CARRERA DE COMPUTACIÓN

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA

TEMA:

RED INALÁMBRICA DE BANDA ANCHA CON SEGURIDAD PERIMETRAL EN LAS ÁREAS URBANAS Y RURALES DEL CANTÓN TOSAGUA

AUTOR:

MICHAEL JHONNY SANTANA MONTESDEOCA

TUTOR:

ING. MARLON RENNE NAVIA MENDOZA, MG.

CALCETA, JULIO 2016

DERECHOS DE AUTORÍA

Michael Jhonny Santana Montesdeoca, declara bajo juramento que el trabajo aquí descrito es de su autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

……..

MICHAEL J. SANTANA MONTESDEOCA

CERTIFICACIÓN DE TUTOR

Marlon Renne Navia Mendoza certifica haber tutelado la tesis RED INALÁMBRICA DE BANDA ANCHA CON SEGURIDAD PERIMETRAL EN LAS ÁREAS URBANAS Y RURALES DEL CANTÓN TOSAGUA, que ha sido desarrollada por Michael Jhonny Santana Montesdeoca, previa la obtención del título de Ingeniero en Informática, de acuerdo al REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

……

ING. MARLON R. NAVIA MENDOZA, MG.

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han APROBADO la tesis RED INALÁMBRICA DE BANDA ANCHA CON SEGURIDAD PERIMETRAL EN LAS ÁREAS URBANAS Y RURALES DEL CANTÓN TOSAGUA, que ha sido propuesta, desarrollada y sustentada por Michael Jhonny Santana Montesdeoca , previa la obtención del título de Ingeniero en Informática, de acuerdo al REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

…… ……

ING. JOSE G. INTRIAGO CEDENO, MG — **MIEMBRO**

ING. R. JOFFRE MOREIRA PICO, MG — **MIEMBRO**

……

ING. LUIS C. CEDEÑO VALAREZO, MG

PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que me dio la oportunidad de obtener una educación superior de calidad y en la cual he forjado mis conocimientos profesionales día a día;

Al Ing. Cesar Moreira por guiarme y brindarme el apoyo constante para terminar con éxito mi tesis, al Ing. Leonardo Sánchez Lucas por permitirme realizar este trabajo en el Gobierno Autónomo Descentralizado Municipal del cantón Tosagua y por su apoyo total en las actividades realizadas, al Ing. Marlon Navia por sus tutorías que contribuyeron a la finalización de mi trabajo y las demás personas del GAD MUNICIPAL que de una u otra manera hicieron posible la finalización de esta investigación.

……..

MICHAEL J. SANTANA MONTESDEOCA

DEDICATORIA

A Dios, por darme la dicha de tener vida y salud, fuerza en cada instante difícil que tuve para cumplir mis objetivos, y por su infinito amor.

A mi madre, por ser un ejemplo para mí, que a pesar de que no tuvo a mi padre que la apoyara supo salir adelante dándome como lección que en la vida hay que luchar para conseguir nuestros sueños y por muy difícil que sea el camino tenemos que seguir adelante.

A mi abuela, por inspirarme amor para realizar cada actividad porque como ella dice si alguien no hace algo con amor, nunca será feliz.

……..

MICHAEL J. SANTANA MONTESDEOCA

CONTENIDO

CONTENIDO DE CUADROS Y FIGURAS

RESUMEN

El objetivo principal de la implementación de la red inalámbrica de banda ancha con seguridad perimetral en las áreas urbanas y rurales del cantón Tosagua, es brindar el servicio de internet gratuito a los lugares beneficiados, donde los habitantes puedan acceder con facilidad a los servicios que ofrece la red de área mundial, evitando gastos a los comuneros ya sea por el coste del servicio o por transporte. Para llevar a cabo este trabajo se utilizó la metodología de cascada utilizando un orden secuencial en cada una de las actividades. Comenzando con visitas en los lugares beneficiados con el fin de determinar los requerimientos técnicos para el despliegue de la red, así mismo entrevistas al Director del Departamento de Tecnología del GADM de Tosagua para observar la infraestructura tecnológica con la que contaba la dependencia. Una vez que se recopilo la información necesaria, se diseñó la topología de la red inalámbrica, además se utilizó el software Radio Móvil para comprobar la factibilidad de los enlaces, así como la ubicación estratégica de los equipos. Luego se procedió a la instalación y configuración de los equipos inalámbricos en los lugares establecidos, también se determinó la solución firewall para proveer de seguridad perimetral a la red, siguiendo con la instalación y configuración de la distribución PfSense. Una vez terminada la instalación de los equipos y la implementación del firewall, se efectuaron pruebas para corroborar el buen funcionamiento de la infraestructura, donde se pudo evidenciar el cumplimiento de los objetivos planteados.

PALABRAS CLAVES

Acceso a internet, wifi, firewall, seguridad de red, vulnerabilidad inalámbrica.

ABSTRACT

The main objective of the implementation of the wireless broadband network perimeter security in urban and rural areas of the canton Tosagua is providing free internet service to the beneficiaries places where people can have easy access to services that the global area network provides, avoiding expenses such as; cost of service or transport. To carry out this thesis waterfall methodology was used using a sequential order in each of the activities. This process started visiting the places where the beneficiaries live in order to determine the technical requirements for the deployment of the network, observation was made through some interviews to the Director of Technology Department of Tosagua GADM as well as the technological infrastructure that. Once the necessary information is compiled, the wireless network topology was designed, in addition Mobile Radio software was used to check the feasibility of the links and the strategic location of the equipment. He proceeded to the installation and configuration of wireless devices in established places, the firewall solution was also determined to provide perimeter security to the network, following the installation and configuration of pfSense distribution. After the installation of equipment and the implementation of the firewall, tests were conducted to confirm the proper functioning of the infrastructure which could demonstrate compliance with the objectives.

KEY WORDS

Internet access, wifi, firewall, network security, wireless vulnerability.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

En la actualidad un alto porcentaje de la población a nivel mundial se encuentra interconectada a través del internet, lo que permite estar en constante comunicación, acortando las distancias, posibilitando realizar tareas y transacciones en segundos.

En el Ecuador el uso del internet ha contribuido a aumentar la conexión a fuentes de información, mejorando la comunicación en zonas rurales y urbanas a nivel nacional, lo que ocasiona un impacto positivo a nivel económico, social y tecnológico. Sin embargo, la provincia de Manabí tiene uno de los porcentajes más bajos en relación al acceso a la tecnología de información y comunicación con un 29,5%, según datos del INEC correspondientes al año 2013 (INEC, 2013).

El Cantón Tosagua cuenta con zonas urbanas y rurales, con una población de 10751 y 17423 habitantes respectivamente según datos del INEC (INEC, 2010). No obstante, estas zonas no cuentan con una completa cobertura del servicio de internet a nivel domiciliar, y en las áreas donde hay acceso este suele tener un costo.

La carencia del servicio de internet gratuito, sobre todo en la zona rural del cantón Tosagua, incide en los aspectos académicos y laborales debido a que en la actualidad es fundamental estar en constante comunicación y tener disponibilidad de fuentes primarias de información, lo que aporta al desarrollo personal y social. Esta carencia afecta, entre otros grupos, a la población estudiantil, que deben trasladarse desde sus domicilios a lugares donde se cuente con el acceso a internet para poder acceder a información académica, a personas que por motivos de trabajo deban movilizarse hacia estos sitios y

necesiten comunicarse, a pequeños empresarios que quieran promocionar sus productos a través de la web, y en general a todos quienes necesiten de acceder a estos servicios y no puedan, ya sea por motivos económicos o logísticos.

Por todo esto se evidencia la necesidad de implementar una infraestructura tecnológica que permita a la población tosagüense facilidad para el acceso a internet, sin descuidar la seguridad en cada una de las comunicaciones realizadas por los usuarios finales.

El aspecto de seguridad informática es muy importante y ha tenido mucha relevancia en los últimos años, sobre todo por el tema de las amenazas a la privacidad de la información. No solo se debe tomar en cuenta el control de acceso, para tener un registro de quién ingresa a la red y con qué fin, sino también los mecanismos que prevengan los posibles ataques desde dentro de la red.

Debido a estos problemas el autor de este proyecto se plantea la siguiente interrogante:

¿De qué manera se podrá facilitar el acceso a internet en las áreas urbanas y rurales del cantón Tosagua, tomando en cuenta aspectos de seguridad?

1.2. JUSTIFICACIÓN

A nivel mundial el acceso a internet ha contribuido con el desarrollo de muchas instituciones, pueblos, naciones; el tener al alcance las tecnologías de información es una manera con la que se puede informar de forma inmediata y oportuna. En el cantón Tosagua provincia de Manabí se hace indispensable implementar redes que permitan acceder a todos los beneficios que proporciona una red mundial como el internet, ofreciendo mecanismos de seguridad, erradicando la brecha digital y fomentando el uso de las tecnologías de información y comunicación.

Por las razones mencionadas anteriormente se ha considerado que existe la necesidad de implementar zonas wifi para permitir el acceso a los servicios de internet gratuito que el gobierno autónomo descentralizado municipal desea llevar a cabo, debido a que en la actualidad no existe este servicio en el cantón. La dotación de la red inalámbrica de banda ancha ayudará a los habitantes del cantón Tosagua acceder de forma más fácil a los servicios de Internet, evitando gastos asociados a los ciudadanos que se les beneficiaría con el servicio. Este proyecto de tesis en lo social beneficiará a todos los habitantes de las zonas rurales y urbanas del cantón donde permitirá acceder a un medio global de comunicación.

El proyecto de tesis se justifica en lo legal por lo estipulado en el Art. 8 literal h de la Ley Orgánica de Educación Superior y su Reglamento, teniendo como fines contribuir en el desarrollo local y nacional de manera permanente, a través del trabajo comunitario o extensión universitaria (Asamblea Nacional, 2010).

El Plan Nacional del Buen Vivir en su objetivo 11.3, literal C, indica que se debe “Impulsar la calidad, la seguridad y la cobertura en la prestación de servicios públicos, a través del uso de las telecomunicaciones y de las TIC; especialmente para promover el acceso a servicios financieros, asistencia técnica para la

producción, educación y salud". Con esta implementación se estará contribuyendo a la consecución de este objetivo (SENPLADES, 2013).

En el reglamento de tesis de grado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López en su artículo 2 enuncia que: Todo tema de tesis de grado estará relacionado con las líneas de investigación de la carrera del postulante, enmarcado en las áreas y prioridades de investigación establecidas por la ESPAM MFL en concordancia con el Plan Nacional para el Buen Vivir (ESPAM MFL, 2012).

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar una red inalámbrica de banda ancha con seguridad perimetral para brindar servicio comunitario de internet en las áreas urbanas y rurales del cantón Tosagua.

1.3.2. OBJETIVOS ESPECÍFICOS

- Identificar los requerimientos técnicos en las zonas beneficiadas para el despliegue de la red.
- Diseñar la topología de Red Inalámbrica adecuada de acuerdo a los requerimientos.
- Implementar los diferentes enlaces inalámbricos y puntos de accesos para las zonas WIFI con su respectiva configuración.
- Configurar el servidor Firewall que concentra toda la seguridad perimetral y el respectivo control de acceso a los usuarios finales.
- Efectuar pruebas para corroborar el buen funcionamiento de la red.

1.3.3. IDEA A DEFENDER

- ✓ La implementación de una red inalámbrica de banda ancha en las áreas urbanas y rurales del cantón Tosagua permitirá a los habitantes utilizar un servicio comunitario de internet seguro.

CAPÍTULO II. MARCO TEÓRICO

2.1. REDES DE COMPUTADORAS

2.1.1. INTRODUCCIÓN A LAS REDES DE COMPUTADORAS

En este sentido, Tanenbaum y Wetherall (2012) refieren que en cada uno de los tres últimos siglos ha estado dominado por una nueva tecnología o invento. El siglo XVIII fue el auge de los grandes sistemas mecánicos que impulsaron la Revolución Industrial. El siglo XIX fue la era de las máquinas de vapor. Durante el siglo XX, la tecnología principal fue la recopilación, procesamiento y distribución de información. Entre otros avances que se dieron en este siglo fue la instalación de las redes telefónicas a nivel mundial, la creación de la radio y la televisión, el nacimiento y crecimiento sin precedentes de la computación, el lanzamiento de satélites de comunicaciones y, desde luego, internet.

De la misma manera Tanenbaum y Wetheral (2012) indican que la fusión entre las computadoras y las comunicaciones ha tenido una gran influencia en relación a la forma en que se organizan los sistemas de cómputo. El concepto una vez dominante del "centro de cómputo" como un cuarto con una súper computadora a la que se le llevaba trabajo para procesarlo es ahora totalmente obsoleto (aunque los datacenters que cuentan con centenares de servidores de Internet se están volviendo normales). El viejo modelo de una única computadora para atender todas las necesidades computacionales de la empresa se ha cambiado por un modelo en el cual varias computadoras separadas pero interconectadas realizan el trabajo. A estos sistemas se les conoce como redes de computadoras.

Por otra parte Dordoigne (2015) puntualiza que una red es un medio de comunicación que permite a personas compartir información, servicios, entre otros. La tecnología de las redes informáticas contiene herramientas que permiten a las computadoras compartir recursos y datos.

2.1.2. USO DE LAS REDES DE COMPUTADORAS

2.1.2.1. APLICACIONES DOMÉSTICAS

Tanenbaum y Wetherall (2012) indican que el acceso a internet ofrece a los usuarios domésticos conectividad a las computadoras en otros lugares del mundo. Al igual que en las organizaciones, los usuarios pueden acceder a información, comunicarse con otros usuarios y adquirir productos y servicios mediante lo que se denomina comercio electrónico. Ahora uno de los principales beneficios se lo obtiene al momento conectarse fuera del hogar.

2.1.2.2. TEMAS SOCIALES

Las observaciones de Tanenbaum y Wetherall (2012) revelan que las redes de computadoras permiten a los usuarios subir y ver el contenido en formas que no hubiera sido posible lograr antes. Pero como todo tema tiene su lado negativo, y esta posibilidad trae consigo muchas cuestiones sociales, políticas y éticas sin resolver.

Las redes sociales, los tableros de mensajes, los sitios de compartición de contenido y varias aplicaciones más, permiten a las personas compartir sus formas de pensar con usuarios de pensamientos similares o a veces no tan de acuerdo. Mientras que los temas estén restringidos a cuestiones técnicas o aficiones como la jardinería, no surgirán muchas dificultades.

2.1.3. TIPOS DE REDES

2.1.3.1. RED DE ÁREA LOCAL

Abad (2012) hace referencia que la red de área local (LAN, Local Area Network) es la conglomeración de elementos físicos y lógicos que permiten que exista conexión entre dispositivos en una área privada y restringida, por lo general un área pequeña.

Tanenbaum y Wetherall (2012) son del criterio que las redes de área local, generalmente llamadas LAN (Local Area Networks), son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. Cuando las empresas utilizan redes LAN se les conoce como redes empresariales.

2.1.3.2. REDES DE ÁREA METROPOLITANA

Tanenbaum y Wetherall (2012) indican que una red de área metropolitana (MAN, Metropolitan Area Network) es una red con el objetivo de cubrir una ciudad entera. McHoes y Flynn (2011) la definen como una configuración que genera un área más amplia que una LAN, que puede ser desde varias manzanas hasta una ciudad entera pero sin exceder un contorno de 100 kilómetros. Una red de área metropolitana puede ser propiedad y ser operada por una sola organización y suele ser usada por una gran cantidad personas y organizaciones.

2.1.3.3. REDES DE ÁREA AMPLIA

Tanenbaum y Wetherall (2012) son del criterio que una Red de Área Amplia, o WAN (Wide Area Network), abarca una gran área geográfica, generalmente un país o continente. Un ejemplo de una red de área amplia sería una empresa multinacional donde cada una de sus sucursales se encuentren conectadas desde distintos países o ciudades.

Por otro lado, Abad (2012) considera que las transmisiones en una WAN se realizan a través de líneas públicas. La capacidad de transmisión de estas redes suele ser menor a las redes de área local. Además, son utilizadas por muchos usuarios a la vez, lo que exige un acuerdo en los modos de transmisión y en las normas de interconexión a la red.

2.1.4. MEDIOS DE REFERENCIA

2.1.4.1. MODELO DE REFERENCIA OSI

Carballeiro (2012) hace referencia que el modelo de referencia OSI (Open System Interconnection, en español: Interconexión de Sistemas Abiertos), creado en 1984 por la ISO (International Organization for Standardization) nació de la necesidad de poder comunicarse y trabajar de forma conjunta con las diferentes redes que existían en tiempos anteriores.

Las investigaciones de McHoes y Flynn (2011) manifiestan que este modelo constituye la base para conectar sistemas abiertos para procesamiento de aplicaciones distribuidas. La palabra “abiertos” significa que dos sistemas cualquiera que se ajusten al modelo de referencia y las normas relacionadas puedan conectarse, independiente del vendedor.

2.1.4.2. MODELO DE REFERENCIA TCP/IP

Salvetti (2011) define al modelo de referencia TCP/IP como el estándar abierto de Internet, que hace posible la comunicación entre computadoras remotas. TCP/IP significa Protocolo de control de transmisión/Protocolo Internet. De acuerdo con McHoes y Flynn (2011) el modelo TCP/IP organiza un sistema de comunicación con tres componentes principales: procesos, anfitriones y redes. Los procesos se ejecutan en anfitriones, que a menudo pueden atender múltiples procesos simultáneos que se definen como unidades primarias que necesitan comunicarse. Estos procesos se comunican a través de redes a las que están conectados los anfitriones. Este modelo consta de las siguientes capas:

2.1.4.2.1. CAPA DE ACCESO A REDES

Los protocolos en esta capa proporcionan acceso a una red de comunicación. Algunas de las funciones aquí son el control de flujo, control de errores entre anfitriones, seguridad e implementación de seguridad.

2.1.4.2.2. CAPA DE INTERNET

Específicamente el mecanismo que efectúa son funciones de encaminamiento. En consecuencia, este protocolo suele implementarse dentro de puertas de enlace y anfitriones.

2.1.4.2.3. CAPA ANFITRIÓN-ANFITRIÓN

Atiende mecanismos para transferir datos entre dos procesos en computadoras anfitriones diferentes. Entre servicios proporcionados también incluyen verificación de errores, control de flujo y una capacidad para manipular señales de control de conexión.

2.1.4.2.4. CAPA DE PROCESO/APLICACIÓN

Incluye protocolos para compartición de recursos de computadoras a computadora y de terminal a computadora de acceso remoto. Ejemplos específicos de normas establecidas por el DoD para esta capa son el Protocolo de Transferencia de Archivo (FTP), Protocolo Simple de Transferencia de Correo (CMTP) entre otros.

2.1.5 MEDIOS DE TRANSMISIÓN

Se lo puede definir como el soporte físico que permite el transporte de la información por lo cual es una parte importante en la comunicación de datos. La calidad de la transmisión dependerá de sus características físicas, mecánicas, eléctricas, etc (Abad, 2012).

2.1.5.1. MEDIOS DE TRANSMISIÓN GUIADOS

Tanenbaum y Wetherall (2012) indican, que se pueden utilizar varios medios físicos para la transmisión real. Cada medio tiene sus características en términos de ancho de banda, retardo, costo y facilidad de instalación y mantenimiento. Los medios guiados son como por ejemplo el cable de cobre y la fibra óptica.

2.1.5.1.1. PAR TRENZADO

Katz (2013) define al Par Trenzado como dos alambres de cobre recubiertos por una protección plástica. Estos alambres recubiertos se encuentran trenzados entre sí, enroscados uno al otro. Cada cable tiene su propia carga eléctrica, que genera interferencia, y al trenzar un cable con el otro, cada cable anula la inducción eléctrica de la contraparte. Al trenzar los cables, se logra disminuir significativamente el nivel de interferencia entre ellos, lo cual aumenta la calidad de transmisión.

2.1.5.1.2. FIBRA ÓPTICA

Abad (2012) es del criterio que la fibra óptica posibilita la transmisión de señales luminosas. Por lo general esta suele ser de vidrio u otros materiales plásticos, es insensible a interrupciones electromagnéticas externas. La luz ambiental es una combinación de señales de muchas frecuencias diferentes, por lo que no es una apropiada fuente de señal portadora luminosa para la transmisión de datos.

2.1.5.2. MEDIOS DE TRANSMISIÓN NO GUIADOS

Butler (2013) hace mención que los medios no guiados, o también llamados medios de comunicación sin cable, utilizan ondas electromagnéticas para transmitir señales a través de grandes distancias. Desde el punto de vista de los usuarios, las conexiones inalámbricas no son diferentes de cualquier otra conexión de red: el navegador web, el correo electrónico y otras aplicaciones funcionan como el usuario final lo espera. Pero las ondas de radio tienen algunas propiedades impensadas en relación a una red cableada Ethernet.

2.1.5.2.1. RADIOTRANSMISIÓN

Tanenbaum y Wetherall (2012) hacen referencia que las ondas de radiofrecuencia (RF) se pueden generar fácilmente, pueden recorrer grandes distancias y penetrar edificios sin dificultad, por lo cual son muy utilizados en la comunicación, ya sea en interiores como en exteriores.

2.1.5.2.2. MICROONDAS

Tanenbaum y Wetherall (2012) definen Microondas como ondas que viajan en línea recta y en consecuencia, se pueden enfocar en un espacio estrecho por encima de los 100 MHz. Estas ondas concentran toda la energía en un pequeño haz utilizando una antena parabólica se obtiene una relación señal-ruido mucho más alta, pero las antenas transmisora y receptora deben estar alineadas con mucha precisión.

2.1.5.2.3. ONDAS DE LUZ

Tanenbaum y Wetherall (2012) refieren que la señalización óptica sin guías, también se la conoce como óptica de espacio libre, la cual se la utilizado durante siglos. La señalización óptica mediante láser es naturalmente unidireccional, por lo que cada punto necesita su propio láser y su propio fotodetector. Este medio ofrece un ancho de banda muy alto a un costo muy bajo, además de ser parcialmente seguro debido a que es complicado intervenir un haz tan estrecho.

2.1.6. INTERNET

2.1.6.1. DEFINICIÓN DEL INTERNET

Madrid (2010) define al internet como una red de redes de ordenadores que comparten datos y recursos. Existe una conexión de redes a nivel mundial que permite a los ordenadores (y a las personas) comunicarse entre sí en cualquier parte del mundo. Esto permite tener acceso a información y personas que de otra forma no sería posible.

Kuschnaroff, *et al.,* (2012) puede afirmar que el Internet es una herramienta de investigación y de información fenomenal. Se ha entrado en la vida de personas en una forma extremadamente rápida, ofreciendo una sensación de libertad, y de descubrimientos. Hoy en día, es una herramienta de trabajo de gran alcance.

Proporciona una comunicación rápida y ayuda en la reducción de costes. Sin embargo, también crea inseguridad e incertidumbre.

2.1.6.2. INTERNET DE LAS COSAS

Sosa y Godoy (2014) son del criterio que la IoT (Internet of Things) une los objetos del mundo real con el mundo virtual, para así facilitar la conectividad en cualquier momento y en cualquier lugar para cualquier cosa, no sólo considerando a las personas. Se refiere a un mundo donde los objetos físicos y los seres, los datos y los entornos virtuales; estarían todos ellos interrelacionados entre sí temporal y espacialmente.

La experimentación en la vida real ha evolucionado tan rápidamente que hoy se interactúa con el mundo físico llevando a “Internet” al escenario elegido. Esto se realiza generalmente instalando transceptores en distintos elementos de la vida cotidiana, permitiendo un nuevo modelo de comunicación, ya no solamente entre personas y cosas, sino también entre las cosas entre sí.

2.1.7. SERVICIOS DE REDES

Katz (2013) menciona que los servicios de red proporcionan la capacidad de ampliar los alcances de la productividad en un entorno informático. Permitiendo realizar diversas tareas dentro de la que se encuentra operativa.

2.1.7.1. NAT

El NAT (Network Address Translation) es la metodología que permite tener muchos equipos conectados a internet mediante una única identificación pública. El NAT es un servicio intermedio entre los direccionamientos públicos y privados, proveyendo comunicaciones libres y semitransparentes entre dichos direccionamientos en todo el mundo. Este identifica a todas las máquinas de una red y las equipará de manera independiente hacia otras redes mediante una única IP pública (Katz, 2013).

2.1.7.2. DNS

Katz (2013) señala que el DNS (Domain Naming Service) es el encargado de proveer la resolución de nombres de equipos en cualquier red. Cada equipo en la red posee su propia identificación (dirección IP), esta identificación es única y no puede ser utilizada por dos equipos, estas identificaciones pueden ser difíciles de recordar e incomodas de administrar. Sin embargo, este servicio permite que cada equipo pueda ser identificado de manera única por un nombre por ejemplo www.google.com.

2.1.7.3 DHCP

Katz (2013) es del criterio que el DHCP (Dynamic Host Configuration Protocol) es un servicio que se encarga de proporcionar configuraciones de conectividad a las computadoras que se conectan a una red, de una manera automática, sencilla, remota y masiva. Provee facilidad en el uso de recursos de red, permitiendo que un usuario inexperto pueda recibir conectividad con solo conectarse físicamente a la red.

2.1.7.4. PING

Según Butler (2013) determina que puede considerarse como una herramienta de monitoreo puntual activa, puesto que crea tráfico sondeando a una máquina determinada. La mayoría los sistemas operativos incluyen una versión de la utilidad ping. Utiliza paquetes ICMP para intentar contactar un servidor fijado y le comunica cuánto tiempo lleva conseguir una respuesta.

2.1.8. SOFTWARE DE DIAGRAMACIÓN

Se lo puede definir como un tipo de software que su principal función es la de modelar, representar y visualizar información. Entre otros usos, permite la maquetación también llamada diagramación de flujos de datos, flujos de trabajo, diseños lógicos de redes, la arquitectura de software y organigramas.

2.1.8.1. SMART DRAW

SmartDraw es un software que permite comunicarse visualmente con gráficos de gran alcance como diagramas de flujo, organigramas, mapas de la mente, y mucho más el uso de los controles automáticos rápidos (SmartDraw, 2015).

2.2. REDES INALÁMBRICAS

De acuerdo con Cruz, *et al.,* (2013) determina que las comunicaciones inalámbricas en sus diferentes variantes están tomando cada vez más auge en la vida de los diferentes usuarios y con ello la necesidad de soportar las mismas aplicaciones que en las redes cableadas. Por otra parte menciona Köbel, *et al.,* (2012) se caracterizan por su movilidad pues permiten comunicación inalámbrica a los equipos, entre otros aspectos que garantizan flexibilidad.

Butler (2013) considera que las comunicaciones inalámbricas hacen uso de las ondas electromagnéticas para enviar señales a través de largas distancias. Desde la apariencia del usuario, las conexiones inalámbricas no son diferentes de cualquier otra conexión de red: el navegador web, la mensajería instantánea y otras aplicaciones funcionan como lo espera. Pero las ondas de radio tienen algunas propiedades inesperadas en comparación con una red cableada Ethernet.

2.2.1. TIPO DE REDES INALÁMBRICAS

2.2.1.1. WPAN

Amiri, *et al.,* (2013) son del criterio, Wireless Personal Area Network (WPAN), en español Red Inalámbrica de Área Personal o red de área personal inalámbrica, es en comparación con las redes inalámbricas de área local (WLAN), una red que se puede utilizar para proporcionar velocidades de datos más altas, pero con menor alcance.

2.2.1.2. WLAN

McHoes y Flynn (2011) consideran que es una red de área local que usa tecnología inalámbrica para conectar computadores o estaciones de trabajo dentro del alcance de la red. Debe tomarse en cuenta que en general una red de área local inalámbrica presenta inseguridades debido a su estructura abierta y el problema inherente de mantener fuera a intrusos no autorizados.

