base y la estación cliente Yuyucocha.

Simulación entre la Estación Base y la estación cliente Olimpia Gudiño Vázquez - Cuatro Esquinas.

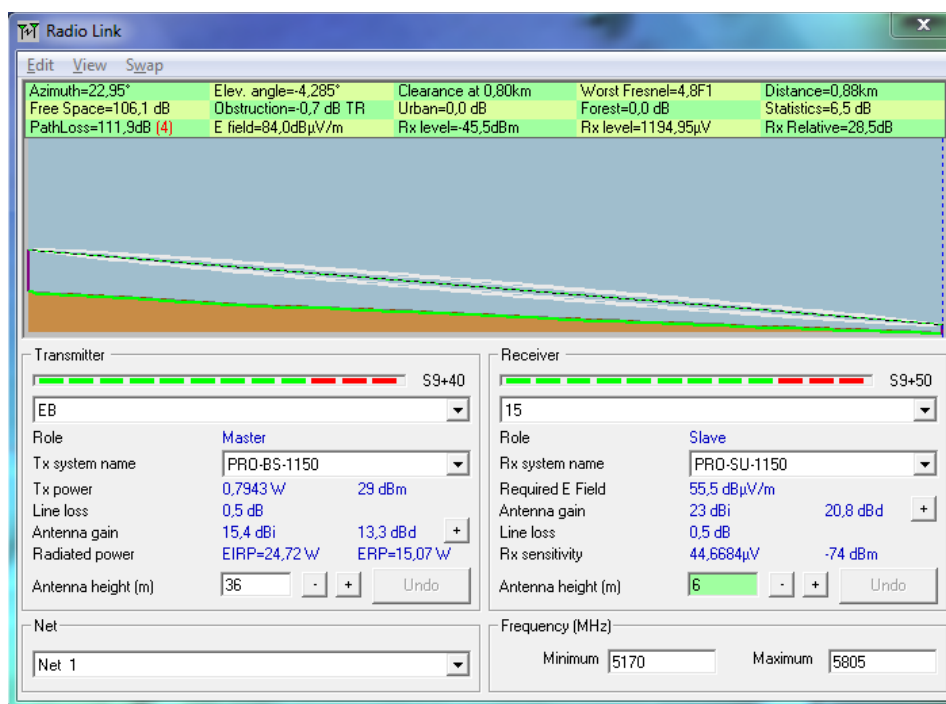


Figura C.15. Simulación del enlace Estación Base y la estación cliente Olimpia Gudiño Vázquez - Cuatro Esquinas.

Simulación entre la Estación Base y la estación cliente Colegio Atahualpa – La Candelaria.

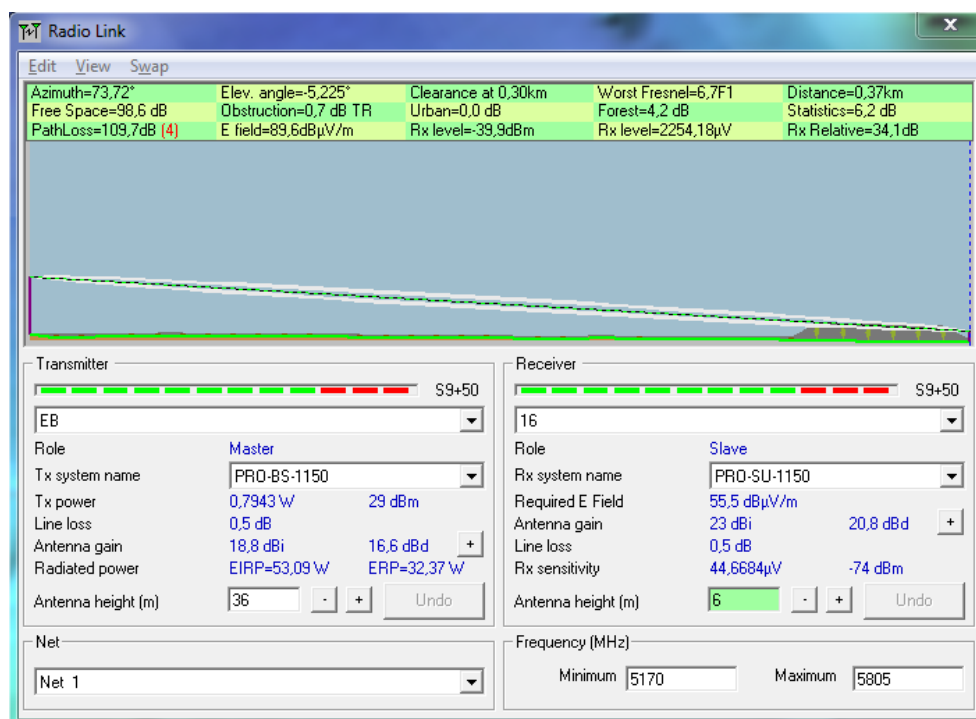


Figura C.16. Simulación del enlace Estación Base y la estación cliente Colegio Atahualpa – La Candelaria.

Simulación entre la Estación Base y la estación cliente José Nicolás Vacas.

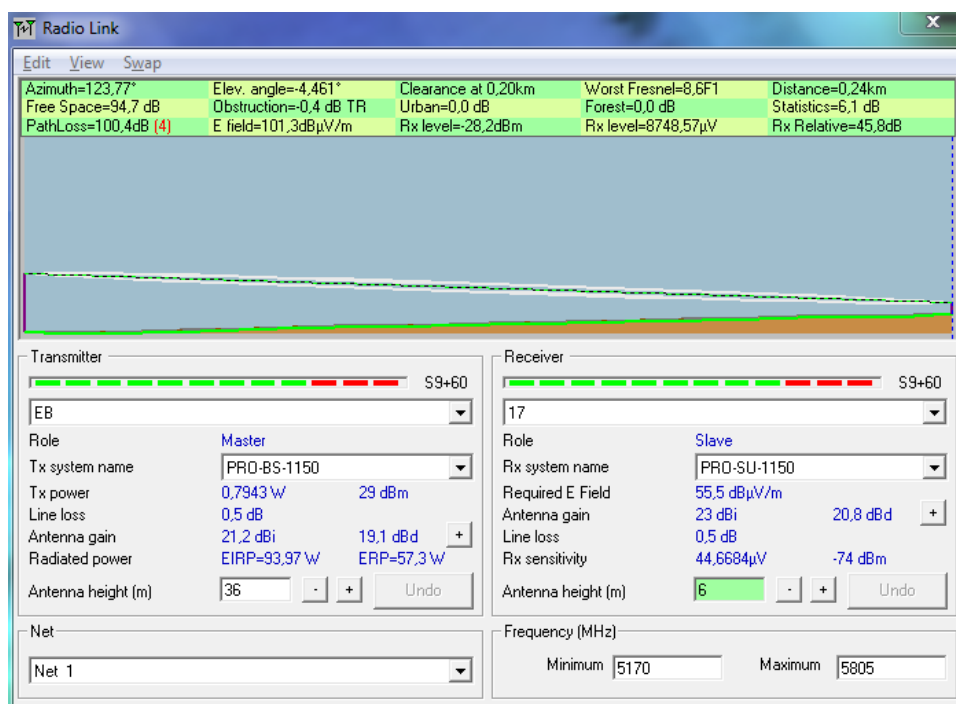


Figura C.17. Simulación del enlace Estación Base y la estación cliente José Nicolás Vacas.

Simulación entre la Estación Base y la estación cliente Avelina Lazo de Plaza – Simón Bolívar.

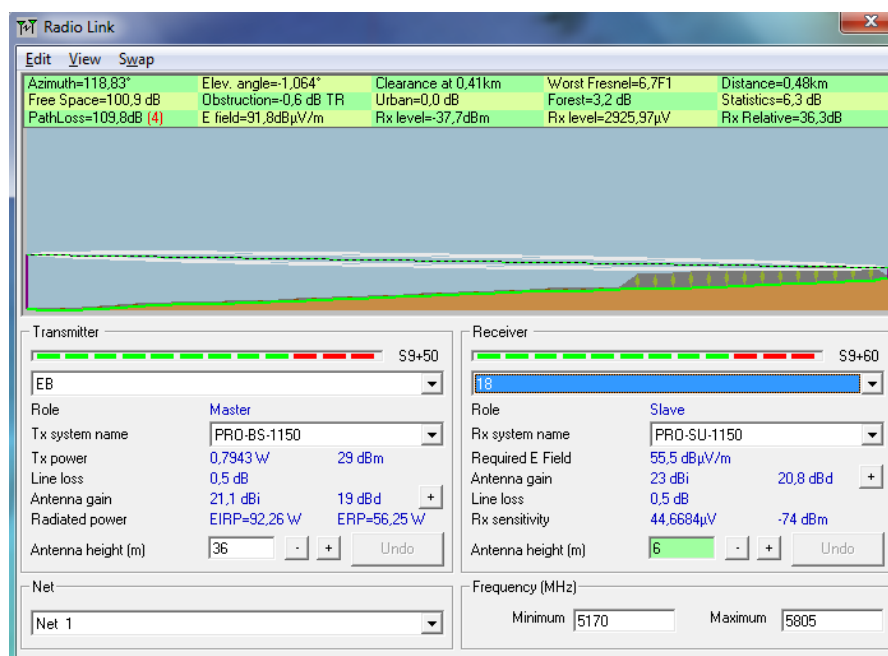


Figura C.18. Simulación del enlace Estación Base y la estación cliente Avelina Lazo de Plaza – Simón Bolívar.

Simulación entre la Estación Base y la estación cliente Juan Miguel Suarez.

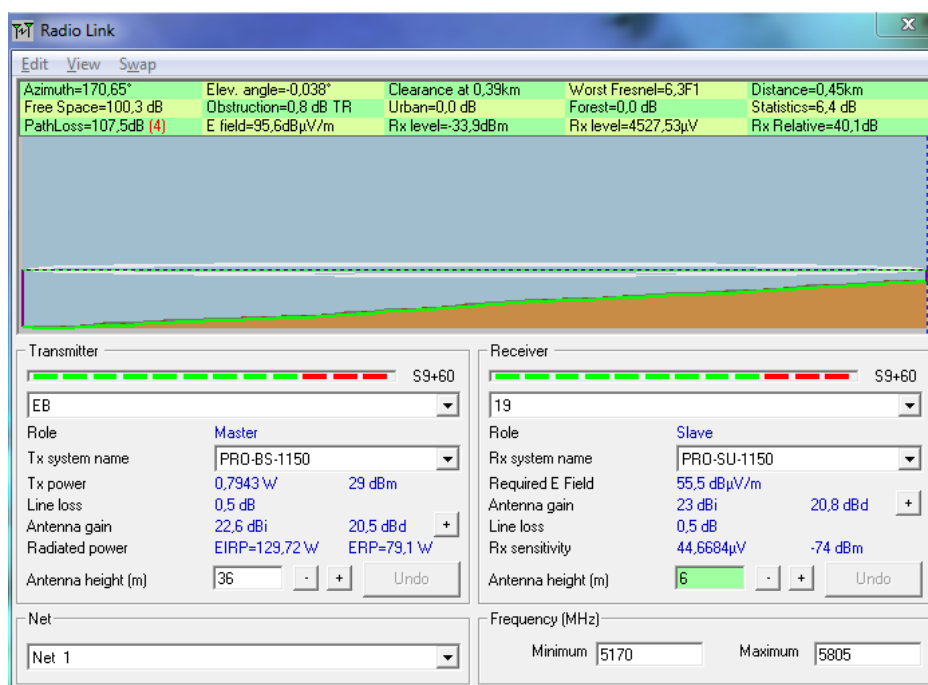


Figura C.19. Simulación del enlace Estación Base y la estación cliente Juan Miguel Suarez.

Simulación entre la Estación Base y la estación cliente Medardo Proaño Andrade - Unidad Artesanal de Caranqui - Bellavista de María.

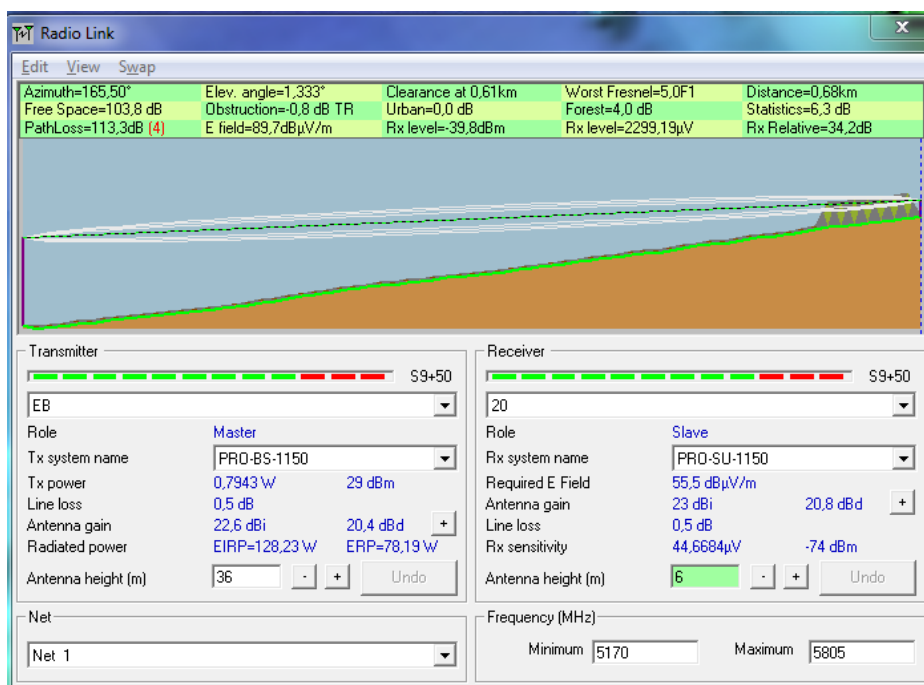


Figura C.20. Simulación del enlace Estación Base y la estación cliente Medardo Proaño Andrade - Unidad Artesanal de Caranqui - Bellavista de María.

Simulación entre la Estación Base y la estación cliente Santa Lucia del Retorno.

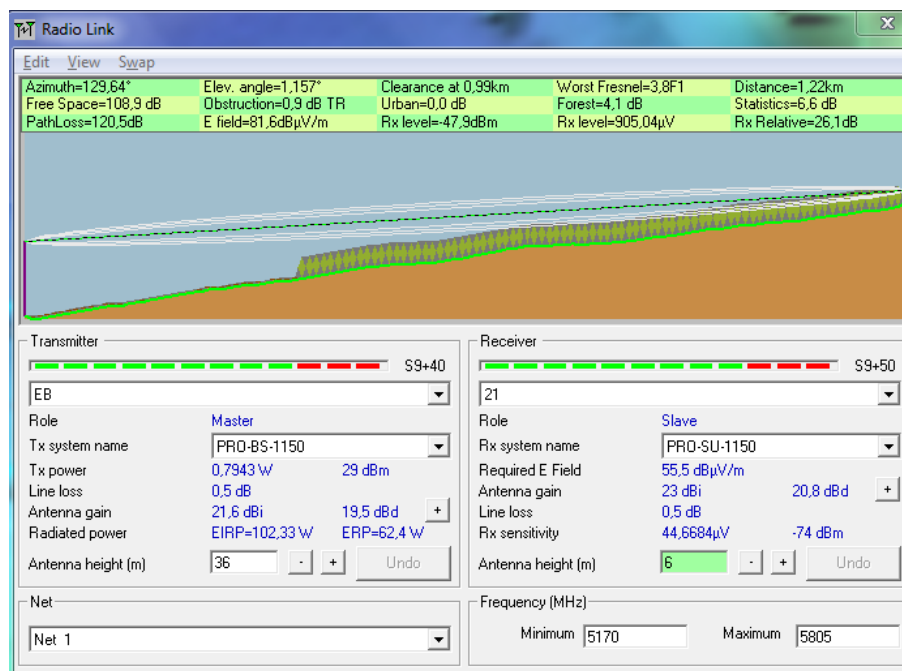


Figura C.21. Simulación del enlace Estación Base y la estación cliente Santa Lucia del Retorno.

ANEXO D

PÁGINAS WEB QUE DEBEN SER GARANTIZADAS EN CONECTIVIDAD MEDIANTE LA CONFIGURACIÓN COMO LISTAS BLANCAS.

La siguiente lista expone páginas que deben considerarse en listas blancas debido a su importancia para el usuario final, por lo tanto deben excluirse del control que trabaja el servidor PROXY. Esta lista debe ser actualizada según las necesidades de los usuarios y sus necesidades.

Páginas gubernamentales

Tabla D.1. Listas Blancas Gubernamentales

Alcaldía de Ibarra	<u>www.ibarra.gob.ec</u>
Presidencia	<u>www.presidencia.gob.ec</u>
Tramites ciudadanos	<u>www.tramitesciudadanos.gob.ec</u>
GPR Gobierno por resultados	<u>gpr.administracionpublica.gob.ec</u>
Gestión Documental	<u>www.gestiondocumental.gob.ec</u>
Compras Públicas	<u>www.compraspublicas.gob.ec</u>
Secretaria Nacional de Educación Superior	<u>www.educacionsuperior.gob.ec</u>
Registro civil	<u>www.registrocivil.gob.ec</u>
Correos del Ecuador	<u>www.correosdelecuador.gob.ec</u>
Concejo Nacional Electoral	<u>www.cne.gob.ec</u>
Ministerio de educación	<u>www.educacion.gob.ec</u>
Ministerio de salud	<u>www.salud.gob.ec</u>
Ministerio de industrias	<u>www.industrias.gob.ec</u>
Ministerio de turismo	<u>www.turismo.gob.ec</u>

Educación

Tabla D.2. Listas Blancas para Educación.