2.2.1.3. WMAN

Alcaraz, *et al.,* (2013) manifiestan que WMAN: Wireless Metropolitan Area Network en español Red Inalámbrica de área metropolitana básicamente está orientado al estándar IEEE 802.16, operando primordialmente en dos capas del modelo OSI (OSI: Open System Interconnection), la capa física (PHY: Physical) y la capa de control de acceso al medio (MAC: Medium Access Control).

2.2.1.4. WWAN

WWAN (Wireless Wide Area Network) en español Red Inalmbrica de Area Extensa, son típicamente redes celulares para telefonía móvil y transmisión de datos. Destacadas tecnologías asociadas son GSM (telefonía móvil 2G) y UMTS (telefonía móvil 3G) (IDEA, 2008).

2.2.2. ESTÁNDARES DE REDES INALAMBRICAS 802.11

En concordancia con Pérez y Galván (2006) cuando las redes inalámbricas empezaron a crecer se presentó el problema de incompatibilidad entre algunas de ellas. Ante dicho problema, se empezó ver la manera de solucionar dicha incompatibilidad y se decidió crear un nuevo estándar para poder lograr una comunicación sin problemas entre las redes inalámbricas. Varios organismos trabajaron en este asunto: la IEEE (Institute of Electrical and Electronics Engineers) y ETSI (European Telecommunications Standards Institute) para lograr el estándar 802.11 el cual fue aceptado en 1997.

Grote, *et al.,* (2007) consideran que el estándar IEEE 802.11 fue desarrollado para proveer conectividad a terminales móviles, como los de las redes de telefonía celular y de las redes de acceso local inalámbricas (WLAN: Wireless Local Access Network). Astaiza, *et al.,* (2013) señala que en años recientes, se ha generado mucho interés en el diseño de redes inalámbricas para las redes de acceso dadas las bondades que ellas presentan, en particular se puede apreciar que el estándar 802.11 ha presentado una gran aceptación y por consiguiente es fundamental el estudio detallado de su comportamiento.

2.2.2.1. 802.11

Bengochea (2011) señala que el estándar 802.11 en sus inicios estableció dos técnicas de transmisión para radiofrecuencia: FHSS y DSSS, y una especificación de transmisión infrarroja que no ha sido desarrollada. Por otra parte, Rincón y Cano (2007) consideran que el protocolo IEEE 802.11 es un estándar que define los dos niveles más bajos de la arquitectura OSI (capas física y de enlace).

Cázares, *et al.,* (2012) indica que el protocolo IEEE 802.11 es un estándar de comunicación inalámbrica y es orientado a la implementación de aplicaciones de adquisición de datos, medición y control de procesos, así como aplicaciones para compartir datos multimedia.

2.2.2.2. 802.11B

Bengochea (2011) es del criterio que la contribución de 802.11b fue el aumento de las tasas de transmisión de 5.5Mbps y 11Mbps. Para llevar a cabo esto, DSSS fue la técnica seleccionada para la capa física debido a que FHSS no puede trabajar con tasas de transmisión mayores a 2Mbps. 802.11b puede interoperar con sistemas 802.11 DSSS, pero no puede hacerlo con sistemas 802.11 FHSS.

2.2.2.3. 802.11G

El estándar 802.11g, conocido como ERP-OFDM, llega a tasas de transmisión de 54Mbps, utilizando técnicas de modulación provenientes de 802.11a. Además, al uso ERP-OFDM, el estándar 802.11g puede utilizar un modo de operación llamado ERP-DSSS, que básicamente establece compatibilidad con 802.11b (HR-DSSS) (Bengochea, 2011).

2.2.2.4. 802.11N

Bengochea (2011) hace referencia que este estándar se basa en la utilización de varias antenas de forma simultánea, teniendo hasta un máximo de cuatro para recepción y cuatro para transmisión, esta característica se le conoce como MIMO (Multiple Input Multiple Output). Tiene varios modos de operación, por lo que es compatible con 802.11a y 802.11g. Teóricamente con la utilización de esta tecnología se pueden llegar a tasas de transmisión de 600Mbps.

2.2.3. TECNOLOGÍAS

2.2.3.1. WIFI

Hidalgo (2013) considera que WIFI (Wireless Fidelity) en español Fidelidad inalámbrica, es utilizada genéricamente cuando se habla a cualquier red en el estándar 802.11, tanto 802.11b, 802.11a, banda dual, entre otras. Moreira (2011) es del criterio que en un sentido literal WiFi no significa nada, es una marca comercial que también se utiliza para designar a las tecnologías inalámbricas. Pero es cada vez más sinónimo de una sociedad pautada por el avance de las nuevas tecnologías de la información y comunicación (TICs), por la lógica mercantil, y por las relaciones (o conexiones) más amplias y fluidas.

2.2.3.2. AIRMAX

AirMax permite a cada cliente enviar y recibir datos utilizando intervalos de tiempo pre-programados designado por un controlador inteligente AP. Este método de "intervalo de tiempo" elimina las colisiones de nodos ocultos y

maximiza la eficiencia del tiempo de emisión. Proporciona muchas magnitudes de mejoras en el rendimiento de latencia, rendimiento y escalabilidad en comparación con todos los demás sistemas al aire libre en su clase (UBNT, 2013).

2.2.4. FÍSICA DE RADIO

2.2.4.1. DEFINICIÓN DE UNA ONDA

Butler (2013) señala que es un medio o un objeto, que está oscilando de forma reiterada con un determinado número de ciclos por unidad de tiempo. Cuando esas oscilaciones recorren (esto es, cuando no están presas a un lugar) es decir ondas propagándose en el espacio. Una onda tiene cierta velocidad, frecuencia y longitud de onda.

2.2.4.2. FUERZAS ELECTROMAGNÉTICAS

Los resultados de Hidalgo (2013) confirman que las fuerzas electromagnéticas son fuerzas entre cargas y corrientes eléctricas. Sabiendo que las fuerzas eléctricas son la fuerza entre cargas eléctricas y las fuerzas magnéticas es la fuerza entre corrientes eléctricas.

2.2.4.3. POLARIZACIÓN

Las investigaciones de Butler (2013) demuestran que la polarización describe la dirección del vector del campo eléctrico. En una antena bipolar alineada verticalmente (el trozo de alambre recto), los electrones sólo se mueven de arriba a abajo, no hacia los lados (porque no hay lugar hacia donde moverse) y, por consiguiente, los campos eléctricos sólo apuntan hacia arriba o hacia abajo verticalmente.

2.2.4.4. EL ESPECTRO ELECTROMAGNÉTICO

De acuerdo con las valoraciones Hidalgo (2013), las ondas electromagnéticas abarcan un amplio rango de frecuencias y correspondientemente, de longitudes

de onda nombrado espectro electromagnético. La parte del espectro más conocido por los seres humanos es probablemente la luz, la porción visible del espectro electromagnético.

2.2.4.5. ANCHO DE BANDA

En este sentido, Butler (2013) señala que el ancho de banda es puramente una medida de rango de frecuencia. Si un equipo usa el rango de 2.56 GHz a 2.62 GHz, el ancho de banda sería 0.08 GHz (es decir 80 MHz). El término ancho de banda es comúnmente utilizado para algo que se debería llamar tasa de transmisión de datos, por ejemplo “mi conexión a Internet tiene 2 Mbps de ancho de banda”, lo que significa que ésta puede trasmitir datos a 2 megabits por segundo.

2.2.4.6. FRECUENCIAS Y CANALES

Hidalgo (2013) es del criterio que la banda 2,4 GHz en el estándar 802.11b/g, el espectro está dividido en partes iguales distribuidas sobre la banda en canales individuales. Guevara y Serna (2013) hacen referencia que la comunicación WiFi se establece a través de 14 canales y cada uno ocupa 22MHz de ancho de banda, pero están separados sólo por 5 MHz. El cuadro 2.1 muestra los canales inalámbricos, con sus respectivas frecuencias, para la banda de 2.4GHz.

Cuadro 2.1. Canales IEEE 802.11b/g Wifi

Banda	Frecuencia	Canal
2.4GHz	2412.0 MHz	1
2.4GHz	2417.0 MHz	2
2.4GHz	2422.0 MHz	3
2.4GHz	2427.0 MHz	4
2.4GHz	2432.0 MHz	5
2.4GHz	2437.0 MHz	6

2.4GHz	2442.0 MHz	7
2.4GHz	2447.0 MHz	8
2.4GHz	2452.0 MHz	9
2.4GHz	2457.0 MHz	10
2.4GHz	2462.0 MHz	11
2.4GHz	2467.0 MHz	12
2.4GHz	2472.0 MHz	13
2.4GHz	2484.0 MHz	14

2.2.4.7. COMPORTAMIENTO DE LAS ONDAS DE RADIO

Las investigaciones de Butler (2013) demuestran que algunas reglas simples pueden ser de gran ayuda para la implementación de redes inalámbricas:

Las ondas más largas tienen mayor alcance

Las ondas con longitudes de onda más largas tienden a viajar más lejos que las que tienen longitudes de onda más cortas.

Las ondas más largas rodean los obstáculos

Cuanto más larga la longitud de onda, mejor viaja a través y alrededor de obstáculos.

Las ondas más cortas pueden transmitir más datos

Cuanto más rápida sea la oscilación de la onda, mayor cantidad de información puede transportar.

2.2.4.8. ABSORCIÓN

Hidalgo (2013) hace referencia que cuando las ondas electromagnéticas atraviesan algún obstáculo, por lo general se debilitan o atenúan, la cantidad de potencia perdida depende de la frecuencia y, lógicamente, del material. Para microondas, los dos materiales más absorbentes son:

Metal.- Los electrones pueden moverse libremente en los metales, y son capaces de oscilar y por lo tanto absorber la energía de una onda que los atraviesa.

Agua.- Las microondas provocan que las moléculas de agua se agiten, capturando algo de la energía de las ondas.

2.2.4.9. REFLEXIÓN

Los hallazgos de Butler (2013) esclarecen que al igual que la luz visible, las ondas de radio son reflejadas cuando entran en contacto con los objetos apropiados: para las ondas de radio, las principales fuentes de reflexión son el metal y el agua. Las reglas para la reflexión son simples: el ángulo con el cual una onda incurre en una superficie es el mismo ángulo con el cual es desviada.

2.2.4.10. DIFRACCIÓN

Las investigaciones de Hidalgo (2013) demuestran que, difracción es el comportamiento de las ondas cuando, al incidir en un cierto material, dan la impresión de doblarse. Es el efecto de “ondas doblando las esquinas”.

2.2.4.11. INTERFERENCIA

CONATEL y SENATEL (2012) definen, efecto de una energía no deseada resultado a una o varias emisiones, radiaciones, inducciones o sus combinaciones sobre la recepción de un equipo de radiocomunicación, que se presenta como degradación de la calidad, falseamiento o pérdida de la información.

2.2.4.12. LÍNEA VISUAL

Butler (2013) ha indicado, línea visual (también línea de visión, línea de vista), frecuentemente abreviada como LOS (por su sigla en inglés, Line of Sight), es fácil de entender cuando se habla acerca de la luz visible: es decir si se puede ver un punto B desde un punto A, existe línea visual. Dibujar simplemente una

línea desde un lugar A a un lugar B, y si no hay nada en el camino, existe línea visual.

2.2.4.13. ZONA DE FRESNEL

Escudero (2007) define a la Zona de Fresnel como el espacio alrededor del eje que contribuye a la transferencia de potencia desde el transmisor hacia el receptor. Con esto, podemos averiguar cuál debería ser la máxima penetración de un obstáculo en esta zona para contener las pérdidas

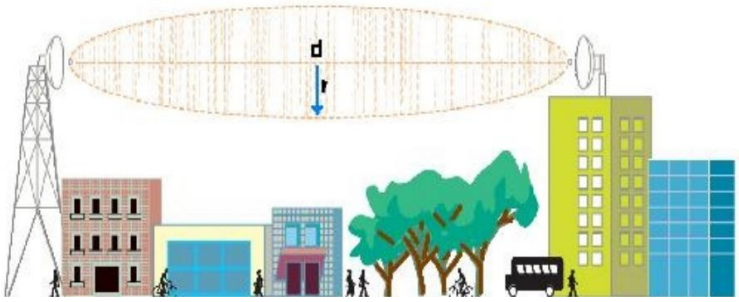


Figura 2.1. Zona de Fresnel

2.2.4.14. POTENCIA

Hidalgo (2013) define Potencia como cualquier onda electromagnética que contiene energía, o potencia y se puede sentir cuando se gusta (o sufre) del calor del sol. La potencia P es de gran importancia para conseguir que los enlaces inalámbricos funcionen: se necesita un mínimo de potencia para que el receptor le dé sentido a la señal.

2.2.4.15. MODULACIÓN

Butler (2013) considera que la modulación es una estrategia para modificar la amplitud, la frecuencia o la fase de la portadora de acuerdo con la información que se quiere transmitir. La información original se recupera en el destino por medio de la correspondiente demodulación de la señal recibida.

2.2.5. MEDIDAS DE GANANCIA

Bengochea (2011) es del criterio, el decibel (dB) resulta una herramienta muy útil que expresa una relación logarítmica entre una salida y una entrada. La ventaja de utilizar decibeles es la facilidad que brinda al realizar operaciones, debido a que las ganancias expresadas en decibeles simplemente se suman o se restan. El uso de estas unidades en el área de comunicaciones es habitual. La mayoría de los documentos técnicos expresan las ganancias con esta medida.

2.2.5.1. DB.

Bengochea (2011) hace referencia, los decibeles son una medida adimensional que expresan una ganancia o pérdida, a partir de un cociente de una potencia de salida y una de entrada. La fórmula para obtener la relación entre dos potencias y expresarla en decibeles se la puede observar en la fórmula 2.1, donde Ps y Pe son la potencia de salida y entrada respectivamente.

$$dB = 10Log\frac{Ps}{Pe} \quad \textbf{[2.1]}$$

2.2.6. TOPOLOGÍAS

2.2.6.1. PUNTO A PUNTO

Butler (2013) es el criterio que los enlaces punto a punto generalmente se usan para conectarse a Internet donde no existe acceso al mismo. Uno de los lados del enlace punto a punto estará conectado a Internet, mientras que el otro utiliza el enlace para acceder a la red de área mundial. Tanenbaum y Wetherall (2012) son de la opinión que en un enlace punto a punto sólo hay un emisor y un receptor.

2.2.6.2. PUNTO A MULTIPUNTO

Carballeiro (2012) considera que el enlace punto a multipunto, sirve para enlazar diferentes puntos remotos hacia un punto central. Consta de un nodo realizando

funciones de transmisor y más de un equipo con la función de receptor. De esta manera se conectan varias redes o computadoras distantes.

2.2.6.3. MULTIPUNTO A MULTIPUNTO

Los resultados de Hidalgo (2013) confirman, multipunto a multipunto, también denominado red ad hoc o en malla (mesh). En este tipo de red no existe un nodo central, cada equipo de la red transporta el tráfico de tantos como sea necesario, y todos se comunican directamente entre sí. El beneficio de este diseño de red es que aún si ninguno de los equipos inalámbricos es alcanzable desde el punto de acceso central, de igual manera pueden comunicarse entre sí.

2.2.7. SIMULADORES

Las investigaciones de López y García (2010) definen que permiten diseñar experimentos, en condiciones controladas, garantizando homogeneidad en las respuestas del sistema y por tanto mayor confianza en los resultados que lance un estudio determinado.

2.2.7.1. RADIO MOBILE

Los resultados de Barbecho (2011) demuestran, es un Software de libre distribución para el cálculo de radio enlaces de larga distancia, usando un modelo de terreno irregular (ITM), y como modelo de propagación en el rango de las frecuencias de 20MHz a 20GHz. Radio Mobile es una herramienta confiable para el análisis de factibilidad de los enlaces inalámbricos y de fácil configuración.

2.3. INFRAESTRUCTURA TECNOLÓGICA

Gómez (2011) es del criterio, se entiende por infraestructura tecnológica al grupo de todos los elementos tecnológicos hardware y software: servidores, computadores, portátiles, impresoras, switches, routers, firewall, escaners, cableado estructurado, software informático, equipos de comunicación, internet,

entre otros. Munévar (2013) considera, conjunto de equipos de hardware y de software que combinados operacionalmente brindan el soporte al flujo de la información.

2.3.1. RADIO BASES INALÁMBRICAS

Según las investigaciones de Hidalgo (2013) consideran que los radios de microondas generan señales usando como medio de transmisión la atmósfera terrestre, entre los equipos que hacen la función de transmisores y receptores, con el objetivo de brindar una mejor emisión y recepción, estos equipos por lo general se encuentran en la cima de torres a distancias de entre 25 y 50 metros.

2.3.2. ANTENAS

Suqui (2010) es del criterio, una antena es un elemento importante en un enlace, específicamente cuando este tiene que alcanzar una gran distancia o cubrir un área explícita. Acevedo, *et. al.* (2009) hacen referencia que una antena es la parte de un dispositivo transmisor o receptor con el objetivo de radiar o recibir ondas electromagnéticas, las cuales se propagan a través del espacio

2.3.2.1. ANTENAS OMNIDIRECCIONALES

Los resultados de Bengochea (2011) confirman que la radiación emitida por una antena omnidireccional se asemeja a la forma de una dona, es decir transmiten ondas de 360 grados, pensando que se da en tres dimensiones; las antenas omnidireccionales emiten su energía hacia todas direcciones.

2.3.2.2. ANTENAS SEMIDIRECCIONALES

Bengochea (2011) hace referencia que las antenas semidireccionales, dirigen un gran porcentaje de su energía hacia una dirección específica. La forma generalmente de estas antenas es plana, la mayor parte de su energía es radiada por el lóbulo principal mientras que la energía radiada por los lóbulos traseros es mínima.

2.3.2.3. ANTENAS ALTAMENTE DIRECCIONALES

Bengochea (2011) es del criterio que en las antenas altamente direccionales el patrón de radiación es muy angosto, por este motivo estas permiten crear enlaces punto a punto en grandes distancias (varios kilómetros). Este tipo de antenas son muy sensibles a la alineación; con una mínima variación se puede afectar cuantiosamente su desempeño.

2.3.3. PoE

Hidalgo (2013) señala que el Power Over Ethernet (PoE) cumple la función de alimentar con corriente continua a las bases de radio para su funcionamiento, utiliza los hilos del cable Ethernet que no son utilizados, para la alimentación de los equipos.

2.3.4. TORRES

De acuerdo con las valoraciones de Hidalgo (2013), todas las radios bases requieren de un sitio elevado o torres que le permitan obtener un mayor alcance. El tipo y altura de una torre para telecomunicaciones va liado básicamente a:

- El sistema de telecomunicación a implementar
- El terreno utilizable
- Tipo y cantidad de radios base
- Restricciones en la desplazabilidad de dichas antenas en función del sistema instalado.

2.3.5. CABLEADO

Según las investigaciones de Butler (2013) demuestran que este es un aspecto importante de la implementación de una infraestructura tecnológica, debido a un cableado adecuado va a asegurar una transferencia eficiente de energía y/o datos.

2.3.6. CONECTORES

Los resultados de Butler (2013) confirman que por medio de los conectores el cable puede ser interconectado a un equipo de comunicación o a otro cable según sea el caso.

2.3.6.1. RJ-45

Santiago (2010) es del criterio que la RJ-45, es una interfaz física frecuentemente usada para conectar redes de cables, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack lo que indica que es parte del Código Federal de Regulaciones de Estados Unidos. Este tipo de conector posee ocho "pines" o conexiones eléctricas, que habitualmente se usan como extremos de cables de par trenzado.

2.3.7. ROUTER

Escudero (2007) hace referencia, un router o enrutador permite interconectar varias redes en donde estas deben utilizar el mismo protocolo. Un enrutador trabaja en las 3 primeras capas del modelo OSI y utiliza las direcciones ip de los equipos que toma de la capa de red, las cuales corresponden a un protocolo específico. Este tiene la capacidad de mejorar las rutas recorridas por los paquetes para llegar a su destino utilizando tablas de enrutamiento que se reconstruyen constantemente aumentando su eficiencia.

2.3.8. SWITCH

Dordoigne (2015) considera que es un componente clave en las redes locales, los equipos de trabajo y los servidores están conectados directamente a estos equipos. La gestión de este hardware inteligente la realiza un microcontrolador o incluso un microprocesador. Los conmutadores se dividen en función de su capacidad de tratamiento respecto del modelo OSI. Los de nivel 2 (N2) realizan

operaciones hasta la capa de datos. Los de nivel 3 (N3) pueden trabajar con encabezados de capa 3 (Red).

2.4. SEGURIDAD EN REDES

Los resultados de Bustamante (s.f) confirman que la seguridad en redes implica que es conservar la integridad, disponibilidad, privacidad, control y autenticidad de los datos que interactúan en el computador, a través de instrucciones basadas en una política de seguridad tales que admitan el control de lo adecuado. Katz (2013) es del criterio que hhablar de seguridad de una manera concreta es muy complicado ya que el término en sí, se relaciona con las necesidades y niveles aceptables de cada administrador.

2.4.1. CONFIDENCIALIDAD

De acuerdo con Kurose y Ross (2010) puede concluirse que solo el emisor y el receptor deseado deberán entender el adjunto de los mensajes transmitidos. Puesto que los entrometidos pueden interceptar los mensajes, es definitivamente obligatorio que los mensajes sean cifrados de una u otra manera, con el objetivo que un mensaje interceptado no pueda ser comprendido por el que lo ha interceptado.

2.4.2. AUTENTICACIÓN DEL PUNTO TERMINAL

En relación con Kurose y Ross (2010) puede inferirse que el emisor así como el receptor tienen la obligación de confirmar la identidad del otro durante el proceso de comunicación (confirmar que el otro es de hecho quien dice ser).

2.4.3. INTEGRIDAD DEL MENSAJE

Según Kurose y Ross (2010) se refiere a la confiabilidad de que el contenido de un mensaje entre un emisor y receptor no ha sido modificado durante el proceso de transmisión ni de manera maliciosa ni por accidente alguno.

2.4.4. SEGURIDAD EN REDES INALÁMBRICAS

Cervigón y Ramos (2011) consideran que las redes inalámbricas, además de proveer muchos beneficios, constituyen también un alto punto de riesgo en las mismas. La facilidad de uso y su movilidad han causado que su utilización se incremente en especial cuando se utilizan dispositivos móviles. Sin embargo, el problema de las mismas es que cualquier intruso puede acceder a las ondas de radio, por lo que si la red no está adecuadamente protegida toda la información que circula la misma se hace vulnerable.

2.4.4.1. ATAQUES EN REDES WIFI

De acuerdo con las valoraciones de Balseca (2013) indica que existen dos ataques que son:

Ataques pasivos.- Es cuando algún intruso puede acceder a la información, pero este no realiza ninguna alteración de la misma. Dentro de esta categoría se encuentran dos tipos:

- **Vigilar/Espiar.** Es aquel en el que el atacante espía el contenido de las transmisiones para revelar el contenido de dicha información, se utiliza un aparato inalámbrico y un software denominado Sniffer.
- **Analizar el Tráfico**. Permite al intruso capturar la información transmitida y revelar datos sobre los parámetros de la comunicación, como el ESSID, contraseñas, Direcciones MAC o IP, etc.

Ataques Activos.- Su objetivo principal es tener acceso a la red, estos crean acciones evidentes en la red, por lo que facilitan su descubrimiento pero son dificultosos de prevenir. Se enuncia las actividades más comunes:

- **La Suplantación.** Es una sustracción de identidad que consiste en hacer creer que es un usuario autorizado para acceder a la información.
- **Retransmisión.** El intruso se ubica entre el emisor y el receptor, recibe la información y la retransmite, para evadir ser descubierto.
- **Modificación.** Se basa en alterar mensajes originales agregando o quitando parte del contenido.

- **Denegación de Servicio.** El atacante imposibilita la utilización normal de las transmisiones Wi-Fi. Estos ataques son complicados de evitar y muy fáciles de realizar.

2.4.5. SEGURIDAD EN LA COMUNICACIÓN

2.4.5.1. IPSEC

Al referirse a este aspecto, Kurose y Ross (2010) puntualizan que el protocolo de seguridad IP, más conocido como IPsec, provee seguridad en la capa de red. IPsec provee seguridad a los datagramas IP intercambiados por dos entidades de la capa de red, incluyendo hosts y routers.

Tanenbaum y Wetherall (2012) son del criterio que en el diseño IPsec los servicios principales son confidencialidad, integridad de datos y protección contra ataques de repetición. Este diseño se basa en criptografía de clave simétrica para todos sus servicios, debido a que es imprescindible un alto desempeño.

2.4.5.2. REDES PRIVADAS VIRTUALES

Pellejero *et al.,* (2005) son del criterio que las redes privadas virtuales permiten conectar de una manera segura a las compañías con otras oficinas de su organización, empleados a distancia, personas con móviles, proveedores, entre otros.

Barreto (2013) esclarece, una VPN es, una Red Privada Virtual, que utiliza una tecnología de túnel para transmitir los datos de beneficiarios de un lado a otro de la red del ISP a la que está conectada. La palabra "túnel" significa que los datos están cifrados desde el momento que entran a la VPN hasta el instante en el que salen de ella.

2.4.6. SEGURIDAD PERIMETRAL

Las investigaciones Ramos (2011) esclarecen que es la arquitectura y elementos de red que proveen de seguridad al perímetro de una red interna frente a otra que generalmente es el Internet.

Emperanza (2014) hace referencia que el perímetro se lo considera como el lugar donde la compañía y el dispositivo se encuentran. Sin importar si la organización retiene la infraestructura de los recursos de información, o una parte de ella, en algún punto hay una división entre la red pública y la red privada.

2.4.6.1. FIREWALLS

Bustamante (s.f) es del criterio que básicamente un firewall es una computadora o servidor que se encarga de filtrar el tráfico de información entre dos redes. Kumar *et al.,* (2014) ha indicado que los cortafuegos protegen una red de confianza a partir de una red que no se confía. Se pueden encontrar firewall basados en software o en hardware.

Fabuel (2013) ha indicado, la ubicación tradicional de un cortafuego es el punto de conexión de la red interna de la organización con la red exterior, que habitualmente es el internet; de esta forma se protege la red interna de intentos de accesos no autorizados desde fuera, que puedan aprovechar debilidades de los sistemas de la red interna.

2.4.6.1.1. FIREWALL UTM

Los resultados Portantier (2013) confirman que un firewall UTM (Unified Threat Management en español Gestión Unificada de Amenazas) es un tipo de firewall que contiene varias capacidades en un mismo equipo o dispositivo, como antivirus, antispam, filtrado web, y muchas otras funcionalidades.

2.4.6.2. PFSENSE

LLC (2016) es del criterio, el proyecto pfSense es una distribución libre para uso como firewall y router, está basado en el sistema operativo FreeBSD con un núcleo personalizado e incluyendo paquetes de software libre de terceros para una funcionalidad adicional. PfSense, con la ayuda del sistema de paquete, es capaz de proporcionar la misma funcionalidad o más de los servidores de seguridad comercial común. Incluye una interfaz web para la configuración de todos los componentes incluidos.

2.5. METODOLOGÍAS DE IMPLEMENTACIÓN

2.5.1. METODO DE DESARROLLO EN CASCADA

Pressman (2010) hace referencia que el modelo de la cascada, a veces llamado ciclo de vida clásico, sugiere un enfoque sistemático y secuencial, que comienza con la especificación de los requerimientos por parte del cliente y avanza a través de planeación, modelado, construcción y despliegue, para concluir con el apoyo del software terminado.

Según Velázquez (2012) indica que el levantamiento de requerimientos es muy riguroso y los analistas definen a priori todos los requerimientos funcionales y no funcionales relacionados con el proyecto. Normalmente, una fase no puede iniciar sin que la fase anterior haya sido revisada y aceptada por el cliente o usuario final, sin que esto signifique el sistema cumplirá con sus necesidades. El método de desarrollo en cascada consta de las siguientes fases:

- **Requisitos:** Es la primera fase de la metodología, por lo cual en esta etapa se reúne toda la información necesaria para la implementación del producto.
- **Diseño:** Describe la estructura del producto en base a la información proporcionada en la fase de requisitos, se suele representar mediante diseños, diagramas y texto.
- **Implementación:** En esta etapa se realiza el desarrollo del producto, es decir se implementa lo diseñado en la fase anterior. Esta fase suele ser

una de las más complicadas y las que conlleva tiempo de más al desarrollador.

- **Verificación:** Aquí se realizan todas las pruebas suficientes para verificar que el producto ha sido desarrollado y funciona como se lo espera.
- **Mantenimiento:** Esta es la fase donde una vez implementado el producto con el pasar del tiempo recibirá un cierto mantenimiento para que su funcionalidad no disminuya.

CAPÍTULO III. DESARROLLO METODOLÓGICO

En la implementación de la Red Inalámbrica de banda ancha con seguridad perimetral en las áreas urbanas y rurales del cantón Tosagua, la cual permite acceder a internet de manera gratuita a los ciudadanos de las zonas beneficiadas, se utilizó la metodología en cascada, la misma que consta de las siguientes fases:

- Requisitos
- Diseño
- Implementación
- Verificación
- Mantenimiento

3.1. METODOLOGÍA CASCADA

3.1.1. REQUISITOS

3.1.1.1. ENTREVISTA CON ALCALDE DEL GADM DEL CANTÓN TOSAGUA

El Alcalde del cantón Tosagua en campaña política manifestó tener un proyecto de internet gratuito para el cantón, el cual lo incluyó dentro de su plan de trabajo: Sabiendo de dicho proyecto, se realizó una entrevista no estructura con el burgomaestre, donde se pudo conocer la predisposición de realizar dicho proyecto, pero de la manera más económica sin afectar el resultado final.

El burgomaestre en la segunda entrevista mencionó, que se requería proporcionar internet gratuito a las siguientes áreas urbanas: Parque Central, Plaza Los Amarillos, Ciudadela El Recreo, Ciudadela San Cristóbal, Parque el Niño, Parque el Maestro, San Roque Abajo y Ciudadela Humberto Gonzales. Como también a las áreas rurales como: el Parque Central (Parroquia San José de Bachillero, Parque Central (Parroquia Ángel Pedro Giler), Comunidad Caleño, Comunidad Los Micos, Comunidad Monte Oscuro, Comunidad Casical, Comunidad Mutre Afuera y Comunidad El Tambo.

3.1.1.2. SITUACIÓN PREVIA DEL DEPARTAMENTO DE TECNOLOGÍA

El departamento de tecnología se encuentra en las instalaciones del Gobierno Autónomo Descentralizado Municipal del cantón Tosagua, ubicado en la calle Bolívar entre Ascázubi y Jorge López, el cual tiene como objetivo administrar eficientemente los recursos informáticos, mediante la utilización de tecnologías de información y la automatización de procesos, a fin de apoyar de manera eficaz la gestión y la toma de decisiones en beneficio de la municipalidad y colectividad.

Se recopiló la información iniciando con una entrevista no estructurada o informal con el Director del Departamento de Tecnología, donde se pudo conocer que el municipio contaba con ciertos equipos inalámbricos que se encontraban colocados en algunos parques de la ciudad, los cuales fueron instalados y configurados por técnicos de la empresa que le proveía el servicio de internet anteriormente; por lo que existía la necesidad de volver a configurarlos, para que presten servicio a la ciudadanía.

Para obtener más información acerca de las condiciones generales del departamento de tecnología en la institución, se procedió a realizar un levantamiento de información mediante un Checklist. El director del departamento llenó el mencionado instrumento, el mismo que puede ser observado en el anexo A1.1.

3.1.1.3. IDENTIFICACIÓN DE LAS CONDICIONES AMBIENTALES EN LOS LUGARES DONDE SE VA A REALIZAR LA COBERTURA

Para identificar las condiciones en los lugares que se iban a beneficiar con el servicio, se realizó visitas en cada uno de los sitios, para determinar si existían edificios, arboles u otro tipo de objeto que dificulten la línea de visión de los equipos inalámbricos. De la misma manera para determinar las condiciones ambientales se consultó en los Planes de Desarrollo y Ordenamiento Territorial de las parroquias de Tosagua, San José de Bachillero y Ángel Pedro Giler,

información como temperatura, humedad, y velocidad del viento, como información complementaria a considerar en el diseño. Cabe mencionar que se lo realizó de esta manera por no contar con equipos para determinar estos parámetros en los lugares.

3.1.1.4. DIAGNOSTICAR LAS FRECUENCIAS DE TRASMISIÓN DE LOS EQUIPOS Y CANAL DE COMUNICACIÓN

Con el fin de determinar la frecuencia a utilizar en los equipos de comunicación, se realizó un escaneo de las redes inalámbricas en el cantón, con puntos de acceso inalámbricos de 2.4 GHz y 5.8 GHz respectivamente, para determinar qué frecuencia y canal se encontraba menos saturada o utilizada, esto con el objetivo de disminuir interferencia al momento de la implementación. En las figuras 3.1 y 3.2, se puede observar dicha exploración donde se muestra información como la dirección MAC, nombre de la red (ESSID), cifrado, señal, ruido y frecuencia con su respectivo canal de cada uno de los equipos.

Dirección MAC	ESSID	Cifrado	Señal, dBm	Ruido, dBm	Frecuencia, GHz	Canal
00:15:6D:8A:5C:C4	S11	WPA2	-93	-95	2.417	2
00:15:6D:D8:04:0B	ServiNet	WPA2	-90	-96	2.457	10
00:15:6D:D8:04:74	ServiNetSUR	WEP	-78	-96	2.442	7
00:27:22:1A:C6:FA	SERVIBACHI	WEP	-89	-95	2.427	4
DC:9F:DB:50:75:3B	ALCALDE LEONARDO SANCHEZ	-	-91	-96	2.412	1
DC:9F:DB:50:76:4B	Gad-Tosagua	-	-93	-96	2.412	1
DC:9F:DB:52:CA:74	PUNTO DE ORO	WPA	-81	-96	2.442	7
14:B9:68:C7:72:A0	NEVER	WPA	-82	-96	2.462	11
30:B5:C2:A7:DE:6E	ALEYDA	WPA2	-87	-96	2.412	1
48:EE:0C:45:81:BE	WENDY	WPA2	-88	-96	2.412	1

Figura 3.1. Captura de pantalla del escaneo de equipos de 2.4 GHZ

Dirección MAC	SSID	Nombre del dispositivo	Encriptación	Señal / Ruido, dBm	Frecuencia, GHz	Canal
E4:8D:8C:B6:BF:09	TECglo	TOS-0-3	NONE	-86 / -92	5.32	64
DC:9F:DB:46:7E:99	NST1	AP NST1 TOSAGU	WEP	-89 / -92	5.785	157
44:D9:E7:66:AF:76	AzziNet	PI	NONE	-86 / -96	5.825	165
4C:5E:0C:2F:2A:49	TECglo	BACHI	NONE	-89 / -92	5.32	64
04:18:D6:C6:69:6D	Casical-Tosagua	Tosagua-Mutre	WPA2	-86 / -92	5.265	53
04:18:D6:A6:D7:23	S8Bachillero	Servinet8bachi	WPA2	-89 / -91	5.68	136
DC:9F:DB:46:7D:88	NST2	AP AP02MERCRED	WPA2	-86 / -91	5.735	147

Figura 3.2. Captura de pantalla del escaneo de equipos de 5.8 GHZ

3.1.2. DISEÑO

3.1.2.1. DISEÑAR LA TOPOLOGÍA DE RED INALÁMBRICA A UTILIZAR Y SOFTWARE DE SIMULACIÓN DE RADIO ENLACES

En la segunda fase de la metodología, luego del análisis respectivo en base a la información recopilada, se realizó el respectivo diseño de la infraestructura, así como la topología lógica de red en donde se utilizó el software SmartDraw.

Para un correcto diseño, se vio la necesidad de utilizar un simulador de enlaces, en la actualidad existen diversos de estos softwares con múltiples facilidades que permiten generar una simulación lo más real posible. Con el fin de utilizar el software propicio para este trabajo se realizó un análisis de los diferentes simuladores disponibles.

3.1.2.2. DEFINIR LA UBICACIÓN ESTRATÉGICA DE LOS EQUIPOS DE COMUNICACIÓN ANTENAS

Para la determinación de cada una de las ubicaciones de los equipos se tomó en cuenta información recopilada en la fase de requisitos, además de aquello se realizó varias visitas en los lugares con el objetivo de encontrar el lugar propicio para los equipos.

Se utilizó el Software Radio Mobile, el cual ayudó a obtener los datos más importantes, tales como infraestructura, topología, y la ubicación de los equipos. Este Software permitió realizar simulación de cada uno de los enlaces, primero se colocó cada uno de los sitios donde se implementaron los equipos de comunicación tal como se muestra en la figura 3.3, donde se registró la ubicación del equipo en la Parroquia Bachillero, una vez culminado con todos los elementos de la red se generó un gráfico de todos los lugares de la infraestructura, tal como se lo puede observar en la figura 3.4.

Figura 3.3. Sitio Bachillero ingresado a Radio Mobile Online

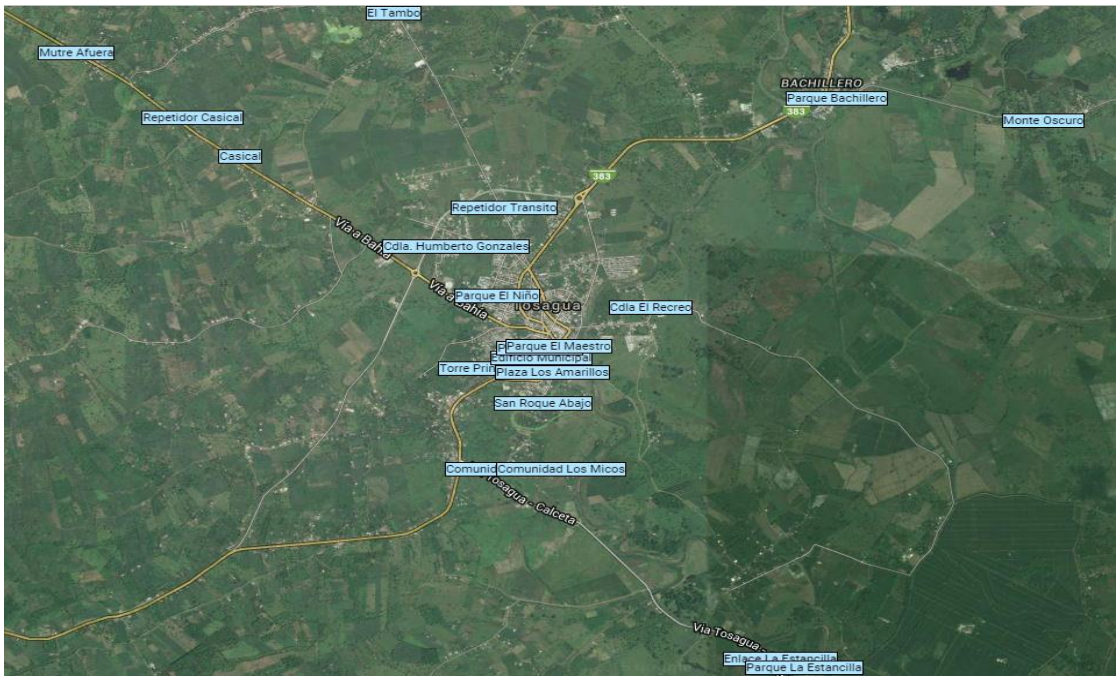


Figura 3.4. Todos los sitios ingresados al Software

Luego se ingresó la información de cada enlace para realizar la simulación, este proceso se lo puede observar en la figura 3.5, de esta manera se podía verificar si el sitio y la altura eran adecuados o de ser necesario, cambiar dichos parámetros.

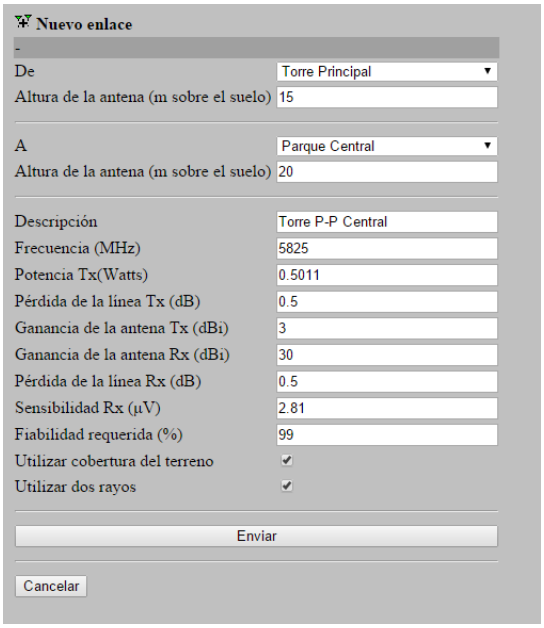


Figura 3.5. Datos para el Enlace desde la Torre hacia el Parque Central

Luego de realizar todas las simulaciones, se volvió a visitar cada uno de los sitios para verificar que en cada uno de estos lugares se cuente con: acceso para la ubicación de los equipos de repetición y finales, energía eléctrica, infraestructura, seguridad, etc. De esta manera comprobar que el diseño de la red se pueda implementar sin mayores inconvenientes, permitiendo interconectar algunas zonas y urbanas del cantón Tosagua para al acceso del servicio de internet.

3.1.2.3. DETERMINAR LOS EQUIPOS A UTILIZAR

En la determinación de los equipos a utilizar, se realizó un análisis de coste beneficio para decidir la tecnología a implementar, donde se tomaron en cuenta aspectos como vida útil de los equipos, costos, seguridad, existencia de equipos inalámbricos en la institución entre otros.

3.1.3. IMPLEMENTACIÓN

3.1.3.1. IMPLEMENTAR LOS DIFERENTES ENLACES INALÁMBRICOS Y PUNTOS DE ACCESOS PARA LAS ZONAS WIFI CON SU RESPECTIVA CONFIGURACIÓN

Se realizó la implementación de cada uno de los equipos en los lugares determinados en la fase anterior, comenzando por la infraestructura es decir torres y mástil tal como se muestra en la foto 3.1.

Foto 3.1. Mástil colocado en el Sitio de Casical

Continuando con la instalación se realizó el enlace desde el palacio municipal hacia la torre principal ubicada en la loma de la ciudadela San Cristóbal, después se instalaron los equipos que harían el papel de repetidores en la torre anteriormente mencionada. Se procedió con la instalación y configuración de todos los equipos en las zonas previstas como se muestra en la foto 3.2. En algunos sitios existieron problemas no contemplados en la fase del diseño, los mismos que fueron resueltos en el transcurso de la ejecución del proyecto.

Foto 3.2. Autor preparando un equipo para su instalación

Luego de realizar cada enlace previsto, se procedió a efectuar pruebas de conexión a cada uno de los equipos, con el fin de obtener respuesta y verificar que existía una conexión. Para esto se utilizó el comando PING desde la consola de Windows así como la herramienta PING TEST incorporada en los equipos utilizados (ver anexo A7.1.).

3.1.3.2. CONFIGURAR EL SERVIDOR FIREWALL QUE CONCENTRA TODA LA SEGURIDAD PERIMETRAL Y EL RESPECTIVO CONTROL DE ACCESO A LOS USUARIOS FINALES

En esta actividad se comenzó con el análisis respectivo para determinar el Firewall a implementar, para lo cual se realizó un estudio entre diferentes sistemas firewall open source. Para esto se evaluaron aspectos como: información de soporte disponible, rendimiento, seguridad, filtrado web, entre otros, con el objetivo de obtener un sistema de seguridad perimetral robusto. Además, se realizó un levantamiento de información mediante una entrevista no estructurada al director del departamento para determinar los sistemas o servidores a proteger de la red externa, de la misma forma para realizar políticas de seguridad que protegerían la red interna (ver anexo A1.8.).

Luego se procedió a implementar el sistema de seguridad Firewall, para lo cual se utilizó un servidor disponible con las características que requiere el software para su buen funcionamiento. Lo primero que se hizo fue respaldar la información que almacenada el equipo para luego formatear e instalar el Software tal como se lo muestra en figura 3.6.

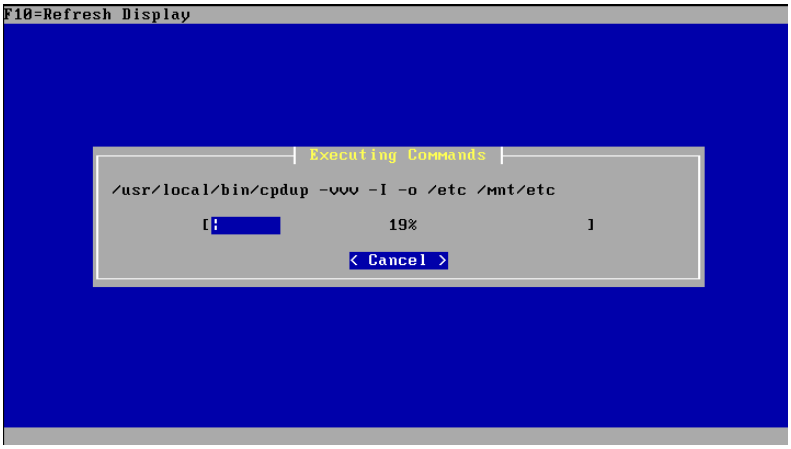


Figura 3.6. Proceso de instalación del Software Firewall.

Una vez terminado el proceso de instalación se definieron las dos tarjetas de red del servidor, una que es la tarjeta de red para la LAN y otra para la WAN. Seguidamente se configuró la tarjeta de red WAN con una dirección IP pública, la cual el proveedor de internet suministró a la institución y la tarjeta de red LAN se configuro por DHCP por lo que este servicio ya viene activado una vez instalado el sistema de seguridad. Luego se procedió a ingresar a la administración del servidor vía web con las credenciales por defecto, admin como usuario y pfsense como clave de acceso, en donde muestra información del equipo físico como se observa en la figura 3.7.

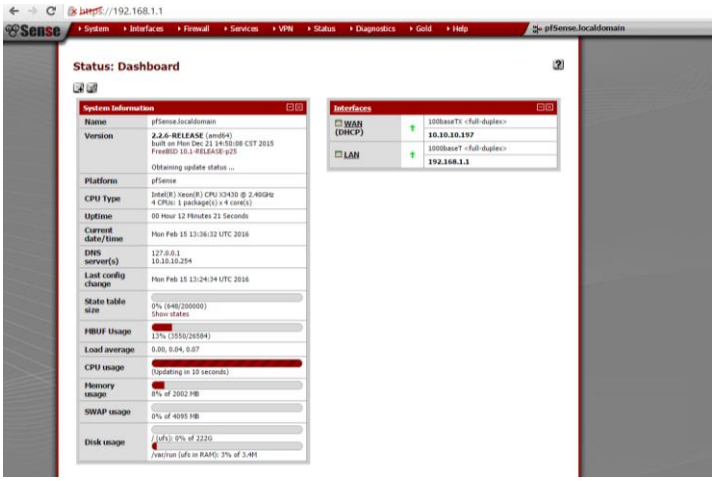


Figura 3.7. Administración web del Firewall PfSense.

Una vez en la administración vía web se realizó toda la configuración del firewall agregando las IP Virtuales de los servidores, mapeo de 1 a 1 donde traducirá las IP públicas a privadas, reglas para permitir acceso a ciertos equipos por puertos específicos entres otras configuraciones para proteger la red interna de la red externa. Además de esto se instaló un paquete para el control de acceso a los usuarios de la red con el fin de permitir ciertos sitios web en determinados horarios como también controlar el ancho de banda en cada uno de los puntos de accesos.

3.1.4. VERIFICACIÓN

En esta fase se realizaron las pruebas de verificación, una de ellas realizar pruebas desde cada uno de los equipos inalámbricos que realizarían la función de Access Point hacia al servidor que concentraría la seguridad perimetral mediante la herramienta Ping Test (ver anexo A7.10).

Luego se comprobó el acceso a internet desde los equipos de los usuarios finales en las distintas zonas beneficiadas (ver anexo A7.15) donde se utilizaron equipos portátiles, tabletas, celulares, entre otros equipos de los usuarios. Además, se

constató el control de acceso a diferentes sitios web bloqueados en el servidor (ver anexo A7.17).

Como la última actividad de esta fase se evaluó el ancho de banda en diferentes horarios y en ciertos lugares beneficiados donde existía gran concurrencia de usuarios, para lo cual se utilizó el sitio web www.speedtest.net/es que permitió corroborar el ancho de banda asignado a cada zona WI-FI. También se evaluó el ancho de banda para servidores públicos (ver anexo A7.13) y directores, de acuerdo a las políticas ingresadas en el firewall.

3.1.5. MANTENIMIENTO

Esta fase no consta en el presente trabajo de tesis, no obstante de acuerdo a la experiencia adquirida del autor en la implementación de la infraestructura, se realizó una lista de pasos a seguir en caso de que existan problemas en la red inalámbrica.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

La implementación de la Red Inalámbrica de banda ancha con seguridad perimetral en las áreas urbanas y rurales del cantón Tosagua, permitió obtener los siguientes resultados:

En la fase de requisitos de la metodología utilizada, se desarrollaron dos actividades; la primera fue identificar las situaciones ambientales en las zonas beneficiadas para el despliegue de la red. Información como la temperatura, humedad, y velocidad del viento; se obtuvo de los Planes de Desarrollo y Ordenamiento Territorial de las parroquias Tosagua, Ángel Pedro Giler y San José de Bachillero. A partir de esta información se analizó y determinó la variable "Obstrucciones", que se obtuvo mediante visitas en cada una de las zonas, tal como se muestra en el cuadro 04.01.

Cuadro 04.01 Situación ambientales de las zonas beneficiadas con el enfoque de obstrucción.

Lugares	**Temperatura (Grados Celcius)**	**Humedad (%)**	**Obstrucciones**	**Viento (m/seg)**
ZONAS URBANAS				
Parque Central	26/25	81	SI	1.6
Plaza Los Amarillos	26/25	81	SI	1.6
Ciudadela El Recreo	26/25	81	NO	1.6
Ciudadela San Cristóbal	26/25	81	NO	1.6
Parque el Niño	26/25	81	SI	1.6
Ciudadela Huberto Gonzales	26/25	81	SI	1.6
Ciudadela San Roque Abajo	26/25	81	NO	1.6
Parque el Maestro	26/25	81	SI	1.6
ZONAS RURALES				
Parque Central (Parroquia Bachillero)	25/27	81	SI	1.6
Parque Central (Parroquia Ángel Pedro Giler)	26	81	NO	1.6
Comunidad Los Micos	26/25	81	SI	1.6

Comunidad Caleño	26/25	81	NO	1.6
Comunidad Monte Oscuro	25/27	81	SI	1.6
Comunidad Casical	26/25	81	SI	1.6
El Tambo	26/25	81	NO	1.6
Mutre Afuera	26/25	81	SI	1.6

Por otro lado, la segunda actividad fue diagnosticar las frecuencias de transmisión de los equipos de comunicación en las áreas de cobertura. Para esto se realizó un levantamiento de información, tal como lo muestra el cuadro 04.02, con el número y porcentajes de equipos que trabajan en frecuencias de 2.4 y 5.8 GHZ respectivamente, además de la información sobre los canales que utilizan. Con esta información se determinó que la frecuencia a utilizar debería ser la de 5.8 GHZ, debido a que esta se encuentra menos saturada en los lugares donde se beneficiará con el servicio de internet y el canal seria el 44, porque este no está utilizado por ningún equipo y se evitaría interferencias en los enlaces. Cabe mencionar que esta frecuencia será la empleada para los enlaces, mientras que para los clientes se utilizará 2.4GHz, por ser la usada por dispositivos finales.

Cuadro 04.02. Número de equipos con sus respectivas frecuencias y canales en Tosagua

Frecuencia	**2,4 GHZ**						**5.8 GHZ**					
Canal	**1**	**2**	**4**	**7**	**10**	**11**	**53**	**64**	**136**	**147**	**157**	**165**
Nro de Redes	4	1	1	2	1	1	1	2	1	1	1	1
Total	**10**						**7**					
Porcentajes	**58,82**						**41,18**					

En la fase de Diseño de la metodología utilizada, se desarrollaron tres actividades; la primera fue diseñar la topología de red inalámbrica a utilizar. Se procedió a realizar el diseño de la infraestructura con la que contaba la institución en ese momento, tal como lo muestra la figura 04.01.

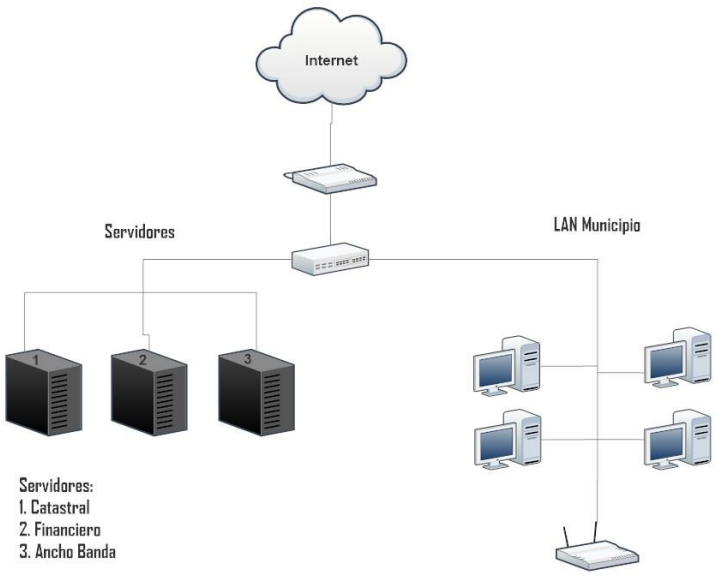


Figura 04.01. Diseño lógico de la infraestructura existente en la institución.

Seguidamente de acuerdo a la información obtenida en la fase de requisitos se procedió a realizar el diseño lógico de la infraestructura donde se incluyó la red inalámbrica así como la solución de sistema de seguridad perimetral, esta topología se la muestra en la figura 04.02.