Bibliotechnia	www.bibliotechnia.com/bibliotechnia20/
BiblioMedex	www.bibliomedex.com/
BioONE	www.bioone.org/
Cabi	www.cabi.org/dfb
Cengage	infotrac.galegroup.com/default
Digitalia	www.digitaliapublishing.com/
EBL	www.ebib.com/
Ebrary	www.ebrary.com/corp/
e-LIBRO	www.e-libro.com/editoriales/
Wikipedia	es.wikipedia.org
Google	www.google.com
Universidad Técnica del norte	www.utn.edu.ec
Universidad Católica sede Ibarra	www.pucesi.edu.ec
Universidad UNIANDES	www.uniandesonline.edu.ec
Universidad de Loja	www.utpl.edu.ec
Teodoro Gómez de la torre	www.tgt.edu.ec
Sanchez	www.salesianosibarra.edu.ec
San Francisco	www.colegiosanfrancisco.edu.ec
Juan Miguel Suarez	www.escuelajuanmiguel-suarez.blogspot.com

Servicios Online Empresas

Tabla D.3. Listas Blancas para servicios Online

Banco del Pichincha	www.pichincha.com
Cooperativa Atuntaqui	www.atuntaqui.fin.ec
Banco de Guayaquil	www.bancoguayaquil.com
Produbanco	www.produbanco.com
Banco solidario	www.banco-solidario.com
Banco del estado	www.bancoestado.com
Banco de Fomento	www.bnf.fin.ec
Corporación Nacional de Telecomunicaciones	www.cnt.gob.ec
Empresa de agua potable y alcantarillado de Ibarra	www.emapaibarra.gob.ec
Empresa eléctrica del norte	www.emelnorte.com
Claro	www.claro.com.ec
Movistar	www.movistar.com.ec
Amazon	www.amazon.com
Ebay	www.ebay.com
Mercado libre	www.mercadolibre.com.ec
Olx	www.olx.com.ec

Redes Sociales, correo electrónico, informativos.

Tabla D.4. Listas Blancas para redes sociales.

Hotmail	www.hotmail.com
Gmail	www.gmail.com
Facebook	www.facebook.com
Twitter	www.twitter.com
Youtube	www.youtube.com
Instagram	www.instagram.com
Diario del Norte	www.elnorte.ec
El comercio	www.elcomercio.com.ec
El telégrafo	www.telegrafo.com.ec
La hora	www.lahora.com.ec

ANEXO E

COMPARACIÓN DE SOFTWARE PARA LOS SERVICIOS DEL DISEÑO.

Comparación de Software propuesto para el diseño de red.

Firewall Proxy

Tabla E.2. Comparación de Software para el Firewall.

Requerimientos	Clear OS	Endian Firewall	Squid	Shorewall
Firewall control de tráfico de paquetes	SI	SI	NO	SI
Firewall políticas restrictivas	SI	SI	NO	SI
Proxy transparente	SI	SI	SI	NO
Proxy Base de datos ya establecida de páginas perjudiciales	SI	SI	SI	NO
Proxy permite configurar listas blancas y negras personalizadas	SI	SI	SI	NO
Permite administración del cache de filtrado	SI	SI	SI	NO
Flexible para la administración.	NO	SI	SI	SI

Se selecciona el software Endian Firewall 2.5.2 debido a que cumple con todos los requisitos del sistema.

VoIP y video Streaming

Tabla E.2. Comparación de software para VoIP y video streaming.

Requerimientos	TRIXBOX	ELASTIX	ASTERISKNOW
Versión	2.2.8 (CE)	2.4.0	3.0.0
Soportar mínimo 22 extensiones tanto para VoIP como Videollamada con capacidad de crecimiento.	SI	SI	SI
Debe soportar el códec de voz: G.729	SI	SI	SI
Debe permitir la utilización del protocolo H.264	NO	SI	NO
Debe soportar el manejo de extensiones SIP y analógicas.	SI	SI	SI
Soportar administración remota Web	SI	SI	SI
Debe brindar reportes de cada llamada.	SI	SI	NO
Soportar flexibilidad al momento de crear modificar y eliminar una extensión en los dos servicios.	SI	SI	SI
Soportar aplicaciones de softphone para computadoras de escritorio portátiles y dispositivos inalámbricos.	SI	SI	SI
La herramienta debe tener licencia GPL de Software Libre.	SI	SI	SI
Marcas reconocidas por el mercado.	SI	SI	SI

Software Seleccionado elastix 2.4.0 debido a que cumple todos los requisitos del diseño.

Softphone

Tabla E.3. Comparación de software softphone

Requerimientos	Zoiper	X-line	Twinkle
Versión	3.2.2	4.5.5	1.4.2
Soporta códec H.264 para videstreaming.	si	si	si
Soporta códec de vos G.729 para voz.	si	si	si
Permite enviar y recibir video-llamadas.	si	si	si
Soporta videoconferencias.	si	si	no
Identificador de llamada entrante.	si	si	si
Puede trabajar con múltiples fabricantes del servidor de voz IP.	si	si	si
Que sistemas operativos soporta.	Linux	Windows	Linux
Marcas reconocidas por el mercado.	si	si	si

Se selecciona el software X-line para Windows y Zoiper para Linux.

Gestor de Red

Tabla E.4. Comparación de software para gestor de red.

Requerimiento	Nagíos	DUDE	PRTG
Visualización de todos los equipos de comunicación de la red mediante el monitoreo por protocolo SNMP.	si	si	si
Debe soportar las pruebas básicas de conectividad a todos los equipos como son ping, traceroute acceso web a los equipos	si	si	Si
Alarmas de conectividad para las notificaciones de los cortes de servicios y fallas en los equipos de comunicación.	Si	si	Si
Monitoreo de velocidad de transmisión a cada interface de red de cada equipo implementado en la conectividad de la red.	no	si	Si
La herramienta debe tener licencia GPL de Software Libre.	Si	si	No pero existe una versión gratuita con un limitante de

			sensores para su utilización
Debe proporcionar reportes de conectividad de tráfico de red con todos los equipos de comunicación instalados.	Si	si	si

EL proyecto propone la utilización del software PRTG debido a los reportes corporativos que brinda el software ya que son requisitos de la entidad reguladora para su control mensual. Cabe mencionar que es un software propietario pero se puede utilizar versiones gratuitas con limitación de sensores de trabajo.

Virtualización

Tabla E.5. Comparación de software para virtualización.

Requerimientos	Citrix XenServer	Virtual Box	VMWARE
Versión	6.2	4.2.22	6.0.1
Flexible a la gestión de recursos de hardware como son memorias, cpu, disco duro.	si	si	Si
Soporta difentes sistemas operativos tanto en software libre como propietario sistemas en sus máquinas virtuales.	si	si	Si
Administración Web	si	si	Si
Permite conectar periféricos directamente a las máquinas virtuales	si	si	si
Soporta licenciamiento GLP	si	si	Existen versiones libres para fabricantes de hardware específicos

Se propone la utilización de VMWARE debido a su implementación a nivel empresarial pero se recomienda realizar la compra de un hardware que incluya la utilización libre de esta herramienta.

ANEXO F

COMPARACIÓN DE HARDWARE PARA LOS SERVIDORES Y CONECTIVIDAD INALÁMBRICA.

Punto de acceso para los diferentes centros de informática.

Tabla F.1. Comparación de hardware para Puntos de acceso en los centros de informática.

Requerimientos	Cisco	Ubiquiti	Trednet
Modelo	WAP4410N	Unifi AP (UAP)	TEW-692GR
Soporta protocolo 802.11 b/g/n	si	si	Si
Trabaja en modo Router o Puente	Si	si	no
Rango de Cobertura minimo de 50 metros	si	si	Si
Soporta PoE	si	si	No
Throughput de 300 Mbps o mas	si	si	si
Marcas reconocidas por el mercado	si	si	si
Soporta protocolo SNMP	si	si	si
Costo	220 \$	79 \$	71 \$

Se trabajara con el AP Ubiquiti Unifi AP (UAP) debido a que cumple con todos los requisitos que exige el diseño y además es económico con respecto a cisco otro fabricante que también cumple con los mismos requisitos.

Teléfono IP para cada centro de informática.

Tabla F.2. Comparación de hardware para Teléfonos IP.

Requerimientos	Fanvil	Cisco	Grandstream
Modelo	Fanvil C56	Smb Spa303-g1	Gxp280
Soporta SIP 2.0	si	si	si
Soporta códec G.729	si	si	si
Soporta 2 interfaces Ethernet para funcionar como puente	si	si	si
Soporta PoE	si	si	si
Trabaja con servidores de VoIP multimarca	si	si	Si
Marcas reconocidas por el mercado	si	si	si
Costo	89 \$	159 \$	99 \$

Se selecciona el teléfono IP Grandstream Gxp280 por su precio y además porque se puede encontrar en el país para su compra a pesar que todos las demás marcas cumplen con lo requerido en el diseño.

Switch de acceso para los diferentes centros de informática.

Tabla F.3. Comparación de hardware para Switch de acceso.

Requerimientos	Cisco	Mikrotik	ubiquiti
Modelo	Sf 100d-08	RB2011iL-RM	EdgeRouter PRO ER-8
Modo de trabajo: cortar y enviar (Cut-Through)	si	si	si
Contiene 8 puertos Ethernet de 100/1000 Mbps	si	si	si
Soporta PoE	si	si	si
Soporta protocolo SNMP	si	si	Si
Soporta configuración del portal cautivo	no	si	no
Costo	69 \$	99 \$	178 \$

Se utilizara el switch Mikrotik RB2011iL-RM debido a que soporta el portal cautivo necesario para su servicio en cada centro de informática.

Radio y antena para centros de informática de recepción.

Tabla F.4. Comparación de hardware para radio y antena de estación cliente.

Requisito	Alvarion (BreezeACCESS VL Subscriber Unit)	Albentia (ARBA Pro)	Netkrom ISPAIR CPE 510
Soporta IEEE 802.16d	SI	SI	SI
Bandas 5.725 – 5,850 GHz	SI	SI	SI
Potencia >= 1 W (30 dBm)	SI	SI	SI
Ancho de banda del canal 20 MHz	SI	SI	SI
Duplexación TDD , FDD	SI	SI	SI
Modulación OFDM (BPSK, QPSK, 16 QAM, 64 QAM)	SI	SI	SI
Velocidad de Transferencia de 5 Mbps simétrico	SI	SI	SI
Antena Sectorial directiva incluida o conector N para una antena exterior	SI	SI	SI
Puede trabajar con otras marcas de antenas en Estación Base.	NO	SI	SI
Precio	601.48 \$	896.99 \$	349 \$

Se selecciona el equipo Netkrom ISPAIR CPE 510 debido a su bajo precio a pesar que el equipo de marca Albentia también cumple con los requisitos pero el precio es muy alto solo para una estación cliente.

Radio y antena para Puntos de acceso en la estación base.

Tabla F.5. Comparación de hardware para radio y antena en la estación base.

Requisito	Alvarion (BreezeACCESS VL)	Albentia (ARBA Pro)	Airspan (MicroMaxd Base Station)
Soporta IEEE 802.16d	SI	SI	SI
Bandas 5.725 – 5,850 GHz	SI	SI	SI
Potencia >= 1 W (30 dBm)	SI	SI	SI
Ancho de banda del canal 20 MHz	SI	SI	NO
Duplexación TDD , FDD	SI	SI	SI
Modulación OFDM (BPSK, QPSK, 16 QAM, 64 QAM)	SI	SI	SI
Velocidad de Transferencia de 17 Mbps	SI	SI	SI
Antena Sectorial de 120° o conector N para antena externa	SI	SI	NO
Permite escalabilidad al añadir nuevos usuarios	SI	SI	SI
Permite escalabilidad para diferentes marcas	NO	SI	NO
Precio	2.930 \$	4.166 \$	3.500 \$

Se selecciona el dispositivo Albentia ARBA PRO debido a que cumple con todos los requisitos del diseño.

Switch de distribución en la estación base.

Tabla F.6. Comparación de hardware para Switch de distribución.

Requerimientos	Ubiquiti	Mikrotik	Cisco
Modelo	EdgeRouter PRO ER-8	RB2011iL- RM	Sf 100d-08
Conexión mínima de 8 puertos Ethernet	si	si	si
Modo de trabajo: cortar y enviar (Cut-Through)	si	si	Si
Velocidad mínima en cada puerto de 10/100/1000 Mbps	si	si	Si
Soporta administración mediante una IP fija	si	si	Si
Marcas reconocidas en el mercado	si	si	Si
Soporta protocolo SNMP	si	si	Si
Soporta PoE	si	si	Si

Soporta Administración Web	si	si	si
Costo	178 \$	99 \$	69 \$

Como se demuestra en la anterior tabla todos los modelos cumplen con los requerimientos pero se selecciona la marca Ubiquiti EdgeRouter PRO ER-8 debido a que esta marca presenta informes de performance con respecto a las demás marcas mencionadas y sus resultados son superiores de acuerdo a la empresa de pruebas Tolly.

Radio y antena para Estación Base enlace punto a punto.

Tabla F.7. Comparación de hardware para radio en el enlace punto a punto.

Requisitos	Alvarion (BreezeACCESS VL)	Albentia (ARBA Pro)	Airspan (MicroMaxd Base Station)
Soporta IEEE 802.16d	SI	SI	SI
Bandas 5.725 – 5,850 GHz	SI	SI	SI
Potencia >= 1 W (30 dBm)	SI	SI	SI
Ancho de banda del canal 20 MHz y 10 MHz	SI	SI	NO
Duplexación TDD , FDD	SI	SI	SI
Modulación OFDM (BPSK, QPSK, 16 QAM, 64 QAM)	SI	SI	SI
Velocidad de Transferencia de 17 Mbps	SI	SI	SI
Incluye una antena directiva o proporciona un conector N para una antena externa	NO	SI	NO
Precio	2.930	4.166	3.500

Se selecciona la marca Albentia (Arba Pro) para el enlace punto a punto debido a que cumple con los requerimientos que propone el diseño a implementarse.

Antena

Tabla F.8. Comparación de hardware para antena en el enlace punto a punto.

Requisitos	Netkrom Wideband Parabolic Grid Antena	Ubiquiti Rocket Dish Airmax
Trabaja en las bandas 5.725 – 5.850 GHz	SI	SI
Soporta polarización vertical y horizontal	SI	SI
Puede trabajar en distancias mínimas de 0.39 Km	NO	SI
Precio	102	149,99

Se selecciona la antena Ubiquiti Rocket Dish Airmax ya que cumple los requerimientos impuestos por el diseño propuesto.

Switch de distribución en red administrador

Tabla F.9. Comparación de hardware para Switch de distribución de la red administrador.

Requerimientos	Ubiquiti	Mikrotik	Cisco
Modelo	EdgeRouter PRO ER-8	RB2011iL- RM	Sf 100d-08
Conexión mínima de 8 puertos Ethernet	Si	si	si
Modo de trabajo: cortar y enviar (Cut-Through)	Si	si	Si
Velocidad mínima en cada puerto de 10/100/1000 Mbps	Si	si	Si
Soporta administración mediante una IP fija	Si	si	Si
Marcas reconocidas en el mercado	Si	si	Si
Soporta protocolo SNMP	Si	si	Si
Soporta Administración Web	Si	si	si
Costo	178 \$	99 \$	69 \$

Como se demuestra en la anterior tabla todos los modelos cumplen con los requerimientos pero se selecciona la marca Ubiquiti EdgeRouter PRO ER-8 debido a que esta marca presenta informes de performance con respecto a las demás marcas mencionadas y sus resultados son superiores de acuerdo a la empresa de pruebas Tolly.

Servidor destinado para máquinas virtuales.

Requerimientos del software a ser virtualizado:

PRTG

- Procesador: mínimo 2 núcleos con una frecuencia mínima de trabajo de 3.16 Ghz.
- Memoria RAM: 1 GB.
- Disco Duro: 10 GB.
- Tarjeta de red: Velocidad de 1000 Mbps.

Elastix

- Procesador: mínimo 2 núcleos con una frecuencia mínima de trabajo de 3.16 Ghz.
- Memoria RAM: 512 MB.
- Disco Duro: 40 GB.
- Tarjeta de red: Velocidad de 1000 Mbps.

Tabla F.10. Comparación de hardware para servidor destinado a máquinas virtuales.

Requerimientos	HP	IBM	Dell
Modelo	Servidor ML10 HP ProLiant	IBM X3250M4	PowerEdge R320
Procesador de mínimo 2 núcleos con frecuencia de trabajo de 3.16 GHz	si	si	si
Memoria RAM de 2 Gb	si	si	Si
Disco duro mínimo de 50 GB con capacidad de crecimiento.	si	si	Si
2 tarjetas de red de 1000 Mbps con capacidad de crecimiento	si	si	si
Soluciones RAID para discos duros	si	si	si
Soporta Virtualización mediante software con requerimientos del sistema y licencia sin costo para la firma	no	si	no
Flexibilidad para el aumento y reemplazo de recursos en hardware.	si	si	si
Marcas reconocidas en el mercado	si	si	Si
Costo	664.55 \$	2321 \$	2479 \$

Este servidor está destinado para alojar el servidor de VoIP y el administrador de la red, por lo tanto se toma en cuenta los requerimientos de cada servicio en hardware y además se recomienda tener un crecimiento considerable para diversas aplicaciones que pueden demandar en un futuro próximo.

Se selecciona el servidor IBM X3250M4

Servidor Firewall Proxy

Requerimientos del software Endian Firewall seleccionado

- Procesador: mínimo 2 núcleos con una frecuencia mínima de trabajo de 3.16 Ghz.
- Memoria RAM: 512 MB.
- Disco Duro: 40 GB.
- Tarjeta de red: Velocidad de 1000 Mbps con puertos para añadir mínimo 4 tarjetas.

Tabla F.11. Comparación de hardware para servidor firewall proxy.

Requerimientos	HP	IBM	Dell
Modelo	Servidor ML10 HP ProLiant	IBM X3250M4	PowerEdge R320
Procesador de mínimo 2 núcleos con frecuencia de trabajo de 3.16 GHz	si	si	si
Memoria RAM de 512 GB	si	si	Si
Disco duro mínimo de 40 GB con capacidad de crecimiento.	si	si	Si
4 tarjetas de red de 1000 Mbps con capacidad de crecimiento	si	si	si
Flexibilidad para el aumento y reemplazo de recursos en hardware.	si	si	si
Marcas reconocidas en el mercado	si	si	Si
Costo	664.55 \$	2321 \$	2479 \$

Para este servicio se selecciona el modelo Servidor ML10 HP ProLiant debido a su precio ya que todos los servidores analizados cumplen con los requisitos del diseño.

Rack de Piso

Tabla F.12. Comparación de hardware para Rack de piso.

Requerimientos	Beaucoup	NCS Jaguar
Soporta 28 U para posicionamiento de equipos	si	si
Conexión integrada con una sola tierra	si	si
Rieles para posicionamiento de gabinete configurable	Si	No
Contorno cerrado con puertas con rejillas	Si	No
Marcas reconocidas en el mercado	Si	si
Costo	1200 \$	109.50 \$

Se selecciona el rack de piso Bleacon ya que cumple con los requisitos del diseño

Rack de Pared.