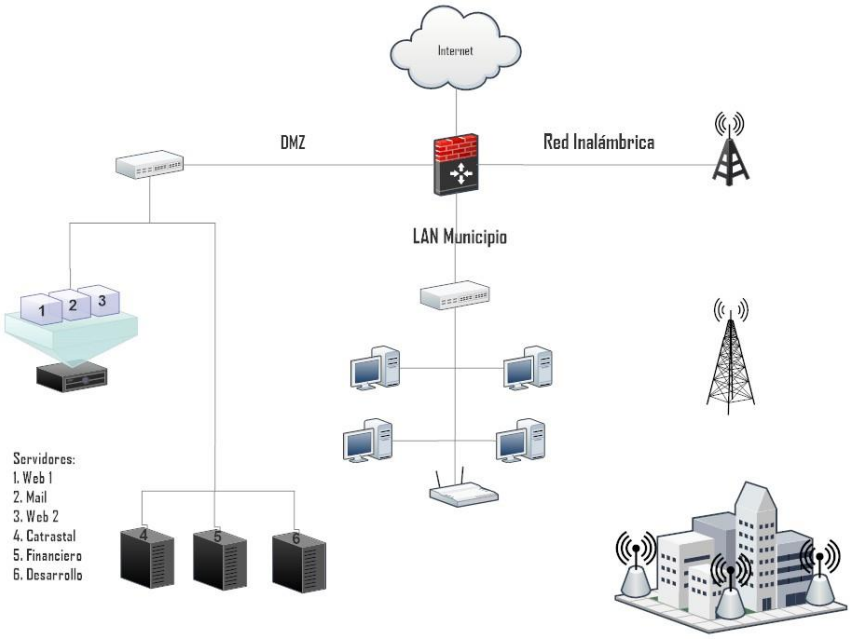


Figura 04.02. Diseño lógico de la infraestructura que se implementó en la institución.

Se determinó que el Simulador de Enlaces a utilizar seria Radio Mobile por ser un software gratuito y con grandes prestaciones. A pesar que es importante recalcar que existe otro simulador con mejores características pero su uso es licenciado como lo es ICS TELECOM. Utilizando el Software Radio Mobile en su versión online se realizó todos los enlaces respectivos para determinar la factibilidad de cada uno de ellos donde esta aplicación mostró toda la información correspondiente. En la figura 04.03 se puede observar dicha información, específicamente de un enlace.

Performance		
Distance	**0.507**	**km**
Precisión	9.9	m
Frecuencia	5825.000	MHz
Potencia de Radiación Isotrópica Equivalente	0.891	W
Ganancia del sistema	157.03	dB
Fiabilidad requerida	99.000	%
Señ recibida	-79.91	dBm
Señ recibida	22.62	µV
Márgen de escucha	**18.12**	**dB**

Figura 04.03. Enlace Torre Principal-Edificio Municipal

Finalmente se procedió a realizar la topología de la Red Inalámbrica con la ubicación estratégica de los equipos como se lo puede observar en la figura 04.04, esto se realizó gracias al simulador de enlaces utilizado y a las visitas realizadas en los sitios.

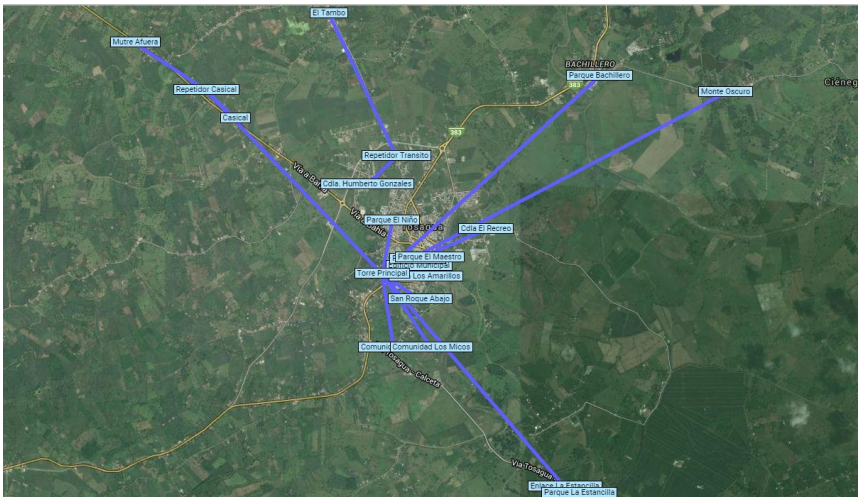


Figura 04.04. Topología de la Red Inalámbrica con ubicaciones estratégicas de los equipos

Como última actividad de la fase de diseño, fue determinar los equipos a utilizar. Los equipos a utilizar en este trabajo fueron los de la tecnología AirMax, debido a un análisis realizado. Se efectuó una calificación de acuerdo a criterios del autor, consultas a profesionales del área, foros en internet y expertos; con la escala del 0 al 3, donde 0 es la peor calificación (menos conveniente) y 3 la mejor (más conveniente). Esta evaluación se muestra en el cuadro 04.03.

Cuadro 04.03. Comparativa de marcas

Parámetros \ Marcas	**Marca 1**	**Marca 2**	**Marca 3**
Vida Útil	3	2	2
Administración	1	3	2
Costo/Característica	3	2	2
Disponibilidad en el medio	3	2	2
Utilización en el medio	3	3	2
Enlaces con línea de Visión	2	3	3
Enlaces sin líneas de visión	2	3	3
Existencia en la Institución	3	0	0
TOTAL	20	18	16

En esta fase de implementación consta de varias actividades, la primera fue el montaje de la infraestructura es decir colocar las torres y mástil, en los lugares estratégicos con los respectivos equipos.

A continuación, se procedió a la configuración de cada uno de los equipos de la red donde el autor pudo agrupar en dos partes; la primera el grupo de los equipos que permiten tener conexión entre los enlaces, toda esta información se muestra en el cuadro 04.04.

Cuadro 04.04. Equipos del grupo de enlaces

Nombre	Descripción	Equipo
TX-PRINCIPAL	Equipo de la Torre Principal	Rocket M5
RX-EDIFICIO	Equipo en el Edificio Municipal	AirGrid M5
TX-ESTANCILLA	Equipo en la Torre de la Escuela de la Estancilla	Rocket M5
RX-PRINCIPAL ESTANCILLA	Equipo de la Torre Principal	NanoStation M5
RX-ESTANCILLA PARQUE	Equipo del Parque de la Estancilla	NanoStation M5
TX-PRINCIPAL2	Equipo de la Torre Principal hacia El Parque El Niño	PowerBeam M5
RX-PRINCIPAL CASICAL	Equipo de la torre principal	NanoStation M5
RX-BACHILLERO	Equipo de la Torre de Bachillero	NanoStation M5
TX-CASICAL	Equipo de la Torre de Casical-Tosagua	Rocket M5
RX-CASICAL	Equipo en la Escuela de Casical	NanoStation M5
RX-PARQUE CENTRAL	Equipo del Parque Central	NanoStation M5
UBNT (SAN ROQUE ABAJO)	Equipo de San Roque Abajo	NanoStation5 L
RX-PARQUE EL MAESTRO	Equipo del Parque el Maestro	NanoStation M5
RX-PARQUEL DEL NIÑO	Equipo del Parque del Niño	NanoStation M5
RX-EL RECREO	Equipo del Recreo	NanoStation M5
RX-PLAZA LOS AMARILLOS	Equipo Plaza Los Amarillos	NanoStation M5
RX-CALENO	Equipode Caleño	NanoStation M5
RX-LOS MICOS	Equipo de Los Micos	NanoStation M5
TX-CASICAL2	Equipo de la Torre de Casical hacia Mutre	PowerBeam M5
RX-MUTRE	Equipo de Mutre	NanoStation M5
RX-MONTES OSCURO	Equipo de Monte Oscuro	PowerBeam M5

TX-TRANSITO	Equipo de las Oficinas de Transito	Rocket M5
RX-EL TAMBO	Equipo en el Tambo	PowerBeam M5
RX-HUMBERTO GONZALES	Equipo en la Cdla Humberto Gonzales	NanoStation M5

De igual manera se realizó la configuración de los equipos que hacen función de Punto de Acceso a los cuales los ciudadanos tendrían que conectarse para acceder a internet, la información de estos equipos se la muestra en el cuadro 04.05.

Cuadro 04.05. Equipos del grupo de puntos de acceso

Nombre	IP	Equipo
AP-EL RECREO	10.10.10.3	PicoStation2
AP-BACHILLERO	10.10.10.4	PicoStation2
AP-PARQUE EL MAESTRO	10.10.10.5	PicoStation2
AP-PARQUE CENTRAL	10.10.10.6	PicoStation2
AP-PARQUE EL NINO	10.10.10.7	PicoStation2
AP-CASICAL	10.10.10.8	PicoStation M2
AP-ESTANCILLA	10.10.10.9	PicoStation2
AP-PLAZA LOS AMARILLOS	10.10.10.12	PicoStation2
AP-CALENO	10.10.10.13	PicoStation2
AP-LOS MICOS	10.10.10.14	PicoStation3
AP-MUTRE	10.10.10.15	PicoStation M2
AP-SAN ROQUE ABAJO	10.10.10.16	PicoStation2
AP-MONTE OSCURO	10.10.10.17	PicoStation M2
AP-EL TAMBO	10.10.10.18	PicoStation M2
AP-HUMBERTO GONZALES	10.10.10.19	PicoStation M2

Como última parte de la implementación de la red inalámbrica se realizaron pruebas de conectividad entre los diferentes enlaces mediante el comando ping de la consola de Windows, dándo como resultados tiempos de respuesta de 1

milisegundo entre un enlace hacia un equipo de la torre principal, tal como se muestra en la foto 04.01.

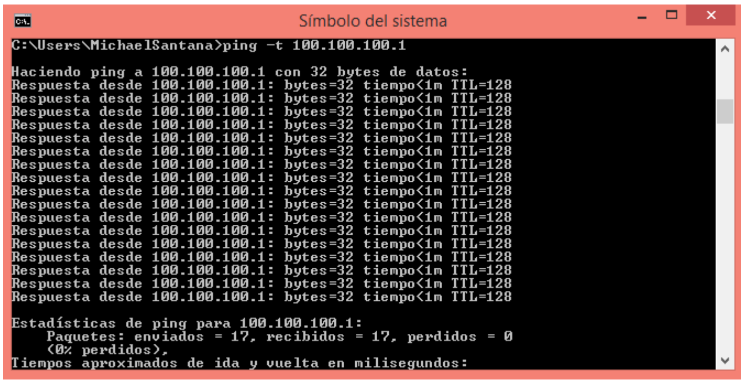


Foto 04.01. Tiempos de respuesta entre equipos de los enlaces

Dentro de la fase de implementación incluye la instalación y configuración del firewall, este objetivo incluye ciertas actividades, en la primera, mediante un estudio realizado por el autor se determinó que el sistema de seguridad a utilizar seria la distribución de PfSense. Se efectuó una calificación de acuerdo a criterios del autor, foros en internet e información obtenida en un ambiente de prueba; con la escala del 0 al 3, donde 0 es la peor calificación (menos conveniente) y 3 la mejor (más conveniente). Esta información se la muestra en el cuadro 04.06.

Cuadro 04.06. Comparativa de Firewalls gratuitos.

Aspectos \ Software	PfSense	Zentyal	IPCop
Información de soporte disponible	3	1	1
Filtrado web	3	3	1
Rendimiento	3	2	3
Seguridad	3	3	2
Interfaz gráfica	2	3	1
Control de Trafico	3	3	2
Modular	3	2	1
Total	**20**	**17**	**11**

Se continuo con la recopilación de información ante el Director de Tecnología se determinó las políticas de seguridad para el sistema Firewall tal como se muestra en el cuadro 04.07. Dentro de estas políticas constan la protección de ciertos servidores de la institución como además las políticas hacia la red internet y la red inalámbrica.

Cuadro 04.07. Políticas de Seguridad del sistema de seguridad perimetral

Nombre	**Descripción**	**Nivel de Seguridad**	**Excepciones**
Acceso Servidor Web 1	Acceso a los servicios del servidor web de la institución	Alto	HTTP
Acceso Servidor Web 2	Acceso a los servicios del servidor web de la Dirección de Transito	Alto	HTTP
Acceso Servidor Web 3	Acceso a los servicios del servidor web de Tramites Online	Alto	HTTP
Acceso Servidor de Correo	Acceso a los servicios del servidor de correo de la institución	Alto	SNMTP, IMAP, POP3, HTTP
Control de Trafico Servidores	Control de Ancho de Banda para servidores públicos con 256 kb/s de subida y bajada.	N/A	N/A
Control de Trafico Directores	Control de Ancho de Banda para Directores de la institución con 512 kb/s de subida y bajada.	N/A	N/A
Control de Acceso Web Servidores	Control de accesos de sitios web como: redes sociales, ocio, porno, entre otros.	Medio	N/A
Control de Acceso Web Directores	Control de acceso de sitios web como: ocio y porno.	Bajo	N/A

Luego se procedió a la instalación y configuración de la distribución PfSense, en donde se agregaron diferentes reglas para proteger la red interna de la red externa tal como se lo muestra en la foto 04.02. Debido a que en la institución existen servidores Webs, se realizó el respectivo mapeo de direcciones públicas a direcciones de la LAN. Además, se instalaron paquetes de seguridad con el fin de bloquear sitio webs para los usuarios finales de la web y controlar el ancho de banda en los puntos de accesos, servidores y directores.

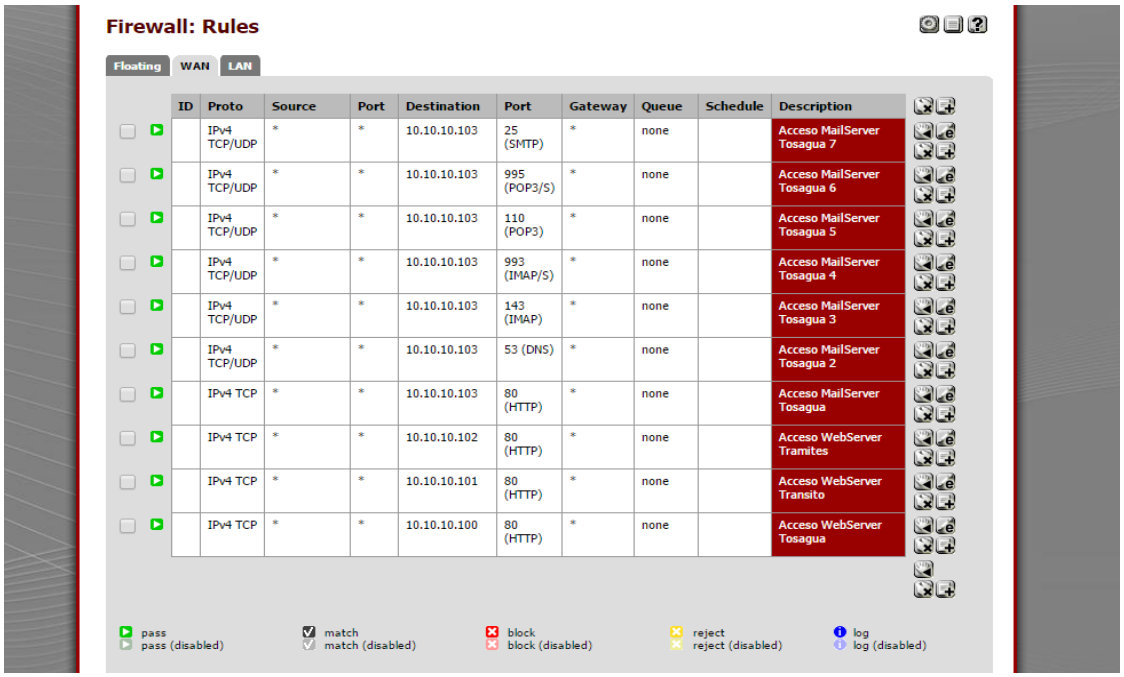


Foto 04.02. Firewall con las diferentes reglas en la WAN.

En la fase de verificación se realizaron diversas actividades con el fin de corroborar el buen funcionamiento de la infraestructura, la primera se efectuó mediante la herramienta Ping Test desde los equipos instalados hacia el servidor, para lo cual se muestran los tiempos de respuesta en el cuadro 04.08.

Cuadro 04.08. Tiempos de respuesta desde los Access Point al Servidor

Access Point	Mínimo (ms)	Máximo (ms)	Promedio (ms)
El Recreo	4.13	5.96	5.27
Bachillero	7.11	63.04	27.76
Parque El Maestro	14.48	30.08	22.37
Parque Central	7.62	16.82	10.51
Parque El Nino	4.44	8.17	6.14
Casical	5.59	16.13	8.07
Estancilla	4.71	10.77	7.98
Plaza Los Amarillos	5.3	8.84	6.58
Caleño	7.5	16.48	11.19

Los Micos	8.06	17.29	12.08
Mutre	6.08	16.23	8.20
San Roque Abajo	7.26	18.09	11.09
Monte Oscuro	4.03	9.45	7.25
El Tambo	4.26	5.92	5.03
Humberto Gonzales	7.83	18.03	12.03
Promedio	**6.56**	**17.42**	**10.77**

Seguidamente se desarrolló pruebas de acceso mediante equipos de los usuarios finales, es decir los ciudadanos, para esto se les comunico que se conectaran a las redes instaladas en la zonas beneficiadas, en donde accedieron a internet con éxito, tal como se muestra en la foto 04.03.

Foto 04.03. Ciudadano accediendo a internet en la Comunidad de Mutre

Finalmente, como última actividad de la fase de verificación, se realizaron test del ancho de banda en las zonas Wi-Fi en diferentes horarios, de la misma manera a las computadoras de la red interna de la institución como también a las de los servidores públicos y directores. Otro aspecto que se tomó en cuenta fue el control de acceso a diferentes sitios webs en la red inalámbrica como en la red interna, para lo cual mediante blacklist se bloquearon ciertas páginas.

La última fase de la metodología fue la de mantenimiento, la cual no consta dentro de este trabajo de tesis, a pesar de aquello se realizó una lista de pasos a seguir en caso de que existan inconvenientes en la infraestructura implementada. Estos pasos se los puede observar en el cuadro 04.09.

Cuadro 04.09. Pasos para el mantenimiento de la infraestructura

Problema	**Causas**	**Solución**
Sin respuesta de equipos de enlace	Uno de los equipos se encuentra sin energía eléctrica	Verificar el suministro eléctrico, cambiar de POE para probar el buen funcionamiento del mismo
	El receptor no está enlazado con el transmisor	Acceder al equipo Receptor y volver a escanear el trasmisor
	Uno de los equipos se reinició de fabrica	Cargar el respaldo de la configuración en caso de no tenerla realizar de nuevo la respectiva configuración
	El receptor no está enlazado con el transmisor y ha cambiado su dirección	Cambiar la dirección del equipo receptor para que tenga una línea de visión al equipo transmisor
Con respuesta pero no se muestra la	El equipo esta inhibido	Acceder al equipo vía SSH y reiniciar el mismo

administración web		
Con respuesta pero no se muestra la administración web y cuando se intenta ingresar vía web se pierde conexión	El equipo se encuentra infectado de un virus llamado Skynet	Se debe buscar en internet la solución, la cual consiste en ingresar vía SHH al equipo y escribir ciertos comandos

DISCUSIÓN

Actualmente constan muchos estudios para realizar implementaciones de redes inalámbricas en el Ecuador, teniendo cada uno de ellos similitudes y diferencias, Hidalgo (2013) muestra en su tesis de grado presentada como requisito para la obtención del título de magister en interconectividad de redes, un análisis sobre las tecnologías inalámbricas, con el fin de mejorar el diseño de la red de comunicaciones existente en el sector rural centro de la provincia de Morona Santiago, específicamente en los cantones de Morona y Sucúa.

Sin embargo, este trabajo de tesis además de realizar un respectivo análisis y diseño, se realizó la implementación de la red inalámbrica de banda ancha con el objetivo de brindar internet gratuito a las áreas urbanas y rurales del cantón Tosagua con la intención de erradicar la brecha digital y poner las TIC’s al alcance de los ciudadanos. Una de las más grandes ventajas de este trabajo frente al antes mencionado, es que se incluye un sistema de seguridad Firewall, que permite proteger la red interna de la red externa, además de brindarle aspectos de seguridad a los usuarios finales, con el respectivo filtrado web, control de ancho de banda, entre otras funcionalidades.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Para el levantamiento de información previa la instalación de una red inalámbrica es importante realizar visitas en situ en las zonas beneficiadas, con el fin de obtener información con mayor precisión de los requerimientos técnicos, también apoyarse de estudios técnicos realizados para consolidar la investigación.
- Utilizando un simulador de enlaces se disminuyen en cierta forma errores en cálculos manuales o visuales, obteniendo información muy cercana a la realidad.
- A la hora de determinar los equipos a utilizar es importante realizar un estudio de acuerdo a la realidad de la institución y del medio, con el fin de tener capacidad para adquirir y cumplir con el proyecto.
- Los equipos utilizados en la implementación prestan estabilidad en los enlaces, siempre y cuando exista línea de vista o exista una obstrucción pequeña como la de un árbol.
- La distribución PfSense es un UTM que si se agregan ciertos paquetes tiende a tener las mismas características o más, que soluciones de seguridad comerciales.
- La red en temporada invernal o en épocas de lluvia, tiende a subir los tiempos de respuesta entre los enlaces, por lo que el ancho de banda en los Access Point es afectado.

RECOMENDACIONES

- Para el levantamiento de información utilizar equipos especiales para determinar situaciones ambientales (temperatura, humedad, viento, entre

otros) en cada uno de los lugares, con el fin de no depender de estudio de otras personas.

- Al momento de realizar el diseño o estudio es importante conocer el presupuesto, para adaptarse al mismo con el fin de no tener imprevistos a la hora de la implementación.
- Utilizar equipos con grandes características en la administración como punto de acceso base, y equipos con un tiempo de vida alto como equipos de estación en los enlaces finales.
- Implementar en todas las entidades públicas sistemas de seguridad perimetral, con el fin de salvaguardar los datos que se manejan tanto en las aplicaciones internas en la red, como también las que brindan servicios a través del internet.
- Manipular aplicaciones que permitan controlar y monitorear todos los equipos inalámbricos, con el fin de verificar el buen funcionamiento de los mismos y comunicar en caso de que exista un problema para la respectiva solución.

BIBLIOGRAFÍA

Abad, A. 2012. Redes Locales - Ciclo Formativo de Grado Medio. Madrid, ES.

Acevedo, M; Castañeda, R; Oleksiy, P. 2009. Diseño de antenas de ranura resonante para su aplicación en redes WiFi. Distrito Federal, MX. Científica. Vol. 13. p 2.

Alcaraz, A; Mondragón, J; García, C; Rojas, J. 2013. Análisis de cobertura de las técnicas de modulación y codificación en redes inalámbricas basadas en IEEE 802.16. Mexico, MX. Científica. Vol. 17. P 3-11.

Amiri, I; Alavi, S; Idrus, S; Nikoukar, A; Ali, J. 2013. IEEE 802.15.3c WPAN Standard Using Millimeter Optical Soliton Pulse Generated by a Panda Ring Resonator. Johor Bahru, MA. IEEE Photonics Journa.

Asamblea Nacional. 2010. Ley Orgánica de Educación Superior. Quito, EC. p 6.

Astaiza, E; Bermudez, H; Méndez, D. 2013. Evaluación del Desempeño de un Modelo Autosimilar para el Tráfico en Redes 802.11. Medellín, CO. Tecno Lógicas.

Balseca, L. 2013. Estado del arte en la detección de intrusiones en Redes 802.1. (En línea). Consultado, 14 de may. 2015. Formato PDF. Disponible en http://repositorio.espe.edu.ec/bitstream/21000/6686/1/AC-RED-ESPE-047230.pdf

Barbecho, R. 2011. Estudio, diseño e implementación de un enlace inalámbrico de largo alcance con antenas direccionales de la empresa Compufácil. Tesis. Ing. Sistemas Informáticos. UTI. Cuenca, EC.

Barreto, O. 2013. VPLS: alternativa de interconexión a través del backbone IP/MPLS de ETECSA. La Habana, CU. Revista Cubana de Ciencias Informáticas. Vol. 7. P 32-43.

Bengochea, J. 2011. Estudios de campo y selección de antenas para redes 802.11bg. Tesis. Ing. Eléctrico Electrónico. Universidad Nacional Autónoma de México. México, MX.

Bustamante, R. s.f. Seguridad en Redes. Tesis. Ing. Electrónica y Telecomunicaciones. Universidad Autónoma del Estado de Hidalgo.

Butler, J. 2013. Redes Inalámbricas en los Países en Desarrollo. 4 ed.

Carballeiro, G. 2012. Redes WIFI en entorno Windows. Buenos Aires, AR. USERS. Vol. 4. p 192.

Cázares, G; Castillo, H; Fonseca, J. 2012. Unidad de adquisición de datos y medición basada en protocolo de comunicación WIFI. El Fuerte, MX. Ra Ximhai.

Cervigón, A y Ramos, M. 2011. Seguridad Informática. 1 ed. Madrid. p 200.

CONATEL (Concejo Nacional de Telecomunicaciones) y SENATEL (Secretaria Nacional de Telecomunicaciones). 2012. Plan Nacional de Frecuencias Ecuador.

Cruz, M; Martínez, R; Crespo, Y. 2013. Análisis de la QoS en redes inalámbricas. México, MX. Tecnologías de la información y las telecomunicaciones.

Dordoigne, J. 2015. Redes Informáticas. Nociones Fundamentales. 5 ed. Eni Ediciones.

Emperanza, A. 2014. Datacenter. Chile. Revista America TIC. 3 ed.

Escudero, A. 2007. Redes Inalámbricas (En Línea). EC. Consultado, 27 de mar. 2016. Formato PDF. Disponible en http://www.itrainonline.org/itrainonline/mmtk/wireless_es.shtml.

Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López” ESPAM MFL, 2012. Manual del Sistema de Investigación Institucional. 2 ed.

Fabuel, C. 2013. Implantación de un sistema de seguridad perimetral. Tesis. Ing. Técnica de Telecomunicación. UPM. Madrid. ES. P 227.

Gómez, P. 2011. Administración de la infraestructura Tecnológica. (En línea). EC. Consultado, 02 de abr. 2016. Formato PDF. Disponible http://quindio.gov.co/home/docs/items/item_100/P-SAD-71Administraciondelainfraestructuratecnologica.pdf

Grote, W; Ávila, C; Molina, A. 2007. Análisis de máximo desempeño para wlan operando a tasas fijas o adaptivas usando el estándar IEEE 802.11 a/b/g. Arica, CH. Ingeniería.

Guevara, R y Serna, E. 2013. Una propuesta de solución al problema de la interferencia entre redes WIFI por solapamiento de canales. Bogotá, CO. Ciencia e Ingeniería Neogranadina. Vol. 23. p 7-16.

Hidalgo, J. 2013. Análisis de tecnologías inalámbricas para mejorar el diseño de la red de comunicaciones en el sector rural centro de Morona Santiago. Riobamba, EC.

IDEA (Agencia de Innovación y Desarrollo de AndalucÍa). 2008. Estudio sectorial de vigilancia tecnológica. Tecnologías Inalámbricas.

INEC (Instituto Nacional de Estadísticas y Censos). 2010. Censo de Población y Vivienda.

INEC (Instituto Nacional de Estadísticas y Censos). 2013. Tecnologías de la Información y Comunicaciones (TIC'S).

Katz, M. 2013. Redes y Seguridad. Primera Edición. Buenos Aires, ARG. Alfaomega Grupo Editor.

Köbel, C; Garcia, W; Habermann, J. 2012. Sistema de balance de carga para redes malladas inalámbricas multi-interfaces. Revista de Ingeniería Electrónica, Automática y Comunicaciones.

Kumar, R; Kumar, H; Issac, B. 2014. Different Firewall Techniques: A Survey. Hefei, CH. IEEE. p 1-6.

Kurose, J y Ross, K. 2010. Redes de Computadoras Un enfoque descendente. 5 ed. Pearson Educación.

Kuschnaroff, F; Bayma, F; Souto, E. 2012. INTERNET: MONITORED FREEDOM. São Paulo, BR. Journal of Information Systems and Technology Management.