Tabla F.13. Comparación de hardware para Rack de pared.

Requerimientos	Beaucoup
Dimensiones 380 x 540 x 500	Si
Soporta 7 U para posicionamiento de equipos	Si
Conexión integrada con una sola tierra	Si
Soporta ventilador	Si
Contorno con puertas de rejilla y desmontables	si
Marcas reconocidas en el mercado	Si
Costo	173 \$

La marca Beaucoup es una firma que trabaja en Ecuador y es la única que se puede encontrar localmente lo que se elige por su mercado y si cumple los requerimientos del diseño.

UPS Grande

Tabla F.14. Comparación de hardware para UPS grande.

Requerimientos	CDP	APC
Modelo	B-smart 1508	APC Smart- UPS 750VA USB
Alarma acústica	Si	Si
Tiempo de recarga de baterías mínima de 3 horas	No	Si
Dimensionamiento físico para instalar en un Rack de piso estándar.	Si	Si
Voltaje de entrada de 110 V regulable	Si	Si
Frecuencia de entrada 60 Hz regulable	Si	Si
Frecuencia de salida 60 Hz regulable	No	Si
Voltaje de salida nominal 110 y 220 regulable	Si	Si
Administración web	no	si
Marcas reconocidas en el mercado	Si	Si
Costo	259 \$	623 \$

Se selecciona el UPS APC-Smart-UPS-750VA ya que cumple los requisitos del diseño.

UPS Pequeño

Tabla F.15. Comparación de hardware para UPS pequeño.

Requerimientos	CDP	FORZA
Modelo	G-UPR- 506	NT-501
Alarma acústica	Si	Si
Tiempo de recarga de baterías mínima de 10 minutos	si	Si
Dimensionamiento físico para instalar en un Rack de pared estandar.	Si	Si
Numero de tomas mínimo 4		Si
Voltaje de entrada de 110 V regulable	Si	Si
Frecuencia de entrada 60 Hz regulable	Si	Si
Frecuencia de salida 60 Hz regulable	Si	Si
Voltaje de salida nominal 110 y 220 regulable	Si	Si
Marcas reconocidas en el mercado	Si	Si
Costo	50 \$	55 \$

Se selecciona CDP debido al precio ya que los dos cumplen con los requisitos del diseño.

ANEXO G

COMPARACIÓN DE EQUIPOS PROPUESTOS Y EQUIPOS A UTILIZARSE EN EL PROTOTIPO.

Tabla G.1. Comparación de hardware y equipos que van hacer utilizados.

#	Equipos requeridos en el diseño	Equipos Utilizados en el prototipo
2	Punto de acceso Ubiquiti Unifi AP (UAP)	Punto de acceso Ubiquiti Unifi AP (UAP)
2	Switch Mikrotik RB2011iL-RM	Switch Mikrotik RouterBoard 750G
1	Radio y antena Netkrom ISPAIR CPE 510	Radio y antena Ubiquiti Air GridM5 AG-HP-5G-27
2	Teléfonos IP Grandstream Gxp280	Softpone X-line- SmartPhone Samsung Galaxy GT-S5830M
1	Radio y antena Albentia (ARBA Pro)	Radio y antena Ubiquiti Air GridM5 AG-HP-5G-27
1	Switch Ubiquiti EdgeRouter PRO ER-8	Switch trendnet TE100-S8/A
1	Servidor IBM X3250M4	CPU Clon Hurricane (Intel Core 2 Duo – Memoria RAM 2 GB – Disco Duro 500 GB)
1	Servidor ML10HP Proliant	CPU Clon Delux (Intel Pentium 4 – Memoria RAM de 1 GB – Disco duro 80 GB)
1	Varios (Cables y conectores)	Cables y Conectores

El prototipo de red en la conectividad inalámbrica implementada utiliza equipos con características similares a las propuestas para el diseño de red en punto de acceso y la estación cliente, su comparación de características se muestra en la tabla G.2.

Tabla G.2. Comparación de radio y antena como estación base y estación cliente para utilización en la red prototipo.

Requisito	Equipo que propone el diseño Albentia (ARBA PRO-BS-1150)	Equipo utilizado en el prototipo Ubiquiti AG-HP-5G27
Tecnología	WIMAX IEEE 802.16d	Airmax / IEEE 802.11n
Frecuencias	5.725 – 5.850 GHz	5.725 – 5.850 GHz
Tipo de trabajo del radio	Punto de Acceso	Punto de Acceso / Estación
Tipo de antena	Sectorial	Directiva
Tecnología de antenas	MIMO	MIMO
Trabajo del canal asignado	OFDM	OFDM
Modulación de subportadora	(ACM) BPSK, QPSK, 16 QAM, 64 QAM	(MCS) BPSK, QPSK, 16 QAM, 64 QAM
Protocolo de acceso al medio	TDMA	CSMA/CA (Airmax - TDMA)
Duplexación	TDD	No
QoS	Si	Si
Ancho de banda del canal	20 MHz	20 MHz
Potencia de Transmisión	26 dBm	25 dBm
Antena incluida	Sectorial 120º (23 dBi)	Directiva (27 dBi)
Modos de networking	Bridging / Router	Bridging / Router
Funcionalidades capa 3	Ruteo Estático Dinámico – NAT- DHCP	Ruteo Estático Dinámico–NAT- DHCP
Alimentación Eléctrica	PoE	PoE
Precio estimado Ecuador	4.166	86,24

ANEXO H

ADMINISTRACION DE SERVIDOR FIREWALL ENDIAN

Instalacion:

Una vez que inicialice el instalador se presentara la pantalla de la figura H.1 donde indica el inicio del programa.

```
ISOLINUX 3.31 2006-09-25 Copyright (C) 1994-2005 H. Peter Anvin

Welcome to Endian Firewall, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

-----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
-----

Press RETURN to boot Endian Firewall default installation.

Or, if you are having trouble you can try these options...
Type:  nopcmcia to disable PCMCIA detection
       nousb to disable USB detection
       nousborpcmcia to disable both PCMCIA & USB detection
       dma to enable ide dma (SiS chipset workaround)

boot: _
```

Figura H.2. Inicialización del instalador Firewall Endian.

En la siguiente pantalla se selecciona el idioma como se muestra en la figura H.2



Figura H.2. Selección del idioma de trabajo.

El instalador nos indica la información del disco duro y la partición que se realizara con la instalación.

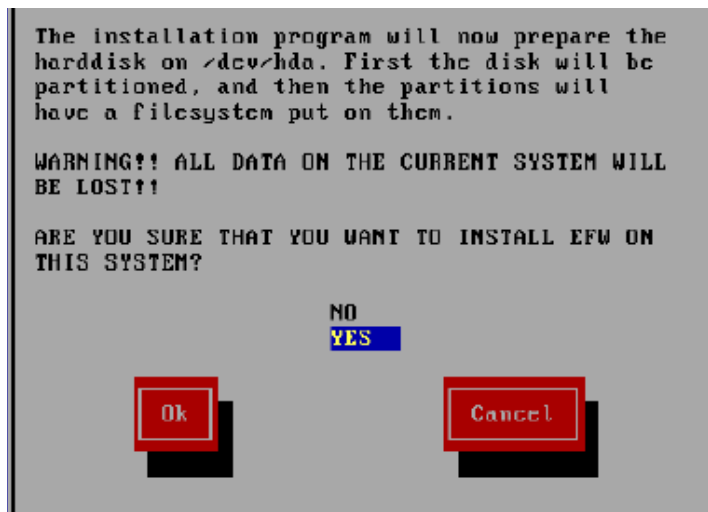


Figura H.3. Configuración del disco duro.

Permite seleccionar la utilización de un puerto serial para consola

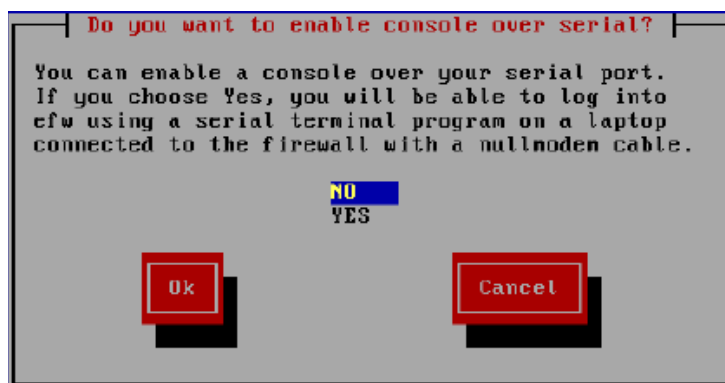


Figura H.4. Seleccionar el puerto de consola.

Después de la instalación de los paquetes necesarios nos permite configurar la IP para su administración web, cabe mencionar que el puerto por defecto que se instala es el 10443 y la IP que trabajaremos es la 192.168.1.1/24.



Figura H.5. Configurar IP de administración web.

Una vez culminada la instalación debe aparecer la siguiente página de la figura H.6 y después debe reiniciarse toda la máquina para empezar a utilizar el servicio.

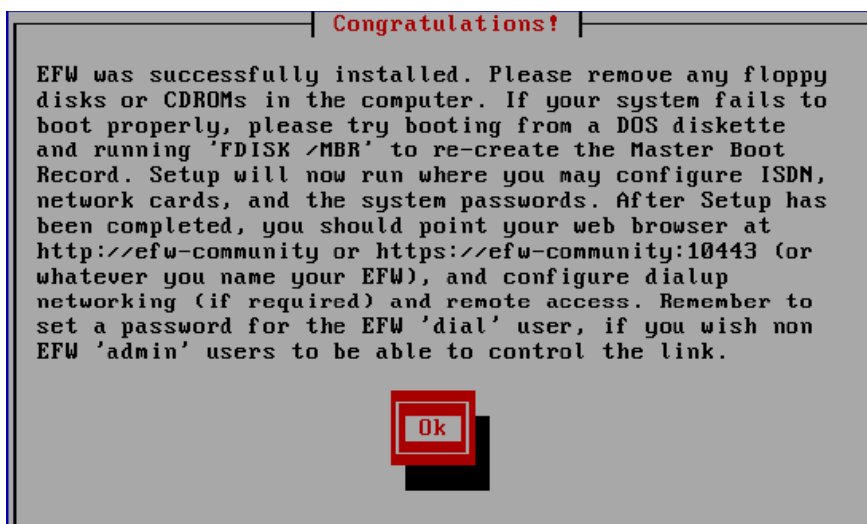


Figura H.6. Pantalla final de la instalación del firewall Endian.

Acceso al sistema y cambio de clave de seguridad

Una vez instalado ingresamos al sistema mediante un navegador por medio de un computador conectado a una tarjeta de red del servidor.

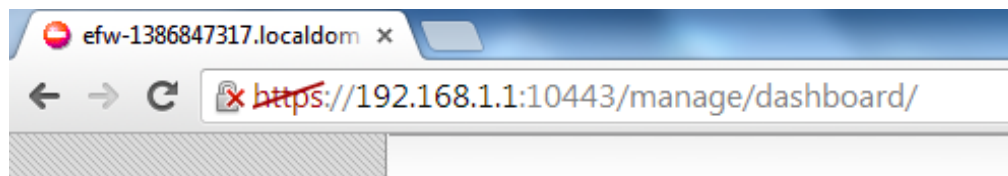


Figura H.7. Ingreso al sistema con la IP designada y el puerto por defecto.

Después de ingresar por primera vez la interface pide configuraciones que se omitirán ya que se pueden realizar después, lo importante es configurar las claves de acceso para ingresar al sistema.

Contraseñas

99 Cambiar contraseñas

Contraseña (admin) de la interfaz web	Contraseña de marcado	Contraseña SSH (raíz)
Contraseña *	Contraseña *	Contraseña *
<input type="password"/>	<input type="password"/>	<input type="password"/>
Confirmar contraseña *	Confirmar contraseña *	Confirmar contraseña *
<input type="password"/>	<input type="password"/>	<input type="password"/>
<input type="button" value="Cambiar contraseña"/>	<input type="button" value="Cambiar contraseña"/>	<input type="button" value="Cambiar contraseña"/>

Figura H.8. Cambio de clave para el ingreso al sistema.

Una vez cambiada la contraseña podemos ingresar al sistema para configurar lo solicitado por el diseño.

Configuración de las tarjetas de red impuestas por el diseño.

Ingresamos a la pestaña Sistema/Configuración de red.



Figura H.9. Configuración de tarjetas de red en firewall Endian.

Según la figura H.9 el sistema identifica a cada tarjeta con un color por lo tanto se añade la IP o Gateway de la red a cada tarjeta y con la máscara el sistema identifica el segmento de red que se necesita trabajar.



Figura H.10. Configuración de tarjetas de red en firewall Endian para la red Servidores y Barrio Central.

Siguiendo la configuración nos pide ingresar los datos de la salida al internet que se utilizara, siempre le asigna una interface de color rojo para este servicio. En nuestro caso la ip designada para la salida al internet es 192.168.10.2/24 con Gateway 192.168.10.1 como se muestra en la figura

The screenshot shows the 'Configuración de red' (Network Configuration) page in the Endian Firewall Community web interface. The page is titled 'Paso 4/8: Preferencias de acceso a Internet' (Step 4/8: Internet access preferences). The configuration is for a connection named 'ROJO (Conexión a Internet (WAN), no fiable)'. The IP address is set to 192.168.10.2 and the subnet mask is /24 - 255.255.255.0. The gateway is set to 192.168.10.1. The interface list shows four interfaces: eth3 (Realtek_2), eth2 (VIA_2), eth0 (VIA_2), and eth1 (VIA_2). The eth1 interface is highlighted with a red circle, indicating it is the selected interface for this configuration.

Puerto	Link	Descripción	MAC	Dispositivo
4	✗	Realtek_2	64:66:b3:03:72:db	eth3
3	✗	VIA_2	00:06:4f:53:74:a2	eth2
1	✓	VIA_2	1c:bd:b9:85:65:cc	eth0
2	✓	VIA_2	00:14:2a:b5:08:9d	eth1

Figura H.11. Configuración de tarjetas de red en firewall Endian para la red Servidores y Barrio Central.

Configuración de reglas de tráfico de salida y tráfico entre subredes.

Ingresamos a la pestaña Firewall / Trafico de salida / Añadir nueva regla al Firewall.

Configuración del firewall de salida

Reglas actuales

[Añadir una nueva regla al firewall](#)

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	192.168.0.0/18	ROJO	ICMP/8 ICMP/30	→	Trafico Autorizado	⬇️ ✓ ✎ 🗑️
2	192.168.0.0/18	ROJO	TCP+UDP/443 TCP+UDP/80 TCP+UDP/25 TCP+UDP/110 TCP+UDP/143 TCP+UDP/993 TCP+UDP/995 TCP+UDP/53	→	Trafico Autorizado	⬆️ ⬇️ ✓ ✎ 🗑️
3	192.168.0.0/18	ROJO	<CUALQUIERA>	→	Negar todo el trafico de diferentes puertos	⬆️ ✓ ✎ 🗑️

Legenda Activado (clic para desactivar) Desactivado (clic para activar) ✎ Editar 🗑️ Eliminar

Mostrar reglas del sistema >>

Figura H.12. Configuración de reglas en el firewall.

Agregamos las reglas de salida de tráfico ya establecidas por el diseño:

Configuración del firewall de salida

Reglas actuales

Editor de reglas de salida del firewall

Origen Tipo: **RedIP** Destino: **<ROJO>**

Escriba las redes de destino (una por línea):
192.168.0.0/18

Esta regla se aplicará a toda la red ROJA

Servicio/Puerto
Servicio: Definido por el usuario Protocolo: **TCP + UDP** Puerto de destino (uno por línea): 443, 80, 25

Acción: **PERMITIR con IP** Observación: Trafico Autorizado Posición: Después de la regla #1

Registrar todos los paquetes aceptados

Figura H.12. Configuración de parámetros para las reglas en el firewall.

Las reglas en el tráfico de salida quedan como se muestra en la figura H.13

The screenshot shows the 'endian firewall community' web interface. The 'Firewall' tab is selected in the top navigation bar. The main content area is titled 'Configuración del firewall de salida' and displays a table of 'Reglas actuales' (Current Rules). The table has columns for '#', 'Origen', 'Destino', 'Servicio', 'Política', 'Observación', and 'Acciones'. Three rules are listed:

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	192.168.0.0/18	ROJO	ICMP/8 ICMP/30	Permitido	Trafico Autorizado	[Icons: Up, Down, Check, Edit, Delete]
2	192.168.0.0/18	ROJO	TCP+UDP/443 TCP+UDP/80 TCP+UDP/25 TCP+UDP/110 TCP+UDP/143 TCP+UDP/993 TCP+UDP/995 TCP+UDP/53	Permitido	Trafico Autorizado	[Icons: Up, Down, Check, Edit, Delete]
3	192.168.0.0/18	ROJO	<CUALQUIERA>	Denegado	Negar todo el trafico de diferentes puertos	[Icons: Up, Check, Edit, Delete]

Below the table, there is a legend: **Leyenda** Activado (clic para desactivar) Desactivado (clic para activar) Editar Eliminar. At the bottom, there is a button 'Mostrar reglas del sistema >>'.

Figura H.13. Configuración de parámetros para las reglas del tráfico de salida en el firewall.

Configuración de tráfico de entrada al sistema

Ingresamos a la pestaña Firewall / Acceso al sistema / Añadir una nueva regla de acceso al sistema.

The screenshot shows the 'endian firewall community' web interface. The 'Firewall' tab is selected in the top navigation bar. The main content area is titled 'Configuración de acceso al sistema'. The left sidebar has 'Acceso al sistema' selected. The main content area displays a table of 'Reglas actuales' (Current Rules). The table has columns for '#', 'Dirección de origen', 'Destino de origen', 'Servicio', 'Política', 'Observación', and 'Acciones'. Two rules are listed:

#	Dirección de origen	Destino de origen	Servicio	Política	Observación	Acciones
1		ROJO	TCP/10443 TCP/161	Permitido	Administración del UTM	[Icons: Up, Down, Check, Edit, Delete]
2		ROJO	ICMP/8 ICMP/30	Permitido	Administración Remota	[Icons: Up, Down, Check, Edit, Delete]

Below the table, there is a legend: **Leyenda** Activado (clic para desactivar) Desactivado (clic para activar) Editar Eliminar. At the bottom, there is a button 'Mostrar las reglas de los servicios del sistema >>'.

Figura H.14. Configuración de parámetros para las reglas del tráfico de entrada al sistema en el firewall.

Configuramos las reglas para el acceso al sistema con el puerto 1443 y permitir el tráfico SNMP con el puerto 161 como ejemplo de las reglas que impone el diseño de red.

The screenshot shows the 'Configuración de acceso al sistema' window in WinBox. The 'Editar regla de acceso al sistema' form is active. The 'Interfaz de origen' dropdown is set to 'ROJO'. The 'Puerto de destino' field contains '10443' and '161'. The 'Acción' dropdown is set to 'PERMITIR con IP'. The 'Observación' field contains 'Administración del UTM'. The 'Posición' dropdown is set to 'Primero'. There are buttons for 'Actualizar regla' and 'Cancelar' at the bottom.

Figura H.14. Configuración de parámetros para las reglas del tráfico de entrada al sistema en el firewall.

Las reglas se muestran como en la figura H.15

The screenshot shows the 'Configuración de acceso al sistema' window in WinBox, displaying a list of rules. The table below shows the details of the rules.

#	Dirección de origen	Interfaz de origen	Servicio	Política	Observación	Acciones
1		ROJO	TCP:10443 TCP:161	✓	Administración del UTM	⬇️ ✓ ✎ 🗑️
2		ROJO	ICMP:8 ICMP:30	✓	Administración Remota	⬆️ ✓ ✎ 🗑️

Figura H.15. Reglas de tráfico de entrada al sistema.

Configuración de tráfico desde la red de servidores hacia las demás subredes.

Ingresamos a la pestaña Firewall/ Trafico entre zonas / añadir una nueva regla de firewall inter-zona

endian firewall community

Sistema Estado Red Servicio **Firewall** Proxy VPN Registros

Configuración del firewall Inter-Zona

Reglas actuales

➕ Añadir una nueva regla de firewall Inter-Zona

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	192.168.2.0/24	192.168.0.0/18	TCP/161 TCP/5060	→	SNMP - SIP	⬇️ ⬆️ ⬇️
2	192.168.2.0/24	192.168.0.0/18	ICMP/8 ICMP/30	→	ping	⬆️ ⬆️ ⬆️

Leyenda: Activado (clic para desactivar) Desactivado (clic para activar) Editar Eliminar

Mostrar las reglas de los servicios del sistema >>

Configuración del firewall Inter-Zona

Habilitar firewall Inter-Zona >>

Registro aceptó las conexiones de Inter-Zona

Guardar

Figura H.16. Configuración de reglas para tráfico entre subredes.

Configuramos según los requisitos del diseño.

endian firewall community

Sistema Estado Red Servicios **Firewall** Proxy VPN Registros

Configuración del firewall Inter-Zona

Reglas actuales

Editar la regla de zona del firewall

Origen Tipo * RedIP Destino Tipo * RedIP

Escriba las redes/IP (una por línea): 192.168.2.0/24 Escriba las redes/IP (una por línea): 192.168.0.0/18

Servicio/Puerto Servicio * Definido por el usuario Protocolo * ICMP Puerto de destino (uno por línea) 8 30

Política Acción * PERMITIR con IP Observación ping Posición * Después de la regla #1

Activado Registrar todos los paquetes aceptados

Figura H.17. Configuración de parámetros de reglas.

Las reglas ya configuradas se muestran como en la figura H.18

The screenshot shows the 'endian firewall community' web interface. The main menu includes 'Sistema', 'Estado', 'Red', 'Servicios', 'Firewall', 'Proxy', 'VPN', and 'Registros'. The 'Firewall' section is active, displaying 'Configuración del firewall Inter-Zona'. On the left, there is a sidebar with options like 'Redirección de puertos / NAT', 'Tráfico de salida', 'Tráfico entre zonas', 'Tráfico VPN', 'Acceso al sistema', and 'Diagramas de firewall'. The main content area shows a table of 'Reglas actuales' (current rules) with columns for '#', 'Origen', 'Destino', 'Servicio', 'Política', 'Observación', and 'Acciones'. Two rules are listed: Rule 1 for TCP/161 and TCP/5060 with observation 'SNMP - SIP', and Rule 2 for ICMP/8 and ICMP/30 with observation 'ping'. A legend at the bottom indicates that a checked box means 'Activado' and an unchecked box means 'Desactivado'. There are also icons for 'Editar' and 'Eliminar'.

#	Origen	Destino	Servicio	Política	Observación	Acciones
1	192.168.2.0/24	192.168.0.0/18	TCP/161 TCP/5060	→	SNMP - SIP	↓ ✓ ✎ 🗑️
2	192.168.2.0/24	192.168.0.0/18	ICMP/8 ICMP/30	→	ping	↑ ✓ ✎ 🗑️

Figura H.18. Reglas ya configuradas de tráfico entre subredes.

Configuración del escenario para la administración del FIREWALL.

Paso 1: Ingresar a la administración web en un navegador

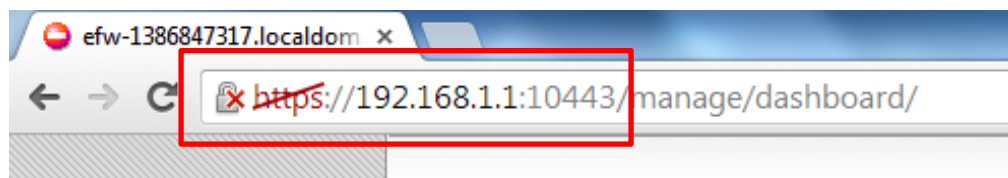


Figura H.19. Ingresamos al sistema.

Paso 2: Ingresar a la pestaña Firewall/Redirección de puertos/NAT/Agregar nueva regla.

endian firewall community

Sistema Estado Red Servicios **Firewall** Proxy VPN Registros

Redirección de puertos / NAT de destino

Redirección de puertos / NAT

Tráfico de salida

Tráfico entre zonas

Tráfico VPN

Acceso al sistema

Diagramas de firewall

>> Redirección de puertos / NAT de destino NAT fuente Tráfico enrutado de entrada

>> Reglas actuales

Agregar nueva regla de reenvío de puerto / NAT de destino

#	Dirección IP de llegada	Servicio	Política	Traducir a	Observación	Acciones
1	192.168.10.2 (Enlace main)	TCP/5000		192.168.2.2 : 5000	monitoreo de equipos	
PERMITIR con IP desde:				<CUALQUIERA>		

Leyenda: Activado (clic para desactivar) Desactivado (clic para activar) Editar Eliminar

Mostrar reglas del sistema >>

Status: Conectado: main (0d 5h 18m 50s) Uptime: 14:32:14 up 5:19, 0 users, load average: 0.08, 0.02, 0.01

Endian Firewall Community release 2.5.2 (c) Endian

Figura H.20. Configuración de nueva regla NAT.

Paso 3: Para la configuración es necesario tener los siguientes requerimientos

- Dirección IP de Llegada
- Servicio de entrada: Protocolo y puerto
- Ip de Traducción:
- Puerto:

Sistema Estado Red Servicios **Firewall** Proxy VPN Registros

Redirección de puertos / NAT de destino

Redirección de puertos / NAT >> Redirección de puertos / NAT de destino NAT fuente Tráfico enrutado de entrada

Reglas actuales >>

Editor de regla de reenvío de puerto / NAT de destino Modo simple | [Modo avanzado](#)

Dirección IP de llegada

Tipo * Zona/VPNEnlace activo

Seleccione las interfaces (mantenga presionado CTRL para seleccionar varias)

- <CUALQUIER Enlace activo>
- Enlace main - IP: Todos los conocidos
- Enlace main - IP: 192.168.10.2
- Zona VERDE - IP: Todos los conocidos
- Zona VERDE - IP: 192.168.1.1
- Zona AZUL - IP: Todos los conocidos

Servicio/Puerto de entrada

Servicio * Definido por el usuario

Puerto/rango de entrada (uno por línea, por ejemplo 80, 80:88) 5000

Protocolo * TCP

Traducir a *

Insertar IP 192.168.2.2 Puerto/rango (ej. 80, 80:88) 5000 NAT NAT

Activado Registro Observación monitoreo de equipos Posición * Primero

[Actualizar regla](#) o [Cancelar](#) * Este campo es obligatorio.

Figura H.21. Configuración de nueva regla NAT.

Paso 4: Llenar los campos con los datos solicitados y se muestra como en la figura H.22

Ayuda Cerrar sesión

endian firewall community

Sistema Estado Red Servicios **Firewall** Proxy VPN Registros

Redirección de puertos / NAT de destino

Redirección de puertos / NAT >> Redirección de puertos / NAT de destino NAT fuente Tráfico enrutado de entrada

Reglas actuales >>

[Agregar nueva regla de reenvío de puerto / NAT de destino](#)

#	Dirección IP de llegada	Servicio	Política	Traducir a	Observación	Acciones
1	192.168.10.2 (Enlace main)	TCP/5000		192.168.2.2 : 5000	monitoreo de equipos	

PERMITIR con IP desde: <CUALQUIERA>

Leyenda: Activado (clic para desactivar) Desactivado (clic para activar) Editar Eliminar

Mostrar reglas del sistema >>

Status: Conectado: main (0d 5h 22m 47s) Uptime: 14:36:11 up 5:23, 0 users, load average: 0.00, 0.00, 0.00
Endian Firewall Community release 2.5.2 (c) Endian

Figura H.22. Regla NAT con los parámetros configurados.

ANEXO I

MANUAL PARA CONFIGURAR UNA PÁGINA WEB EN LISTAS BLANCAS Y NEGRAS EN EL SERVIDOR PROXY.

Pasos para la configuración de listas blancas y negras para el servicio PROXY del Endian Firewall 2.5.2

Paso 1: Ingresar a la administración web en un navegador

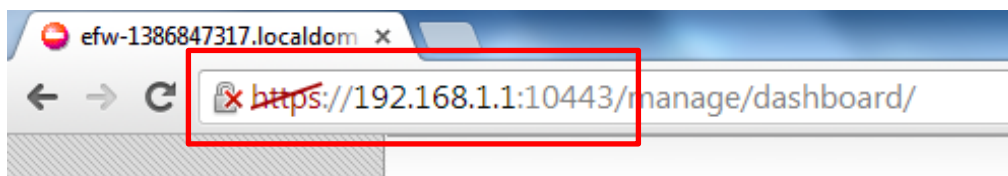


Figura I.1. Ingresar al servidor Proxy

Paso 2: Ingresar a la pestaña PROXY/Filtro de contenido/content2

A screenshot of the Endian Firewall Community web interface. The top navigation bar includes 'Sistema', 'Estado', 'Red', 'Servicios', 'Firewall', 'Proxy', 'VPN', and 'Registros'. The 'Proxy' tab is highlighted with a red box. Below the navigation bar, the 'Filtro de contenido' configuration page is shown. The 'Filtro de contenido' tab is also highlighted with a red box. The page displays options for scheduling automatic blacklist updates (Cada hora, Diariamente, Semanalmente, Mensualmente) and a 'Guardar' button. Below this, there is a section for forcing an update with an 'Actualización' button. The page also shows the last update dates for blacklists and phrases. At the bottom, there is a table with columns for '#', 'Nombre del perfil', and 'Acciones'. The table lists two profiles: 'content1' (Perfil predeterminado (content1)) and 'content2' (nuevo (content2)). The 'Acciones' column for 'content2' has a red box around the edit and delete icons. A legend below the table explains the icons: a pencil for 'Editar perfil' and a trash can for 'Borrar perfil'. At the very bottom, the status bar shows system information and the version 'Endian Firewall Community release 2.5.2 (c) Endian'.

Figura I.2. Ingresar a listas blancas y negras

Paso 3: Configurar las listas blancas y negras según lo requerido

The screenshot shows the 'endian firewall community' web interface. The main navigation bar includes 'Sistema', 'Estado', 'Red', 'Servicios', 'Firewall', 'Proxy', 'VPN', and 'Registros'. The 'Proxy' tab is selected, and the 'HTTP proxy: Contentfilter' configuration page is displayed. The 'Filtro de contenido' sub-tab is active, showing settings for automatic blacklist updates (set to 'Mensualmente') and a section for custom black and white lists. The 'Listas negras y blancas personalizadas' section is highlighted with a red box, showing two text areas: 'Permitir los siguientes sitios' (Allow the following sites) containing a list of domains like gub.ec, www.youtube.com, www.hotmail.com, www.ebay.com, www.facebook.com, google.com, www.pichincha.com, and www.taringa.net; and 'Bloquear los siguientes sitios' (Block the following sites) which is currently empty.

Figura I.3. Configurar listas blancas y negras

Para el ejemplo se configura en:

Listas blancas: www.taringa.net

Listas negras: www.tierragamer.com

Por último se guarda los cambios y se confirma la negación y permiso de las páginas configuradas.

ANEXO J

MANUAL DE ADMINISTRACIÓN DEL SERVIDOR DE VOIP Y VIDEO STREAMING.

Instalación del servicio:

Para la instalación es necesario descargar el software e inicializamos el instalador en donde nos muestra la primera pantalla como en la figura J.1.



Figura J.1. Instalación de Elastix 2.4.0

Seleccionamos el idioma del software y el teclado a ser utilizado



Figura J.2. Selección del idioma



Figura J.3. Selección del idioma del teclado.

Seleccionamos la partición a ser utilizada



Figura J.4. Selección de la partición para el sistema Elastix.

Configuración de la interface de red con la ip asignada en nuestro prototipo 192.168.2.3/24

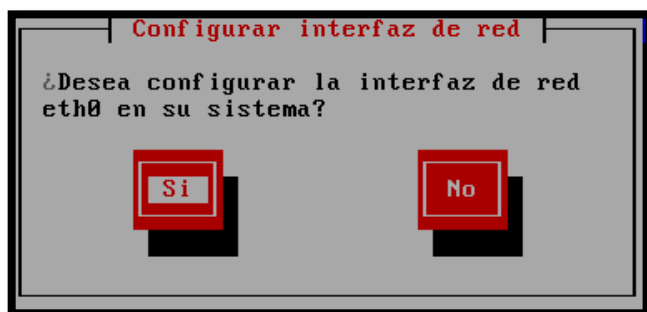


Figura J.5. Confirmar interfaz de red.



Figura J.6. Configuración de la IP

Configuración de contraseña de acceso al sistema Elastix.

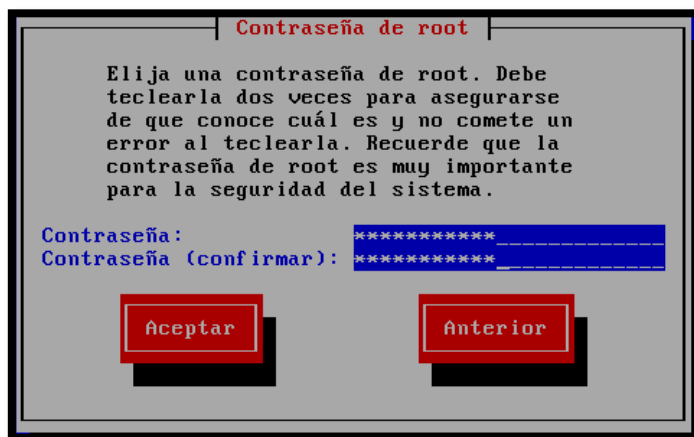


Figura J.7. Configuración de contraseña para el acceso al sistema Elastix.

Una vez cargado todos los paquetes se presenta la pantalla en la figura J.8 donde se confirma la instalación completa del sistema ELASTIX 2.4.0.

```
Kernel 2.6.18-348.1.1.el5 on an i686
ELASTIX-GRUP04 login: networking3
Password:
Login incorrect

login:
Login incorrect

login: root
Password:

Welcome to Elastix
-----
Elastix is a product meant to be configured through a web browser.
Any changes made from within the command line may corrupt the system
configuration and produce unexpected behavior; in addition, changes
made to system files through here may be lost when doing an update.

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://192.168.1.100

[root@ELASTIX-GRUP04 ~]#
```

Figura J.8. Pantalla de finalización del sistema Elastix.

Creación de una nueva extensión con número 123 como ejemplo para el servicio VoIP.

Paso 1: Ingresamos a la interface gráfica del servidor mediante la IP el usuario y la clave previamente configurados.

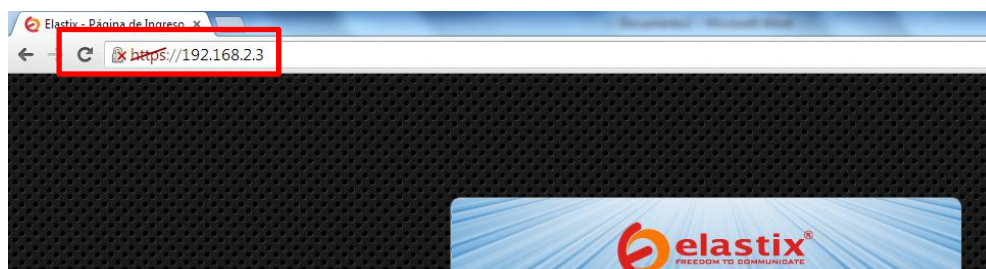


Figura J.9. Ingresamos al servidor elastix.

Paso 2: Ingresamos a la pestaña PBX/Add Extension y seleccionamos el protocolo SIP para un dispositivo genérico.

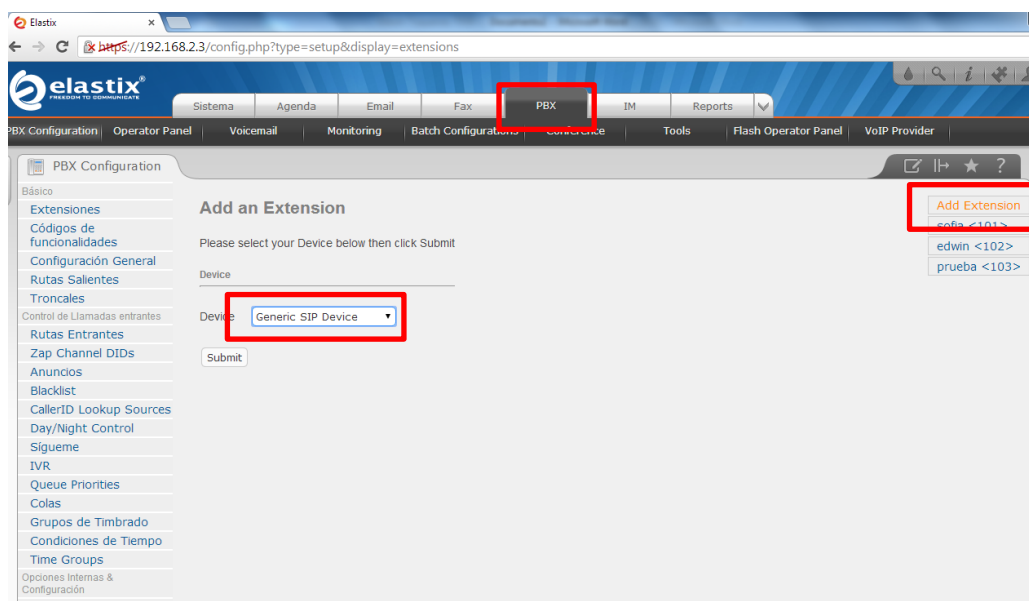


Figura J.10. Configuración de una nueva extensión.