LLC (Electric Sheep Fencing). 2016. PfSense. (En Línea). EC. Consultado. 10 de abr. 2016. Formato HTML. Disponible en https://www.pfsense.org/getting-started.G

López, A y García, N. 2010. SIMULACIÓN DE TRÁFICO EN REDES INALAMBRICAS MEDIANTE NS2. Pereira, CO. Scientia Et Technica. Vol. 16. p 155-160.

McHoes, A y Flynn, I. 2011. Sistemas Operativos. Sexta Edición, Mexico, DF. Cengage Lerarning Editores S.A.

Madrid, N. 2010. Artículo Científico: La adicción a Internet. (En línea). Consultado, 14 de may. 2015. Formato HTML. Disponible en http://www.futurosinjuego.org/t784-articulo-cientifico-la-adiccion-a-internet.

Moreira, G. 2011. Democracia WiFi: Dinámicas de la política y la comunicación en la era digital. Maracaibo, VE. Quórum Académico. Vol. 8. p 3.

Munévar, S. 2013. Diseño de una infraestructura tecnológica funcional dentro de un plan piloto propuesto para la implementación de teletrabajo. Tesis. Ing. Sistemas. Universidad EAN. Bogotá, CO. P 15.

Pellejero, I; Andreu, F; Lesta, A. 2005. Seguridad en redes WLAN. Conozca lo esencial para su empresa. Colección Guías Técnicas.

Pérez, H y Galván R. 2006. Redes Inalámbricas 802.11n el Nuevo Estándar. Aguascalientes, MX. Conciencia Tecnológica.

Portantier, F. 2013. Seguridad Informática. 1 ed. Argentina. p 192.

Pressman, R. 2010. Ingeniera del software. Un enfoque práctico. 7 ed. Mexico, MX. McGraw-Hill.

Ramos, A. 2011. Information Security Enciclopedia. Seguridad Perimetral. Madrid, ES. Revista Intypedia.

Rincón, D y Cano, C. 2007. Mitigación de la Dependencia a Largo Plazo del Tráfico en Redes WLAN IEEE 802.11. IEEE LATIN AMERICA TRANSACTIONS.

Salvetti, D. 2011. Redes Wireless - Instalación, configuración y mantenimiento de hardware y software. Buenos Aires, AR. USERS. Vol. 220. p 320.

Santiago, G. 2010. Manual para Radialistas Analfatécnicos. (En línea). EC. Consultado, 07 de abr. 2016. Formato PDF. Disponible en http://www.analfatecnicos.net/archivos/79.ConexionesRJ45-Wikipedia.pdf

SENPLADES (Secretaria Nacional de Planificación y Desarrollo). 2013. Plan Nacional de Desarrollo / Plan Nacional para el Buen Vivir 2013-2017. 1 ed. Quito, EC.

SmartDraw. 2015. SmartDraw User Guide. SmartDraw Software, LLC. Consultado, 06 de ene. 2016. Disponible en https://www.smartdraw.com/support/smartdraw-user-guide.pdf.

Sosa, E y Godoy, D. 2014. Internet del Futuro. Desafíos y perspectivas. Posadas, Misiones, AR. Revista Ciencia y Tecnología.

Suqui, K. 2010. Estudio e implementación de un radio enlace con tecnología Mikrotik para el I.S.P. JjSistemas en el cantón Gualaquiza, provincia Morona Santiago. Tesis. Ing. Electrónica. Universidad Politécnica Salesiana Sede Cuenca. Cuenca, EC. p 52-100.

Tanenbaum, A y Wetherall, D. 2012. Redes de Computadoras. 5 ed. México. Pearson Educación.

UBNT (Ubiquiti Networks). 2013. AirMax Sector Datashet. (En línea). EC. Consultado, 25 de mar. 2016. Formato PDF. Disponible en https://dl.ubnt.com/datasheets/airmaxsector/airMAX_Sector_Antennas_DS.pdf.

Velázquez, J. 2012. Desarrollo en Cascada (Waterfall) VS Desarrollo Agile-SCRUM. Northware Software Development. Consultado, 05 de dic. 2015. Disponible en http://www.northware.mx/wp-content/uploads/2013/04/Desarrollo-cascada-vs-Desarrollo-Agile.pdf.

ANEXOS

Anexo 1.

FOTOGRAFÍAS DE LA FASE DE REQUISITOS

FOTO A1.1. Director del departamento llenando checklist

FOTO A1.2. Switch con los que cuenta la institucion

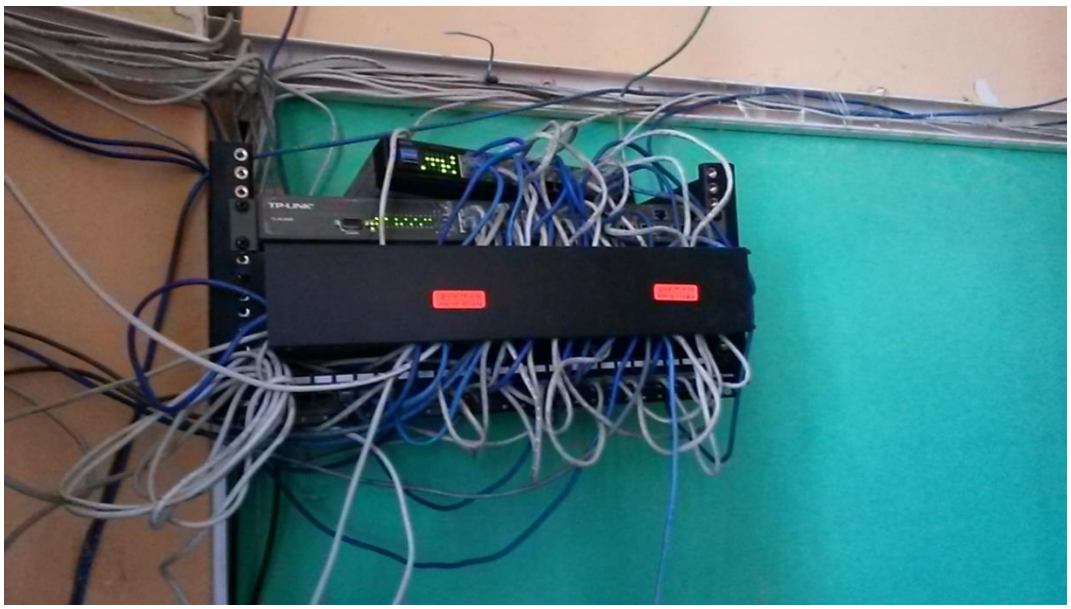


FOTO A1.3. Sevidores en el departamento de tecnologia

FOTO A1.4. Entrevista con el Alcalde del GAD Municipal de Tosagua

FOTO A1.5. Alcalde y concejales en alcaldia

FOTO A1.6. Checklist completada por el Director del Departamento de Tecnología

LISTA DE CHEQUEO DE RECOLECCIÓN DE LA INFORMACION

Objetivo: Conocer el estado actual del departamento de tecnología del GADMC TOSAGUA

Unidad inspeccionada: Tecnologia	Fecha: 6 - Octubre - 2015
Puntos chequeados: 1 ☐ 2 ☐ 3 ☐ 4 ☐	Inspector: Michael Santana

1. Infraestructura			
¿Dispone de una oficina el departamento de tecnología y sistemas?	☑ SI	☐ NO	☐ N/A
¿Dispone de un área física para colocar los equipos informáticos?	☑ SI	☐ NO	☐ N/A
¿Dispone la unidad de un rack para colocar servidores?	☐ SI	☑ NO	☐ N/A

2. tecnologías			
¿Dispone el departamento de computadores dedicado?	☑ SI	☐ NO	☐ N/A
¿Dispone el departamento de equipos inalámbricos?	☑ SI	☐ NO	☐ N/A
¿Dispone el departamento de un firewall?	☐ SI	☑ NO	☐ N/A
¿Dispone el departamento de un router?	☑		

3. normativas			
¿Conoce las políticas de seguridad para los computadores dedicados?	☐ SI	☑ NO	☐ N/A
¿Tiene el departamento un diseño de la infraestructura con la que cuenta?	☐ SI	☑ NO	☐ N/A

4. generalidades			
¿Dispone de impresora el departamento?	☑ SI	☐ NO	☐ N/A
¿Dispone buen acceso de red?	☑ SI	☐ NO	☐ N/P
¿Consta de personal suficiente para cumplir con las necesidades de departamento?	☐ SI	☑ NO	☐

Observaciones

Actualmente se cuenta con los equipos de climatización, de los cuales ya no están operativos debido al cambio de proveedor de Internet.

NOTA: N/A = No aplicable.

FOTO A1.7. Preguntas realizadas al Director del Departamento de Tecnología

ENTREVISTA

NOMBRE: CESAR MOREIRA ZAMBRANO.

UNIDAD: TECNOLOGIA

INSTITUCION: GAD DE TOSAGUA

FECHA: 06-10-2015

1. Que tiempo tiene a cargo el departamento de tecnología
   17 MESES.
2. Como considera la infraestructura del departamento
   MEDIANAMENTE BUENA
3. Realizara futura adquisiciones de equipos tecnológicos, de ser así que equipos compraría
   Si SEGURAMENTE.
   SERVIDORES DE RACK, BLADE CON STORAGE DE ALMACENAMIENTO, Y EQUIPOS INALAMBRICOS
4. Conoce de la importancia en brindar internet gratuito a la ciudadanía
   Si
5. El GADM brinda este servicio a la ciudadanía
   Si
6. De ser positiva la pregunta anterior que tiempo que brinda dicha información y cuantas zonas wifi tiene.
   Solo se brinda el Servicio desde hace 2 meses
   Y existen 3 ZONAS WIFI, pero actualmente no estan Operativos
7. El GADM cuenta con equipos inalámbricos
   si
8. El GADM cuenta con un firewall que concentre la seguridad en la red
   NO
9. De ser positiva la pregunta que tecnología utiliza

Firma

FOTO A1.8. Preguntas para recopilar información sobre las políticas de seguridad

ENTREVISTA

OBJETIVO: Recopilar información para realizar las políticas de seguridad del sistema Firewall

NOMBRE: Cesar Marcial Zambrano.

CARGO/INSTITUCIÓN: Especialista de Informática GADMET.

1. **Dispone de un servidor o computador dedicado disponible para su funcionamiento de inmediato**
   Actualmente Se Cuenta Con Un Servidor que no esta Totalmente Utilizado.
2. **De ser afirmativa la pregunta anterior, indique las características del servidor**
   IBM, Procesador INTEL Xeon de 64BIT. 4GB DE RAM, CPU 3.0 GHZ, Tarjeta de Red. Gigabit ethernet.
3. **El departamento cuenta con servidores web u otros servicios que estén disponibles en el internet**
   SP.
4. **De ser afirmativa la pregunta anterior, indique los servidores con los que cuenta la institución**
   - WEB TOSAGUA
   - WEB TRANSITO
   - WEB TRAMITES
   - MAIL - CORREOS ELECTRONICOS
5. **Se cuenta en la institución con un control de Ancho de Banda así como también un control de acceso para los usuarios de la entidad.**
   NO
6. **De ser negativa la pregunta, indique brevemente que limitadores de velocidad desearía aplicar así como también los sitio webs a bloquear.**
   Servidores Publicos 256 Kbps
   Directivos Departamentales 512 Kbps.
   Paginas A bloquear Todo Internet (Facebook, Twiter, youtube. etc)

Firma

Anexo 2.

CHECKLIST Y ENTREVISTA APLICADOS

LISTA DE CHEQUEO DE RECOLECCIÓN DE LA INFORMACION

Objetivo: Conocer el estado actual del departamento de tecnología del GADMC TOSAGUA

Unidad inspeccionada:	Fecha:
Puntos chequeados: 1 ☐ 2 ☐ 3 ☐ 4 ☐	Inspector:

1. Infraestructura			
¿Dispone de una oficina el departamento de tecnología y sistemas?	☐ SI	☐ NO	☐ N/A
¿Dispone de un área física para colocar los equipos informáticos?	☐ SI	☐ NO	☐ N/A
¿Dispone la unidad de un rack para colocar servidores?	☐ SI	☐ NO	☐ N/A

2. tecnologías			
¿Dispone el departamento de computadores dedicado?	☐ SI	☐ NO	☐ N/A
¿Dispone el departamento de equipos inalámbricos?	☐ SI	☐ NO	☐ N/A
¿Dispone el departamento de un firewall?	☐ SI	☐ NO	☐ N/A
¿Dispone el departamento de un router?	☐ SI	☐ NO	☐ N/A

3. normativas			
¿Tiene el departamento políticas de seguridad para los computadores?	☐ SI	☐ NO	☐ N/A
¿Conoce estas políticas de seguridad?	☐ SI	☐ NO	☐ N/A
¿Aplica estas políticas en el departamento?	☐ SI	☐ NO	☐ N/A

4. generalidades			
¿Dispone de impresora el departamento?	☐ SI	☐ NO	☐ N/A
¿Dispone buen acceso de red?	☐ SI	☐ NO	☐ N/P
¿Consta de personal suficiente para cumplir con las necesidades de departamento?	☐ SI	☐ NO	☐

Observaciones

NOTA: N/A = No aplicable.

ENTREVISTA

NOMBRE: _____

UNIDAD: _____

INSTITUCION: _____

FECHA: _____

1. Que tiempo tiene a cargo el departamento de tecnología

2. Como considera la infraestructura del departamento

3. Realizara futura adquisiciones de equipos tecnológicos, de ser así que equipos compraría

4. Conoce de la importancia en brindar internet gratuito a la ciudadanía

5. El GADM brinda este servicio a la ciudadanía

6. De ser positiva la pregunta anterior que tiempo que brinda dicha información y cuantas zonas wifi tiene.

7. El GADM cuenta con equipos inalámbricos

8. El GADM cuenta con un firewall que concentre la seguridad en la red

9. De ser positiva la pregunta que tecnología utiliza

_____

Firma

ENTREVISTA

OBJETIVO: Recopilar información para realizar las políticas de seguridad del sistema firewall

NOMBRE: _____

CARGO/INSTITUCIÓN: _____

1. **Dispone de un servidor o computador dedicado disponible para su funcionamiento de inmediato**

2. **De ser afirmativa la pregunta anterior, indique las características del servidor**

3. **El departamento cuenta con servidores web u otros servicios que estén disponibles en el internet**

4. **De ser afirmativa la pregunta anterior, indique los servidores con los que cuenta la institución**

5. **Se cuenta en la institución con un control de Ancho de Banda así como también un control de acceso para los usuarios de la entidad.**

6. **De ser negativa la pregunta, indique brevemente que limitadores de velocidad desearía aplicar así como también los sitio webs a bloquear.**

_____

Firma

Anexo 3.

DIAGRAMAS E ILUSTRACIONES DE LA FASE DE DISEÑO

FOTO A3.1. Diagrama de la infraestructura con la que contaba la institución

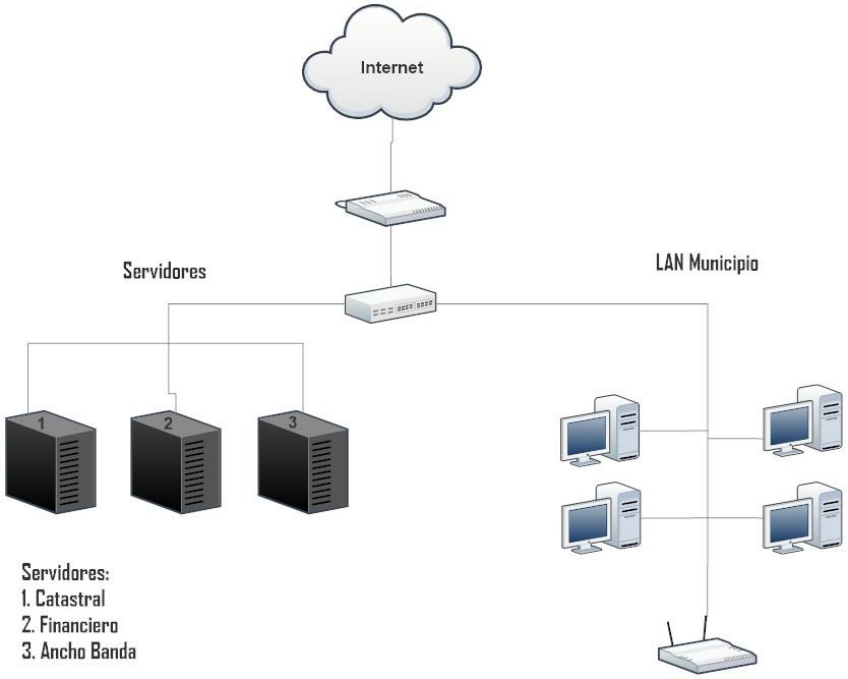


FOTO A3.2. Diagrama de la infraestructura implementada

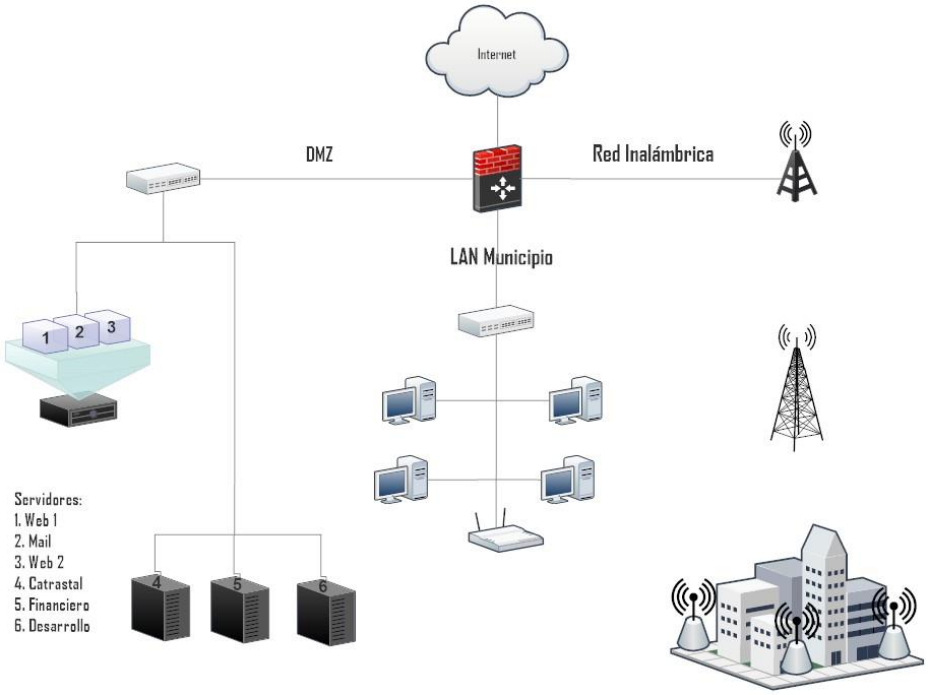


FOTO A3.3. Plataforma web del simulador de enlaces radio mobile

FOTO A3.4. Menú principal del simulador online

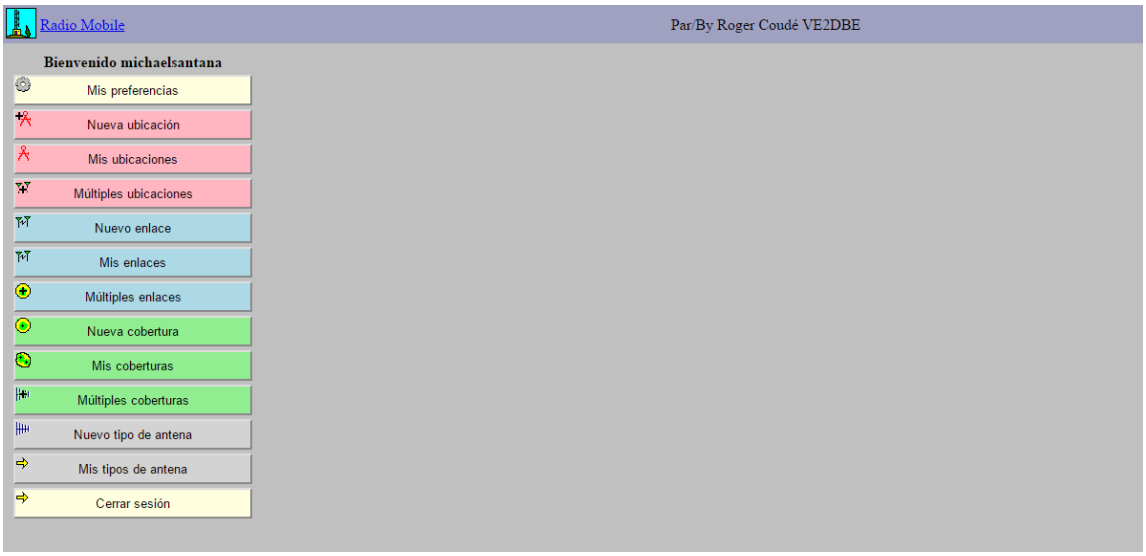


FOTO A3.5. Ingresando la ubicación de uno de los enlaces

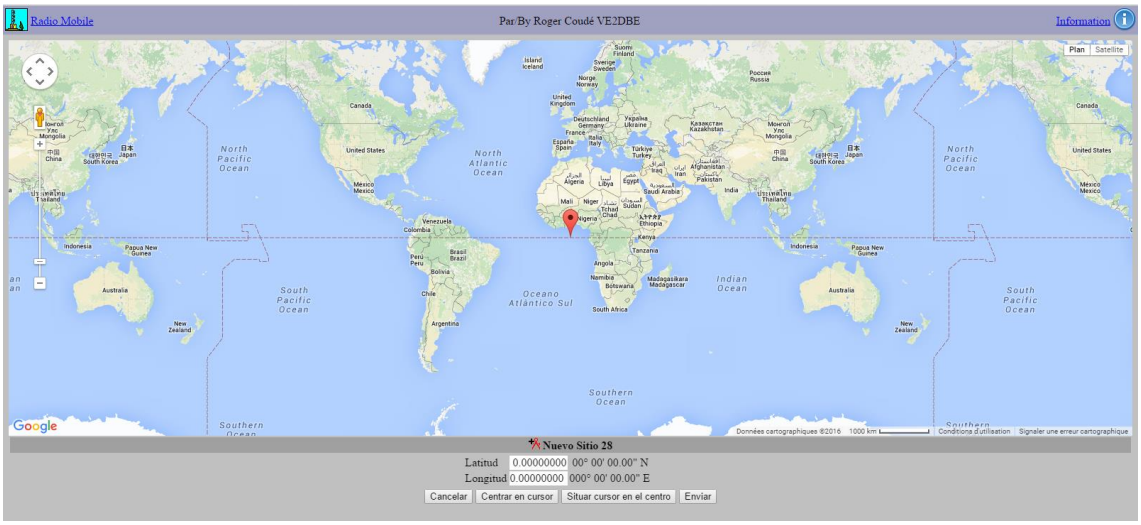


FOTO A3.6. Selecionado el lugar donde se instalaria uno de los equipos para el enlace de la parroquia Bachillero

FOTO A3.7. Ingresando el nombre de uno de los sitios

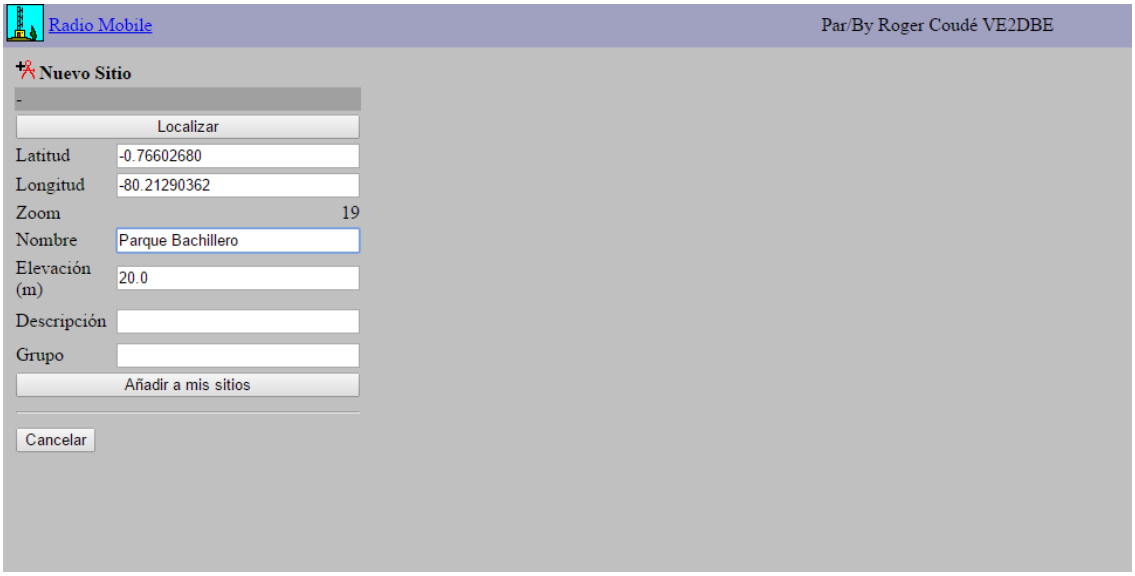


FOTO A3.8. Todos los sitios ingresados al simulador

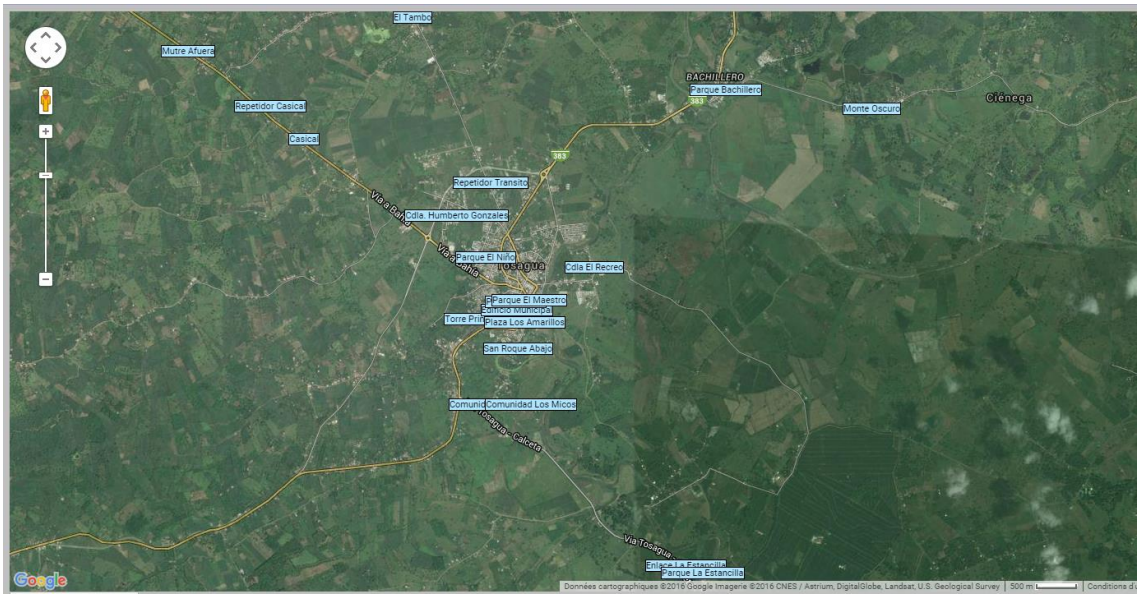


FOTO A3.9. Ingresando la informacion correspondiente para generar un enlace

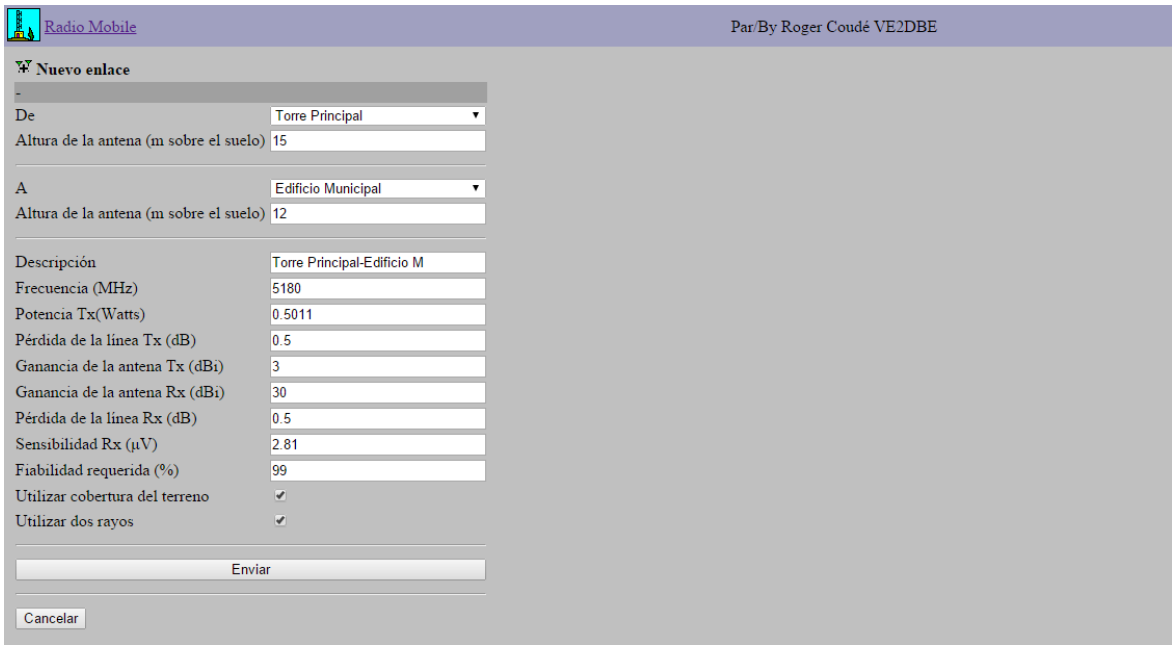
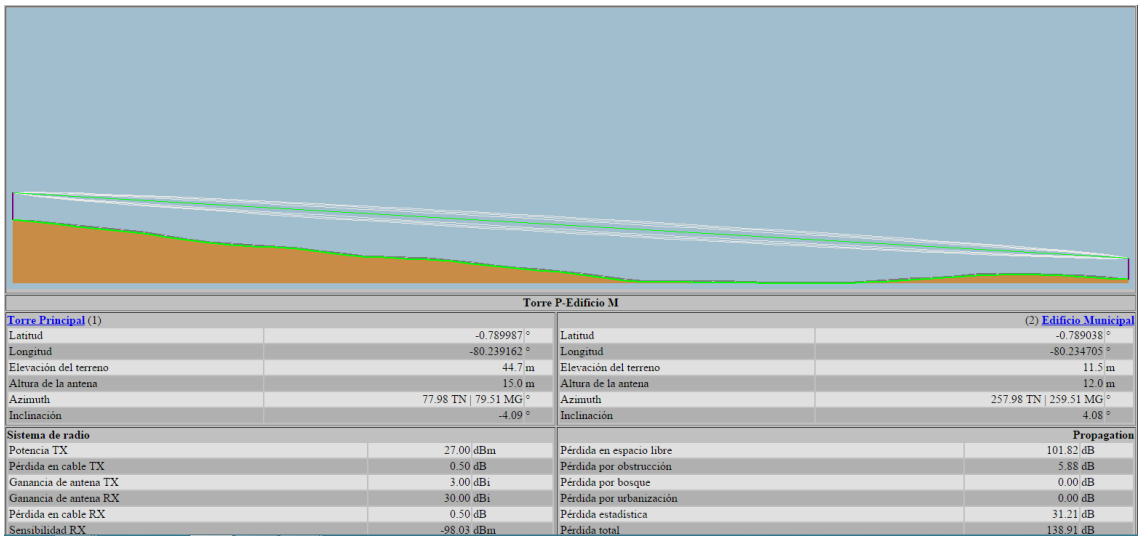


FOTO A3.10. Resultados de la simulación del enlace del edificio a la torre principal



Torre P-Edificio M			
Torre Principal (1)		(2) Edificio Municipal	
Latitud	-0.789987 °	Latitud	-0.789038 °
Longitud	-80.239162 °	Longitud	-80.234705 °
Elevación del terreno	44.7 m	Elevación del terreno	11.5 m
Altura de la antena	15.0 m	Altura de la antena	12.0 m
Azimuth	77.98 TN | 79.51 MG °	Azimuth	257.98 TN | 259.51 MG °
Inclinación	-4.09 °	Inclinación	4.08 °
Sistema de radio		**Propagation**	
Potencia TX	27.00 dBm	Pérdida en espacio libre	101.82 dB
Pérdida en cable TX	0.50 dB	Pérdida por obstrucción	5.88 dB
Ganancia de antena TX	3.00 dBi	Pérdida por bosque	0.00 dB
Ganancia de antena RX	30.00 dBi	Pérdida por urbanización	0.00 dB
Pérdida en cable RX	0.50 dB	Pérdida estadistica	31.21 dB
Sensibilidad RX	-98.03 dBm	Pérdida total	138.91 dB

FOTO A3.11. Resultados de la simulación del enlace del edificio a la torre principal

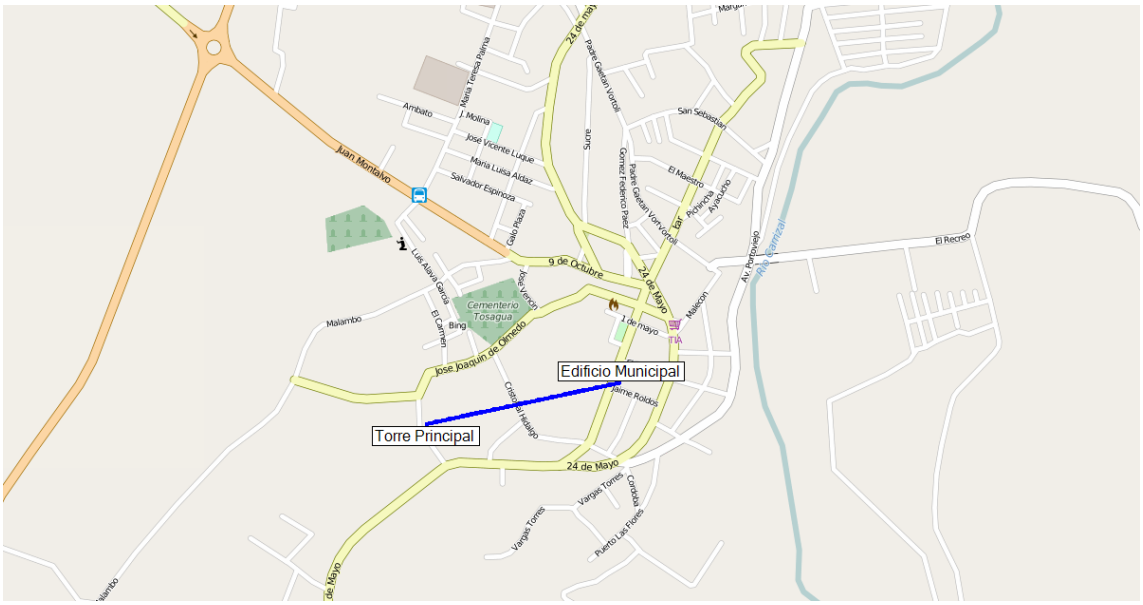
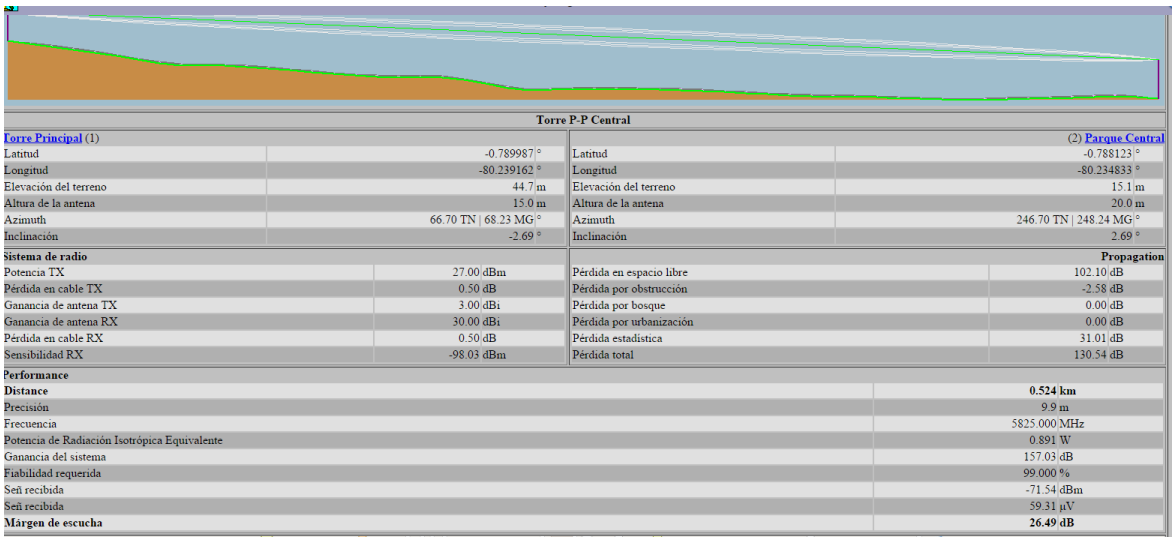


FOTO A3.12. Resultados de la simulación del enlace de torre principal al parque central



Torre P-P Central

Torre Principal (1)		(2) Parque Central	
Latitud	-0.789987 °	Latitud	-0.788123 °
Longitud	-80.239162 °	Longitud	-80.234833 °
Elevación del terreno	44.7 m	Elevación del terreno	15.1 m
Altura de la antena	15.0 m	Altura de la antena	20.0 m
Azimuth	66.70 TN | 68.23 MG °	Azimuth	246.70 TN | 248.24 MG °
Inclinación	-2.69 °	Inclinación	2.69 °

Sistema de radio		Propagation	
Potencia TX	27.00 dBm	Pérdida en espacio libre	102.10 dB
Pérdida en cable TX	0.50 dB	Pérdida por obstrucción	-2.58 dB
Ganancia de antena TX	3.00 dBi	Pérdida por bosque	0.00 dB
Ganancia de antena RX	30.00 dBi	Pérdida por urbanización	0.00 dB
Pérdida en cable RX	0.50 dB	Pérdida estadística	31.01 dB
Sensibilidad RX	-98.03 dBm	Pérdida total	130.54 dB

Performance	
Distance	**0.524 km**
Precisión	9.9 m
Frecuencia	5825.000 MHz
Potencia de Radiación Isotrópica Equivalente	0.891 W
Ganancia del sistema	157.03 dB
Fiabilidad requerida	99.000 %
Señ recibida	-71.54 dBm
Señ recibida	59.31 µV
Márgen de escucha	**26.49 dB**

Anexo 4.

FOTOGRAFÍAS DE LA FASE DE IMPLEMENTACIÓN

FOTO A4.1. Montaje de la torre principal en la ciudadelaSan Cristóbal

FOTO A4.2. Montaje del mastil en un sector estrategico de la comunidad Casical

FOTO A4.3. Llegada de equipos de corto alcalce a la institución

FOTO A4.4. Llegadas de equipos de largo alcance a la institución

FOTO A4.5. Colocacion de equipos en diferentes lugares

FOTO A4.6. Armaje de uno de los equipos inalambricos

FOTO A4.7. Instalación de equipos en la comunidad Monte Oscuro y ciudadela Humberto Gonzáles, respectivamente.

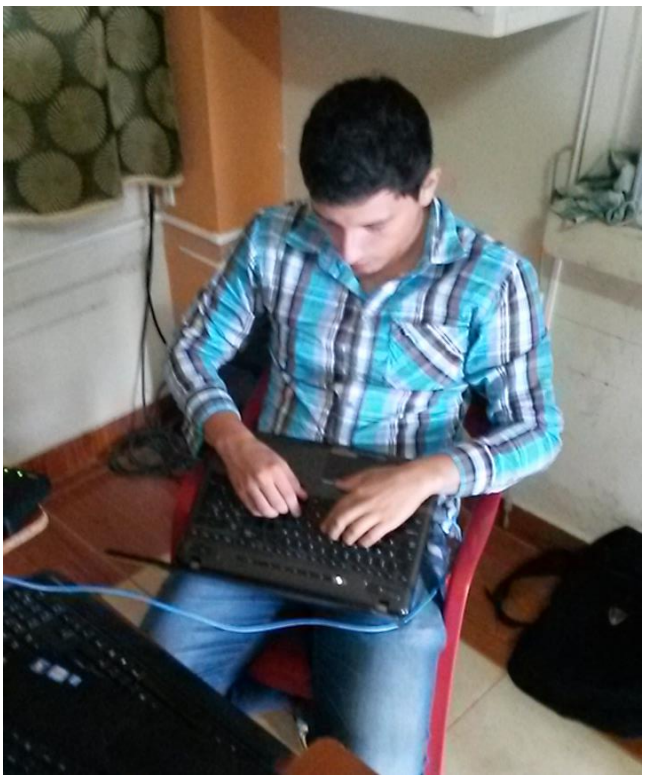
FOTO A4.8. Instalación de punto de acceso en la escuela de Mutre Afuera

FOTO A4.9. Equipos colocados en la torre principal

FOTO A4.10. Equipos colocados en el mastil de Casical

FOTO A4.11. Configuracion de equipos en el sitio Los Micos

FOTO A4.12. Configuracion de equipos en parroquia Ángel Pedro Giler



Anexo 5.

CONFIGURACIÓN E INSTALACIÓN DEL SISTEMA FIREWALL

FOTO A5.1. Servidor que no estaba siendo utilizado en la institución y se utilizó para el Sistema de Seguridad firewall

FOTO A5.2. Pantalla de inicio al momento de ejecutar el PfSense

FOTO A5.3. Configuración de consola previa instalación

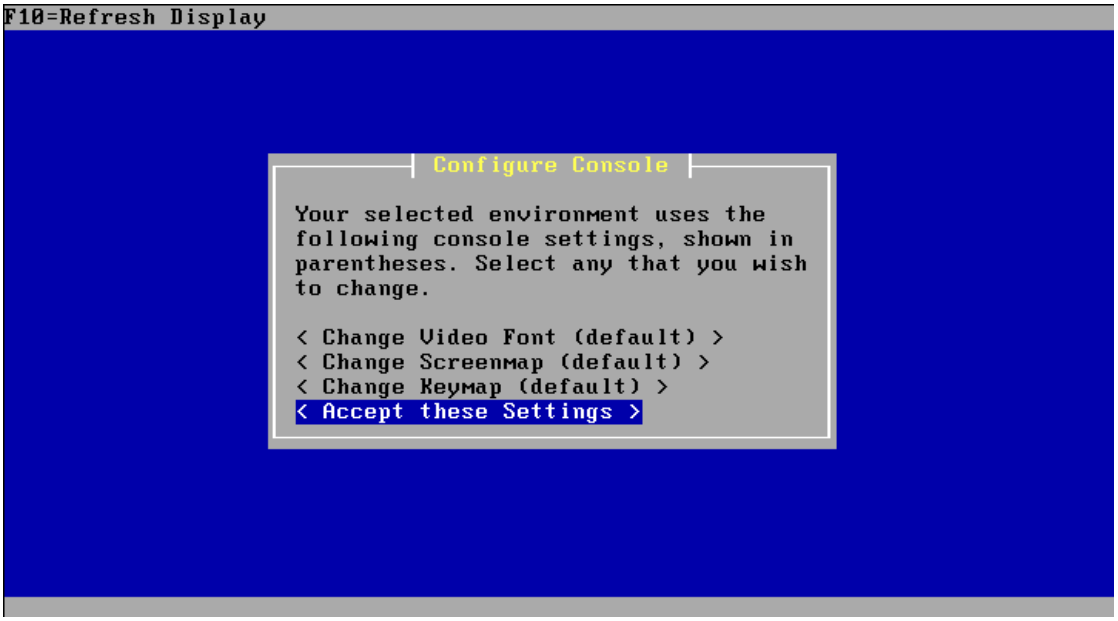


FOTO A5.4. Menú de instalación de la distribución PfSense

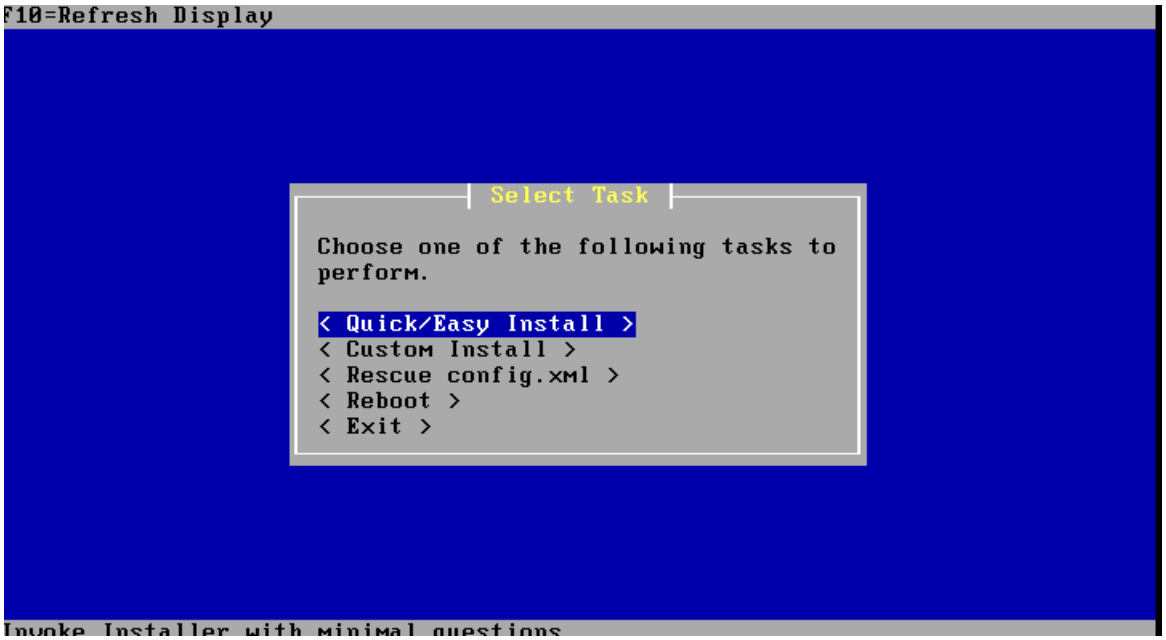


FOTO A5.5. Proceso de instalación del sistema de seguridad

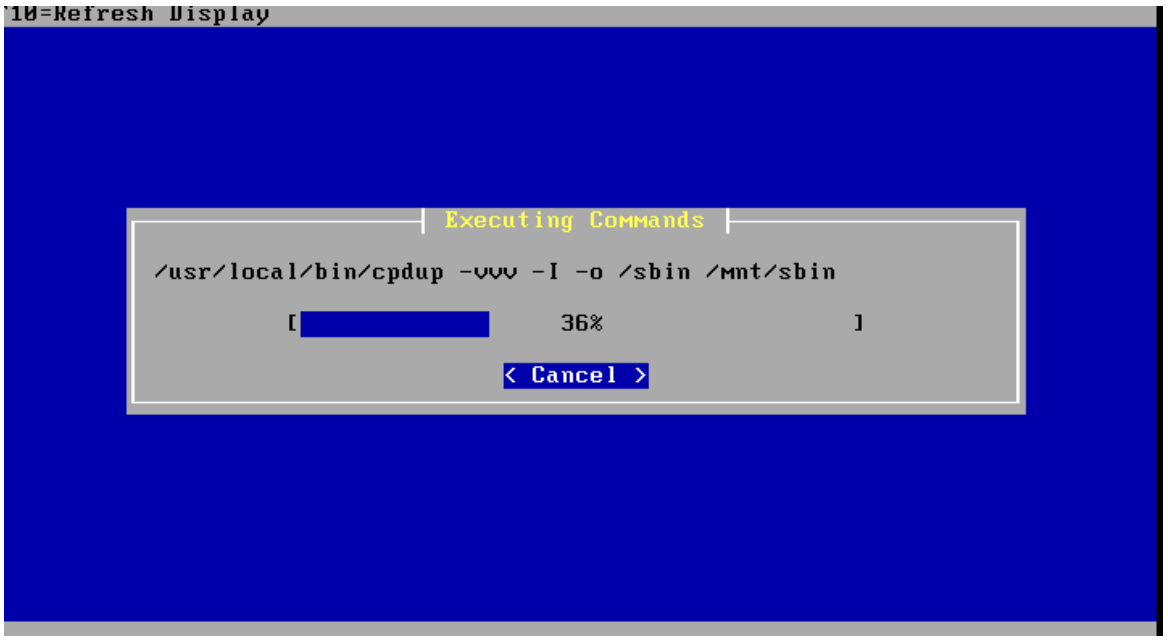


FOTO A5.6. Últimos momentos de la instalación

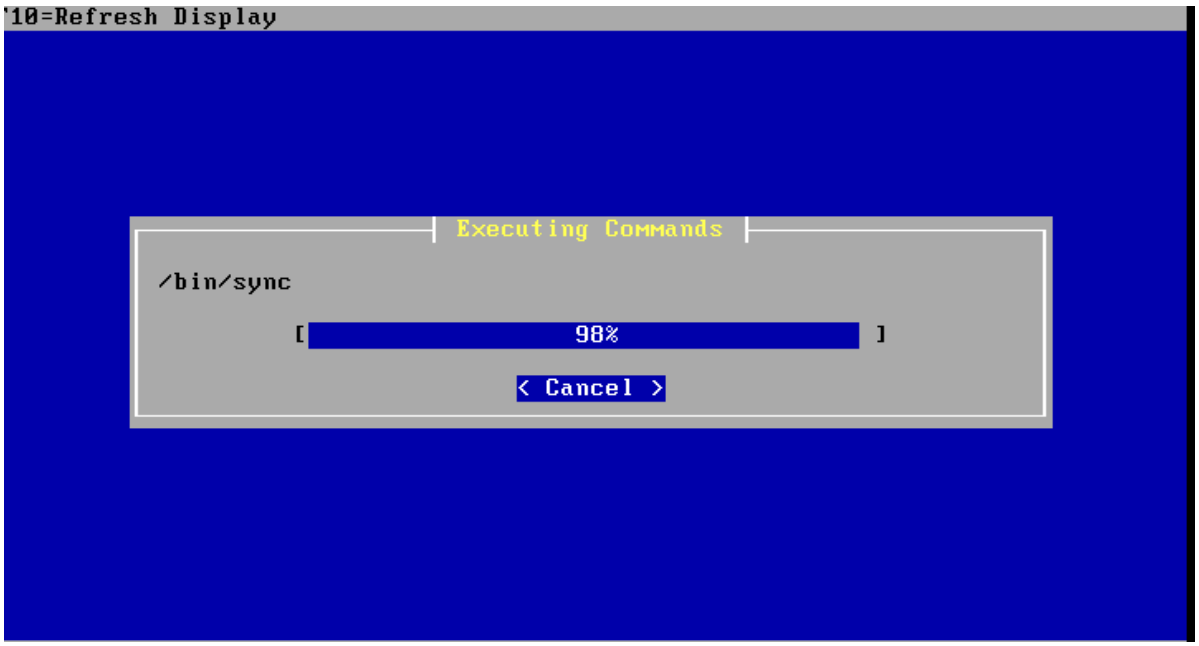


FOTO A5.7. Ventana de autentificación de la administración web del firewall

FOTO A5.8. Ventana de inicio de la administración web

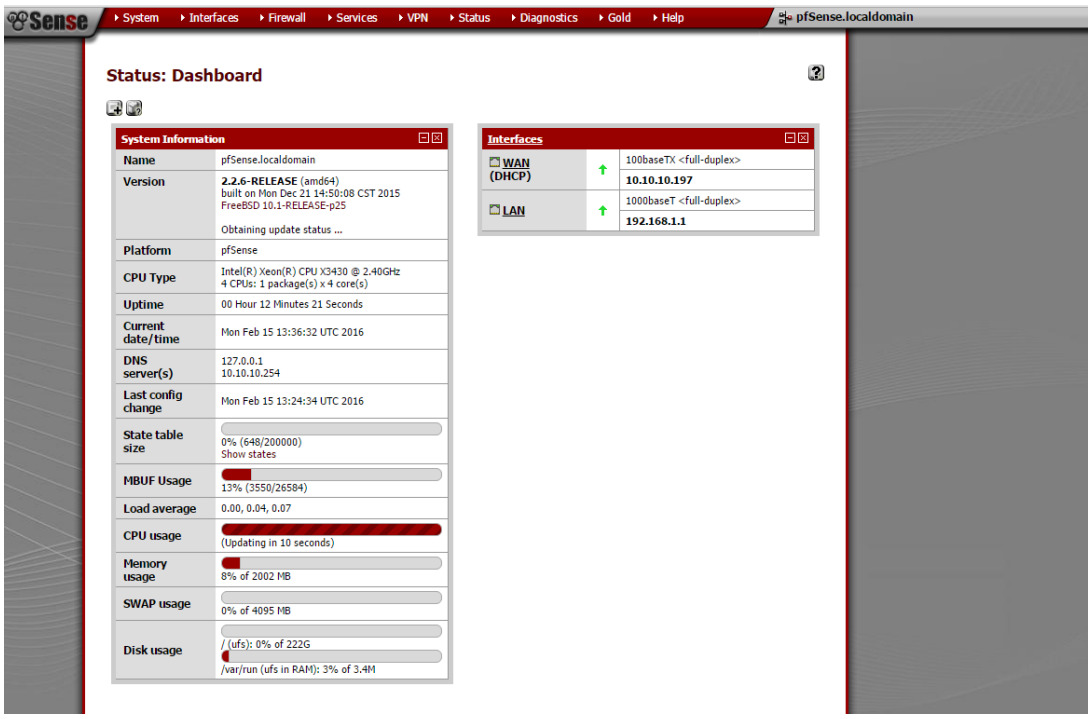


FOTO A5.9. Agregando IP virtuales en el sistema de seguridad

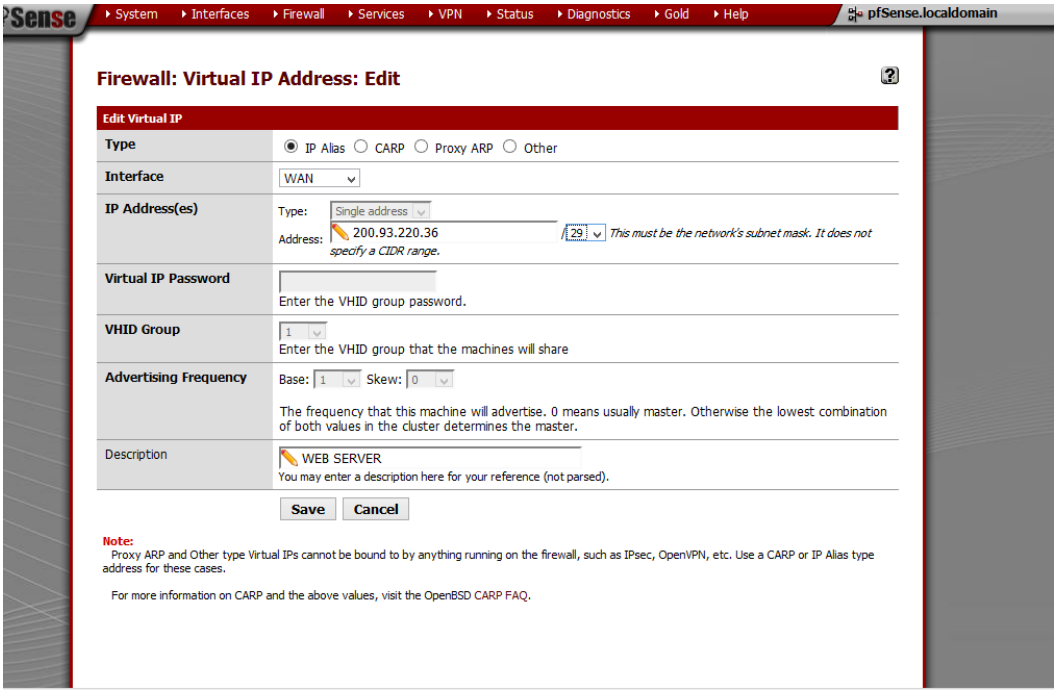


FOTO A5.10. Agregando reglas de NAT 1:1 en el servidor

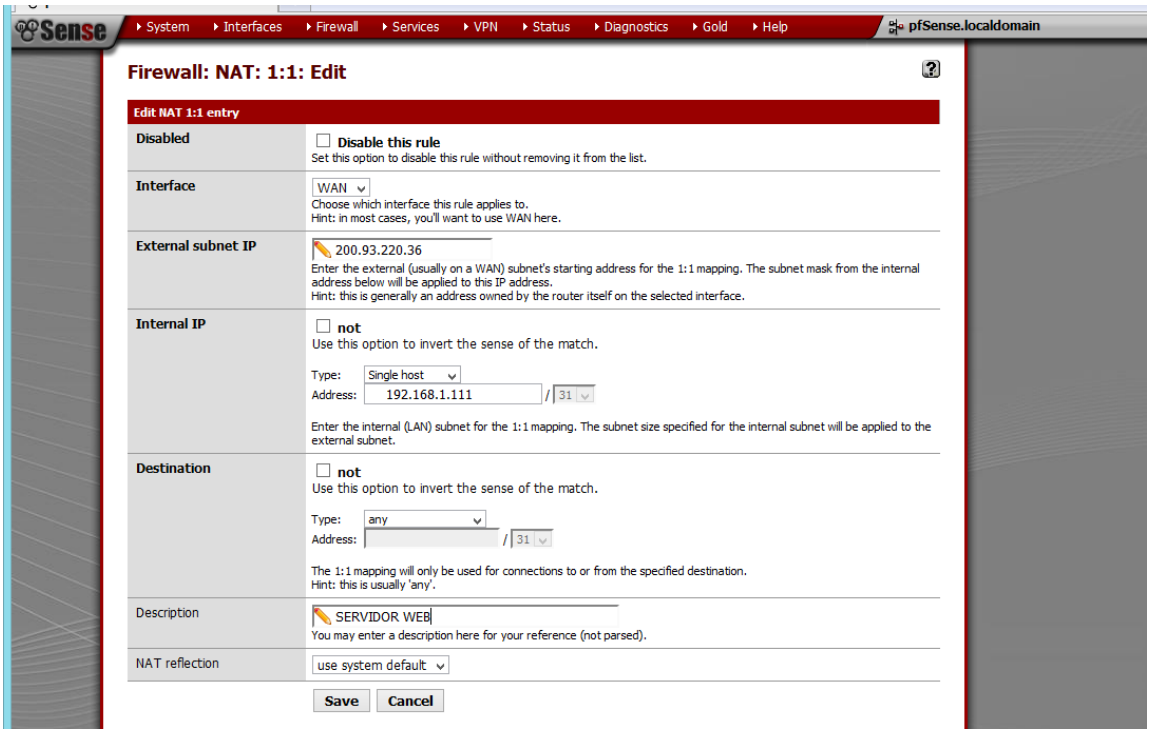


FOTO A5.11. Lista de de Alias generados en el servidor.