Paso 3: Ingresamos el número de la extensión y el nombre del usuario o función.

The screenshot shows the 'Add SIP Extension' configuration page in the Elastix web interface. The 'User Extension' field is highlighted with a red box and contains the value '123'. The 'Display Name' field contains 'Nuevo'. The interface includes a sidebar with navigation options and a top-right 'Add Extension' button.

Figura J.11. Configuración de datos de la nueva extensión.

Paso 4: Se debe configurar una clave personal para la activación de la extensión.

The screenshot shows the 'Device Options' section of the 'Add SIP Extension' configuration page. The 'secret' field is highlighted with a red box and contains a masked password 'XXXXXXXXXX'. The interface includes a sidebar with navigation options and various configuration fields.

Figura J.12. Configuración de contraseña para la nueva extensión.

Por ultimo guardamos los cambios y realizamos la configuración en un teléfono IP o un softphone con los mismos datos.

Creación de una extensión que soporte video streaming:

Paso 1: Una vez creada la extensión según los anteriores pasos ingresamos a la pestaña PBX / freePBX sin embeber.

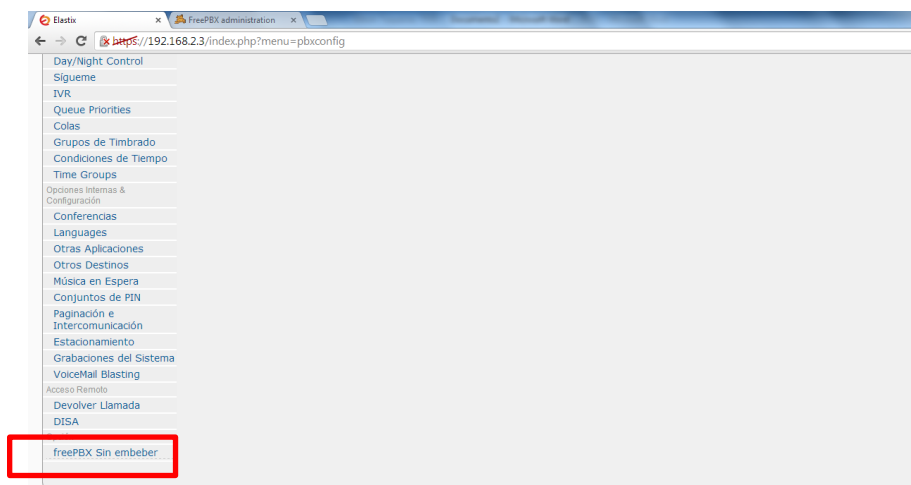


Figura J.13. Ingreso al freePBX para la activación de video streaming.

Paso 2: Ingresamos a Tools / Asterisk IAX Settings

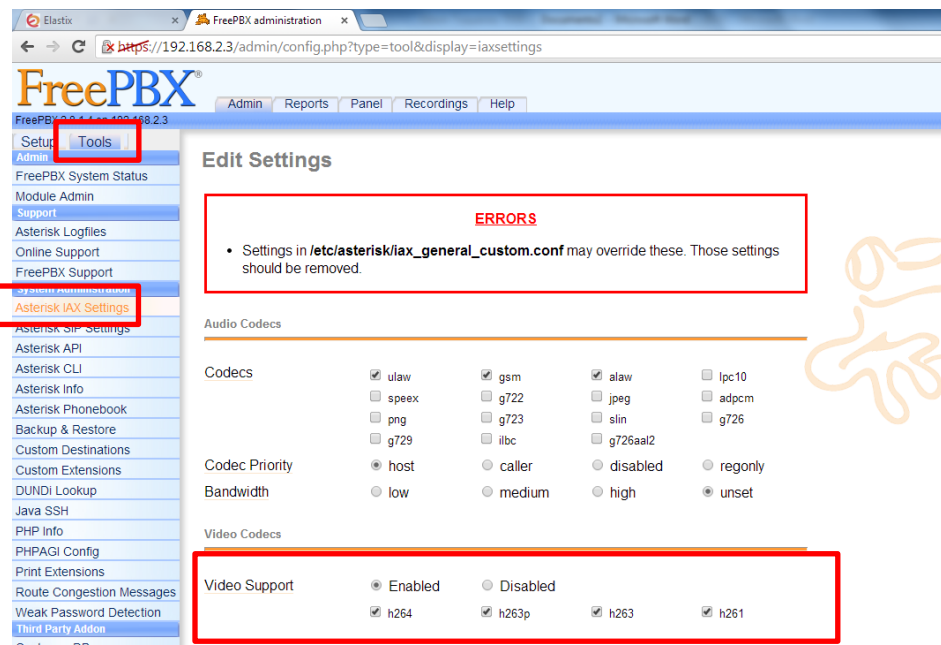


Figura J.14. Activar el soporte de video en el servidor Elsatix.

Por ultimo ingresamos a la extensión que requiere el servicio configuramos el siguiente código `ulaw&h264&h263&h263p` en el campo allow:

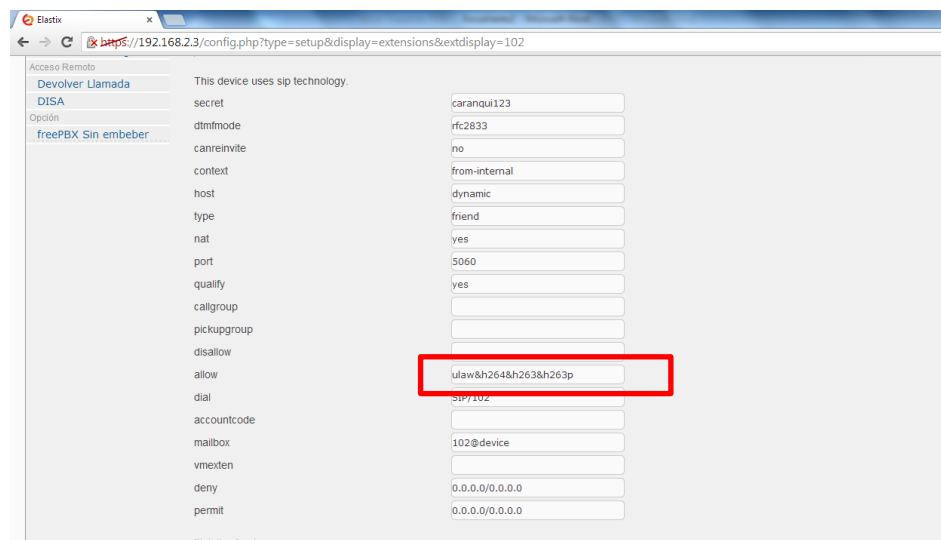


Figura J.15. Activar el servicio en las extensiones para que soporten video streaming.

Ejemplo de configuración de un softphone para la utilización del servicio.

Se configura el softphone X-Lite 4.5.5 para Windows:

Paso 1: ingresamos a la pestaña Softphone / Account Settings

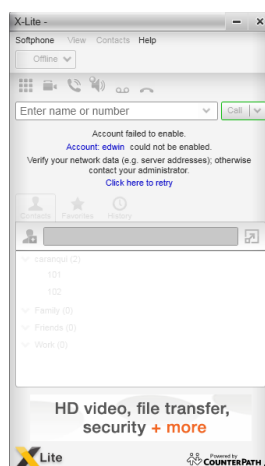


Figura J.16. Softphone X-Lite.

Paso 2: configuramos nuestro ejemplo con la extensión 123, nombre de usuario Nuevo y su contraseña en el servidor con IP 192.168.2.3.

The image shows a 'SIP Account' configuration window with the following details:

- Account name: Nuevo
- Protocol: SIP
- Allow this account for: Call, IM / Presence
- User Details:
 - User ID: 123
 - Domain: 192.168.2.3
 - Password: [masked]
 - Display name: Nuevd
 - Authorization name: [empty]
- Domain Proxy:
 - Register with domain and receive calls
 - Send outbound via:
 - Domain
 - Proxy Address: [empty]
- Dial plan: #1!ala.T;match=1;prestrip=2;

Figura J.17. Configuración de parámetros de extensión ya creada en el servidor.

ANEXO K

ADMINISTRACION DEL GESTOR DE RED PRTG

Instalación

Se debe descargar el instalador de la página oficial la versión estarter que permite su utilización del software con limitación de herramientas que no serán necesarias para los objetivos del proyecto.

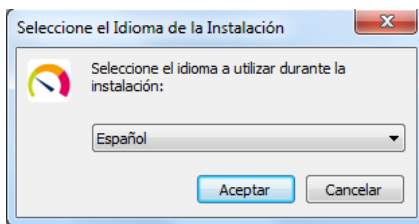


Figura K.1. Seleccionar el idioma de instalación.

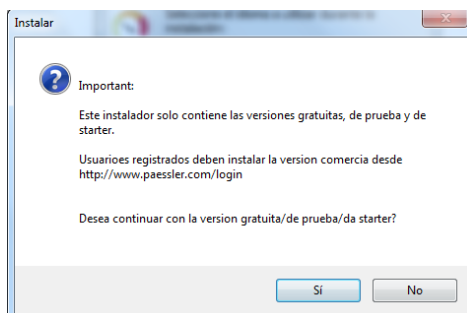


Figura K.2. Confirmar la versión Strater.

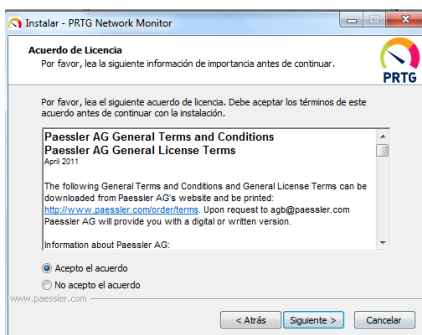


Figura K.3. Aceptar los acuerdos de licencias.

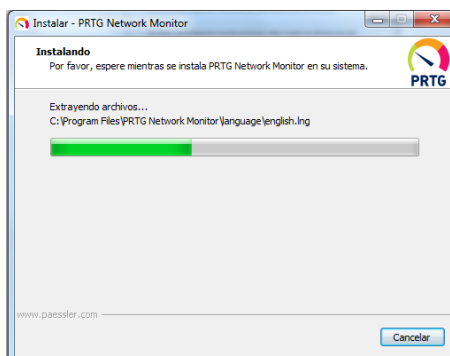


Figura K.4. Empezar la instalación.

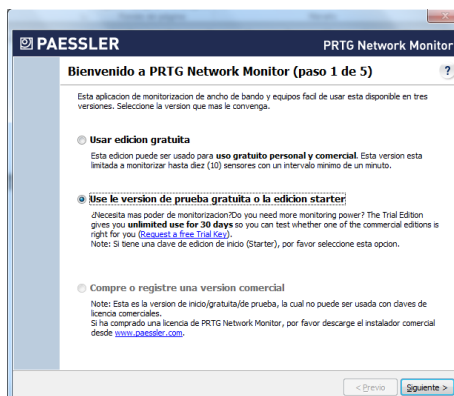


Figura K.5. Seleccionamos la versión Starter.

Ingresamos el nombre de usuario y contraseña que nos proporciona la página oficial una vez registrados para utilizar la versión Starter.

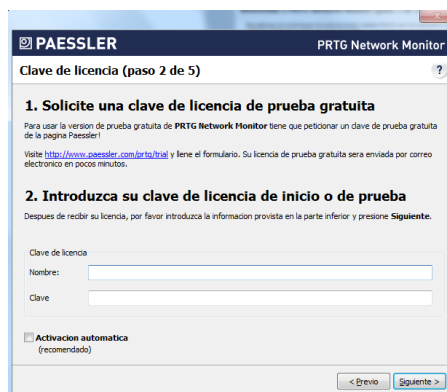
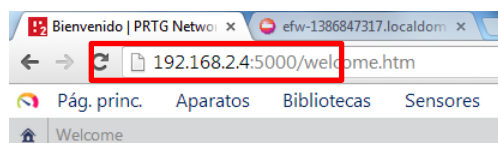


Figura K.6. Ingreso del nombre y clave registradas.

Una vez se termina la instalación ingresamos al sistema PRTG mediante una página web y la ip de la maquina donde se aloja, en nuestro ejemplo es la maquina con IP 192.168.2.4



Iniciar con PRTG Network Monitor

Figura K.7. Ingreso al sistema.

Asignación de un nuevo dispositivo.

Como ejemplo se asignara al gestor de red PRTG el punto de acceso AP Caranqui de la topología prototipo con IP 192.168.1.3/24.

Paso1: Una vez ingresado al sistema creamos grupos de distribución en la pestaña Aparatos / Local probe.

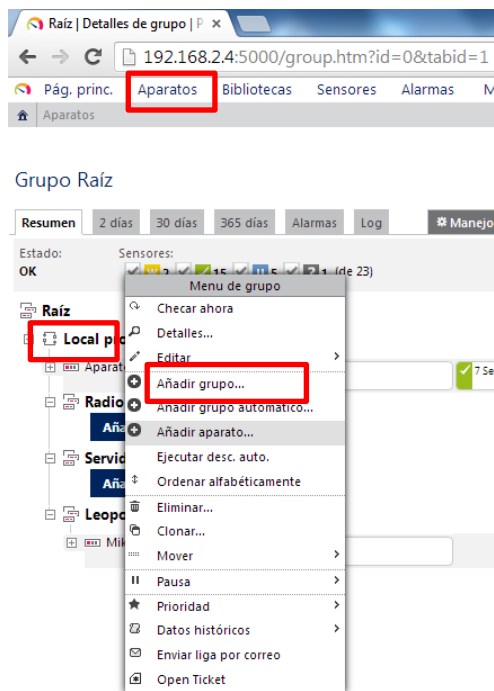


Figura K.8. Nombre del grupo.

Figura K.9. Creación de grupos de distribuciones.

Paso 2: Añadimos un nuevo equipo en la pestaña Añadir aparato

Añadir grupo al grupo Radio Enlace

Nombre del aparato: AP Caranqui

Version de IP:

- Conectar usando IPv4
- Conectar usando IPv6

Dirección de IP/nombre DNS IPv4: 192.168.1.3

Identificadores:

Icono de aparato:

TIPO DE APARATO

Manejo de sensores:

- Manual (sin descubrimiento automático)
- Identificación automática de aparatos (estándar, recomendado)

Continuar > Cancelar

Figura K.10. Creación de nuevo dispositivo.

Añadir grupo al grupo Radio Enlace

DATOS DE ACCESO PARA SISTEMAS WINDOWS

heredado de Radio Enlace (Nombre de dominio o ordenador: <vacío>, Nomb...)

DATOS DE ACCESO PARA SISTEMAS LINUX/SOLARIS/MAC OS (SSH/WBEM)

heredado de Radio Enlace (Nombre de usuario: <vacío>, Registro: 0, Para...)

DATOS DE ACCESO PARA SERVIDORES VMWARE/XENSERVER

heredado de Radio Enlace (Usuario: <vacío>)

DATOS DE ACCESO PARA APARATOS SNMP

heredado de Radio Enlace (Version SNMP: V2, Puerto SNMP: 161, Tiempo lí...)

Version SNMP:

- v1
- v2c
- v3

Cadena de comunidad: public

Puerto SNMP: 161

Tiempo límite de desconexión SNMP (seg): 5

DERECHOS DE ACCESO

heredado de Radio Enlace

Continuar > Cancelar

Figura K.11. Creación de protocolo SNMP.

Verificación de topología de red.

Cuando hay conectividad en todos los equipos se visualiza el gestor de red según la figura K.12

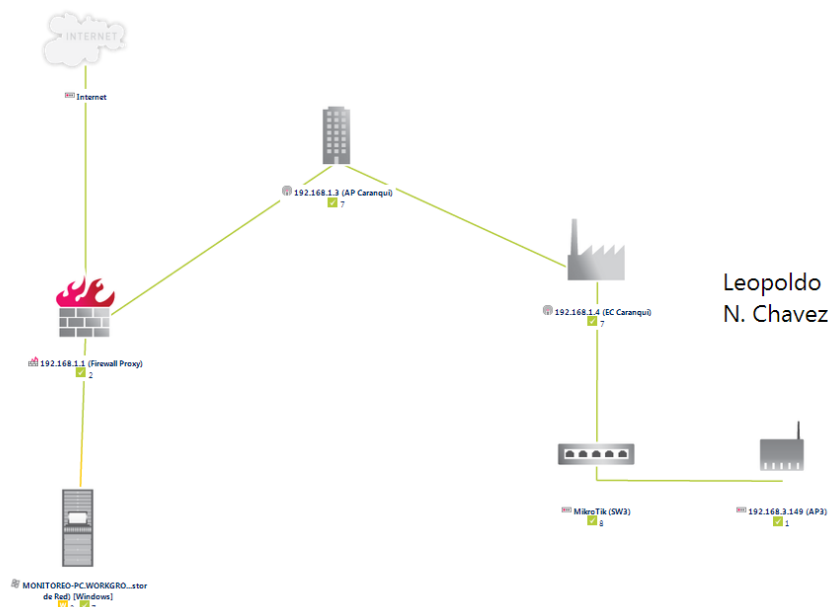


Figura K.12. Topología con conectividad completa.

El escenario presentado para la gestión de red muestra una topología según la figura K.13

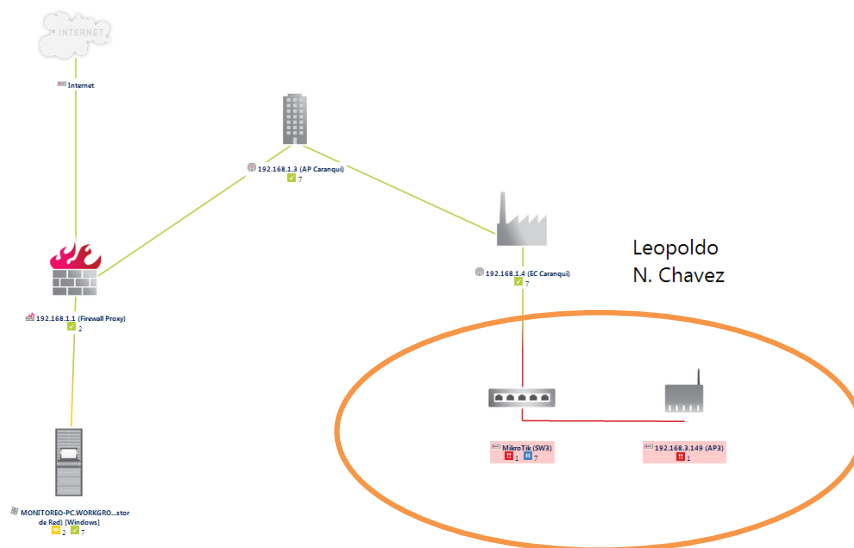


Figura K.13. Topología en escenario de administrador del gestor de red.

Pruebas de conectividad mediante el gestor de red PRTG.

Según la figura K.13 se muestra una falla en los equipos de conectividad del centro de informática Leopoldo N. chaves por lo tanto se realiza pruebas de conectividad:

Paso 1: verificar que sensor tiene la alarma de falla

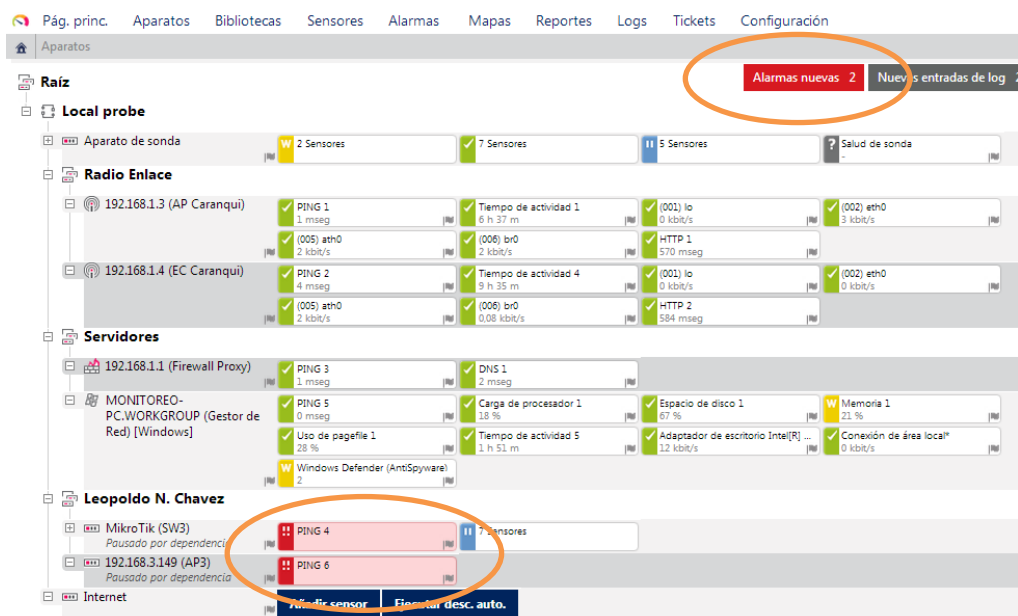


Figura K.14. Alarmas que muestra el gestor de red.

Realizar pruebas de ping y tracert desde la red administrador.

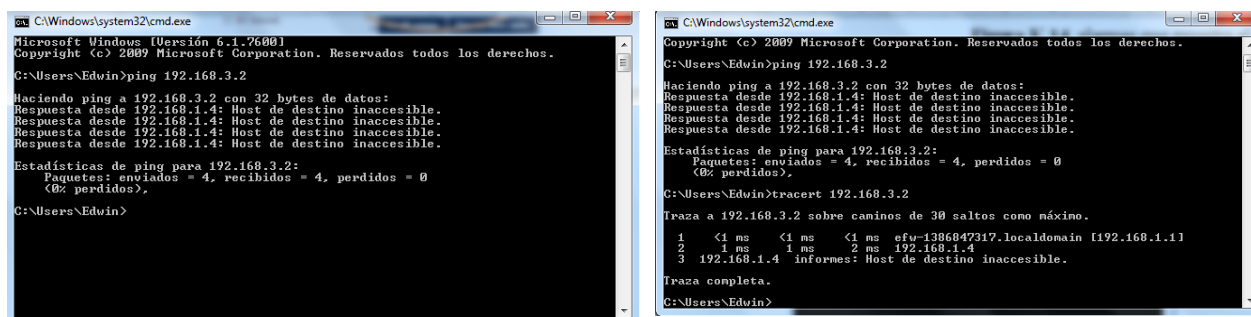


Figura K.15. Pruebas de ping y tracert.

Se verifica los tiempos que estuvo sin conectividad el dispositivo para posibles informes de lo sucedido.

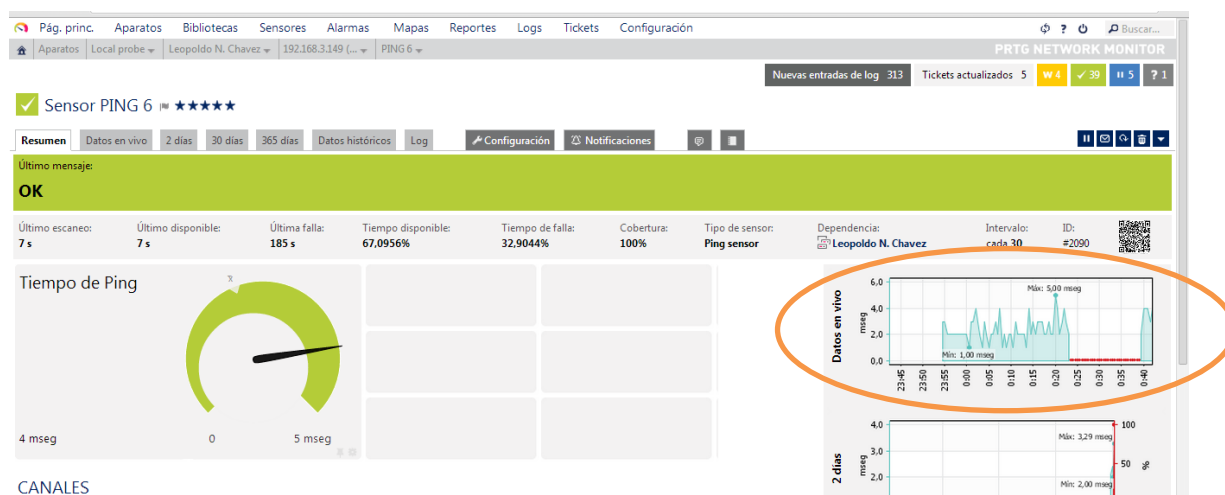


Figura K.16. Datos en vivo de conectividad en el sensor.

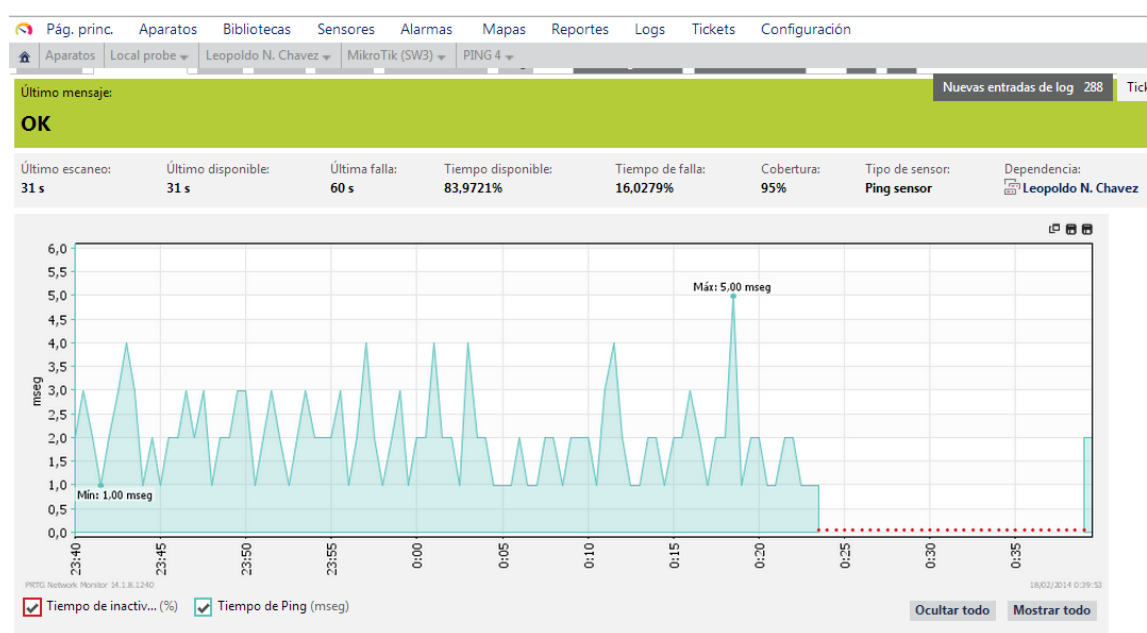


Figura K.17. Verificación de tiempos de falla de conectividad.

ANEXO L

ADMINISTRACIÓN DEL PORTAL CAUTIVO

El portal cautivo permite re direccionar el trafico http de los clientes de la red LAN hacia el hotspot o portal para conseguir la identificación y autenticación al ingreso de la red y acceso al servicio de internet. Es necesario realizar ciertas configuraciones básicas en el dispositivo mikrotik para ello es necesario descargar el software winbox para proceder a configurar de forma gráfica el equipo.



Abrir el programa y darle un click en el recuadro de *Connect To*.

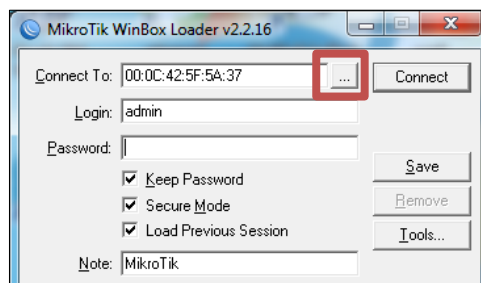


Figura L.1. Conexión de Mikrotik

Seleccionar la dirección MAC de la interfaz por la cual el host está conectado hacia el dispositivo.

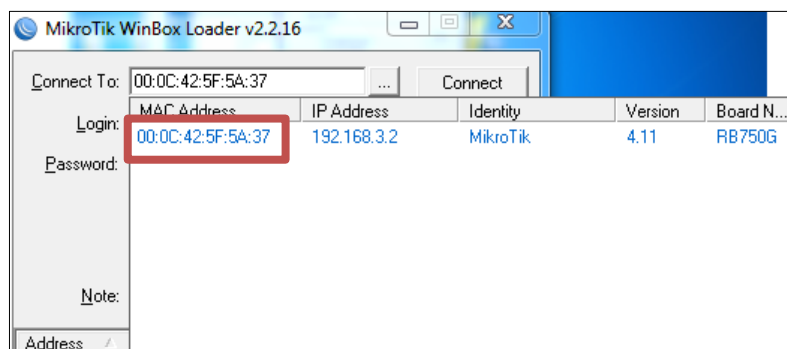


Figura L.2. Selección de dirección MAC.

Dar Click en el botón Connect.



Se visualiza la pantalla principal de configuración de mikrotik en winbox.

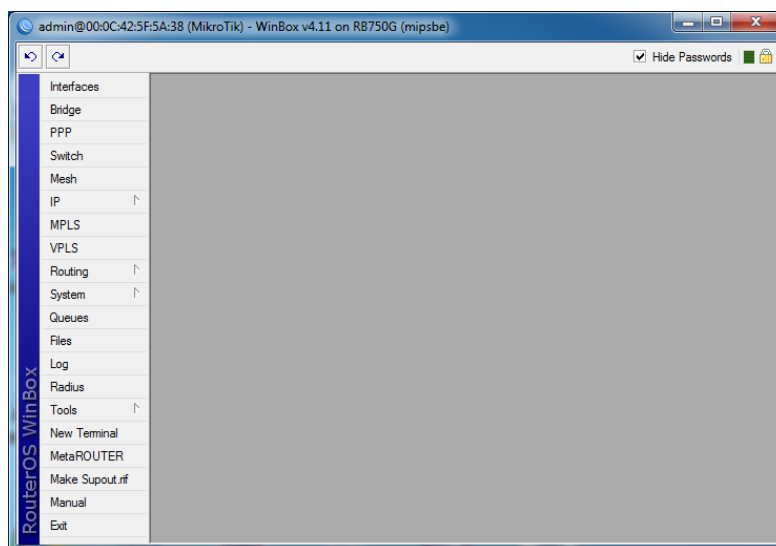


Figura L.3. Inicio de Winbox.

Y se procede a borrar configuraciones posteriores que puedan interferir en la configuración del hotspot.

Dar click en New Terminal y en la ventana terminal digitar el comando *system reset*.

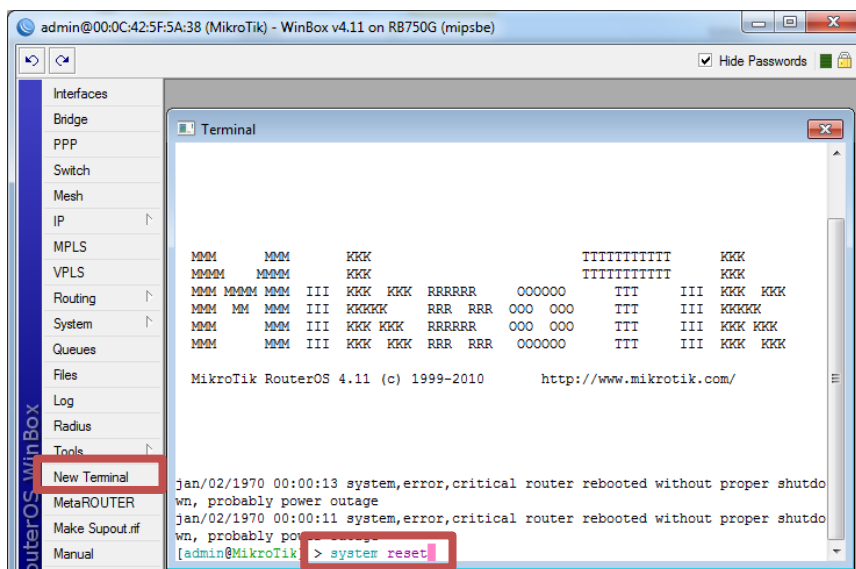
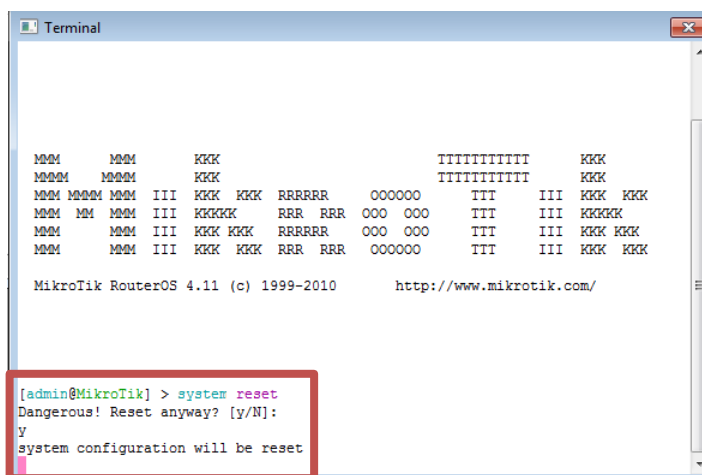


Figura L.4. Terminal de Mikrotik

Al presionar la letra Y se acepta la petición y presionar enter.



```
MMM   MMM   KKK                               TTTTTTTTTT   KKK
MMMM  MMM   KKK                               TTTTTTTTTT   KKK
MMM MMMM MMM III KKK KKK RRRRRR   OOOOOO   TTT   III   KKK KKK
MMM MM  MMM III KKKKK   RRR RRR   OOO OOO   TTT   III   KKKKKK
MMM   MMM III KKK KKK RRRRRR   OOO OOO   TTT   III   KKK KKK
MMM   MMM III KKK KKK   RRR RRR   OOOOOO   TTT   III   KKK KKK

MikroTik RouterOS 4.11 (c) 1999-2010      http://www.mikrotik.com/

[admin@MikroTik] > system reset
Dangerous! Reset anyway? [y/N]:
y
system configuration will be reset
```

Figura L.5. Terminal de Mikrotik

El dispositivo se desconectará, seleccionar OK.

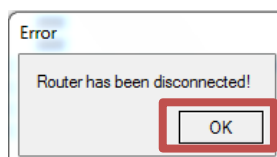


Figura L.6. Desconexión de mikrotik

Es necesario ingresar nuevamente mediante winbox y seleccionar la opción *Remove Configuration* de la pantalla en la que se inicia.