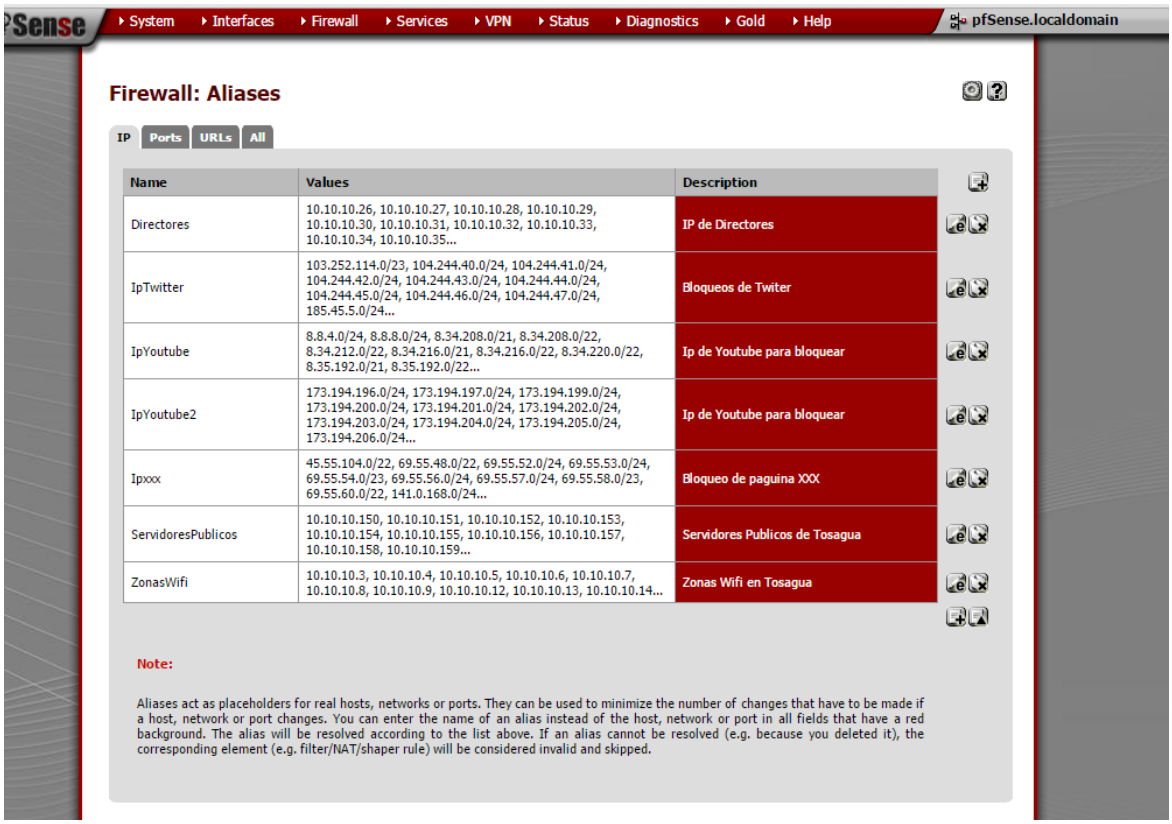


FOTO A5.12. Reglas de Nateo ingresadas al servidor

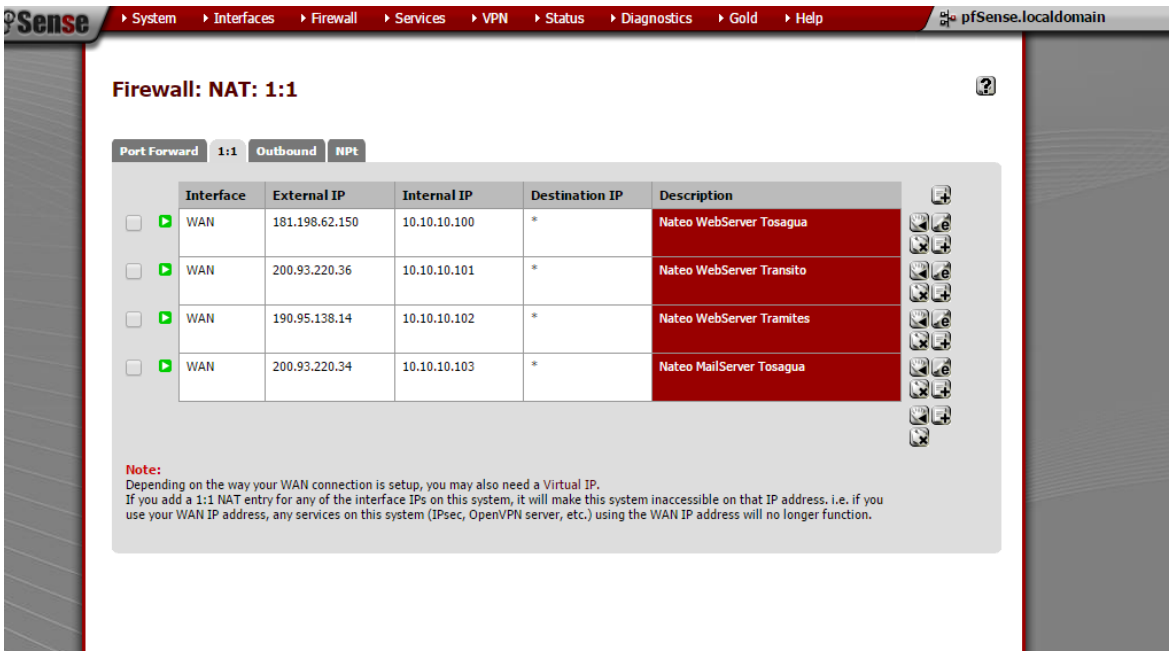


FOTO A5.13. Reglas en la interfaz WAN del servidor

Firewall: Rules

Floating | WAN | LAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		IPv4 TCP/UDP	*	*	10.10.10.103	25 (SMTP)	*	none		Acceso MailServer Tosagua 7
		IPv4 TCP/UDP	*	*	10.10.10.103	995 (POP3/S)	*	none		Acceso MailServer Tosagua 6
		IPv4 TCP/UDP	*	*	10.10.10.103	110 (POP3)	*	none		Acceso MailServer Tosagua 5
		IPv4 TCP/UDP	*	*	10.10.10.103	993 (IMAP/S)	*	none		Acceso MailServer Tosagua 4
		IPv4 TCP/UDP	*	*	10.10.10.103	143 (IMAP)	*	none		Acceso MailServer Tosagua 3
		IPv4 TCP/UDP	*	*	10.10.10.103	53 (DNS)	*	none		Acceso MailServer Tosagua 2
		IPv4 TCP	*	*	10.10.10.103	80 (HTTP)	*	none		Acceso MailServer Tosagua
		IPv4 TCP	*	*	10.10.10.102	80 (HTTP)	*	none		Acceso WebServer Tramites
		IPv4 TCP	*	*	10.10.10.101	80 (HTTP)	*	none		Acceso WebServer Transito
		IPv4 TCP	*	*	10.10.10.100	80 (HTTP)	*	none		Acceso WebServer Tosagua

FOTO A5.14. Reglas en la interfaz LAN del servidor

		IPv4 TCP/UDP	ServidoresPublicos	*	103.243.73.0/24	*	*	none		Bloqueos-Whastapp
		IPv4 TCP/UDP	ServidoresPublicos	*	103.243.74.0/23	*	*	none		Bloqueos-Whastapp
		IPv4 TCP/UDP	ServidoresPublicos	*	103.243.144.0/24	*	*	none		Bloqueos-Whastapp
		IPv4 TCP/UDP	ServidoresPublicos	*	103.243.204.0/22	*	*	none		Bloqueos-Whastapp
		IPv4 TCP/UDP	ServidoresPublicos	*	104.37.3.0/24	*	*	none		Bloqueos-Whastapp
		IPv4 TCP/UDP	ServidoresPublicos	*	103.253.26.0/23	*	*	none		Bloqueos-Whastapp
		IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
		IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule
		IPv4 TCP	*	*	200.93.220.36	80 (HTTP)	*	none		transito
		IPv4 TCP	10.10.10.0/24	*	181.198.62.150	*	*	none		acceso servidor wwww

FOTO A5.15. Agregando limitadores de velocidad en el servidor

FOTO A5.16. Lista de Direcciones IP virtuales

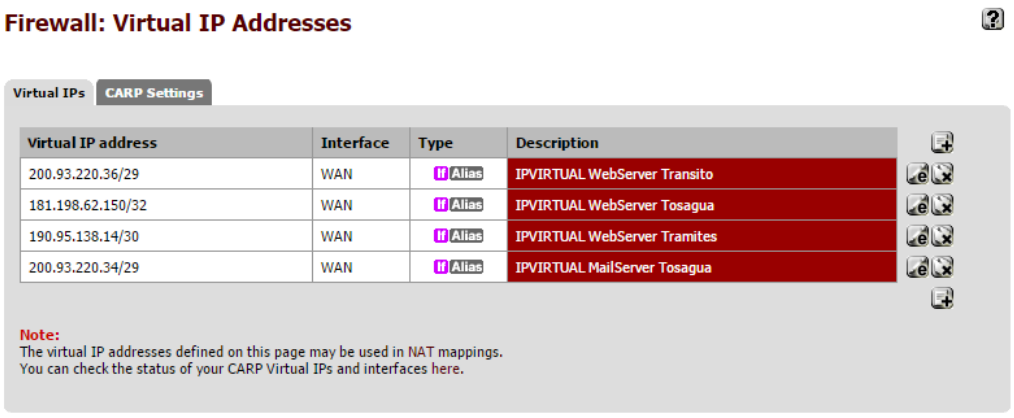


FOTO A5.17. Agregando regla para controlor el limite de velocidad

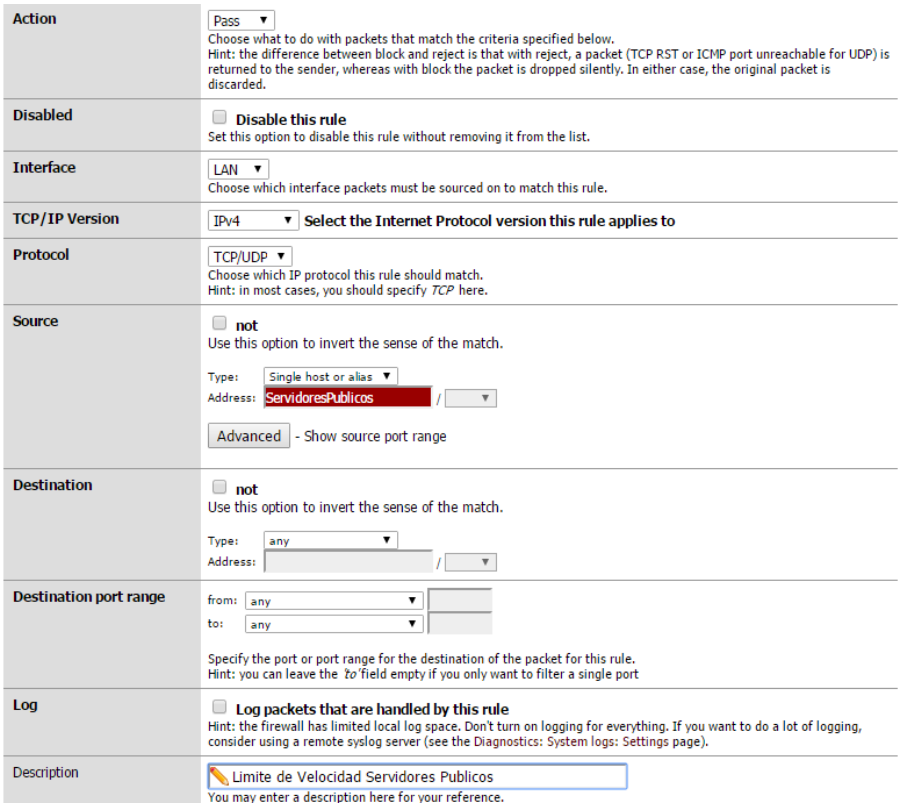


FOTO A5.18. Seleccionando el limitador de velocidad en la regla

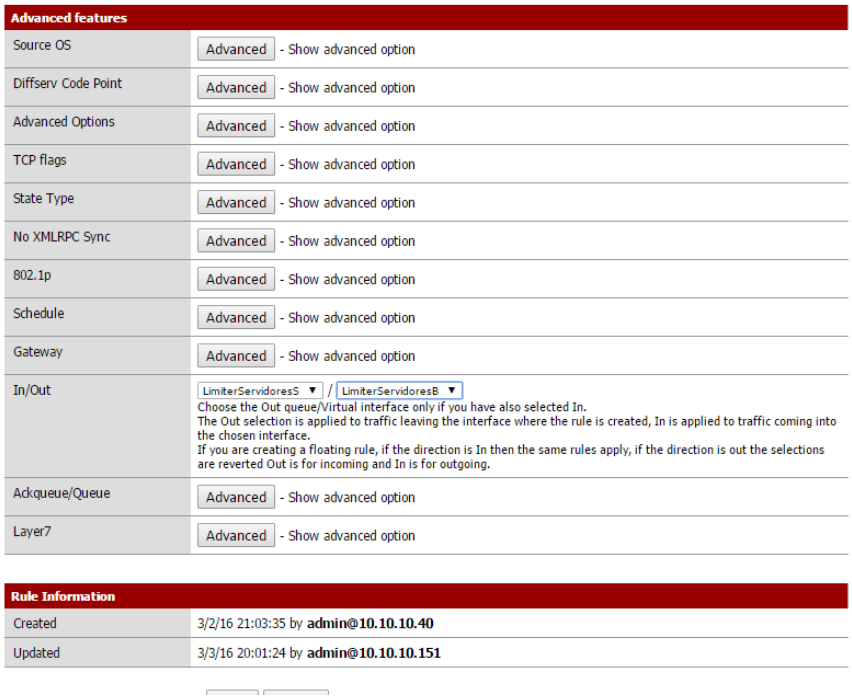


FOTO A5.19. Paquetes instalados para el control web con squiGuard

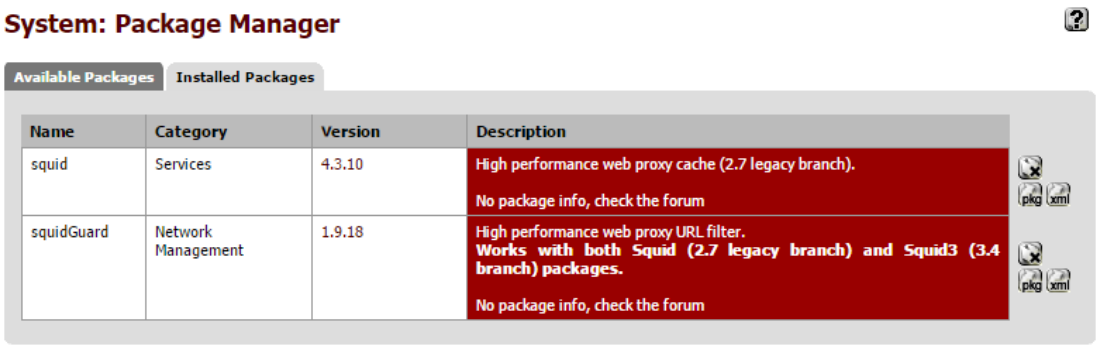
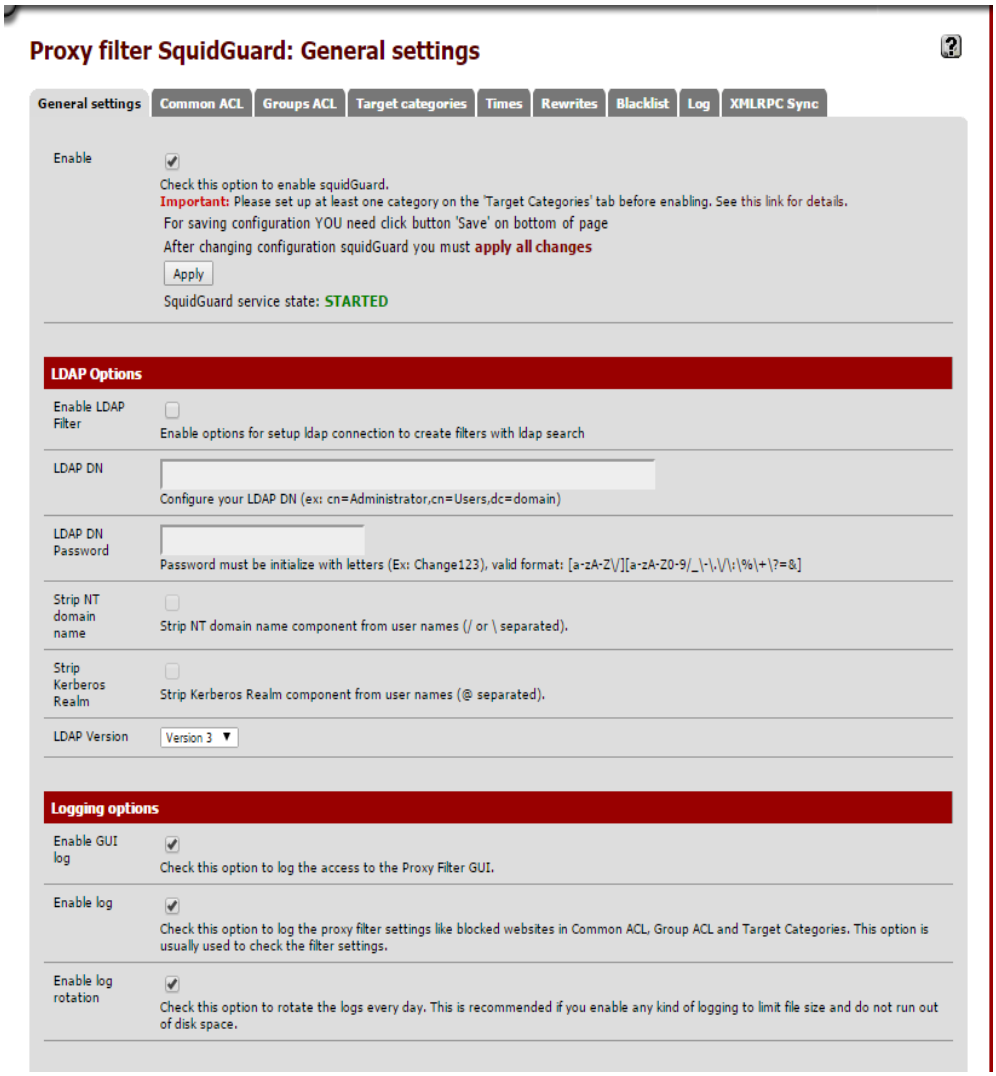


FOTO A5.20. Configuracion del Proxy SquidGuard



Anexo 6.

ILUSTRACIONES DE LA CONFIGURACIÓN DE LOS EQUIPOS INALÁMBRICOS

FOTO A6.1. Equipo Transmisor en la Torre Principal

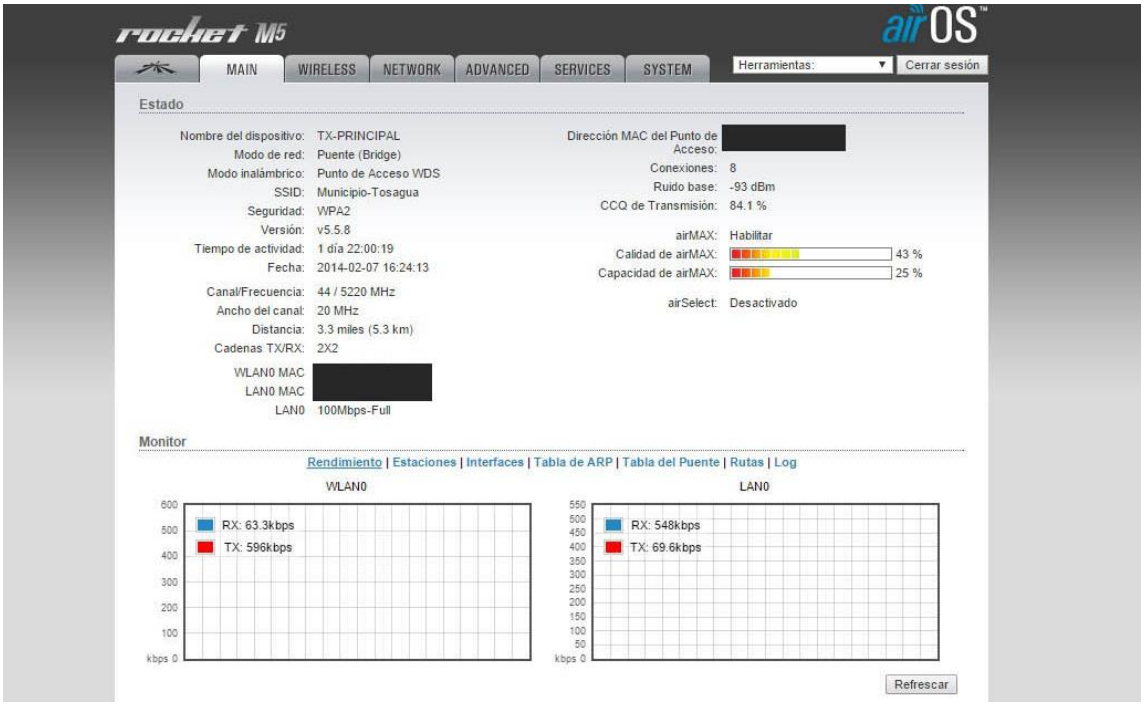


FOTO A6.2. Equipo Receptor en la Torre Principal hacia la Estancilla

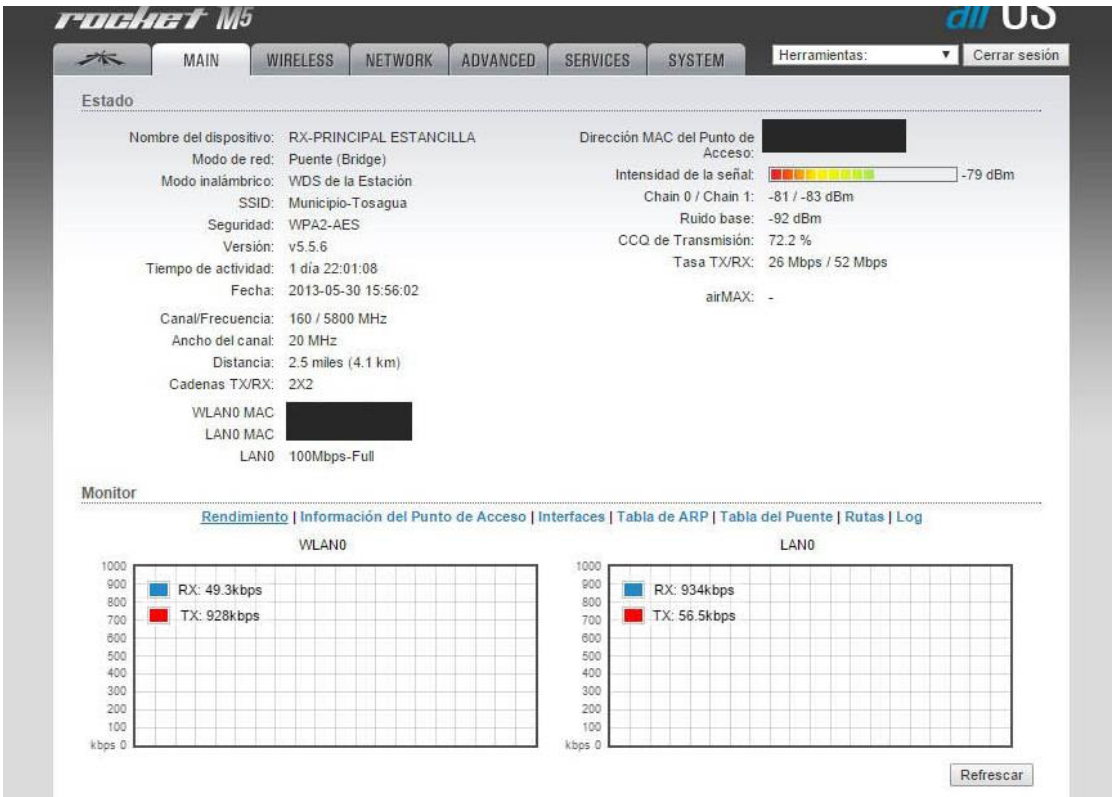


FOTO A6.3. Equipo Receptor del Edificio Municipal

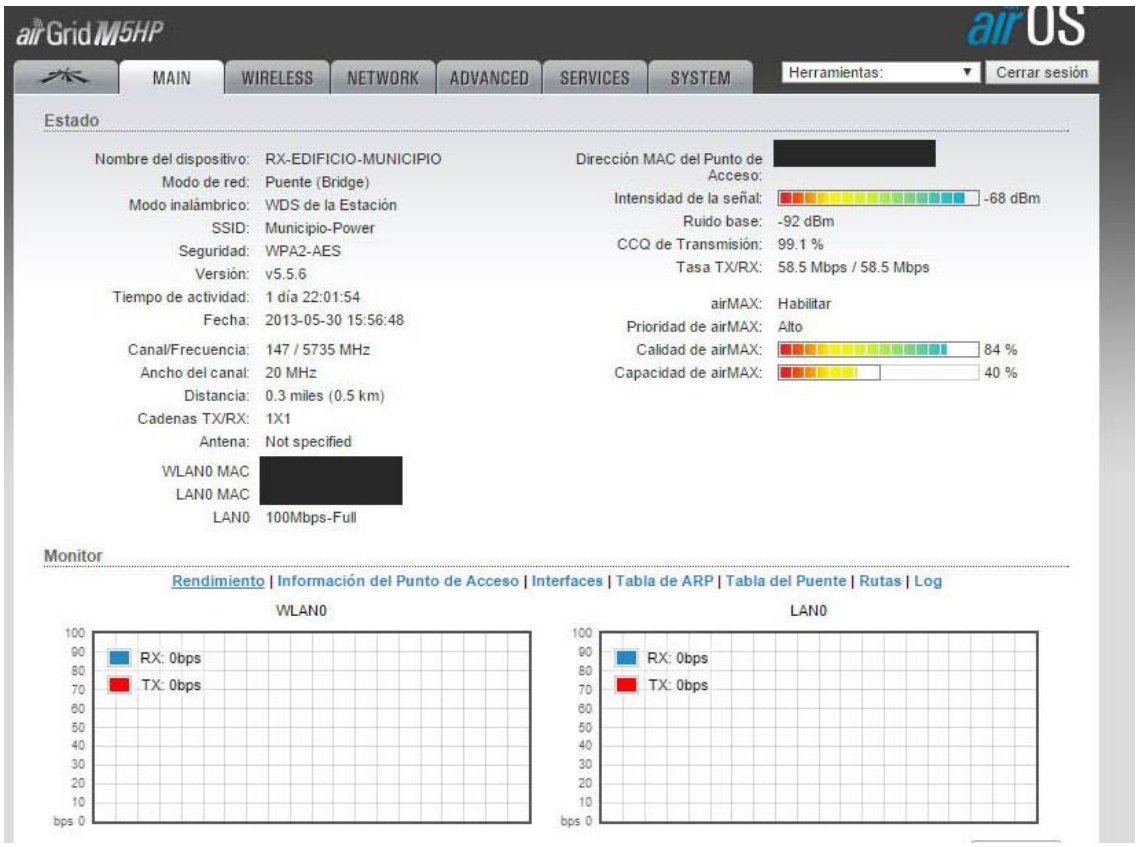


FOTO A6.4. Equipo Receptor del Parque de la Estancilla

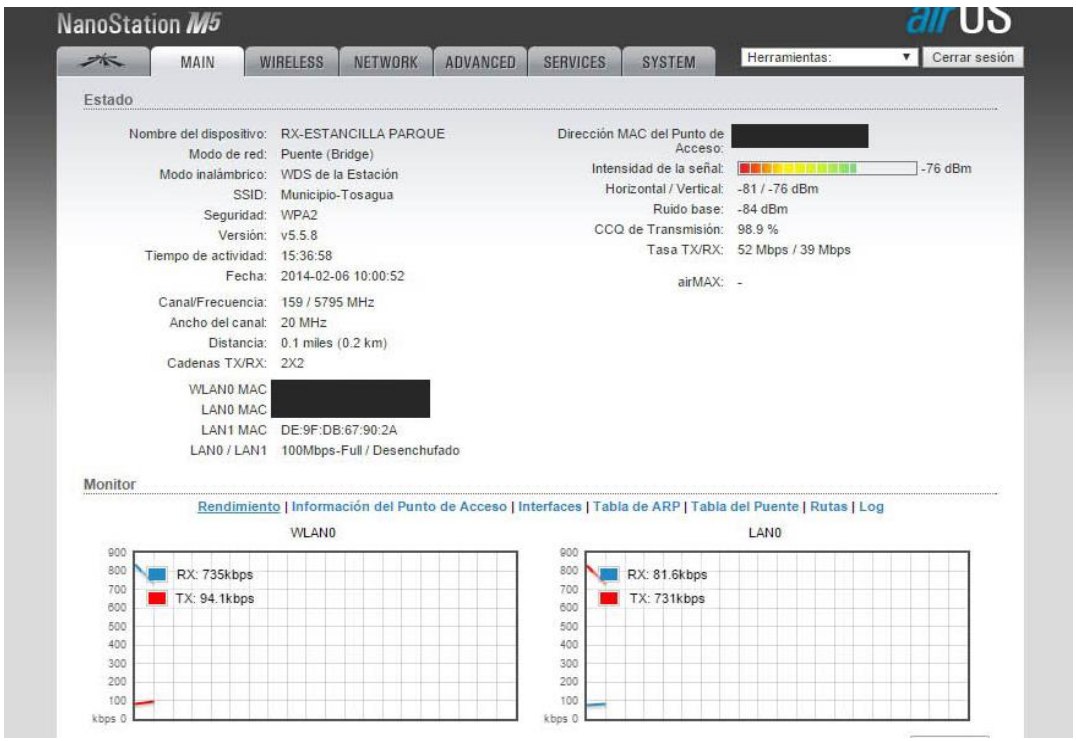
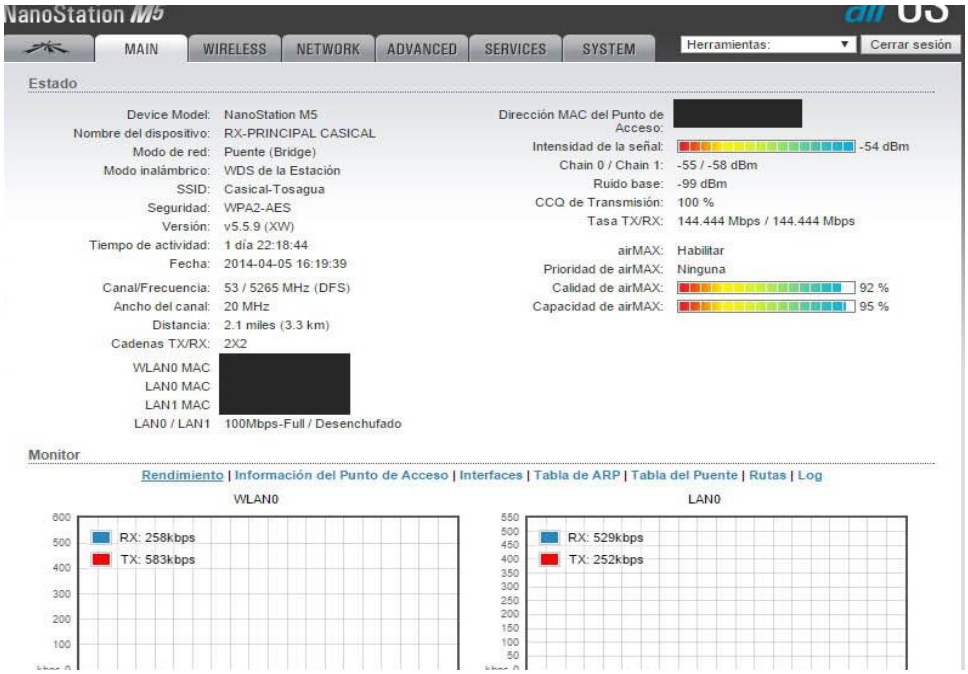


FOTO A6.5. Equipo Transmisor 2 de la Torre Principal

FOTO A6.6. Equipo Receptor ubicado en la Torre de Casical



Anexo 7.

ILUSTRACIONES DE LA FASE DE VERIFICACIÓN

FOTO A7.1. Tiempo de respuestas desde la PC principal hacia el Equipo 1

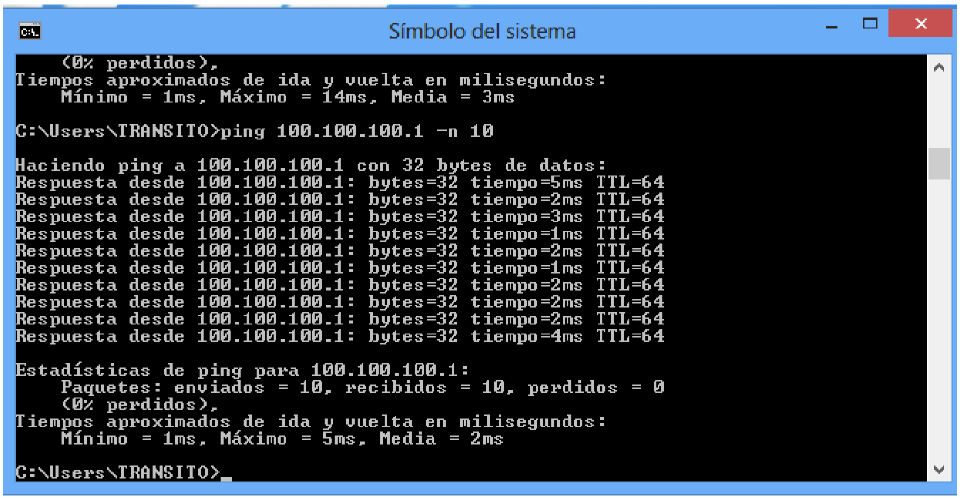


FOTO A7.2. Tiempo de respuestas desde la PC principal hacia el Equipo 2

FOTO A7.3. Tiempo de respuestas desde la PC principal hacia el Equipo 3

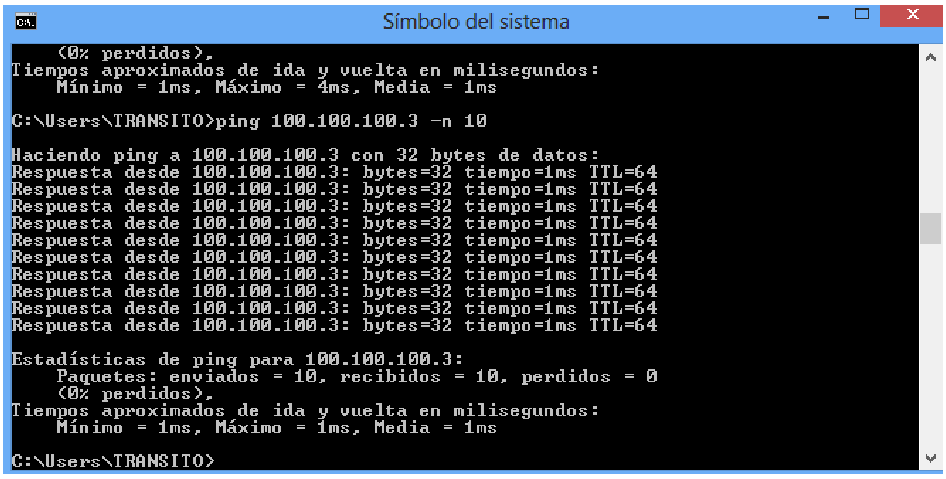


FOTO A7.4. Tiempo de respuestas desde la PC principal hacia el Access Point Nro 3

FOTO A7.5. Tiempo de respuestas desde la PC principal hacia el Access Point Nro 4

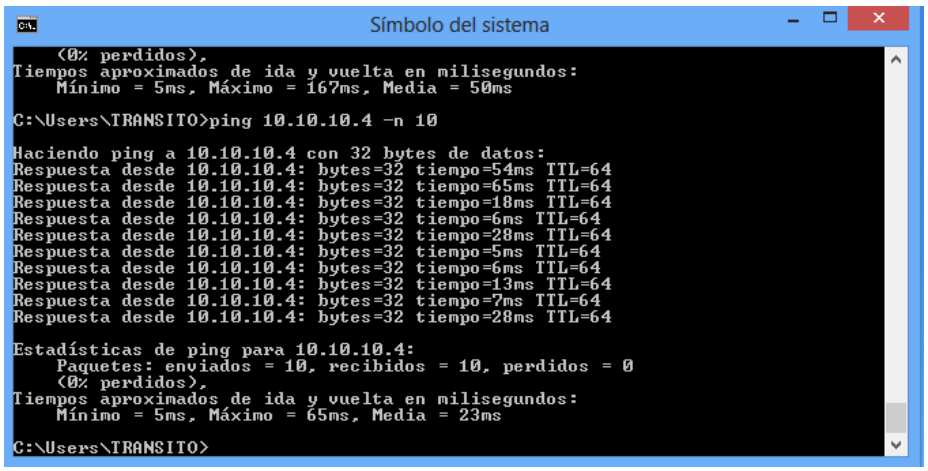


FOTO A7.6. Tiempo de respuestas desde la PC principal hacia el Access Point Nro 5

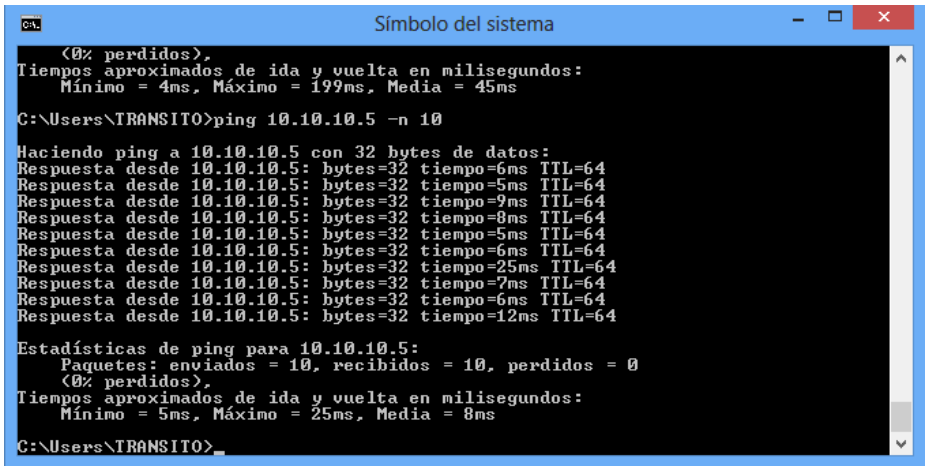


FOTO A7.7. Ping test al Firewall desde Equipo Nro 4

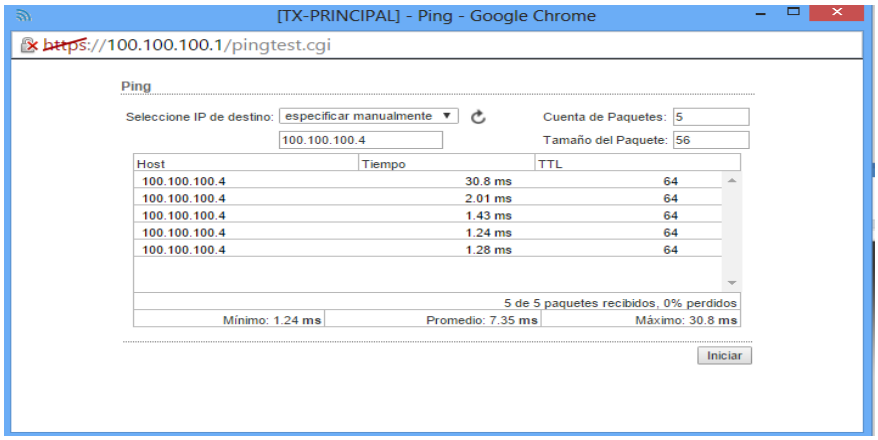


FOTO A7.8. Ping test al Firewall desde Equipo Nro 5

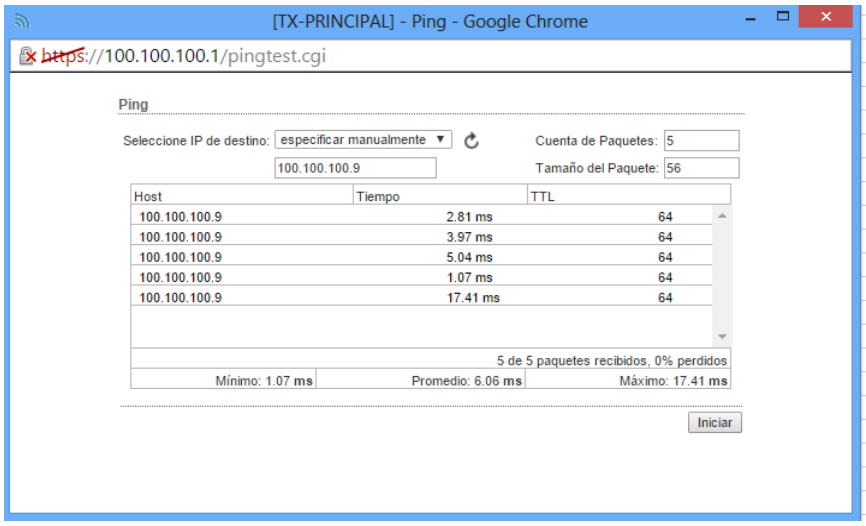


FOTO A7.9. Ping test al Firewall desde Equipo Nro 10

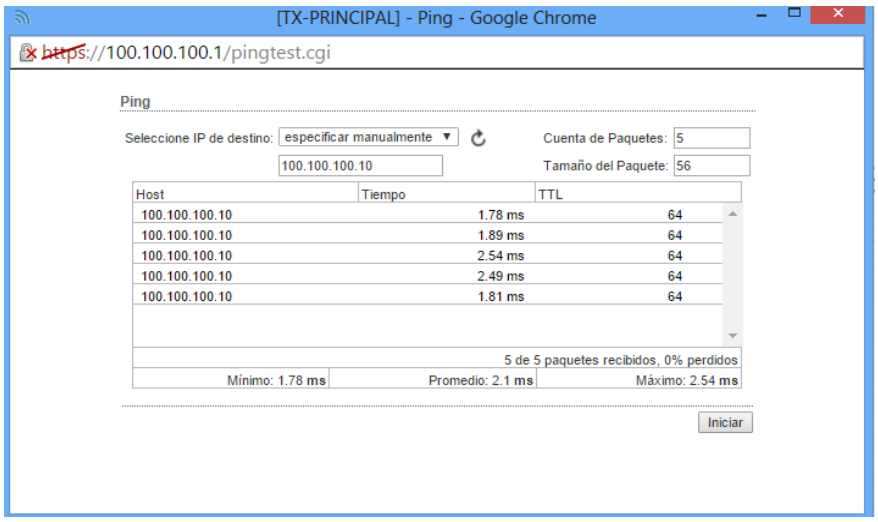


FOTO A7.10. Ping test al Firewall desde el AP Nro 1

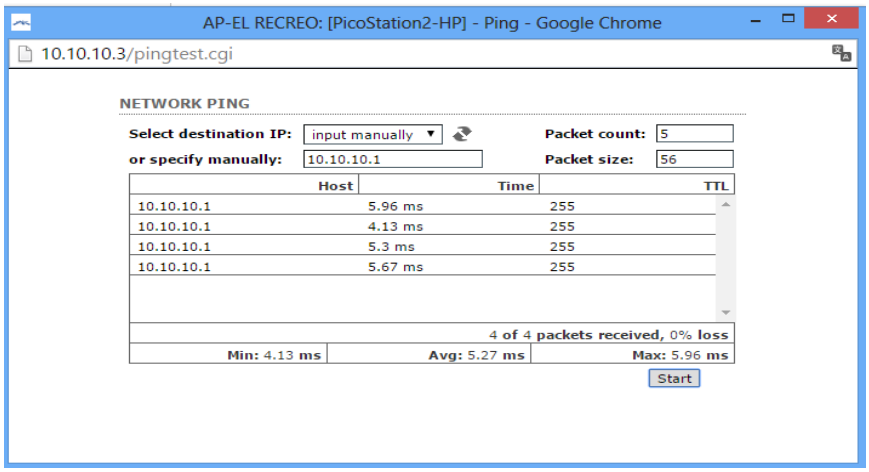


FOTO A7.11. Ping test al Firewall desde el AP Nro 5

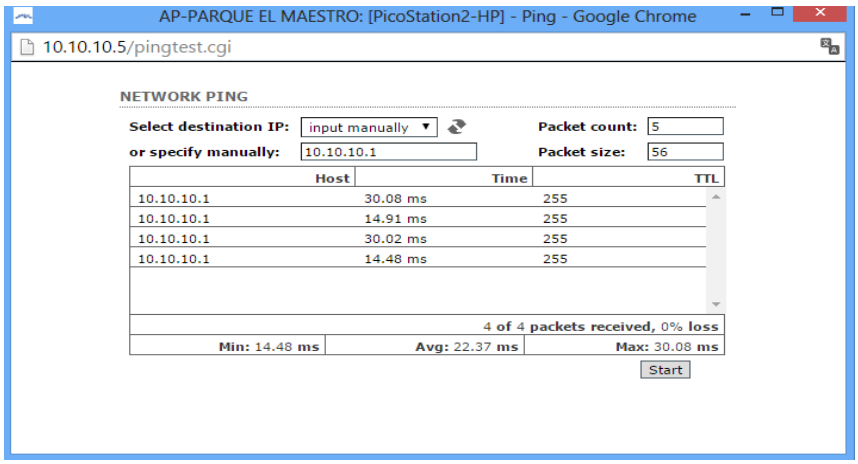


FOTO A7.12. Ping test al Firewall desde el AP Nro 4

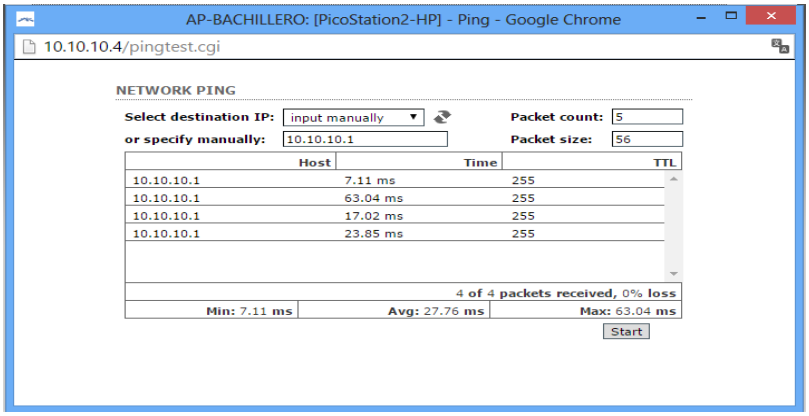


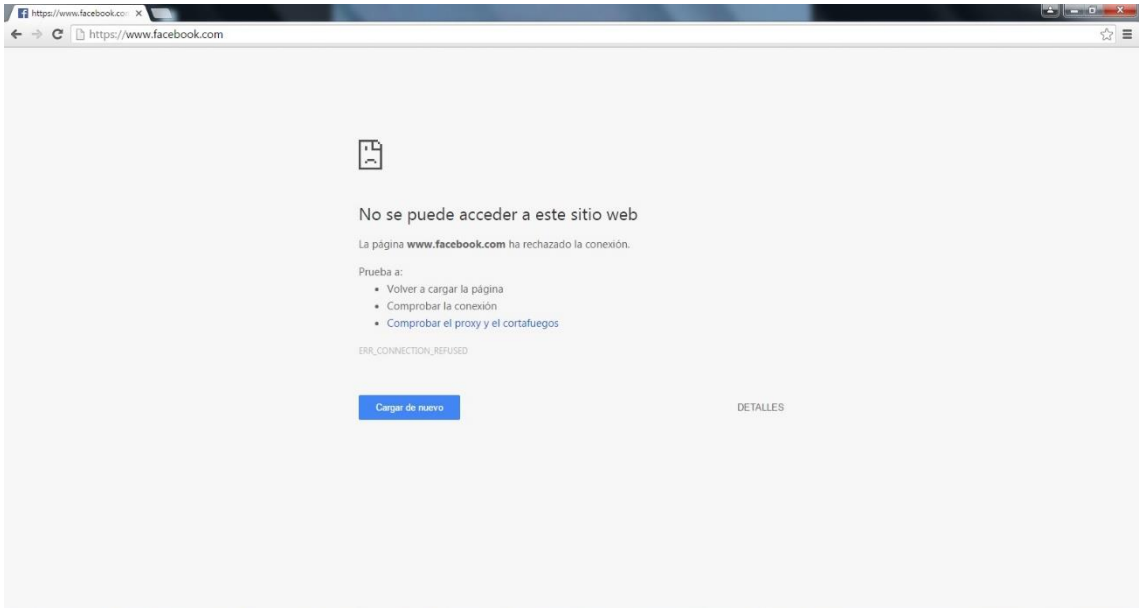
FOTO A7.13. Test de velocidad antes de implementar la solucion

FOTO A7.14. Test de velocidad despues de la implementacion del Firewall

FOTO A7.15. Usuario accediendo a internet en la comunidad Mutre Afuera

FOTO A7.16. Acceso a internet desde la escuela Casical

FOTO A7.17. Bloqueo de Facebook en una PC de un funcionario



Anexo 8.

CERTIFICACION POR PARTE DEL ALCALDE DEL CANTON TOSAGUA

GAD MUNICIPAL TOSAGUA
Un solo Corazón
ADMINISTRACIÓN 2014 - 2019

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN TOSAGUA

ALCALDÍA

CERTIFICADO

Tosagua, abril 11 de 2016

El suscrito Alcalde del Gobierno Autónomo Descentralizado Municipal del Cantón Tosagua, a petición verbal del interesado tiene a bien.

CERTIFICAR.-

Conocer que el estudiante MICHAEL JHONNY SANTANA MONTESDEOCA, portador de la cédula de ciudadanía No. 131332596-9, ha realizado su tesis titulada ***RED INALÁMBRICA DE BANDA ANCHA CON SEGURIDAD PERIMETRAL EN LAS ÁREAS URBANAS Y RURALES DEL CANTÓN TOSAGUA****, en nuestra institución la cual administro.*

Es todo cuanto puedo decir, en honor a la verdad.

El interesado puede hacer uso del presente certificado en lo que él lo estime conveniente.

Atentamente.-

Ing. Leonardo Sánchez Lucas
ALCALDE DEL GAD. MUNICIPAL DEL CANTÓN TOSAGUA
e-mail. ***leonardosanchez28@hotmail.com***
Cel. - 0999170662

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL
ALCALDIA
TOSAGUA - MANABÍ
2014 - 2019

C.c. Archivo.