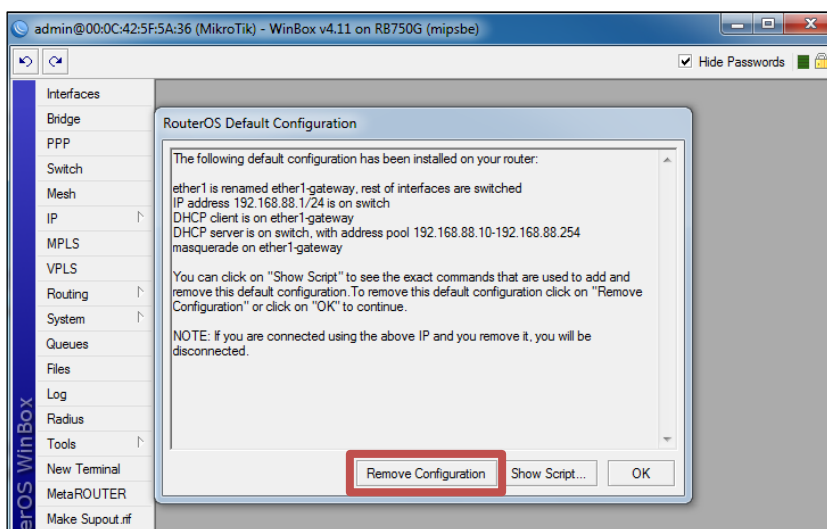


Figura L.7. Configuración por defecto de Router OS

CONFIGURACIÓN DEL HOTSPOT

Se configura los datos iniciales de la interfaz a utilizar para el hotspot en este caso se usa la interfaz eth5 en la cual se debe dar doble click para su configuración

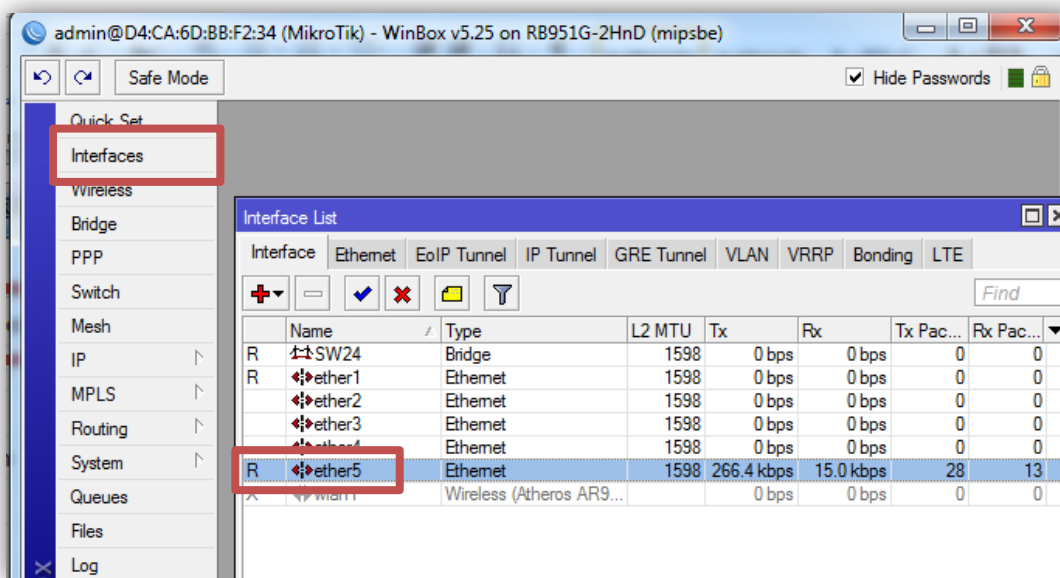


Figura L.8. Configuración de Interfaces.

Cambiar el nombre de la interfaz a HOTSPOT5 y aceptar.

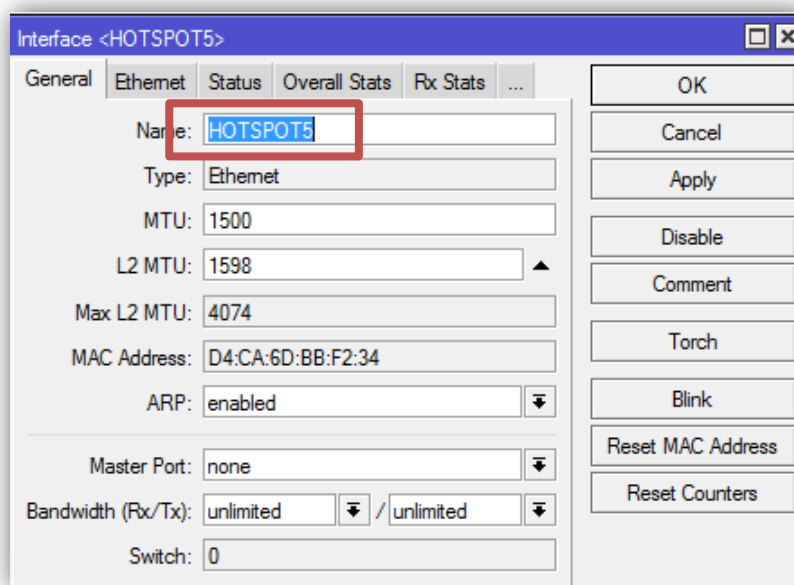


Figura L.9. Configuración de Interfaces.

Ingresar a IP > Addresses

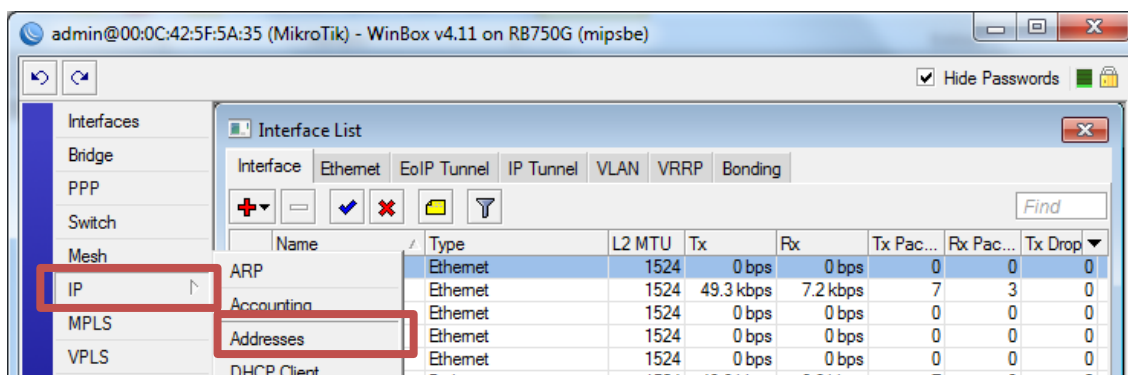


Figura L.10. Configuración de direcciones IP

En Address List presionar el signo +. Asignar la nueva dirección IP 192.168.25.1 de la nueva interfaz HOTSPOT5 seleccionarla con la flecha en interface presione Apply.

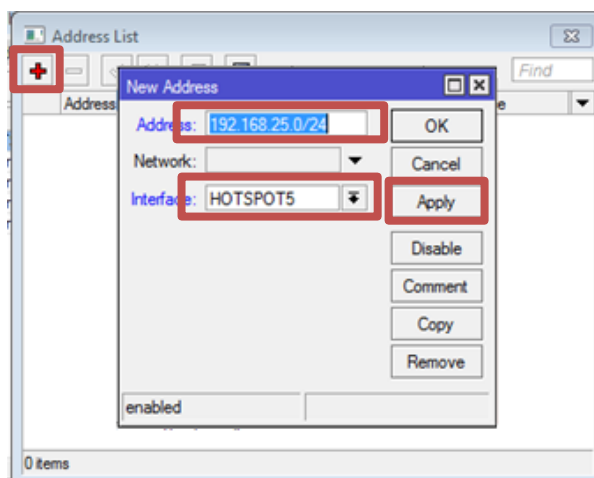


Figura L.11. Configuración de direcciones IP en Hotspot

Presione OK.

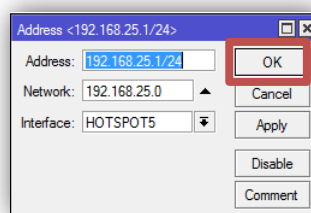


Figura L.12. Configuración de direcciones IP en Hotspot.

En la ventana inicial se dirige a: IP > Hotspot.

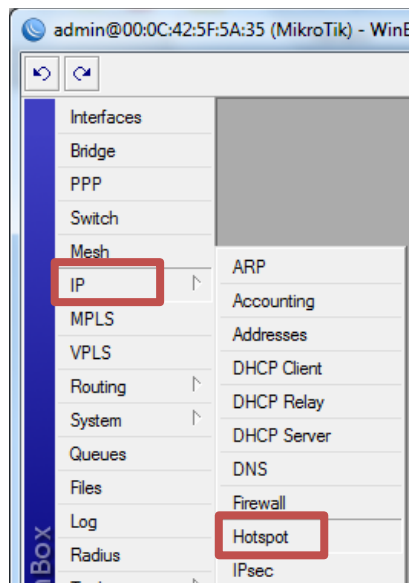


Figura L.13. Configuración de Hotspot

En la ventana Hotspot se dirige a Servers > botón Hotspot Setup.



Figura L.14. Configuración de Hotspot setup

Se inicia con el asistente de configuración de Hotspot Server elige la interface de HOTSPOT5 donde se configura el hotspot server y seleccionar NEXT.

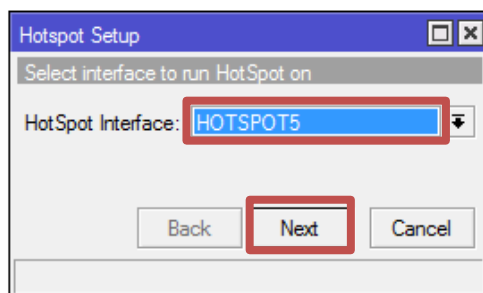


Figura L.15. Configuración de interfec de Hotspot

En Local Address of Network aparece automáticamente la puerta de enlace de los clientes, que en este caso es 192.168.25.1.

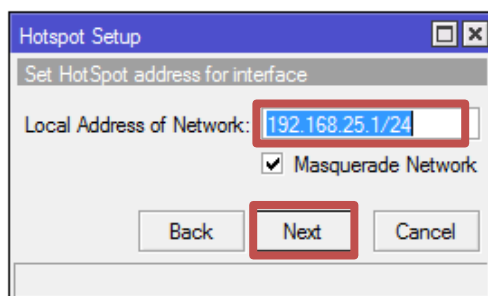


Figura L.16. Configuración de dirección IP de Hotspot

Para Address Pool of Network se ingresa un rango de direcciones IP que serán asignados a los clientes.

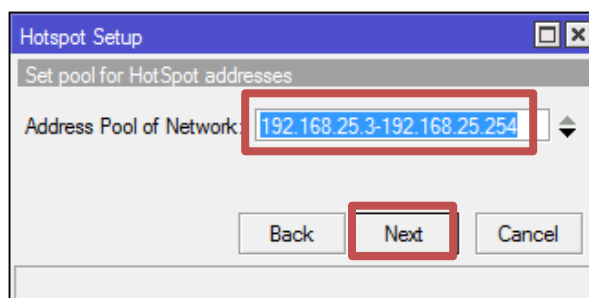


Figura L.17. Configuración de rango de direcciones de Hotspot

Select Certificate, elegir none. Estos certificados son utilizados para validar una página web.

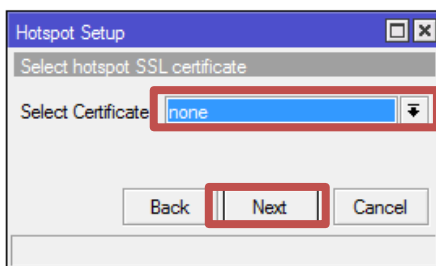


Figura L.18. Configuración de certificados SSL Hotspot

DNS Servers, aparece los valores de DNS agregados en el servidor DNS cache por defecto.

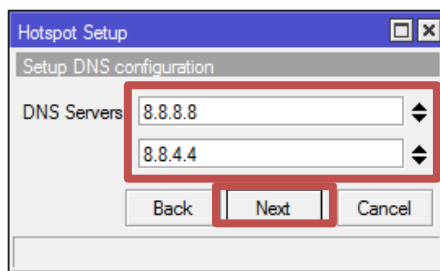


Figura L.19. Configuración de DNS en Hotspot

DNS Name, aquí se coloca un DNS para la red del hotspot, cuando el hotspot esté funcionando y se desee acceder a internet en el navegador se ingresara el nombre del dominio del hotspot asignado: www.caranqui.com en este caso; este nos redireccionará al portal cautivo para autenticar a cada usuario con su respectivo usuario y contraseña asignados.

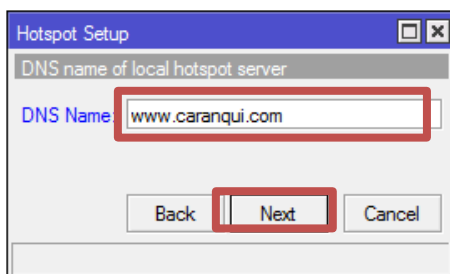


Figura L.20. Configuración de nombre del DNS en Hotspot.

Name of Local Hotspot User, por defecto el nombre de usuario es *caranqui*.

Password for the User, es el password o contraseña de autenticación en este caso la contraseña va en blanco.

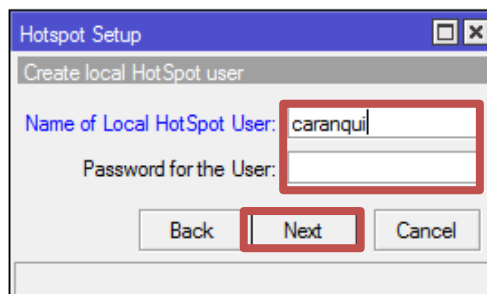


Figura L.21. Configuración de usuario u contraseña de Hotspot

Una vez hecho esto saldrá un mensaje de configuración exitosa del hotspot.

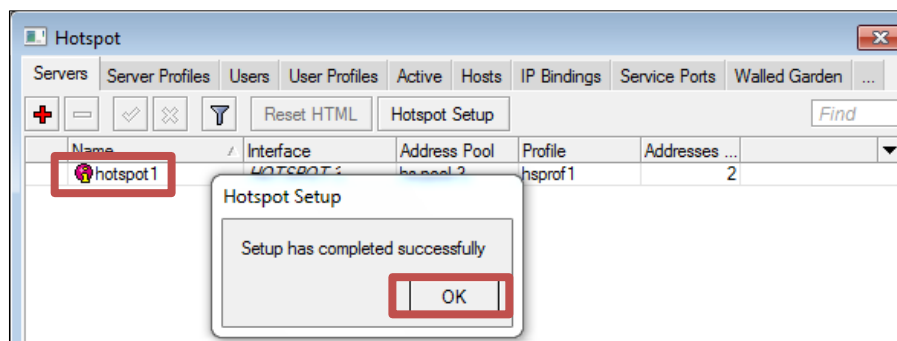


Figura L.22. Configuración de Hotspot finalizada.

Al intentar abrir una nueva página, este mostrará el portal cautivo por defecto de MikroTik.



Figura L.23. Página de inicio de hotspot.

Una vez presentada la página inicial del portal cautivo se procede a la autenticación:

LOGIN: caranqui

PASSWORD:

Según la configuración del hotspot, ahora se podrá utilizar el servicio de internet luego de la autenticación.

CARGAR UNA NUEVA PÁGINA WEB DE INICIO

Para modificar la página web de inicio de hotspot se debe acceder al archivo de la página en:

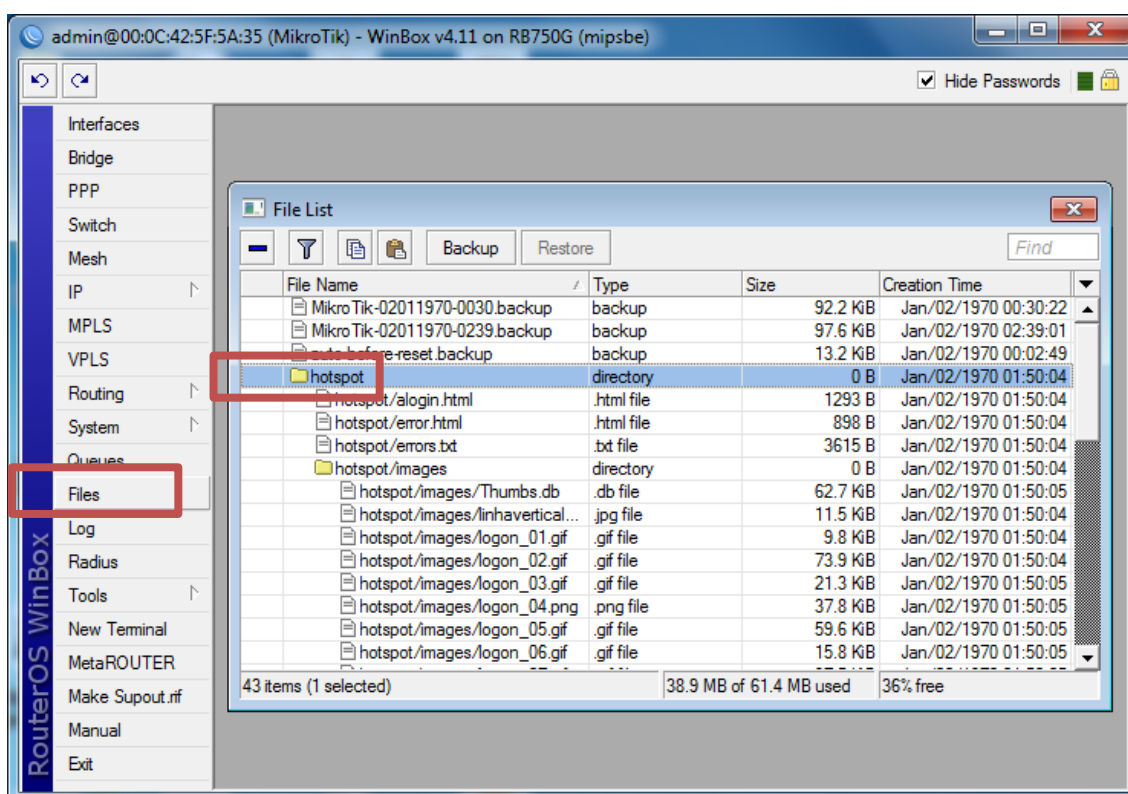


Figura L.24. Archivo de configuración de hotspot.

Copiar la carpeta hotspot arrastrándola hacia el escritorio de tu PC y se descarga.

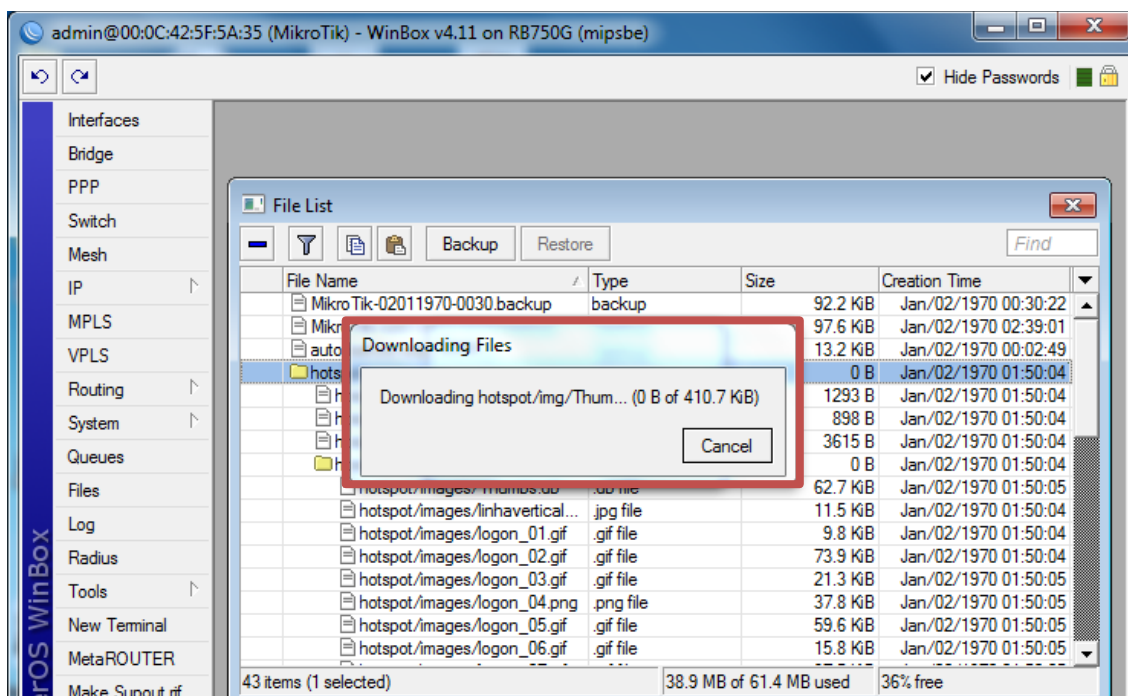


Figura L.25. Descarga de archivo de configuración de hotspot.

Este archivo puede ser modificable haciendo uso de herramientas para edición de páginas web para ello se utilizó el programa KompoZer versión 0.7.10 en la carpeta hotspot se encuentra el archivo login.

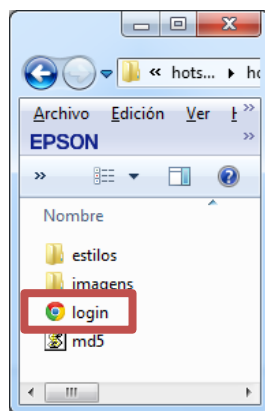


Figura L.26. Carpeta Hotspot y archivo login para edición.

Este archivo debe abrirse mediante el programa KompoZer para realizar la edición correspondiente de la siguiente manera:

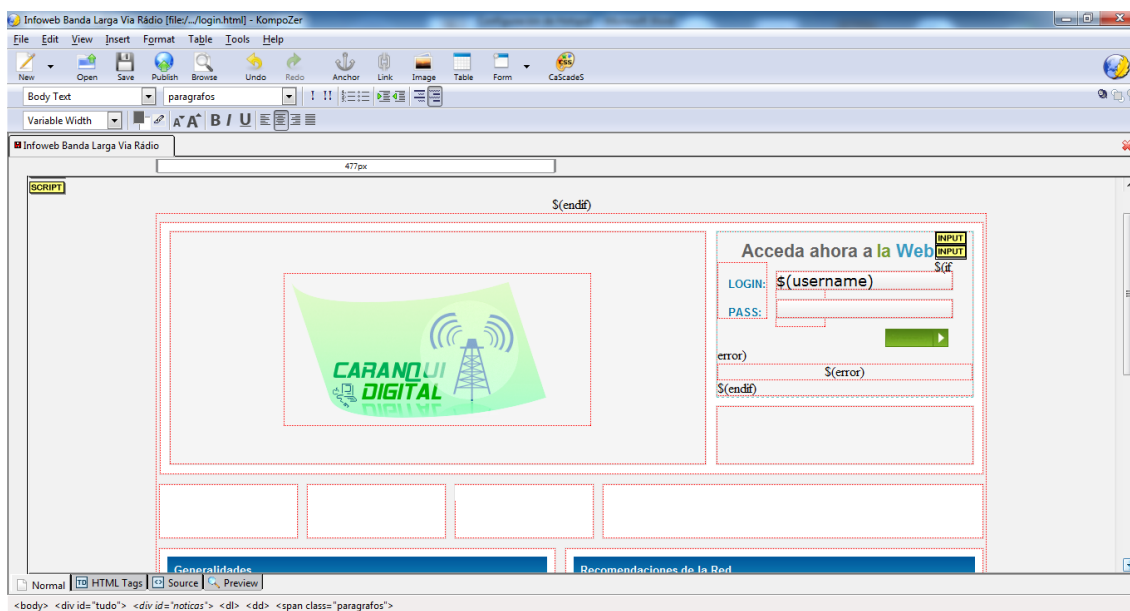


Figura L.27. Edición de la Pagina Web con el logotipo de identificación de la parroquia.

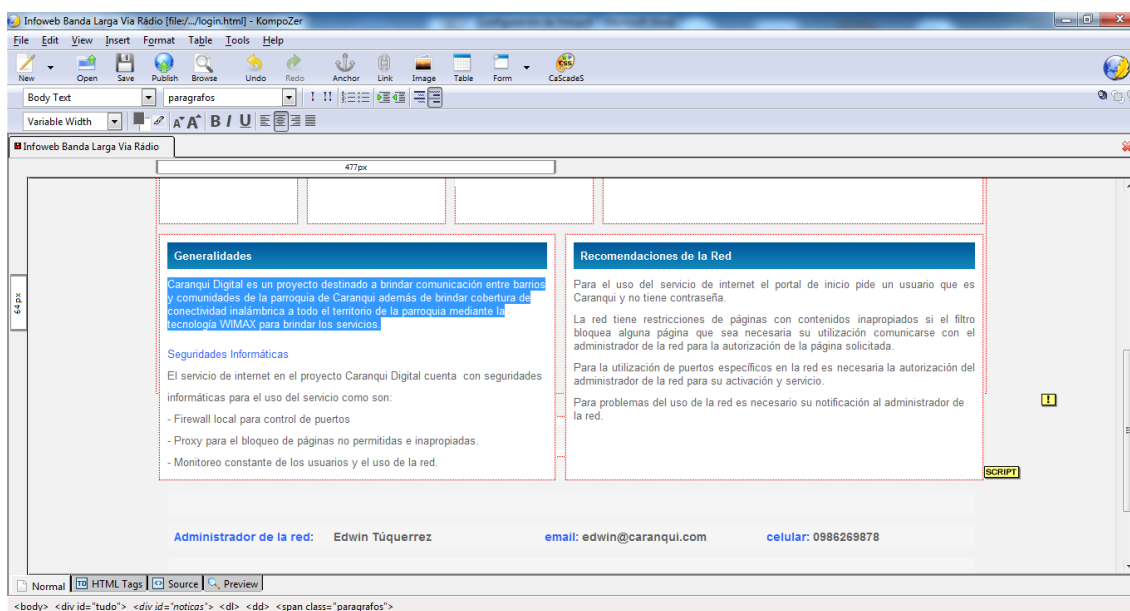


Figura L.28. Edición de la Pagina Web que contiene las recomendaciones de uso del hot spot.

El siguiente paso es borrar el archivo de hotspot que contiene el equipo mikrotik con el signo menos de la ventana File list.

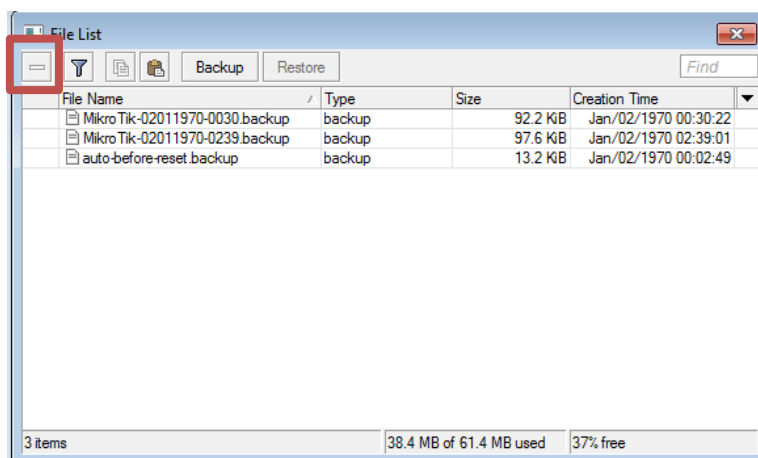


Figura L.26. Borrar archivo de configuración de hotspot.

En la carpeta hotspot que se encuentra cargada en nuestro computador se procede a reemplazar el archivo login rediseñado.

Cargar nuevamente la carpeta hotspot en los archivo de mikrotik arrastrando hacia la ventana. Abrir la nueva página web diseñada mediante el inicio de navegación en la red.



Figura L.27. Página de inicio para autenticación de hotspot final.

ANEXO M

COTIZACION DE EQUIPOS A SER UTILIZADOS EN LA PROPUESTA DE RED.

mmeza - crpfaEmiPedido.Rpt

LA CASA DEL CABLE

Página : 1 de 1

PROFORMA

JUAN SEVERINO E6-59 Y AV.ELOY ALFARO EDIF OSIRIS PB
Teléfonos: 022905402 - 023822250 Fax:
RUC : 0991515011001
QUITO - Ecuador

FechaImp : 11/nov/2013

HoraImp : 10:42:47

PROFORMA : PRA1300504302 CLIENTE : 021371 ESTADO : PENDIENTE

Cliente : 021371 - TUQUERREZ IPIALES EDWIN GEOVANN Dirección : IBARRA / VIA A SAN CRISTOBAL PRINCIPAL NºIdentificación : 1002956330001 Teléfono : 062607913 Zona/Ciudad : QUITO CENTRO/QUITO	Fecha/Pedido : noviembre 11, 2013 Hora/Pedido : 10:39:29 Vendedor : Marcos Meza [mmeza] Forma/Pago : AL CONTADO
---	--

CantPed	Fec.Entreg	Artículo	Descripción	Val.Unitario	SubT.Bruto	Desc	SubT.Net
1	11-11-13	10809 - PRO-BS-1158-	ESTACION BASE 50Mbps ARBA PRO 5725-5875 MHz	4,166.670000	4,166.670000		4,166.67
2	11-11-13	10814 - ACC-SSPOE	SUPRESOR DE DESCARGAS PoE	45.790000	91.580000		91.58
2	11-11-13	10815 - ACC-SSETH	SUPRESOR DE DESCARGA ETHERNET	84.850000	169.700000		169.70
1	11-11-13	10813 - ACC-SSRF	SUPRESOR DE DESCARGAS RF	237.040000	237.040000		237.04
1	11-11-13	10811 - ACC-A120S	ANTENA 120°, 14 dBi, 5GHz, CABLE RF de 1m	739.120000	739.120000		739.12
1	11-11-13	10810 - PRO-SU-1150-2	SUSCRIPTOR ARBA PRO 5150-5875MHz. ANTENA 2	896.990000	896.990000		896.99

SubTotal Bruto : 6,301.10

(-) Dcto. por Artículo : 0.00

(-) Dcto. Directo : 0.00

SubTotal Neto : 6,301.10

Valor IVA : 756.13

Recargo/Flete : 0.00

Total : 7,057.23

Anticipo : 0.00

Son: SIETE MIL CINCUENTA Y SIETE CON 23/100

NOTA : * LOS PRECIOS Y CANTIDADES AQUI COTIZADOS ESTAN SUJETOS A CAMBIOS SIN PREVIO AVISO.

*** NO ACEPTAMOS CAMBIOS NI DEVOLUCIONES. FAVOR REVISAR SU PEDIDO.**

UNA VEZ EMITIDA SU FACTURA, LA ANULACION DE LA MISMA LLEVARA UN CARG ADMINISTRATIVO

*** LA CASA DEL CABLE S.A ES CONTRIBUYENTE ESPECIAL SEGUN RESOLUCION N.NAC-AOGR2008-1477 del 12/dic/2008**

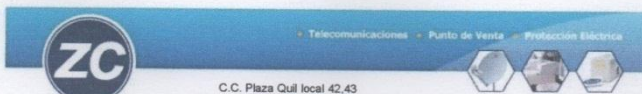
Cartera

Cuota	Valor	Referencia
1	7,057.23	Forma de Pago: AL CONTADO
	7,057.23	



MAYORISTAS

Distribuidor Mayorista

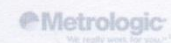


MAYORISTAS

C.C. Plaza Quil local 42,43
Pbx : 04-2286683
www.zcmayoristas.com
Guayaquil-Ecuador

COTIZACION

CLIENTE:	Edwin Tuquerrez	COT.	101013
NOMBRE:	Edwin Tuquerrez	FECHA	31-mar-14
Cantidad	Descripción	Valor u.	Total
1	UBIQUITI UNIFI-UAP- DOMO INDOOR / 20DBM / 2X2 / 802.11 b/g/n 2.4ghz	\$ 79.00	\$ 79.00
1	MIKROTIK ROUTERBOARD RB2011UAS-2HND-IN 600mhz/ 128MB / 5 lan Gigabit / nivel 4	\$ 148.00	\$ 148.00
1	GXP-2160	\$ 139.00	\$ 139.00
1	TOUGHSWITCH POE 8 PRO PUERTOS 12V-24V	\$ 189.00	\$ 189.00
1	UBIQUITI AIRMAX ANTENA 30 DBI / 5,1 A 5,8GHZ / MIMO DISH PARABOLICA	\$ 190.00	\$ 190.00
1	MIKROTIK ROUTER BOARD RB-912UAG-5PhD-OUT	\$ 112.00	\$ 112.00
1	MIKROTIK ROUTERBOARD RB-951G-2HND / 30 DM / 2.5 DBI / 2.4GHZ/ nivel 4	\$ 92.00	\$ 92.00
1	RACK PISO ABIERTO 6FT NEGRO ENCAPSULADA 1.8 MT 36UR	\$ 160.00	\$ 160.00
1	RACK PISO ABIERTO 3FT NEGRO ENCAPSULADA 1MT 24UR	\$ 125.00	\$ 125.00
1	RACK PISO ABIERTO 7FT NEGRO ENCAPSULADA 2MT 44UR	\$ 169.00	\$ 169.00
		SUBTOTAL	\$ 1,403.00
		IVA	\$ 168.36
		TOTAL	\$ 1,571.36



ZC Mayorista S. A.

[Firma Autorizada]
FIRMA AUTORIZADA

NETWORKING: Wireles, Cableado • P.O.S. • Protección Eléctrica

Centro Comercial PLAZA QUIL Local: 42 - 43 • Guayaquil - Ecuador

PBX: 042 286683 • e-mail: info@zcmayoristas.com

www.zcmayoristas.com • Guayaquil - Ecuador

ANEXO N

CENTROS DE INFORMÁTICA DEFINIDOS EN LA PARROQUIA DE CARANQUI.



Figura N.1. Juan de dios Navas -Naranjito



**Figura N.2. Leopoldo N Chávez - San Cristóbal Alto -
San Cristóbal de Caranqui**



Figura N.3. Manzanal



Figura N.4. 20 de Octubre



**Figura N.5. Oscar Efrén Reyes - Ejido de Caranqui
– Unión y Progreso**



Figura N.6. Guayaquil de Caranqui



**Figura N.7. Agustín Cueva Dávila - Vista Hermosa
- 10 de Agosto**



Figura N.8. El Naranjal



Figura N.9. Yuyucocha



**Figura N.10. Olimpia Gudiño Vázquez - Cuatro
Esquinas**



Figura n.11. Colegio Atahualpa – La Candelaria



Figura N.12. José Nicolás Vacas



Figura N.13. Avelina Lazo de Plaza – Simón Bolívar



Figura N.14. Juan Miguel Suarez



Figura N.15. Medardo Proaño Andrade - Unidad Artesanal de Caranqui - Bellavista de María



Figura N.16. Santa Lucia del Retorno



Figura N.17. Central

ANEXO O

LISTADO DE PROYECTOS SIMILARES A LA PROPUESTA

Proyecto	Beneficiarios	Costo total
IMPLEMENTACION DE LA RED DE TELECOMUNICACIONES, CONECTIVIDAD Y CONTENIDOS PARA EL CANTON MONTECRISTI PROVINCIA DE MANABI	Parroquias de Montecristi, La Pila, Aníbal San Andrés.	406659 \$
COMUNICACIÓN Y CONECTIVIDAD PARA EL MANEJO DE INFORMACION DE LA POBLACIÓN DEL CANTON NABÓN	Parroquias de Nabón, Cochapata, Las Nieves (Chaya), El Progreso (Cab. En Zhota).	385083 \$
IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES, CONECTIVIDAD Y CONTENIDOS PARA EL CANTÓN SAN PEDRO DE PELILEO – PROVINCIA DEL TUNGURAHUA	Parroquias de Pelileo, Pelileo Grande, Benítez, Bolívar, Cotaló, Chiquicha, El Rosario (Rumichaca), García Moreno, Guambaló, Salasaca.	564616 \$
IMPLEMENTACIÓN DE UNA RED DE TELECOMUNICACIONES, CONECTIVIDAD Y CONTENIDOS PARA EL CANTÓN PÍLLARO - PROVINCIA DEL TUNGURAHUA	Parroquias de Ciudad Nueva, Píllaro, Baquerizo Moreno, San Andrés, Rumipamba, San José de Poaló, San Miguelito, Marcos Espinel, Presidente Urbina.	334248 \$
PROYECTO PILOTO DE ACCESO A INTERNET EN UNIDADES EDUCATIVAS PÚBLICAS DE LAS ÁREAS RURALES Y URBANO MARGINALES DEL DISTRITO METROPOLITANO DE QUITO	60 escuelas públicas ubicadas en áreas rurales y urbano marginales del Distrito Metropolitano de Quito.	270000 \$
PROYECTO PILOTO ACCESO A INTERNET EN BANDA ANCHA EN UNIDADES EDUCATIVAS DE LAS ÁREAS RURALES Y URBANO MARGINALES DE LA PROVINCIA DE PICHINCHA	Ascázubi, Puerto Quito, Aloasí, Pintag, Pedro Vicente Maldonado, San Bernabé, Pifo, Machachi, Ayora, Nanegalito	96264 \$

ANEXO P

Anexos digitales contenido:

- Encuestas realizadas
- Ley Especial de Telecomunicaciones
- Atribución de Bandas de Frecuencia Ecuador
- Resolución TEL-534-14-CONATEL-2011
- Instructivo Formularios Redes de Acceso Universal de Internet
- Resolución 163-06-CONATEL-2009.
- Resolución TEL-560-18-CONATEL-2010
- Resolución SNT-2011-0617
- Estándar IEEE 802.16-2009
- Estadísticas INEC 2010